# Alibaba Cloud
# Apsara Stack Agility SE

## Operations and Maintenance Guide

**Version: 1912, Internal: V3.1.0**

**Issue: 20200311**

# 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, consequent**

ial, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

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

# Document conventions

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

| Style | Description | Example |
| --- | --- | --- |
| **{} or {a\|b}** | **This format is used for a required value, where only one item can be selected.** | `switch {active\|stand}` |

# Contents

# 1 Operations of basic platforms

## 1.1 Apsara Stack Operations (ASO)

### 1.1.1 Apsara Stack Operations overview

**Apsara Stack Operations (ASO) is an operations management system developed for the Apsara Stack operations management personnel, such as field operations engineers, operations engineers on the user side, and operations management engineers, operations security personnel, and audit personnel of the cloud platform. ASO allows the operations engineers to master the operating conditions of the system in time and perform Operations & Maintenance (O&M) operations.**

**ASO has the following main functions:**

- **Alarm Monitoring**

  **The Alarm Monitoring module allows operations engineers to quickly know the information of alerts generated by the system, locate the problems based on the alert information, track the problem processing, and configure the alerts.**

- **Products**

  **The Products module allows you to click operations and maintenance services of other products on the cloud platform and ISV access configurations to go to the corresponding page.**

- **NOC**

  **Network Operation Center (NOC) provides the operations capabilities such as the visualization of network-wide monitoring, automated implementation , automated fault location, and network traffic analysis, which enhances the operations efficiency of network operations engineers, reduces the operations risk, and greatly improves the quality of Apsara Stack network services.**

- **Storage Operation Center**

  **The Storage Operation Center module contains the pangu section and miniOSS section.**

- **Task Management**

  **The Task Management module allows you to perform O&M operations in ASO, without using command lines.**

- **System Management**

  **The System Management module consists of the user management, two-factor authentication, role management, department management, logon policy management, application whitelist, server password management, operation logs, and authorization. As the module for centralized management of accounts , roles, and permissions, System Management supports the Single Sign-On (SSO ) function of ASO. After logging on to ASO, you can perform O&M operations on all components of the cloud platform or be redirected to the operations and maintenance page without providing the username or password.**

## 1.1.2 Log on to Apsara Stack Operations

**This topic describes how to log on to Apsara Stack Operations (ASO) as users, such as operations engineers.**

**Prerequisites**

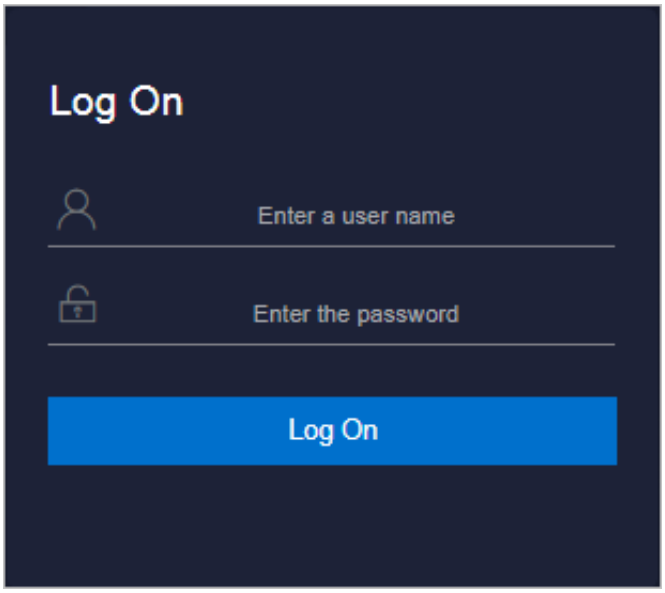
- **ASO access address in the format of http://***region-id***.aso.***intranet-domain-id***.com.**
- **Google Chrome browser (recommended).**

**Procedure**

1. **Open the browser.**

2. **Enter the ASO access address http://*region-id*.aso.*intranet-domain-id*.com in the address bar and then press Enter.**

   Figure 1-1: Log on to ASO

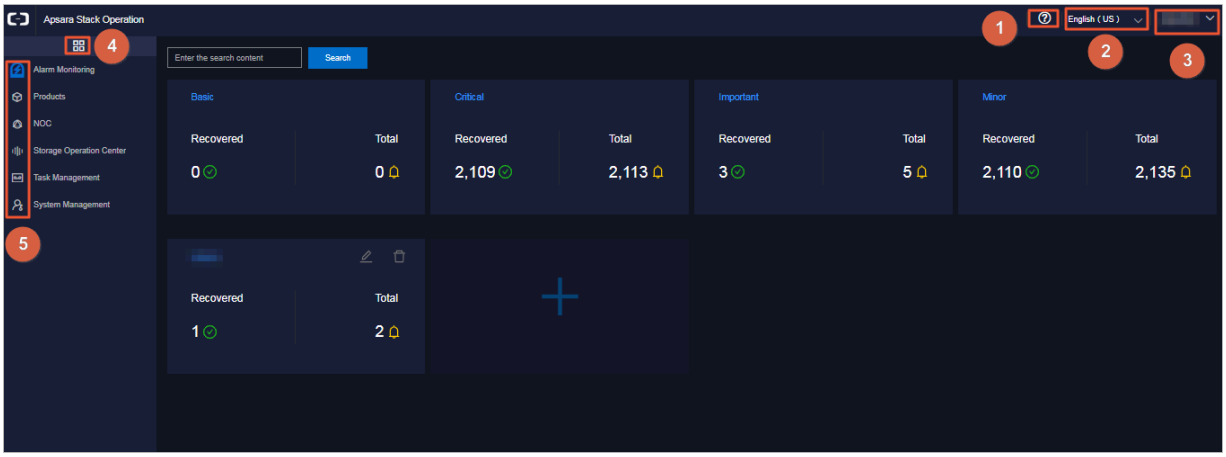
   
   

   **Note:**
   **You can select the language from the drop-down list in the upper-right corner to change the language of ASO.**

3. **Enter the correct username and password.**
   - **The system has three default users:**
     - **Security officer: manages other users or roles.**
     - **Auditor officer: views audit logs.**
     - **System administrator: used for other functions except those of the security officer and auditor officer.**
   - **You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.**
4. **Click Log On to log on to ASO.**

# 1.1.3 Web page introduction

**After you log on to Apsara Stack Operations (ASO), the Alarm Monitoring page appears. This topic allows you to get a general understanding of the basic operations and functions of the ASO page.**




**The description of each area is as follows.**

| Area | | Description |
| --- | --- | --- |
| 1 | Help center | : In the Help Center, you can view the alarm knowledge base and upload other documents related to operations. |
| 2 | Language switching | English ( US ) : Select the language from the drop-down list to change the language of ASO. |
| 3 | Information of the current logon user | : Click this drop-down list to view the information of the current user, modify the password, and complete the logo settings and logon settings. |
| 4 | Expand button | : Move the pointer over this button to expand the left-side navigation pane. |
| 5 | Left-side navigation pane | Click to select a specific Operation & Maintenance (O&M) operation. |

## 1.1.4 Alarm Monitoring

**The Alarm Monitoring module allows operations engineers to quickly know the information of alerts generated by the system, locate the problems based on the alert information, track the problem processing, and configure the alerts.**

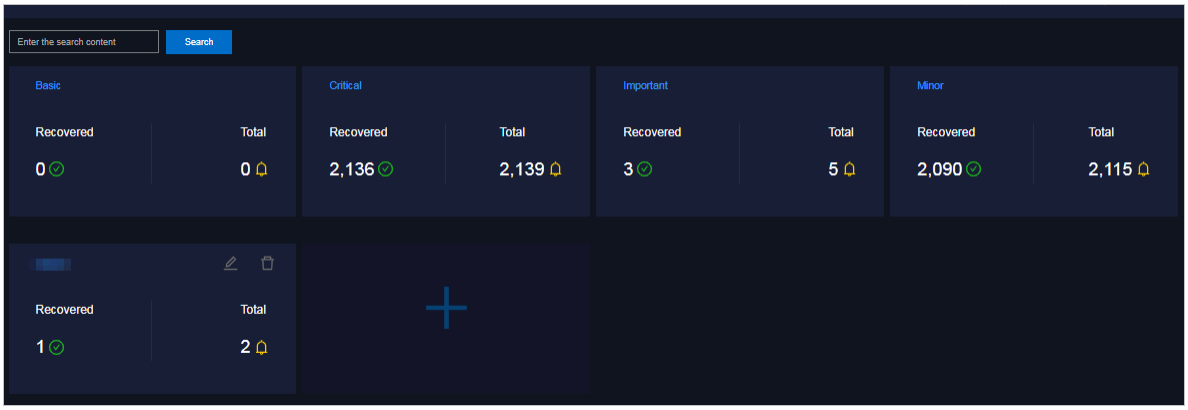
### 1.1.4.1 Overview

**The Alarm Monitoring module allows you to view the overview information of alerts.**

**Procedure**

1. *Log on to Apsara Stack Operations*.

   **By default, the overview page of the Alarm Monitoring module appears after you log on to Apsara Stack Operations (ASO).**




2. **Then, you can:**

   - **View the total number of alerts and the number of recovered alerts in the basic, critical, important, and minor monitoring metrics, and custom filters.**

     **Note:**

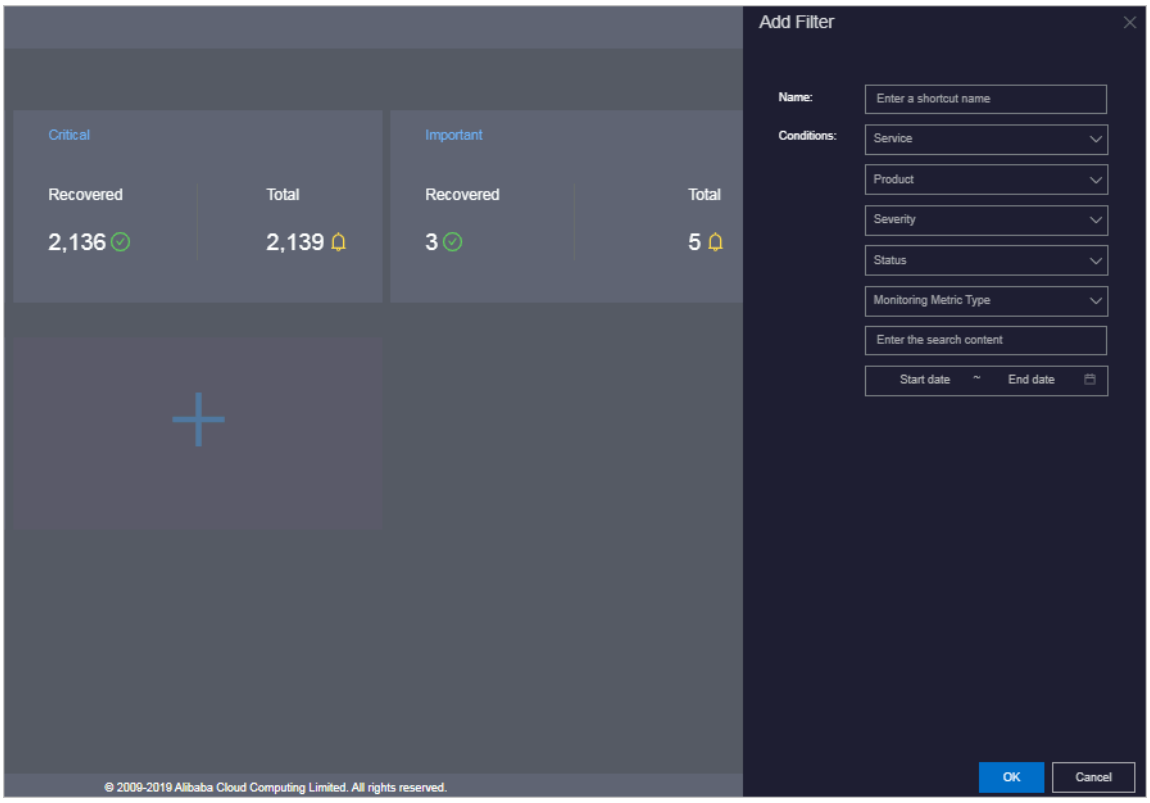
**Click a monitoring metric or custom filter to go to the corresponding Alert Events page.**

- **Search for alerts**

  **Enter a keyword, such as cluster, product, service, severity, status, and monitoring metric name, in the search box at the top of the page and then click Search to search for the corresponding alert event.**

- **Add a custom filter**

  **Click**  **. Complete the configurations on the displayed page.**




**For more information about the configurations, see the following table.**

| Configuration | Description |
| --- | --- |
| Name | The filter name to be displayed on the Alarm Monitoring page. |

| Configuration | Description |
| --- | --- |
| Conditions | Configure the following filter conditions.<br>- Service: The service to which the alerts to be filtered belong.<br>- Product: The product to which the alerts to be filtered belong.<br>- Severity: The severity to which the alerts to be filtered belong.<br>The alert severity has the following six levels:<br>■ P0: indicates the cleared alerts, corresponding to alerts whose Alert Level is Restored in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>■ P1: indicates the critical alerts, corresponding to alerts whose Alert Level is P1 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>■ P2: indicates the major alerts, corresponding to alerts whose Alert Level is P2 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>■ P3: indicates the minor alerts, corresponding to alerts whose Alert Level is P3 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>■ P4: indicates the remind alerts, corresponding to alerts whose Alert Level is P4 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>■ P5: indicate the system alerts, corresponding to alerts whose Alert Level is P5 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>- Monitoring Metric Type: The monitoring metric type to which the alerts to be filtered belong.<br>■ Basic<br>■ Critical<br>■ Important<br>■ Minor<br>- Enter the search content: Enter the information of the alerts to be filtered. |
| | - Select the start date and end date of the alerts to be filtered. |

After adding a custom filter, you can view the overview information that meets the filter conditions in Alarm Monitoring.

- Modify a custom filter

  After adding a custom filter, you can click  as required to modify the filter conditions and obtain the new filter results.

- Delete a custom filter

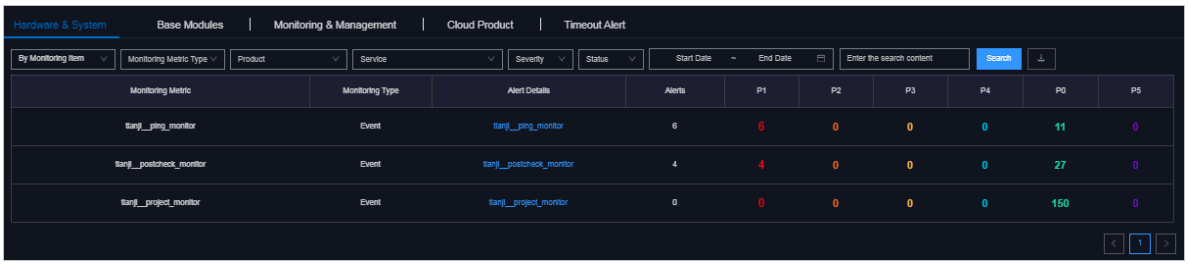
  After adding a custom filter, you can click  as required to delete it if it is no longer in use.

### 1.1.4.2 Alert events

The Alert Events module displays the information of all alerts generated by the system on different tabs. The alert information is aggregated by monitoring item or product name. You can search for alerts based on filter conditions, such as monitoring metric type, product, service, severity, status, and time range when the alert is triggered, and then perform Operation & Maintenance (O&M) operations on the alerts.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Events.



3. **Click the Hardware & System, Base Modules, Monitoring & Management, Cloud Product, or Timeout Alert tab and then you can:**

   - **Search for alerts**

     **At the top of the page, you can search for alerts by Monitoring Metric Type, Product, Service, Severity, Status, Start Date, End Date, and search content.**

   - **View alert sources**

     a. **If the alert information is aggregated by Product Name on this page, click + at the left of the product name to display the monitoring metrics. If the alert information is aggregated by Monitoring Item on this page, skip this step.**
     b. **Find the monitoring metric and severity to which the alerts you are about to view belong, and then click the number in the specific severity column.**
     c. **Move the pointer over the alert source information in blue in the Alert Source column to view the alert source details.**

   - **View alert details**

     a. **If the alert information is aggregated by Product Name on this page, click + at the left of the product name to display the monitoring metrics. If the alert information is aggregated by Monitoring Item on this page, skip this step.**
     b. **Find the monitoring metric and severity to which the alerts you are about to view belong, and then click the number in the specific severity column.**
     c. **Click the value in blue in the Alert Details column. On the displayed Alert Details page, you can view the alert information, such as the summary, reference, scope, and resolution.**

   - **View the original alert information of an alert**

     a. **If the alert information is aggregated by Product Name on this page, click + at the left of the product name to display the monitoring metrics. If the alert information is aggregated by Monitoring Item on this page, skip this step.**
     b. **Find the monitoring metric and severity to which the alert you are about to view belongs, and then click the number in the specific severity column.**
     c. **Click the number in blue in the Alerts column. The Alerts page appears.**
     d. **Click Details in the Alert Information column to view the original alert information.**

   - **Process an alert**

Find the monitoring metric and severity to which the alert you are about to process belongs, and then click the number in the specific severity column.

> **Note:**
> If the alert information is aggregated by Product Name on this page, click + at the left of the product name to display the monitoring metrics.

- If an alert is being processed by operations engineers, click Actions > Process in the Actions column to set the alert status to In process.
- If the processing of an alert is finished, click Actions > Processed in the Actions column to set the alert status to Processed.
- To view the whole processing flow of an alert, click Actions > Alert Tracing in the Actions column.
- View the recent monitoring data

  Click Actions > Exploration in the Actions column at the right of an alert to view the trend chart of a recent monitoring metric of a product.

· Export a report

  Click  at the top of the page to export the alert list.

### 1.1.4.3 Alert history

The Alert History page displays all the alerts generated by the system and the corresponding information in chronological order.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert History.

3. On the Alert History page, you can:

   - Search for alerts

     At the top of the page, you can search for alerts by Monitoring Metric Type, Product, Service, Severity, Status, Start Date, End Date, and search content.

   - Export a list of alerts

     Click  at the top of the page to export a list of history alerts.

   - View alert sources

     Move the pointer over an alert source name in blue in the Alert Source column to view the alert source details.

   - View alert details

     Click an alert name in blue in the Alert Details column. On the displayed Alert Details page, you can view the alert information, such as the summary, reference, scope, and resolution.

   - View the original alert information

     Click Details in the Alert Information column to view the original information of the alert.

## 1.1.4.4 Alert configuration

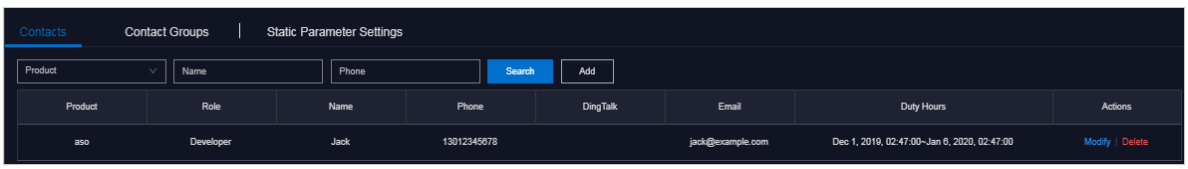
The Alert Configuration module provides you with three functions: contacts, contact groups, and static parameter settings.

### 1.1.4.4.1 Alert contacts

You can search for, add, modify, or delete an alert contact based on business needs.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Configuration. You are on the Contacts tab by default.



3. Then, you can:
   - Search for alert contacts

     Configure the corresponding product name, contact name, and phone number and then click Search. The alert contacts that meet the search conditions are displayed in the list.
   - Add an alert contact

     Click Add. On the displayed Add Contact page, complete the configurations and then click OK.
   - Modify an alert contact

     Find the alert contact to be modified and then click Modify in the Actions column. On the displayed Modify Contact page, modify the information and then click OK.
   - Delete an alert contact

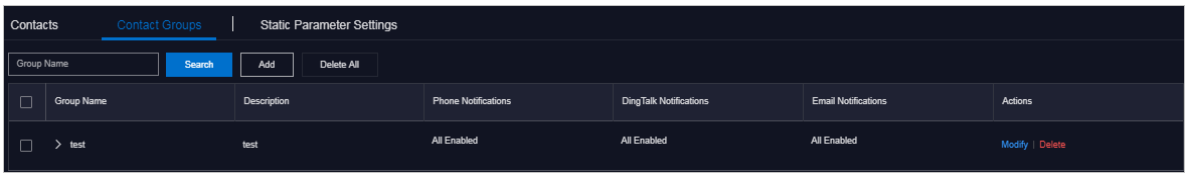
     Find the alert contact to be deleted and then click Delete in the Actions column. Click OK in the displayed dialog box.

### 1.1.4.4.2 Alert contact groups

You can search for, add, modify, or delete an alert contact group based on business needs.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Configuration.
3. Click the Contact Groups tab.



4. Then, you can:
   - Search for an alert contact group

     Enter the group name in the search box and then click Search. The alert contact group that meets the search condition is displayed in the list.
   - Add an alert contact group

     Click Add. On the displayed Add Contact Group page, enter the group name and select the contacts to add to the contact group. Then, click OK.
   - Modify an alert contact group

     Find the alert contact group to be modified and then click Modify in the Actions column. On the displayed Modify Contact Group page, modify the group name, description, contacts, and notification method. Then, click OK.
   - Delete one or more alert contact groups

     Find the alert contact group to be deleted and then click Delete in the Actions column. In the displayed dialog box, click OK.

     Select multiple alert contact groups to be deleted and then click Delete All. In the displayed dialog box, click OK.

### 1.1.4.4.3 Static parameter settings

You can configure the static parameters related to alerts based on business needs. Currently, you can only configure the parameter related to timeout alerts.

**Context**

You cannot add new alert configurations in the current version. The system has a default parameter configuration for timeout alerts. You can modify the configuration as needed.

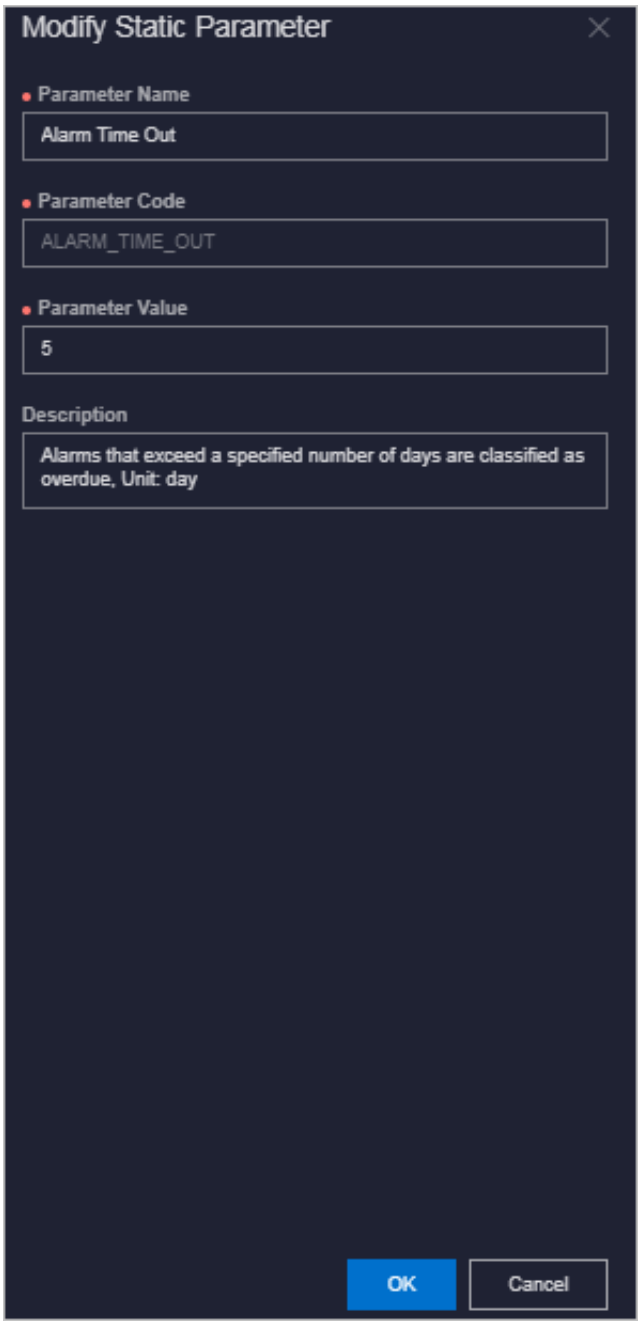
**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Configuration.
3. Click the Static Parameter Settings tab.
4. Optional: Enter the parameter name in the search box and then click Search to search for the static parameter configuration that meets the condition.
5. At the right of the static parameter to be modified, click Modify in the Actions column.

6. **On the Modify Static Parameter page, modify the parameter name, parameter value, and description.**

| Configuration | Description |
| --- | --- |
| Parameter Name | Enter a parameter name related to the configuration . |
| Parameter Value | The default value is 5, indicating 5 days.<br>After completing the configuration, the system displays the alert events that meet the condition according to this parameter value on the Timeout Alert tab of Alarm Monitoring > Alert Events.<br>For example, if the parameter value is 5, the system displays the alert events that exceed 5 days on the Timeout Alert tab of Alarm Monitoring > Alert Events. |

| Configuration | Description |
| --- | --- |
| Description | Enter the description related to the configuration. |




7. Then, click OK.

## 1.1.4.5 Alert overview

**By viewing the alert overview, you can know the distribution of different levels of alerts for Apsara Stack products.**

### Procedure

1. *Log on to Apsara Stack Operations*.

2. In the left-side navigation pane, choose Alarm Monitoring > Alert Overview. The Alert Overview page appears.

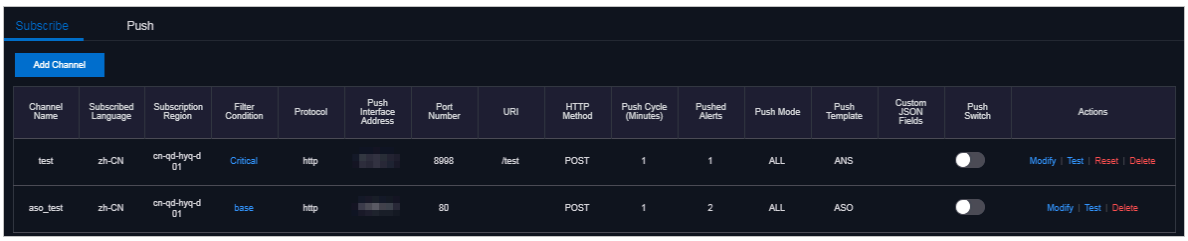

- The column chart displays the number of unsolved alerts in the last seven days .
- The section at the bottom of the page displays the alert statistics in the current system by product.

## 1.1.4.6 Alert subscription and push

The alert subscription and push function allows you to configure the alert notification channel and then push the alert to operations engineers in certain ways.

### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Subscribe/Push.




3. On the Subscribe tab, click Add Channel.
4. On the Add Subscription page, complete the following configurations.

| Configuration | Description |
| --- | --- |
| Channel Name | The name of the subscription channel. |

| Configuration | Description |
| --- | --- |
| Subscribed Language | Select Chinese or English. |
| Subscription Region | Select the region where the subscription is located. |
| Filter Condition | Select a filter condition.<br>· Basic<br>· Critical<br>· Important<br>· Minor<br>· Custom filter |
| Protocol | Currently, only HTTP is supported. |
| Push Interface Address | The IP address of the push interface. |
| Port Number | The port number of the push interface. |
| URI | The URI of the push interface. |
| HTTP Method | Currently, only POST is supported. |
| Push Cycle (Minutes) | The push cycle, which is calculated by minute. |
| Pushed Alerts | The number of alerts pushed each time. |
| Push Mode | Select one of the following methods:<br>· ALL: All of the alerts are pushed in each push cycle.<br>· TOP: Only alerts with high priority are pushed in each push cycle. |
| Push Template | Select one of the following templates:<br>· ASO: The default template.<br>· ANS: Select this template to push alerts by DingTalk, SMS, or email. Currently, you can only configure one channel of this type.<br>Note:<br>A preset ANS template exists if the system already connects with the ANS product. To restore the initial configurations of the template with one click, click Reset. |
| Custom JSON Fields | The person who receives the push can use this field to configure the identifier in a custom way. The format must be JSON. |

| Configuration | Description |
| --- | --- |
| Push Switch | Select whether to push the alerts.<br>If the switch is not turned on here, you can enable the push feature in the Push Switch column after configuring the subscription channel. |

5. After completing the configurations, click OK.

   To modify or delete a channel, click Modify or Delete in the Actions column.

6. Optional: The newly added channel is displayed in the list. Click Test in the Actions column to test the connectivity of the push channel.

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

7. After configuring the push channel and turning on the push switch, you can click the Push tab to view the push records.

## 1.1.4.7 Alert masking

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

### 1.1.4.7.1 Add a masking rule

By adding a masking rule, you can mask alerts that you are not required to pay attention to.

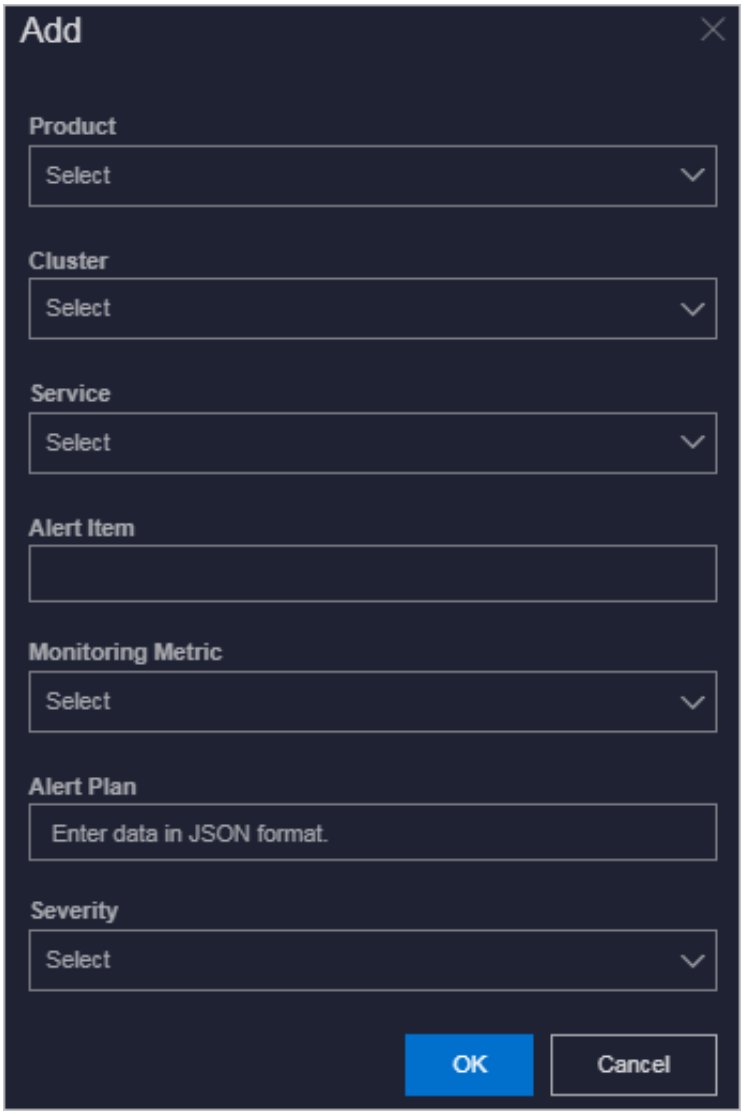
**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Masking.
3. Click Add on the page.
4. On the Add page, complete the configurations to mask a certain type of alerts.

| Configuration | Description |
| --- | --- |
| Product | Optional. The product to which alerts to be masked belong. |

| Configuration | Description |
| --- | --- |
| Cluster | Optional. The cluster to which alerts to be masked belong. |
| Service | Optional. The name of the service to which alerts to be masked belong. |
| Alert Item | Optional. The alert name to be masked.<br>  Note:<br>If the number of alerts is large, you may have to wait for a few minutes when selecting an alert item. |
| Monitoring Metric | Optional. The monitoring metric to which alerts to be masked belong. |

| Configuration | Description |
| --- | --- |
| Alert Plan | Optional. The alert details of the alerts to be masked.<br><br>Example:<br><br>`{"serverrole":"ecs-yaochi.ServiceTest#","machine":"vm010012016074","level":"error"}` |
| Severity | Optional. Alerts are classified into the following levels:<br><br>· P0: indicates the cleared alerts, corresponding to alerts whose Alert Level is Restored in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>· P1: indicates the critical alerts, corresponding to alerts whose Alert Level is P1 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>· P2: indicates the major alerts, corresponding to alerts whose Alert Level is P2 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>· P3: indicates the minor alerts, corresponding to alerts whose Alert Level is P3 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>· P4: indicates the remind alerts, corresponding to alerts whose Alert Level is P4 in Monitoring > Alert History of Apsara Infrastructure Management Framework.<br>· P5: indicates the system alerts, corresponding to alerts whose Alert Level is P5 in Monitoring > Alert History of Apsara Infrastructure Management Framework. |




**Note:**

**If the number of alerts is large, you may have to wait for a few minutes when selecting an alert item.**

5. **Then, click OK.**

**Result**

**The added masking rule is displayed in the alert masking list.**

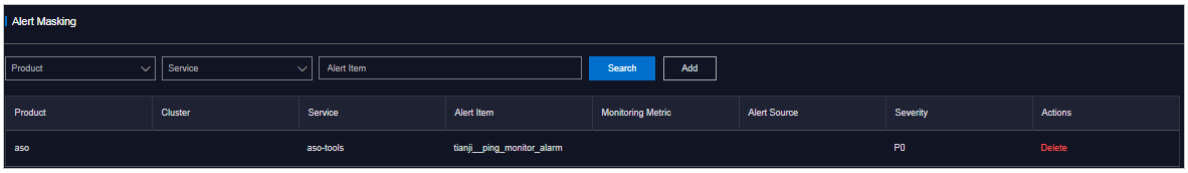
**In Alarm Monitoring > Alert Events and Alarm Monitoring > Alert History, you cannot view alerts that meet the conditions in the masking rule.**

### 1.1.4.7.2 Remove the masking

**You can remove the masking for masked alerts.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Alarm Monitoring > Alert Masking.
3. Optional: Select a product, service, or alert item, and then click Search.
4. Find the alert masking rule and then click Delete in the Actions column to remove the masking.




5. In the displayed dialog box, click OK.

**Result**

After removing the masking, you can view alerts masked by the deleted masking rule in Alarm Monitoring > Alert Events and Alarm Monitoring > Alert History.

## 1.1.5 Products

The Products module allows you to click operations and maintenance services of other products on the cloud platform and ISV access configurations to go to the corresponding page.

### 1.1.5.1 Product list

In the Product List, you can be redirected to the corresponding operations and maintenance page of a product or ISV page by using Single Sign-On (SSO) and redirection.

**Prerequisites**

To be redirected to the ISV page, make sure that the ISV access information is configured on the ISV Access Configurations page. For more information about how to configure the ISV access information, see *Configure the ISV access information*.

**Context**

After logging on to Apsara Stack Operations (ASO), you can view operations and maintenance icons of different products and different ISV icons in the Product List based on your permissions. For example, an operations system administrator can view all the operations and maintenance components of the cloud platform.

The read and write permissions for product operations and maintenance are separated. Therefore, the system can dynamically assign different permissions based on different roles.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Products > Product List.
3. In the Product List, you can view operations and maintenance icons of different products and different ISV icons based on your permissions.

## 1.1.5.2 ISV access configurations

The ISV Access Configurations module allows you to configure, modify, and delete the ISV access information.

### 1.1.5.2.1 Configure the ISV access information

You can configure the ISV access information in the system based on business needs. Then, you can access the corresponding ISV page by clicking the icon in the Product List.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Products > ISV Access Configurations.
3. Click Add on the page.
4. On the displayed Add page, configure the ISV access information.

   For more information about the configurations, see the following table.

| Configuration | Description |
| --- | --- |
| Name | The name of the ISV to be accessed. |
| Key | Generally, enter an identifier related to the ISV business as the key. |
| Icon | Select the icon displayed in the Product List for the ISV to be accessed. |
| Level-one Category and Level-two Category | The category to which the ISV to be accessed belongs in the Product List. |
| Usage | The function of the ISV to be accessed. |
| Access Link | The access address of the ISV to be accessed. |

| Configuration | Description |
| --- | --- |
| Description | The description related to the ISV to be accessed. |

5. Then, click Add.

**Result**

You can view the added ISV icon in Products > Product List. Click the icon and then you can be redirected to the corresponding page.

### 1.1.5.2.2 Modify the ISV access information

If the ISV information is changed, you can modify the ISV access information.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Products > ISV Access Configurations.
3. Optional: In the search box on the page, enter the ISV name and then click Search. Fuzzy search is supported.
4. Find the ISV whose access information is to be modified. Click Modify in the Actions column.
5. On the displayed Modify page, modify the name, key, icon, level-one category, level-two category, usage, access link, or description of the ISV.
6. Then, click Modify.

### 1.1.5.2.3 Delete the ISV access information

You can delete the ISV access information added in the system based on business needs.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Products > ISV Access Configurations.
3. Optional: In the search box on the page, enter the ISV name and then click Search. Fuzzy search is supported.
4. Find the ISV whose access information is to be deleted. Click Delete in the Actions column.
5. In the displayed dialog box, click OK.

**Result**

Then, the ISV information is not displayed in Products > Product List.

# 1.1.6 NOC

**Network Operation Center (NOC) is an all-round operations tool platform that covers the whole network (virtual network and physical network).**

## 1.1.6.1 Network topology

**The Network Topology tab allows you to view the physical network topology.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose NOC > Dashboard.**
3. **On the Network Topology tab, view the physical network topology of a physical data center.**

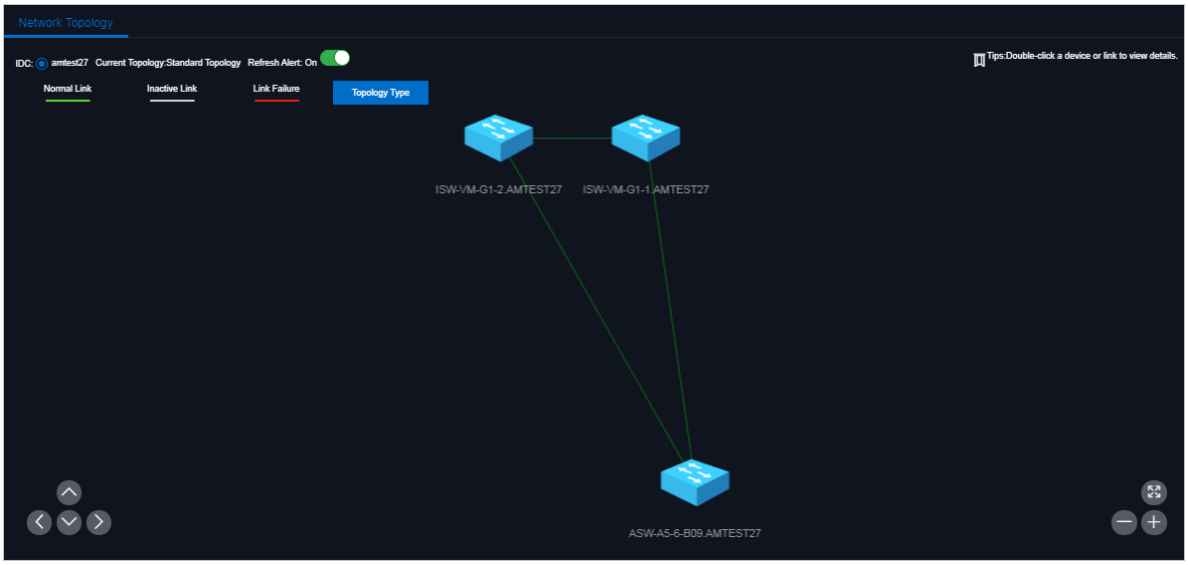
   **You can select Standard Topology or Dynamic Topology as the Topology Type.**

   **Note:**

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

   - **Green: The link works properly.**
   - **Red: The link has an error.**
   - **Grey: The link is inactive.**

   **If the Topology Type is Standard Topology, the Refresh Alert switch is turned on by default. You can turn off the Refresh Alert switch, and then devices or link statuses in the topology are not updated after new alerts are triggered.**



4. In the topology, double-click a connection between two devices to view the links and alerts between the two devices.
5. In the topology, double-click a physical network device to view the basic information and node alerts of the device on the right.

## 1.1.6.2 Resource management

The Resource Management module is used to manage network-related resources, including the information of physical network element devices, virtual network products, and IP addresses.

### 1.1.6.2.1 Device management

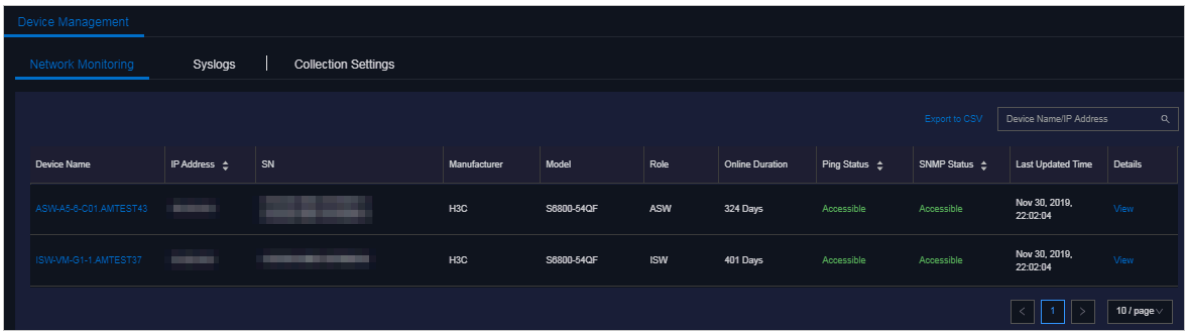
The Device Management page displays the basic information, running status, traffic monitoring, and logs of physical network element devices, and allows you to configure the collection settings of network devices.

#### *1.1.6.2.1.1 View the network monitoring information*

The Network Monitoring tab allows you to view the basic information, running status, and traffic monitoring of Apsara Stack physical network devices, and know the health status of devices in the whole network in time.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Network Monitoring tab under Device Management.




4. Then, you can:
   - View the basic information, ping status, and SNMP status of Apsara Stack physical network devices.

   **Note:**

**You can also click Export to CSV to export the network device information to your local computer as required.**

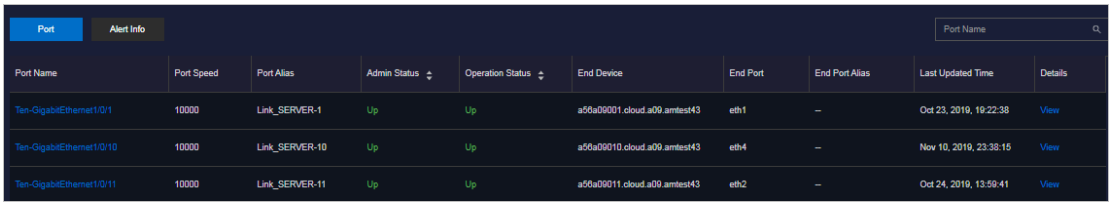
**If a problem exists in the business connectivity or gateway connectivity, the value in the Ping Status column or SNMP Status column changes from green to**

red. Then, the operations personnel are required to troubleshoot the problem.

- In the search box in the upper-right corner, enter the device name or IP address to search for the monitoring information of a specific device.
- View the port information and alert information of a device.
  a. Click a device name, or click View in the Details column at the right of a device.
  b. Under Port, view the port list, port working status, and other link information of the device.
  c. Under Alert Info, view the alert information of the device.

     During the daily operations, you must pay close attention to the alert information list of the device. Normally, no data exists under Alert Info, indicating that the device works properly.

     If alert events occur, unrecovered alert events are displayed in the list. You must handle these exception events in time. After you handle exceptions, the alert events are automatically cleared from the list.
- View the traffic information of a device for a specific port and time range.
  a. Click a device name, or click View in the Details column at the right of a device.
  b. Search for the port that you are about to view by using the search box in the upper-right corner of the Port section. Click View in the Details column at the right of the port.




  c. Select a time range on the right and then click Search to view the traffic in the selected time range.

     You can select 5MIN, 30MIN, 1H, or 6H in the Quick Query section to view the traffic within 5 minutes, 30 minutes, 1 hour, or 6 hours.

### 1.1.6.2.1.2 View logs

The Syslogs tab allows you to view logs of physical network element devices, providing necessary data for fault location and diagnosis information collection if a fault occurs.

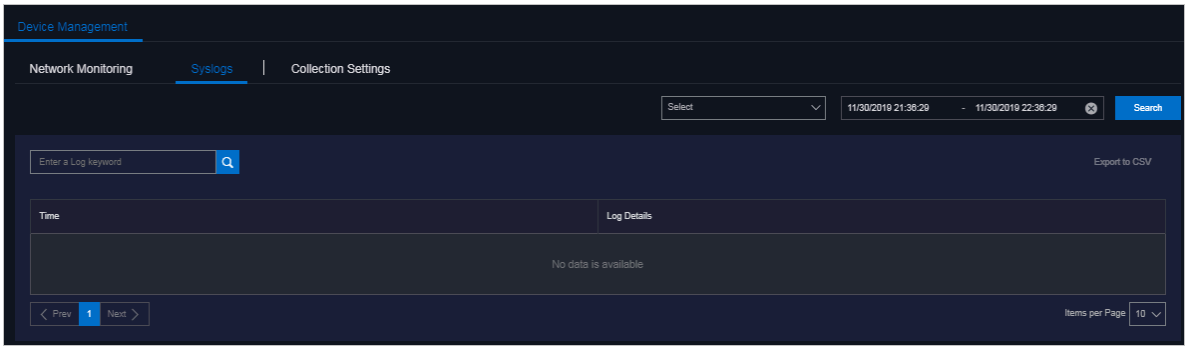
**Context**

During the daily inspection, you can search for logs generated by a specific network device during a specific time range on the Syslogs tab.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Syslogs tab under Device Management.
4. In the upper-right corner, select the name of the device that you are about to view from the drop-down list, and then select a time range. Click Search to view if the device generates system logs during the selected time range.

   No search results exist if the device has a configuration exception or does not generate any logs during the selected time range.




5. Optional: You can filter the search results based on the log keyword.
6. Optional: Click Export to CSV in the upper-right corner to export the search results to your local computer.

### 1.1.6.2.1.3 Collection settings

The Collection Settings tab allows you to configure the collection interval of physical network element devices and manage OOB network segments.

1.1.6.2.1.3.1 Modify the collection interval

You can modify the collection interval to adjust the time interval of collection.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Collection Settings tab under Device Management.
4. In the Collection Interval Settings section, modify the auto scan interval, device scan interval, port scan interval, and link scan interval.

   **Note:**
   To not save your modification before the submittal, click Reset in the upper-right corner to reset the collection interval to the former version.
5. Click Submit.

   One minute later, the modified collection interval of network device information is synchronized to the system.

#### 1.1.6.2.1.3.2 Add an OOB network segment

If this is the first time to use the Network Elements function of Network Operation Center (NOC), you must add the device loopback IP address range planned by the current Apsara Stack network device, which is generally the IP address range of the netdev.loopback field in the IP address planning list.

**Context**

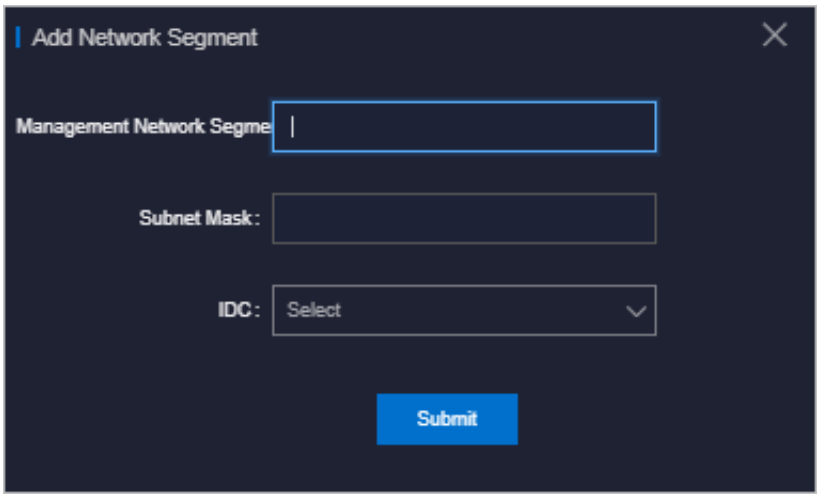
The OOB Network Segments section is used to configure the management scope of a physical network element device. Generally, operations engineers are required to add the loopback IP address range where the network device to be managed resides .

In the Apsara Stack scenario, use the loopback IP address range to configure the management scope of a physical network element device. To expand the network and the loopback IP address range, you must add the IP address range involved in the expansion to the management scope. The way to add an expansion IP address range is the same as that to add the loopback IP address range for the first time. Then, you can search for the IP address range of the managed device on this page.

**Procedure**

1. *Log on to Apsara Stack Operations*.

2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Collection Settings tab under Device Management.
4. In the OOB Network Segments section, click Add Network Segment.
5. In the displayed dialog box, enter the IP address range containing the mask information, subnet mask, and select a data center.




6. Click Submit.

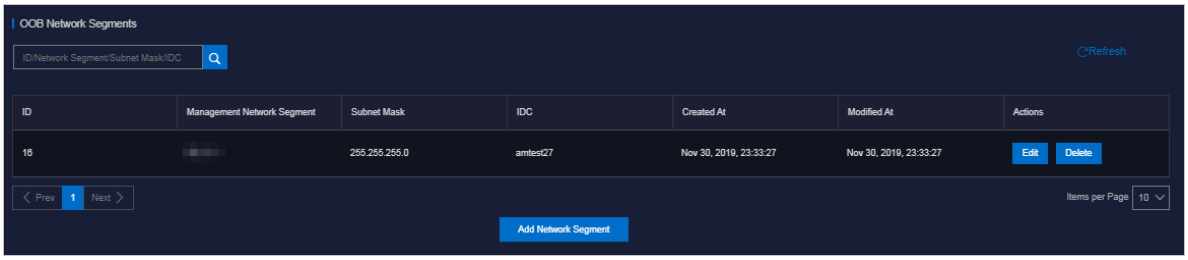
   The initial data is synchronized to the system after the submittal.

#### 1.1.6.2.1.3.3 Modify the OOB network segment information

You can modify the network segment information of your managed device.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Collection Settings tab under Device Management.
4. In the OOB Network Segments section, click Refresh in the upper-right corner to obtain the latest OOB network segment information.



5. Optional: Enter the network segment information in the search box and then press Enter or click the search icon.
6. Find the OOB network segment to be modified and then click Edit in the Actions column.
7. In the displayed dialog box, modify the Management Network Segment, Subnet Mask, or IDC, and then click Submit Change.

#### 1.1.6.2.1.3.4 Delete an OOB network segment

You can delete an OOB network segment that you are not required to manage based on business needs.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Network Elements.
3. Click the Collection Settings tab under Device Management.
4. Find the OOB network segment to be deleted and then click Delete in the Actions column.
5. Click OK in the displayed dialog box.

### 1.1.6.2.2 View the instance monitoring information

The Instance Monitoring tab allows you to view the basic information and water level of an instance, including the bps and pps.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Resource Management > Server Load Balancers.
3. Click the Instance Monitoring tab.
4. Select the cluster where the instance that you are about to view is located from the Cluster drop-down list. Enter the VIP address that you are about to search for in the field and then click Search.
5. View the water level data of this VIP address.

   Select a time range and then click Search or select 5MIN, 30MIN, 1H, or 6H in the Quick Query section to view the operating water level graph of the VIP address in a specific time range.

## 1.1.6.3 Alert management

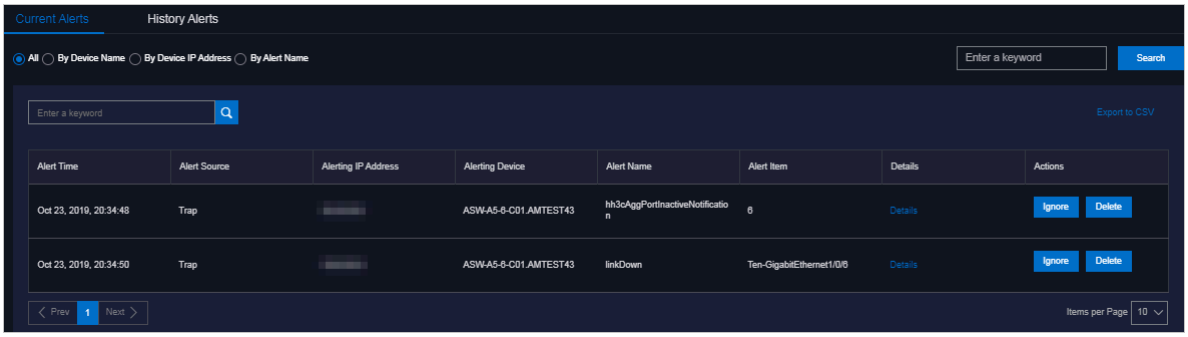
**The Alert Management module provides you with the real-time alert dashboard, history alert dashboard, and the alert settings function.**

### 1.1.6.3.1 View and process current alerts

**You can view and process current alerts on the Current Alerts tab.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose NOC > Alert Management > Alert Dashboard.**
3. **Click the Current Alerts tab.**




4. **Enter a keyword in the search box in the upper-right corner and then click Search.**

   **Alerts that meet the search condition are displayed.**
5. **Optional: You can filter the search results by device name, device IP address, or alert name.**
6. **Click Details in the Details column at the right of an alert to view the detailed alert information.**
7. **Find the reason why the alert is triggered and then process the alert.**

   - **If the alert does not affect the system normal operation, you can click Ignore in the Actions column to ignore the alert.**
   - **If the alert is meaningless, you can click Delete in the Actions column to delete the alert.**

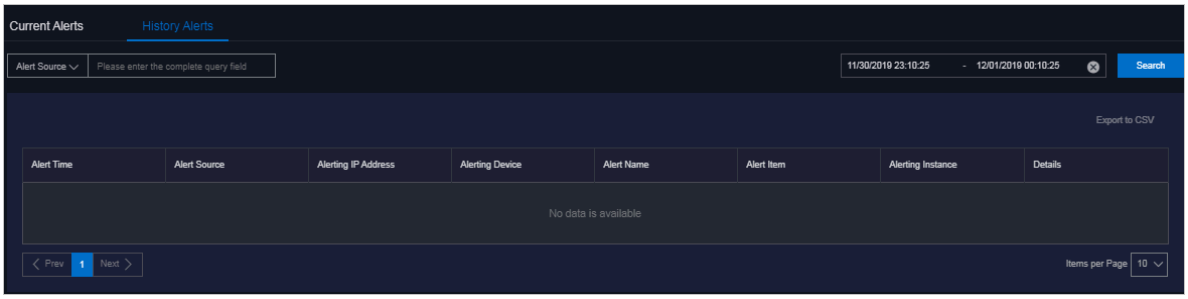
   **After processing an alert, you can search for it on the History Alerts tab.**
8. **Optional: Click Export to CSV to export the alert information to your local computer.**

## 1.1.6.3.2 View history alerts

**You can view history alerts on the History Alerts tab.**

### Procedure

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose NOC > Alert Management > Alert Dashboard.**
3. **Click the History Alerts tab.**




4. **Select Alert Source, Alerting IP Address, Alerting Device, Alert Name, Alert Item, or Alerting Instance from the drop-down list and then enter a keyword in the field. Select a time range and then click Search.**

   **Alerts that meet the search conditions are displayed.**
5. **Click Details in the Details column at the right of an alert to view the detailed alert information.**
6. **Optional: Click Export to CSV to export the alert information to your local computer.**

## 1.1.6.3.3 Add a trap

**If the initially configured trap subscription cannot meet the monitoring requirement, you can add a trap as required for monitoring match.**

### Procedure

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose NOC > Alert Management > Alert Settings.**
3. **On the Alert Settings page, click Configure Trap.**

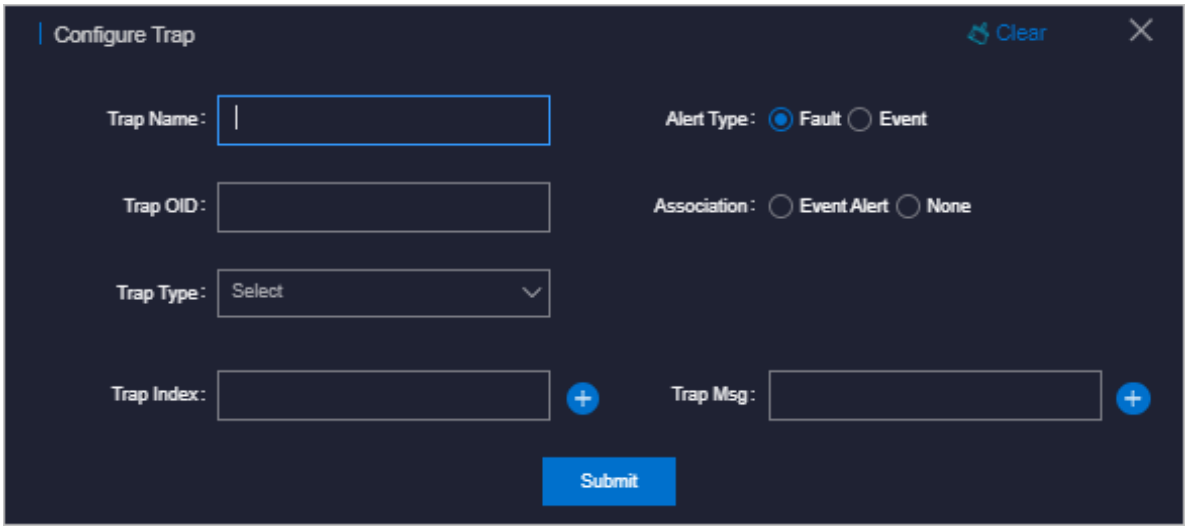
4. In the displayed Configure Trap dialog box, complete the configurations.

   See the following table for the configuration items and descriptions.

| Configuration | Description | Example |
| --- | --- | --- |
| Trap Name | The name of the alert event . | linkdown or BGPneighbor down. You can customize this value. |
| Trap OID | The OID of the alert event. | .1.3.6.1.4.1.25506.8.35.12.1 .12<br>Configure the value strictly according to the device document. You cannot customize this value. |
| Trap Type | The type of the alert event . Select a value from the drop-down list. | - |
| Trap Index | The index ID of the alert item. | This value is the KV information in the trap message, which is used to identify the alert object. Generally, this value can be an API name, protocol ID, or index ID.<br>Configure the value strictly according to the device document. You cannot customize this value. |

| Configuration | Description | Example |
| --- | --- | --- |
| Trap Msg | The message of the alert item. | This value is the KV information in the trap message, which is used to identify the alert data. Generally, this value can be the additional information of the alert item, such as a system message or a message indicating the location of the state machine or the current status.<br>Configure the value strictly according to the device document. You cannot customize this value. |
| Alert Type | Indicates whether this alert is of the fault type or the event type. | - |

| Configuration | Description | Example |
| --- | --- | --- |
| Association | Indicates whether this alert has an event alert.<br>If Fault is selected as the Alert Type and this alert has an association alert, select Event Alert as Association and then add the trap of the association alert. | - |




5. Then, click Submit.

   After the submittal, the system checks if the trap OID and trap name are the same as the existing ones. If not, the alert settings of the added trap are finished.

   The system pays attention to the alert events of the configured trap OID and such alert events are displayed on the Current Alerts and History Alerts tabs of Alert Management > Alert Dashboard.

## 1.1.6.3.4 View a trap

You can view a trap configured in the current system.

### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose NOC > Alert Management > Alert Settings.

3. Enter a keyword in the search box in the upper-right corner and then click Search.

   **Note:**
   After the search results are displayed, you can click Export to CSV in the upper-right corner to export the trap information to your local computer.

4. Optional: You can filter the search results by trap name, trap type, or OID.
5. Find a trap and then move the pointer over Details in the Actions column to view the detailed trap information.

   **Note:**
   If a trap is no longer in use, you can click Delete in the Actions column at the right of the trap.

## 1.1.7 Storage Operation Center

The Storage Operation Center module contains the pangu section and miniOSS section.

### 1.1.7.1 Pangu

The Pangu section displays the pangu grail, cluster information, node information, and pangu cluster status.

#### 1.1.7.1.1 Pangu grail

The Pangu Grail module allows you to view the overview, heatmap of health, and top 5 data of a product.

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Storage Operation Center > Pangu > Pangu Grail.
3. Select the product that you are about to view from the Service drop-down list.

   Pangu Grail displays the data overview, heatmap of health, and top 5 data of each accessed cloud product as of the current date.

   - Overview

     Overview displays the storage space, server information, and health information of the selected product. Values of Abnormal Disks, Abnormal

Masters, Abnormal Chunk Servers, and Abnormal Water Levels in the Health section are displayed in red if they are larger than zero.


- Heatmap of Health

  Heatmap of Health displays the health information of all the clusters in the selected product. Clusters in different health statuses are displayed in different colors.

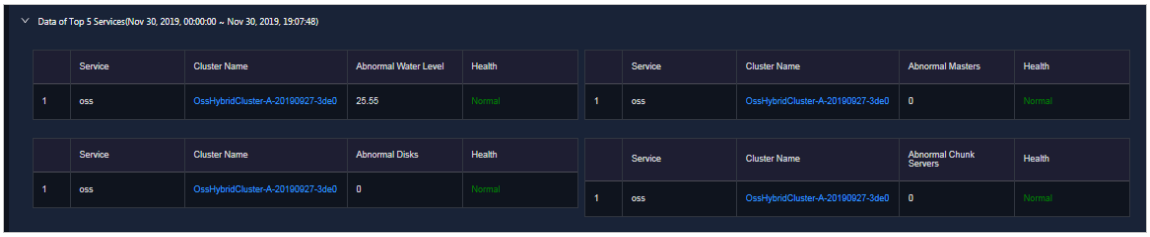
  - Green indicates the normal status.
  - Yellow indicates a warning.
  - Red indicates the abnormal status.
  - Dark red indicates a fatal error.
  - Grey indicates the closed status.

  Click the name of a cluster that is not in the closed status to go to the corresponding cluster information page.


- Data of Top 5 Services

  Data of Top 5 Services displays the data of the top 5 unhealthiest clusters in the time range from zero o'clock to the current time in the current date for the selected product.

  This section displays the top 5 clusters in terms of abnormal water levels, abnormal masters, abnormal disks, and abnormal chunk servers. Click the cluster name to go to the corresponding cluster information page.




## 1.1.7.1.2 Cluster information

**The Cluster Information module allows you to view the overview and run chart of a cluster.**

### Procedure

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose Storage Operation Center > Pangu > Cluster Information.**

   **By default, data of the first cluster in the Cluster Name drop-down list is displayed.**
3. **Select the cluster that you are about to view from the Cluster Name drop-down list.**

   **Note:**
   **All the accessed clusters that are not in the closed status in the current environment are available for you to select from the Cluster Name drop-down list.**

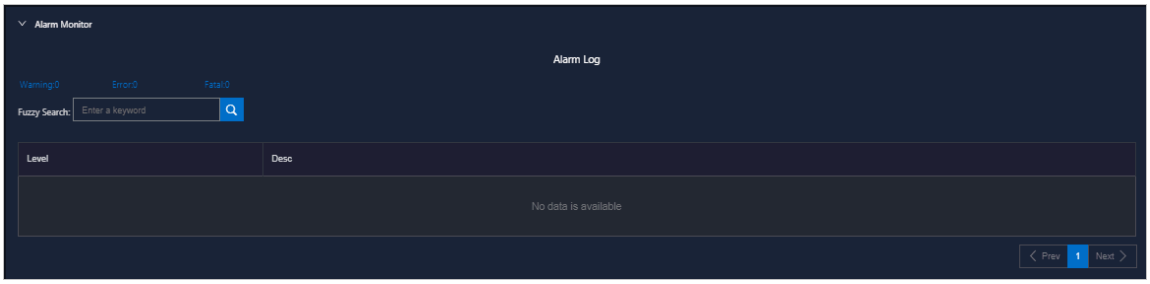
   - **Overview**

     **Displays the storage space, server information, and health information of the selected cluster. Values of Abnormal Water Levels, Abnormal Masters,**

Abnormal Chunk Servers, and Abnormal Disks in the Health section are displayed in red if they are larger than zero.


- **Alarm Monitor**

  Displays the alert information of the selected cluster. You can perform a fuzzy search based on a keyword.




- **Replica**

  Displays the replica information of the selected cluster.

- **Run Chart of Clusters**

  Displays the charts of historical water levels, predicted water levels, number of files, number of chunk servers, and number of disks for the selected cluster .

  Predicted Water Levels predicts the run chart of the next seven days.

**Note:**

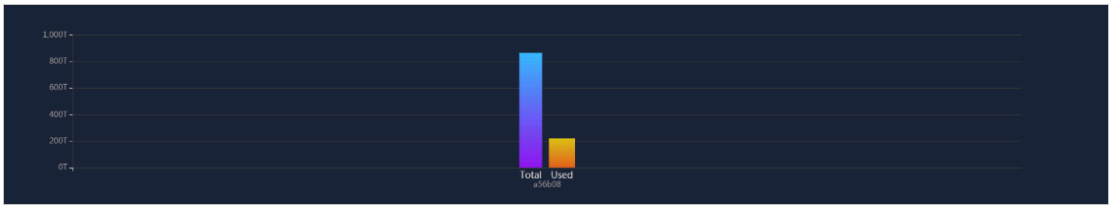
**Predicted Water Levels has values only if Historical Water Levels has a certain amount of data. Therefore, some clusters may only have historical water levels, without predicted water levels.**


- **Rack Information**

  **Consists of Servers in Rack and Storage.**

  - **Servers in Rack displays the number of servers in each rack of the selected cluster.**


  - **Storage displays the total storage and used storage in each rack of the selected cluster.**




## 1.1.7.1.3 Node information

**The Node Information module allows you to view the master information and chunk server information in a cluster.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose Storage Operation Center > Pangu > Node Information.**

   **By default, data, namely the master information and chunk server information, of the first cluster in the Cluster Name drop-down list is displayed.**
3. **Select the cluster that you are about to view from the Cluster Name drop-down list.**

    **Note:**

**All the accessed clusters that are not in the closed status in the current environment are available for you to select from the Cluster Name drop-down list.**

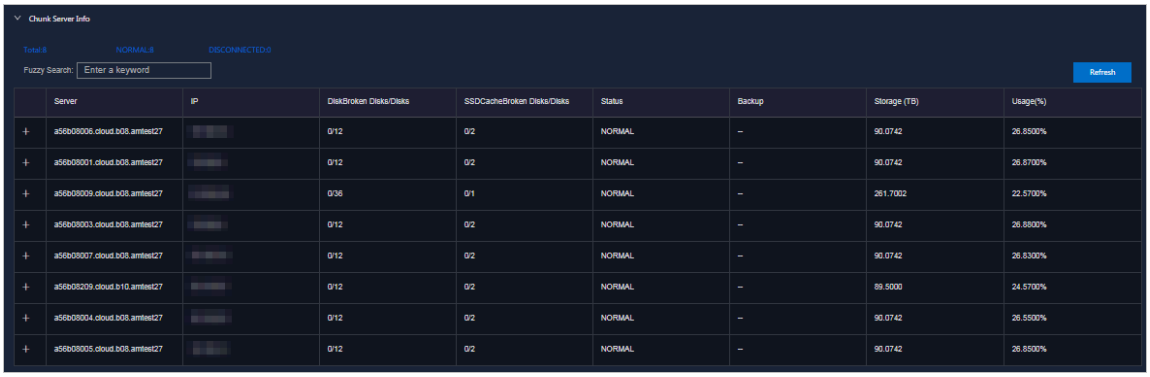
- **Master Info**

  **Displays the master information in the selected cluster. Partial refresh is supported. You can click Refresh to refresh the master information in the selected cluster.**


- **Chunk Server Info**

  **Displays the chunk server information in the selected cluster. Partial refresh is supported. You can click Refresh to refresh the chunk server information in the selected cluster.**

  **Click + to display the disk overview and SSDCache overview in the current chunk server. Fuzzy search is supported.**




## 1.1.7.1.4 Pangu operation

**The Pangu Operation module allows you to view the pangu cluster status.**

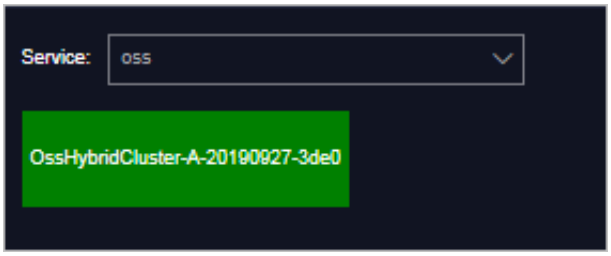
**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose Storage Operation Center > Pangu > Pangu Operation.**

3. Select a product from the Service drop-down list to view the pangu cluster status of this product.

   Clusters in different statuses are in different colors.

   - Green indicates that the cluster works properly.
   - Yellow indicates that the cluster has a warning.
   - Red indicates that the cluster has an exception.
   - Dark red indicates that the cluster has a fatal error.
   - Grey indicates that the cluster is closed.




4. Move the pointer over a cluster name to view the service name, server name, and IP address to which the cluster belongs.

## 1.1.7.2 miniOSS

The miniOSS module provides you with the following functions: monitoring dashboard, user management, permission/quota management, array monitoring, and system management.

### 1.1.7.2.1 Monitoring dashboard

The Monitoring Dashboard module allows you to view the overview, bucket watermark heatmap, user quota watermark heatmap, watermark trend, and network traffic trend of miniOSS in the system, and download logs to your local computer.

**Procedure**

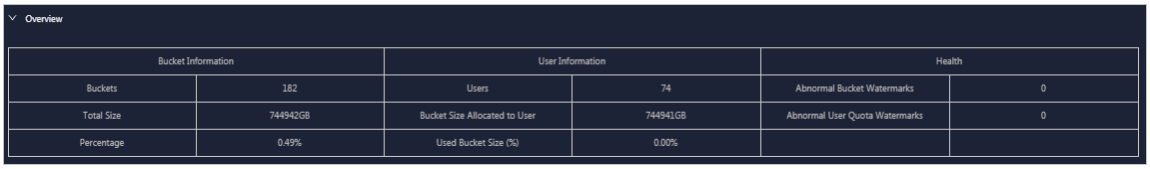
1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Storage Operation Center > miniOSS > Monitoring Dashboard.

3. On this page, you can view the following information:

   - Overview

     Displays the bucket information, user information, and health information of miniOSS.

     Values of Abnormal Bucket Watermarks and Abnormal User Quota Watermarks in the Health section are displayed in red if they are larger than zero.



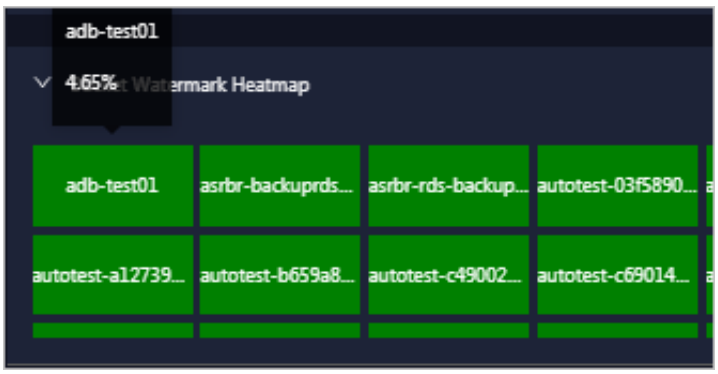

   - Bucket Watermark Heatmap

     Displays the bucket capacity usage.

     The number of sections in Bucket Watermark Heatmap is the same as the value of Buckets in Overview. Buckets in different colors represent different statuses. Where,

     - Green indicates the normal status.
     - Yellow indicates a warning.
     - Red indicates the abnormal status.
     - Dark red indicates a fatal error.
     - Grey indicates the closed status.

     Move the pointer over a bucket section to view the percentage of capacity used by the bucket.




   - User Quota Watermark Heatmap

     Displays the user quota watermark information.

**User quota watermark = used capacity of all buckets of the user/total capacity of all buckets of the user. Different watermark values are displayed in different colors. Where,**

- **Green indicates the normal status.**
- **Yellow indicates a warning.**
- **Red indicates the abnormal status.**
- **Dark red indicates a fatal error.**
- **Grey indicates the closed status.**

**Move the pointer over a section to view the percentage of capacity used by all buckets of a user.**

- **Watermark Trend**

  **Displays the historical water levels and predicted water levels of a user or bucket. Watermark represents the disk utilization, and watermark of a user indicates the disk utilization of a user's buckets.**

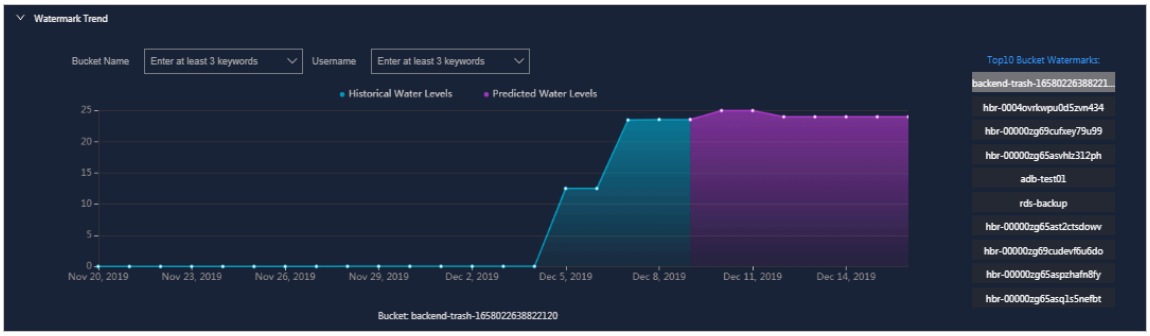
  **Data in the watermark trend comes from scheduled tasks in the system. The system stores or updates data every 30 minutes.**

  **Select a bucket or user from the drop-down list to view the corresponding watermark trend.**

  **Note:**

**You can enter a keyword of a Bucket Name or Username to perform a fuzzy search.**

**The top 10 data in terms of the bucket watermarks are displayed on the right . Click a bucket name in the top 10 data to view the watermark trend of the bucket on the left.**

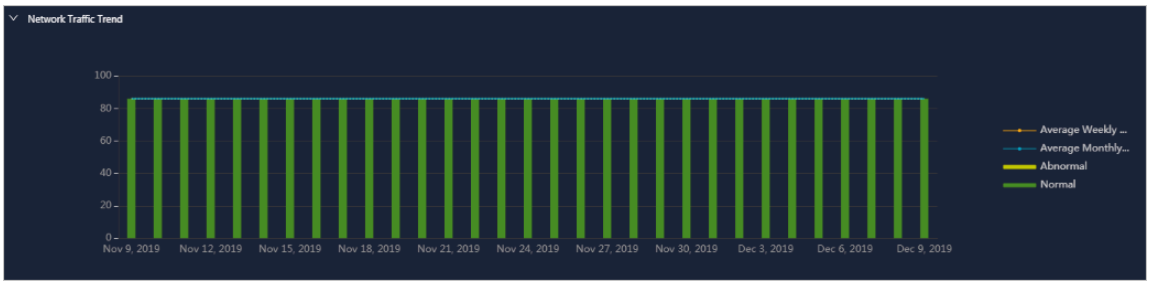



- **Network Traffic Trend**

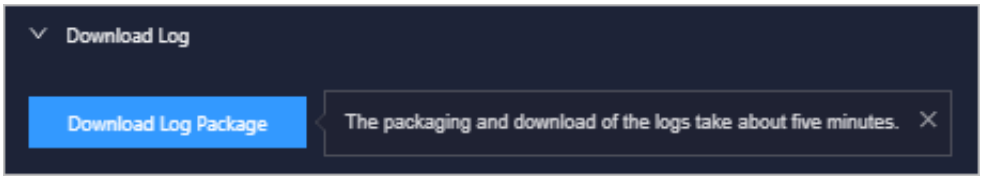
  **Displays the daily network traffic data, namely the normal network traffic , abnormal network traffic, average weekly network traffic, and average monthly network traffic, of miniOSS in the last month.**

  **In the network traffic trend:**

  - **Green indicates the network traffic is normal.**
  - **Yellow indicates the network traffic is abnormal.**
  - **Orange indicates the average weekly network traffic.**
  - **Blue indicates the average monthly network traffic.**




4. **Optional: You can click Download Log Package in the Download Log section and then use the download URL to download logs to your local computer for subsequent review and analysis.**



### 1.1.7.2.2 User management

**The User Management module consists of User List, Bucket List of User, and Network Traffic Control. You can use this module to view the user information, bucket list of a user, and network traffic bandwidth.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose Storage Operation Center > miniOSS > User Management.**
3. **On this page, you can:**
   - **View the user information**

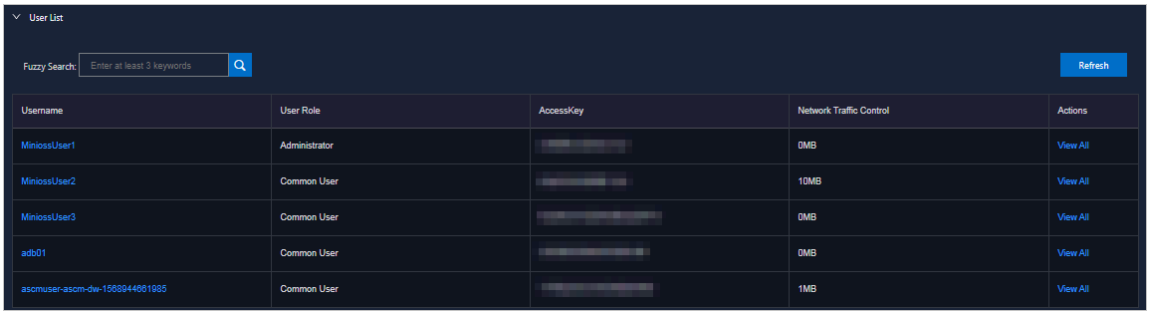
     **All of the users, including the administrator and common users, are displayed in the list by default.**

     **Click View All in the Actions column at the right of a user and view the SecretKey of the user in the displayed dialog box.**

     **In the User List section, enter a keyword with three characters of the username, such as def, and press Enter or click the search icon. Then, you can view the information, namely the username, user role, AccessKey, and network traffic bandwidth, of the user that meets the search condition.**

     **Note:**

After the search, to view all of the users in the list, click Refresh.

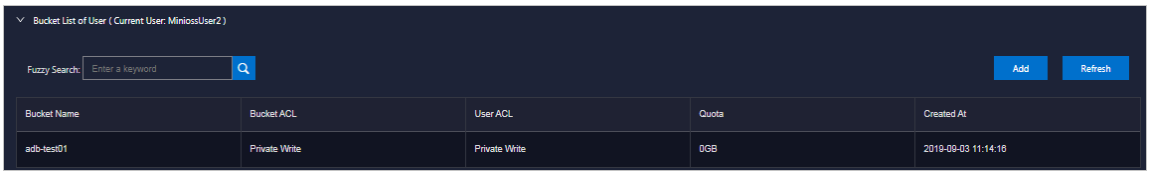



- View the bucket information of a user

  Click a username in the User List section. Then, view the bucket information, namely the bucket name, bucket ACL, user ACL, quota, and bucket creation time, of the user in the Bucket List of User section.

  In the Bucket List of User section, enter a keyword with five characters of the bucket name, such as atest, and press Enter or click the search icon. Then, you can view the information of the bucket that meets the search condition.

  **Note:**
  After the search, to view the information of all buckets, click Refresh.



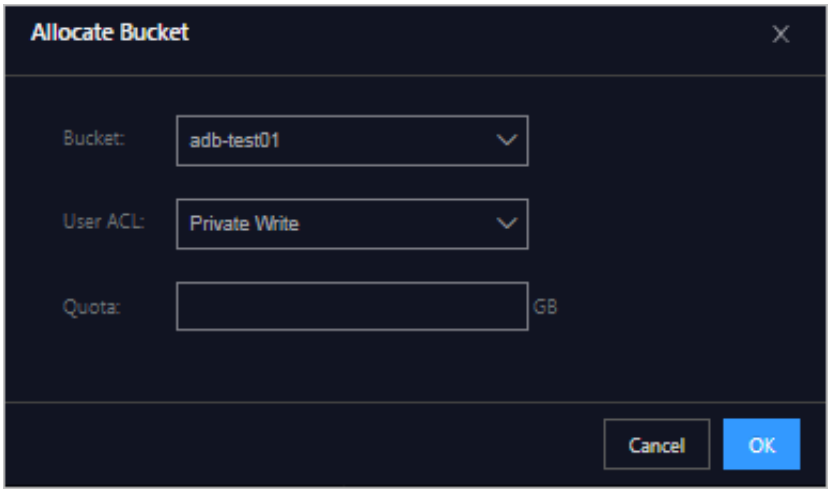

- Add a bucket for a common user

  **Notice:**
  You can only add a bucket for a common user, instead of for an administrator.

  Find the common user for whom you are about to add a bucket in the User List section and then click the username. In the Bucket List of User section, click Add. In the displayed dialog box, select the bucket and user ACL, enter the quota, and then click OK.

  **Note:**

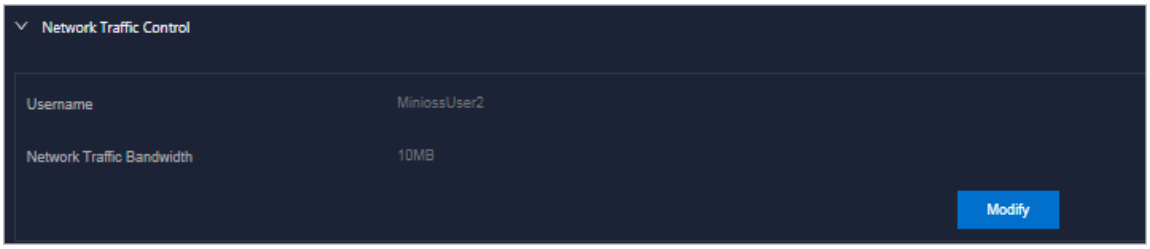
Enter an integer from 0 to 4094 as the quota.




- View the network traffic bandwidth of a user

  Find the user whose network traffic bandwidth you are about to view in the User List section and then click the username. View the network traffic bandwidth of the user in the Network Traffic Control section.
- Modify the network traffic bandwidth of a user

  Find the user whose network traffic bandwidth you are about to modify in the User List section and then click the username. In the Network Traffic Control section, click Modify to modify the network traffic bandwidth of the user and then click Save. The value of network traffic bandwidth must be 0 or a positive integer.




## 1.1.7.2.3 Permission and quota management

The Permission/Quota Management module allows you to view the bucket list and user list of bucket, and add, modify, and delete a bucket.

### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Storage Operation Center > miniOSS > Permission/Quota Management.

3. On this page, you can:

   - View the bucket information

     All of the buckets are displayed in the bucket list by default. In the Bucket List section, you can view the basic information, namely bucket name, bucket ACL, quota, and network traffic bandwidth, of all the buckets.

     Enter a keyword of the bucket name in the search box in the upper-left corner and press Enter or click the search icon. Then, you can view the information of the bucket that meets the search condition.

      **Note:**
     After the search, to view all the buckets in the list, click Refresh.

   - Add a bucket

     In the Bucket List section, click Add. In the displayed dialog box, enter the bucket name and then click OK. The bucket name must be 3 to 63 characters in length, can only contain lowercase letters, digits, hyphens (-), and cannot start or end with a hyphen (-).

   - Modify a bucket

     In the Bucket List section, click Modify in the Actions column at the right of the bucket to be modified. In the displayed dialog box, modify the bucket ACL, quota, and network traffic bandwidth, and then click OK.

   - Delete a bucket

     In the Bucket List section, click Delete in the Actions column at the right of the bucket to be deleted. Click OK in the displayed dialog box.

   - View the information of the user that a bucket belongs

     In the Bucket List section, click a bucket name to view the user information related to the bucket in the User List of Bucket section.

     Enter a keyword of the username in the search box and press Enter or click the search icon. Then, you can view the information of the user that meets the search condition.

      **Note:**
     After the search, to view the information of all the users, click Refresh.

## 1.1.7.2.4 Array monitoring

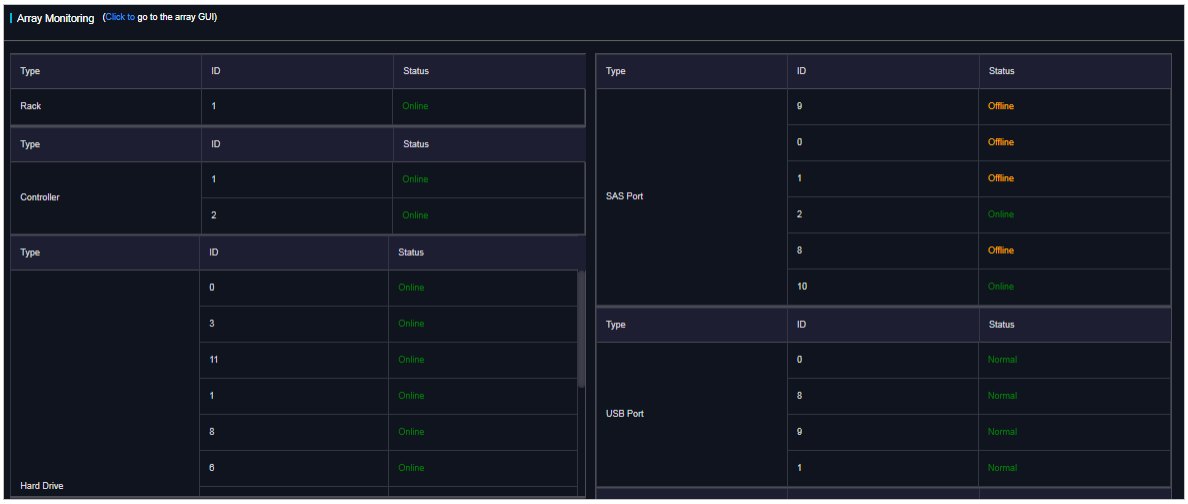
**The Array Monitoring module allows you to know the running status of each device.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose Storage Operation Center > miniOSS > Array Monitoring.**
3. **View the running status of each device.**

   **By default, you can view the status information of all devices.**

   **The device types are as follows: rack, controller, hard drive, rack battery, Power Supply Unit (PSU), fan, FC port, iSCSI port, SAS port, USB port, cluster node, cluster system, block storage, volume information, storage pool information, server, NFS service, CIFS service, FTP service, and file system.**




   **Values in different colors represent different statuses.**

   - **Green indicates the online or normal status.**
   - **Yellow indicates the offline status.**
   - **Red indicates the abnormal status.**

   **On top of the page, click Click to go to the array GUI.**

## 1.1.7.2.5 System management

**The System Management module allows you to modify the bucket watermark threshold and user watermark threshold.**

**Procedure**

1. *Log on to Apsara Stack Operations*.

2. In the left-side navigation pane, choose Storage Operation Center > miniOSS > System Management.
3. On this page, you can:
   - Modify the bucket watermark threshold
     a. In the Bucket Watermark Threshold section, click Modify.
     b. Enter a positive number equal to or less than 100 as the warning value, error value, and fatal error value. Make sure that the warning value is less than the error value and the error value is less than the fatal error value.
     c. Then, click Save.
   - Modify the user watermark threshold
     a. In the User Watermark Threshold section, click Modify.
     b. Enter a positive number equal to or less than 100 as the warning value, error value, and fatal error value. Make sure that the warning value is less than the error value and the error value is less than the fatal error value.
     c. Then, click Save.

## 1.1.8 Task Management

The system allows you to run operations scripts on the cloud platform, which reduces your actions by using command lines, lowers misoperations, and improves the security and stability of the cloud platform.

### 1.1.8.1 Overview

The Task Management module has the following functions:

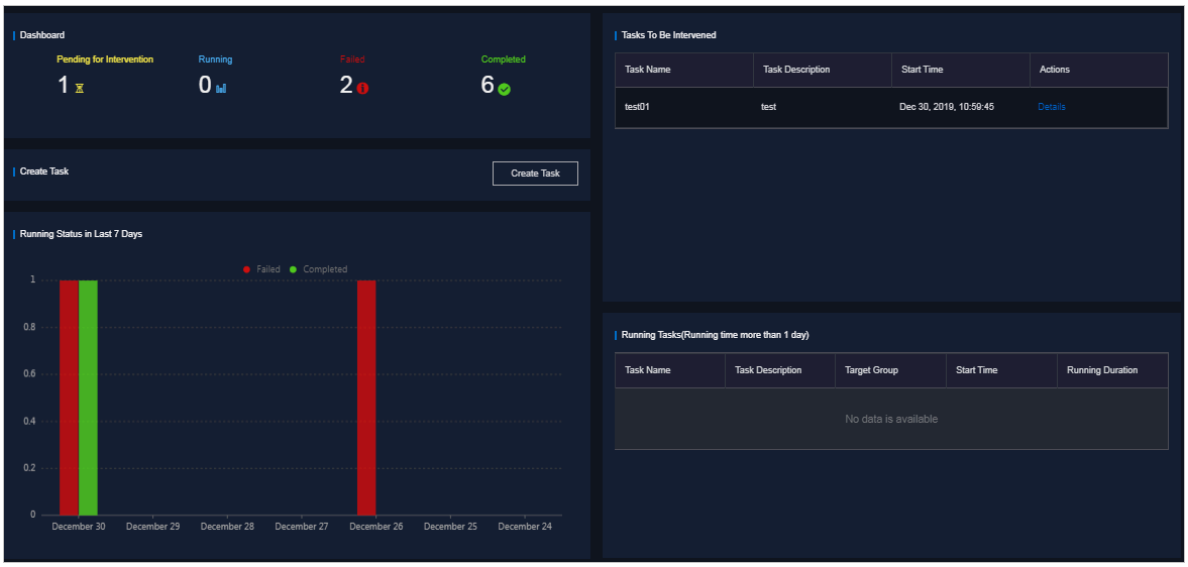
- Supports viewing task overview and creating tasks quickly.
- Supports the following four methods to run tasks: manual execution, scheduled execution, regular execution, and advanced mode.
- Supports the breakpoint function, which allows a task to stop between its two scripts and wait for manual intervention.
- Supports searching for tasks by name, status, and created time.
- Supports running the task on machines in batches.
- Supports uploading the .tar package as the script.

## 1.1.8.2 View the task overview

**The Task Overview page displays the overall running conditions of tasks in the system. You can also create a task on this page.**

### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Overview.




3. On the Task Overview page, you can:
   - In the Dashboard section, view the number of tasks in the Pending for Intervention, Running, Failed, or Completed status in the system.

     Click the status or number to view the task list of the corresponding status.
   - In the Create Task section, click Create Task to create an operations task.

     For more information about how to create a task, see *Create a task*.
   - If a task has a breakpoint and runs to the breakpoint, the task stops and waits for manual confirmation. You can view and process tasks to be intervened in the Tasks To Be Intervened section.
   - In the Running Status in Last 7 Days section, view the running trend of tasks and whether tasks are successful in the last seven days.
   - In the Running Tasks section, view tasks running in the last 24 hours.

## 1.1.8.3 Create a task

**You can create daily changes as tasks to run on the cloud platform.**

### Procedure

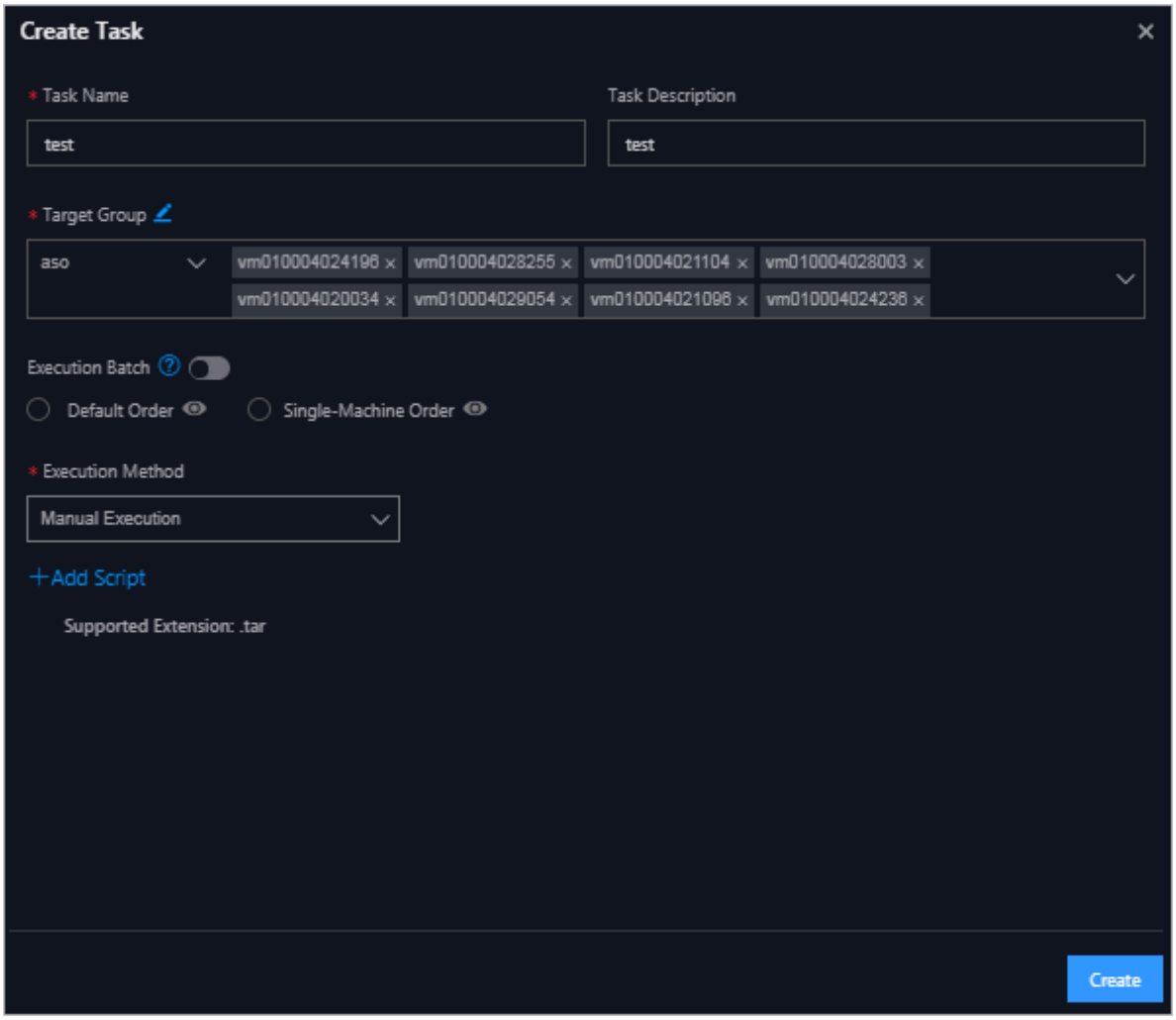
1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Management.
3. Click Create.
4. In the displayed dialog box, configure the task information.

| Configuration | Description |
| --- | --- |
| Task Name | The name of the operations task. |
| Task Description | The description of the operations task. |
| Target Group | The task target. You can configure the target group in the following ways:<br>· Select from the drop-down list by product > cluster > service > server role > virtual machine (VM) or physical machine.<br>· Select a product. Enter the VM or physical machine in the field and then press Enter. You can enter multiple VMs or physical machines in sequence.<br>· Click the  button next to Target Group. In the displayed dialog box, enter the target group, with one VM or physical machine in one line, and then click OK. |

| Configuration | Description |
| --- | --- |
| Execution Batch | Optional. This option appears after you enter the target group.<br>You can select the following options as the Execution Batch.<br>· Default Order<br>If the number of machines is equal to or less than 10, the machines are allocated to different batches by default, with one machine in batch 1, one machine in batch 2, two machines in batch 3, three machines in batch 4, and the other machines in batch 5. You can adjust the batch for machines as needed.<br>If the number of machines is more than 10, the machines are allocated to different batches by default, with one machine in batch 1, three machines in batch 2, five machines in batch 3, N/3-1 (an integer) machines in batch 4, N/3-1 ( an integer) machines in batch 5, until all of the machines are allocated. Where, N is the total number of servers in the cluster. You can adjust the batch for machines as needed.<br>· Single-Machine Order: By default, each batch has one machine. You can adjust the batch for machines as needed.<br>If the execution batch is not selected, the Execution Batch switch is turned off by default, and Target Group is displayed in the Target Group column in the task list of the Task Management > Task Management page. If you select and save the execution batch, the Execution Batch switch is turned on automatically, and Batch Execution Policy is displayed in the Target Group column. |

| Configuration | Description |
| --- | --- |
| Execution Method | If you turn on the Execution Batch switch, the Execution Method can only be Manual Execution and cannot be selected.<br>If the Execution Batch switch is not turned on, you can select one of the following execution methods:<br>· Manual Execution: You must manually start the task. With this option selected, you must click Start in the Actions column to run the task after the task is created.<br>· Scheduled Execution: Select the execution time. The task automatically runs when the time is reached.<br>· Regular Execution: Select the interval and execution times to run the task. The task runs again if the execution condition is met.<br>· Advanced: Configure the command to run the task periodically. |

| Configuration | Description |
| --- | --- |
| Add Script | Click Add Script. Select one or more .tar packages to upload the script file. After the upload, you can delete and reupload the script.<br>After uploading the script, if Manual Execution is selected as the Execution Method, you must select whether to turn on the Intervention Required switch. If the switch is turned on, the task stops and waits for manual intervention after the script runs. |




5. Then, click Create.

## Result

The created task is displayed in the task list.

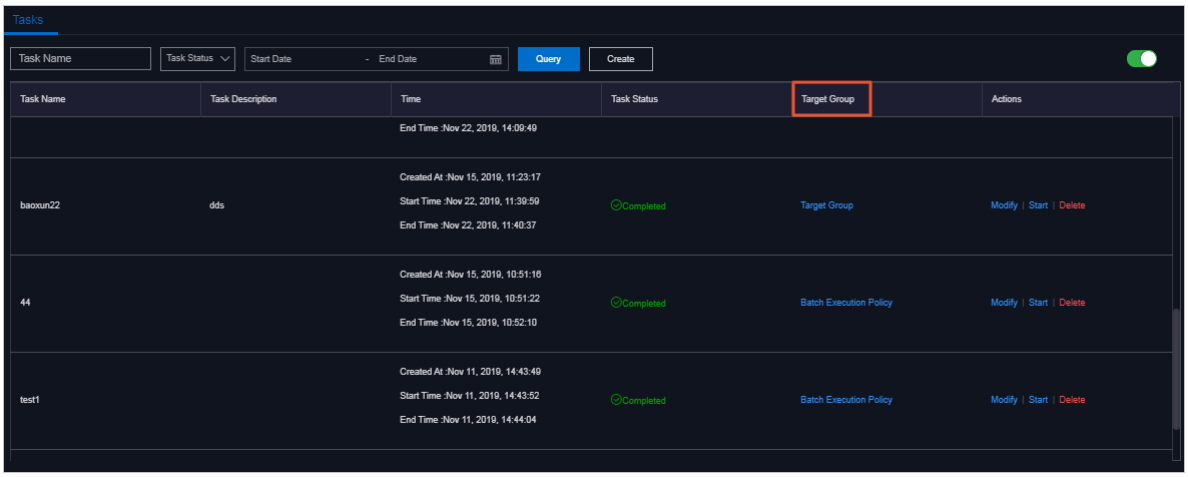
# 1.1.8.4 View the execution status of a task

**After a task runs, you can view the execution status of the task.**

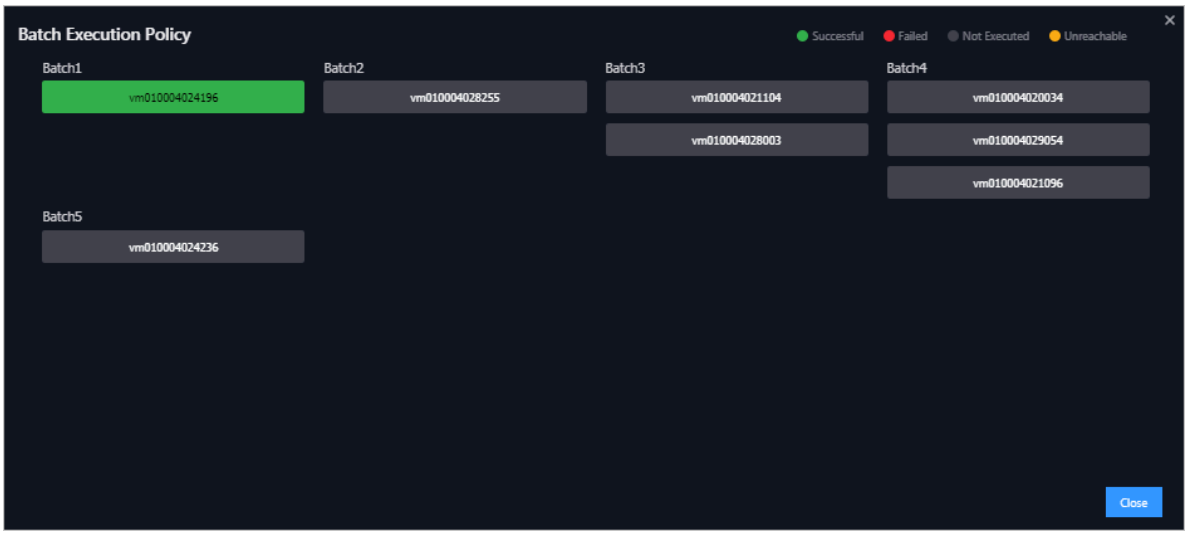
## Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Management.
3. Optional: Enter the task name, select the task status, and configure the start time and end time of the task. Then, click Query to search for the task.
4. Find the task that you are about to view and then click Target Group or Batch Execution Policy in the Target Group column.

> **Note:**
> If the Execution Batch is not selected when you create a task, Target Group is displayed in the Target Group column. If you select the Execution Batch when creating a task, Batch Execution Policy is displayed in the Target Group column.



5. In the displayed dialog box, view the task execution status based on the machine color. Click a machine to view the execution result of the task.




## 1.1.8.5 Start a task

If you select Manual Execution when creating a task, you must manually start the task after the task is created.

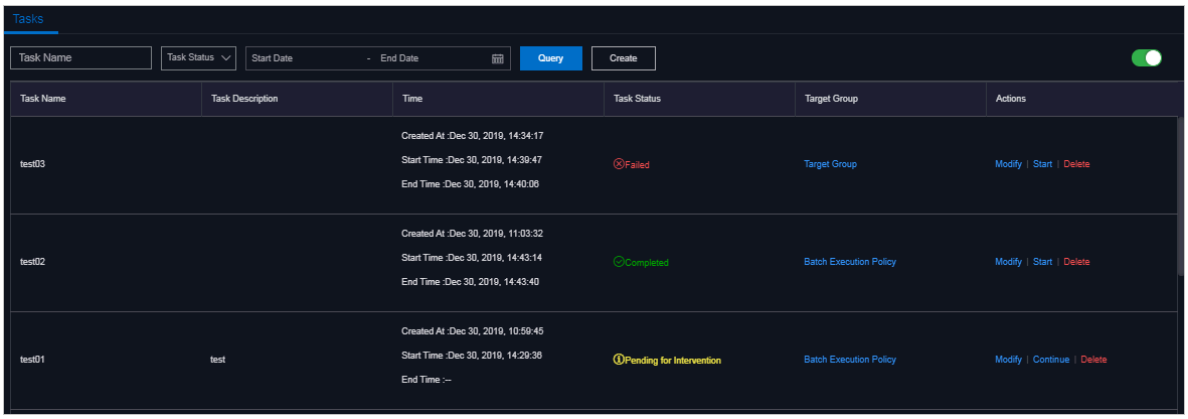
### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Management.
3. Optional: Enter the task name, select the task status, and configure the start time and end time of the task. Then, click Query to search for the task.
4. Find the task that you are about to start and then click Start in the Actions column.
5. In the displayed dialog box, select the batches to start and then click Start.

   For a new task, the system indicates that the task is started after you click Start for the first time. The virtual machines (VMs) or physical machines in batch 1 start to run the task. Click Start again and you can select VMs or physical machines in one or more batches to run the task.

   If the task has the Intervention Required switch turned on, you must intervene the task after clicking Start. The Task Status changes to Pending for Intervention

and you can only continue to run the task by clicking Continue in the Actions column.




## 1.1.8.6 Delete a task

**For better management, you can delete a task that is no longer in use.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Management.
3. Optional: Enter the task name, select the task status, and configure the start time and end time of the task. Then, click Query to search for the task.
4. Find the task to be deleted and then click Delete in the Actions column.
5. Click OK in the displayed dialog box.

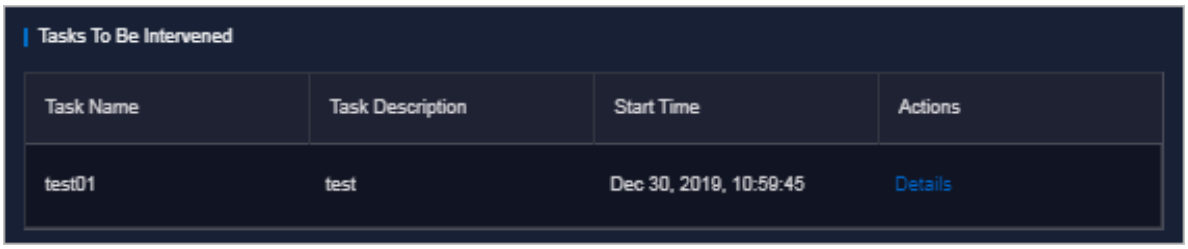
## 1.1.8.7 Process tasks to be intervened

**If a task has a breakpoint and runs to the breakpoint, the task stops and waits for manual confirmation. The task can only continue to run after the manual confirmation.**

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Task Overview.

3. In the Tasks To Be Intervened section, find the task to be intervened and then click Details in the Actions column.




4. On the Task Details tab, check the information and then click Continue to continue to run the task.

## 1.1.8.8 Configure the XDB backup task

**The XDB Backup module allows you to configure the XDB data backup without using command lines. You can configure and modify the backup task on the XDB Backup page to regularly back up platform data and back up data in real time.**

**Procedure**

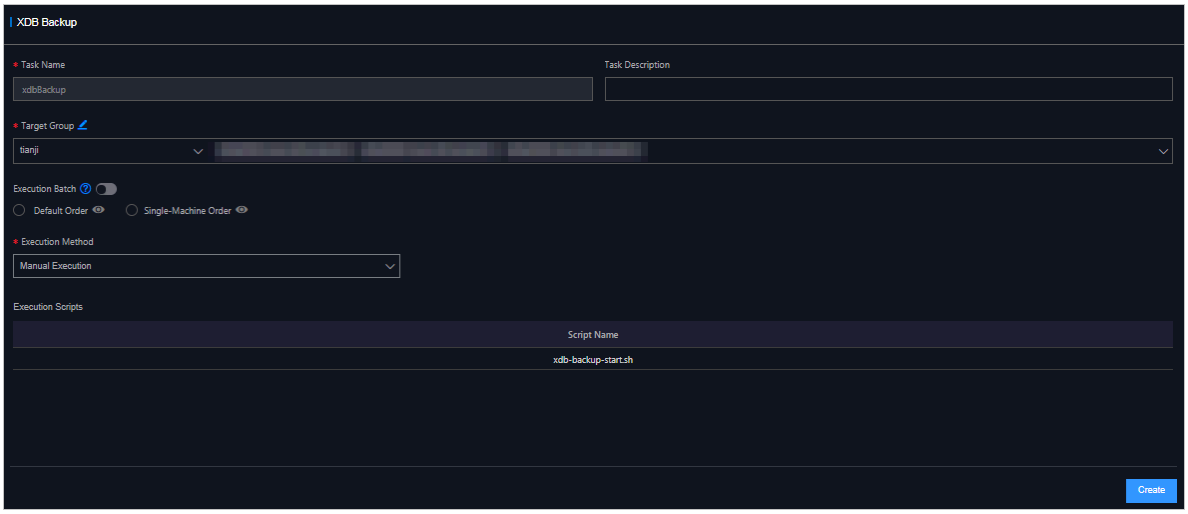
1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose Task Management > Common Tasks > XDB Backup.
3. On the XDB Backup page, configure the XDB backup task information.

| Configuration | Description |
| --- | --- |
| Task Name | The name of the XDB backup task. By default, the name is xdbBackup and cannot be modified. |
| Task Description | The description of the XDB backup task. |

| Configuration | Description |
| --- | --- |
| Target Group | Required. The target of the XDB backup task. You can configure the target group in the following ways:<br>· Select from the drop-down list by product > cluster > service > server role > virtual machine (VM) or physical machine.<br>· Select a product. Enter the VM or physical machine in the field and then press Enter. You can enter multiple VMs or physical machines in sequence.<br>· Click the  button next to Target Group. In the displayed dialog box, enter the target group, with one VM or physical machine in one line, and then click OK. |

| Configuration | Description |
| --- | --- |
| Execution Batch | Optional. This option appears after you enter the target group.<br>You can select the following options as the Execution Batch.<br>· Default Order<br>If the number of machines is equal to or less than 10, the machines are allocated to different batches by default, with one machine in batch 1, one machine in batch 2, two machines in batch 3, three machines in batch 4, and the other machines in batch 5. You can adjust the batch for machines as needed.<br>If the number of machines is more than 10, the machines are allocated to different batches by default, with one machine in batch 1, three machines in batch 2, five machines in batch 3, N/3-1 (an integer) machines in batch 4, N/3-1 ( an integer) machines in batch 5, until all of the machines are allocated. Where, N is the total number of servers in the cluster. You can adjust the batch for machines as needed.<br>· Single-Machine Order: By default, each batch has one machine. You can adjust the batch for machines as needed.<br>If the execution batch is not selected, the Execution Batch switch is turned off by default, and Target Group is displayed in the Target Group column in the task list of the Task Management > Task Management page. If you select and save the execution batch, the Execution Batch switch is turned on automatically, and Batch Execution Policy is displayed in the Target Group column. |

| Configuration | Description |
| --- | --- |
| Execution Method | If you turn on the Execution Batch switch, the Execution Method can only be Manual Execution and cannot be selected.<br>If the Execution Batch switch is not turned on, you can select one of the following execution methods:<br>· Manual Execution: You must manually start the task. With this option selected, you must click Start in the Actions column to run the task after the task is created.<br>· Scheduled Execution: Select the execution time. The task automatically runs when the time is reached.<br>· Regular Execution: Select the interval and execution times to run the task. The task runs again if the execution condition is met.<br>· Advanced: Enter the crontab expression to configure the command, which allows the task to run periodically.<br>For example, `0 20 20 * * ?` indicates that the task runs at 20:20 every day. |
| Execution Scripts | By default, the system automatically loads the XDB backup script. |



4. Then, click Create.

   You can view the created XDB backup task in the task list of the Task Management > Task Management page. The system automatically runs the XDB backup task when the task execution condition is met. If Manual Execution is selected as the Execution Method of the XDB backup task, start the backup task based on the procedures in *Start a task*.

    **Note:**
   After the XDB backup task is created, you can modify the information of the backup task by clicking Modify at the bottom of the XDB Backup page and configuring the XDB backup task again.

   After the XDB backup task runs, operations engineers can view the backup file of each instance under the `/alidata/xdb-backup/instance name` directory on the backup server. The backup file name is in the format of instance name-timestamp (specific to day).tar. At the same time, the temporary backup information under the `/alidata/xdb-backup-tmp` directory of the temporary backup folder is deleted automatically.

## 1.1.9 System Management

System Management centrally manages the departments, roles, and users involved in Apsara Stack Operations (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 such as department management, role management, logon policy management, and user management.

### 1.1.9.1 Department management

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

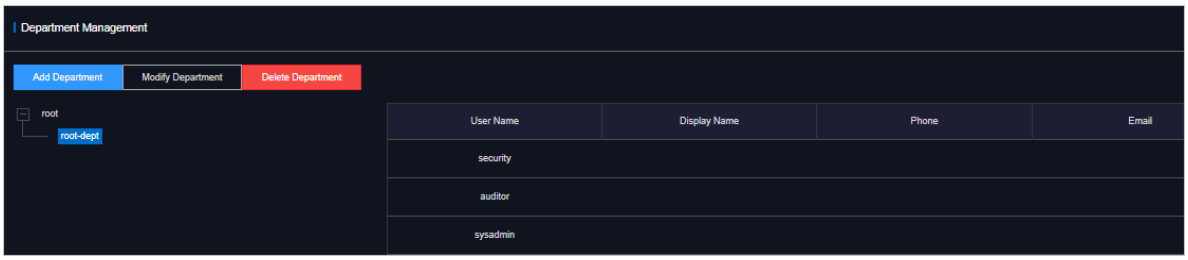
**Context**

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

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

**Procedure**

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Departments.




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

3. On this page, you can:
   - Add a department

     Click Add Department in the upper-left corner. In the displayed Add Department dialog box, enter the Department Name and then click OK. Then, you can view the created department under your selected catalog.
   - Modify a department

     Select the department to be modified in the catalog tree and click Modify Department at the top of the page. In the displayed Modify Department dialog box, enter the Department Name and click OK.
   - Delete a department

     Select the department to be deleted in the catalog tree and click Delete Department at the top of the page. Click OK in the displayed dialog box.

## 1.1.9.2 Role management

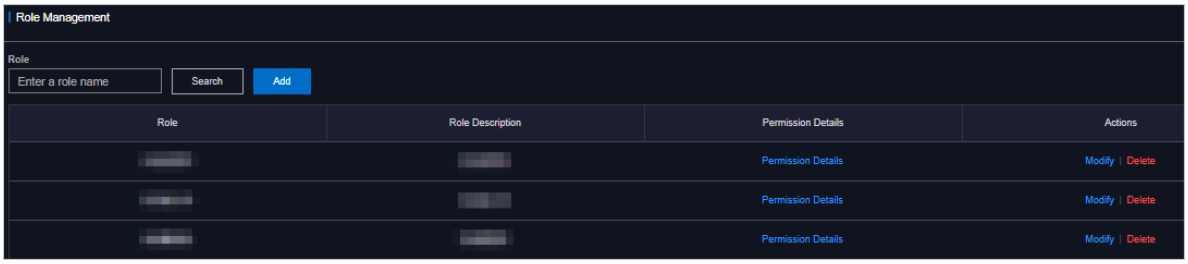
You can add custom roles in Apsara Stack Operations (ASO) to better allocate permissions to users.

**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 Operation Access Manager (OAM) system and cannot be modified or deleted by users. The user-created roles can be modified and deleted.

## Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Roles.




3. On the Role Management page, you can:
   - Search for roles

     **Note:**
     To search for roles in ASO, you must have the ASO security officer role or system administrator role.

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

     **Note:**
     To add a role in ASO, you must have the ASO security officer role.

     Click Add at the top of the page. In the displayed Add dialog box, enter the Role Name and Role Description, select the Base Role, and then click OK.
   - Modify a role

     **Note:**

**To modify a role in ASO, you must have the ASO security officer role.**

**Find the role to be modified, and then click Modify in the Actions column. In the displayed Modify Role dialog box, modify the information and then click OK.**

- **Delete a role**

  **Find the role to be deleted, and then click Delete in the Actions column. Click OK in the displayed dialog box.**

## 1.1.9.3 Logon policy management

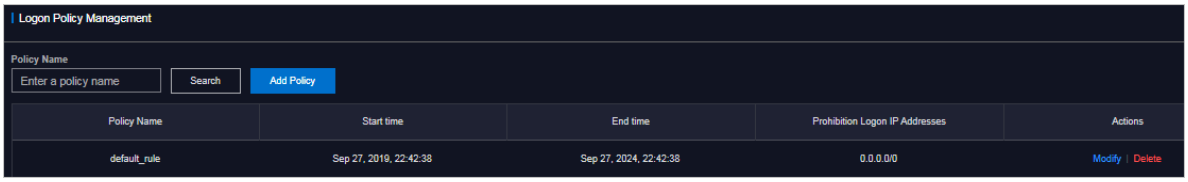
**The administrator can configure the logon polices to control the logon time and logon addresses of users.**

### Context

**The system has a default policy as the initial configuration. You can configure the logon policies as required to better control the read and write permissions of users and improve the system security.**

### Procedure

1. *Log on to Apsara Stack Operations*.
2. **In the left-side navigation pane, choose System Management > Logon Policies.**



3. On the Logon Policy Management page, you can:

   - Search for 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, configure the Policy Name, Start time, End time, and IP addresses prohibited for logon. Then, click OK.

   - Modify a policy

     Find the policy to be modified, and then click Modify in the Actions column. In the displayed Update Policy dialog box, modify the information and then click OK.

   - Delete a policy

     Find the policy to be deleted, and then click Delete in the Actions column. Click OK in the displayed dialog box.

### 1.1.9.4 User management

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

**Prerequisites**

Before you create a user, make sure that:

- A department is created. For more information, see *Department management*.
- A custom role is created, if required. For more information, see *Role management*.

**Context**

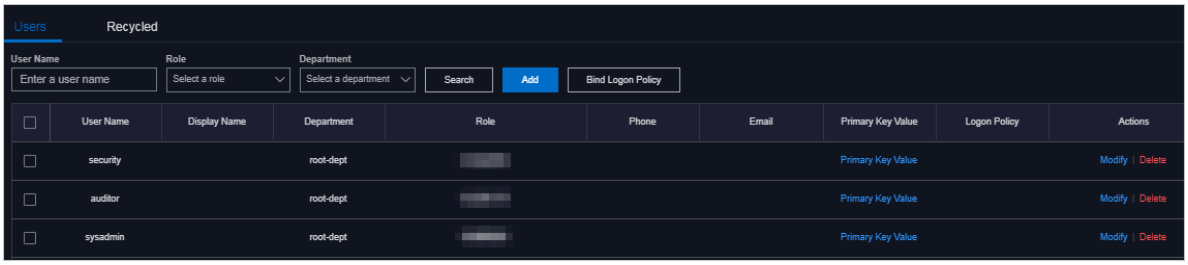
User management provides different permissions for different users. During the system initialization, the system creates three default users: asosysadmin , asosecurity, and asoauditor. The default users are respectively bound to the following default roles: system administrator, security officer, and auditor officer. The permissions of these three roles are as follows:

- The system administrator can view, modify, delete, and add the information in Alarm Monitoring, Network Operation Center (NOC), Storage Operation Center , and Task Management, and view the users, roles, departments, logon policies, and other modules in System Management.

- The security officer can view, modify, delete, and add the users, roles, departments, and logon policies in System Management.
- The security auditor can read and write Apsara Stack Operations (ASO) system logs.

## Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Users. Click the Users tab.




3. On the Users tab, you can:
   - Search for users

     **Note:**
     To search for users in ASO, you must have the security officer role or system administrator role.

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

     **Note:**
     To add a user in ASO, you must have the ASO security officer role.

     Click Add at the top of the page. In the displayed Add User dialog box, configure the information, such as User Name and Password, and then click OK to add the user.

     The added user is displayed in the user list. The Primary Key Value of the user is used to call the application API. In other words, the primary key value is

used for authentication if other applications need to call the applications in ASO.

- Modify a user

  **Note:**
  To modify a user in ASO, you must have the ASO security officer role.

  Find the user to be modified, and then click Modify in the Actions column. In the displayed Modify User dialog box, modify the information and then click OK.

- Delete a user

  Find the user to be deleted, and then click Delete in the Actions column. Click OK in the displayed dialog box.

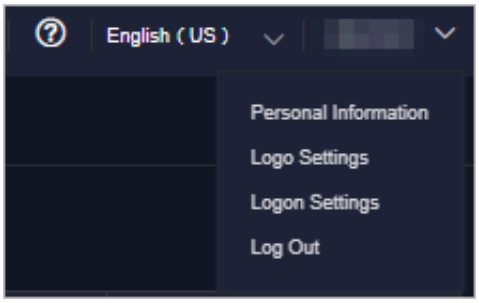
  **Note:**
  Deleted users are in the recycle bin. To restore a deleted user, click the Recycled tab. Find the user to be restored, click Cleared in the Actions column, and then click OK in the displayed dialog box.

- Bind a logon policy

  Select a user in the user list. Click Bind Logon Policy to bind a logon policy to the user.

- View personal information of the current user

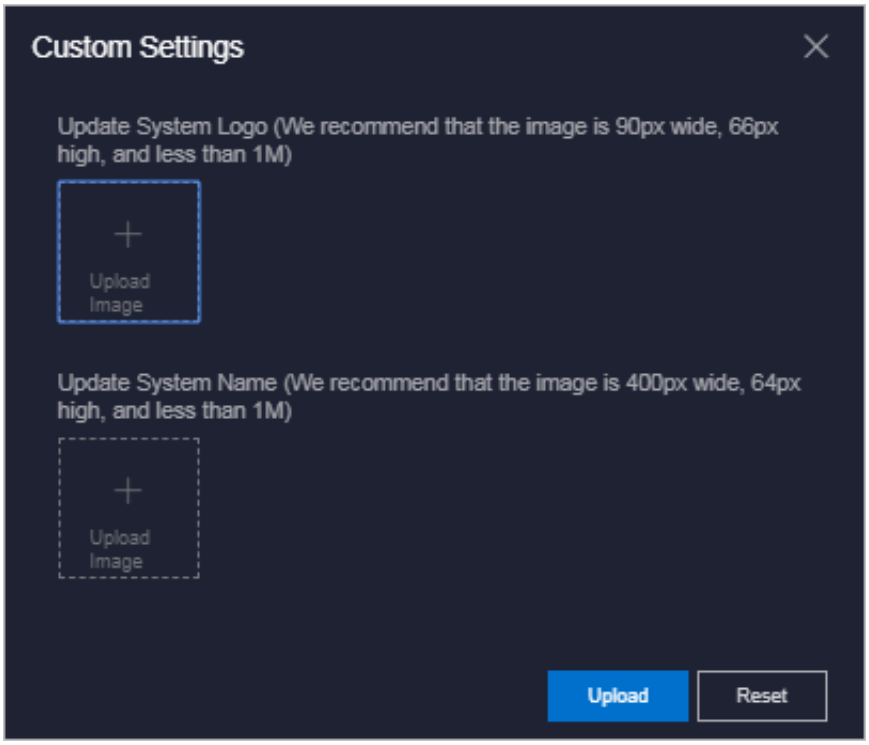
  In the upper-right corner, click the down-arrow button and then select Personal Information. The appeared Personal Information dialog box displays the personal information of the current user.




- Add a custom logo

  In the upper-right corner, click the down-arrow button next to the logon username and then select Logo Settings. In the displayed Custom Settings

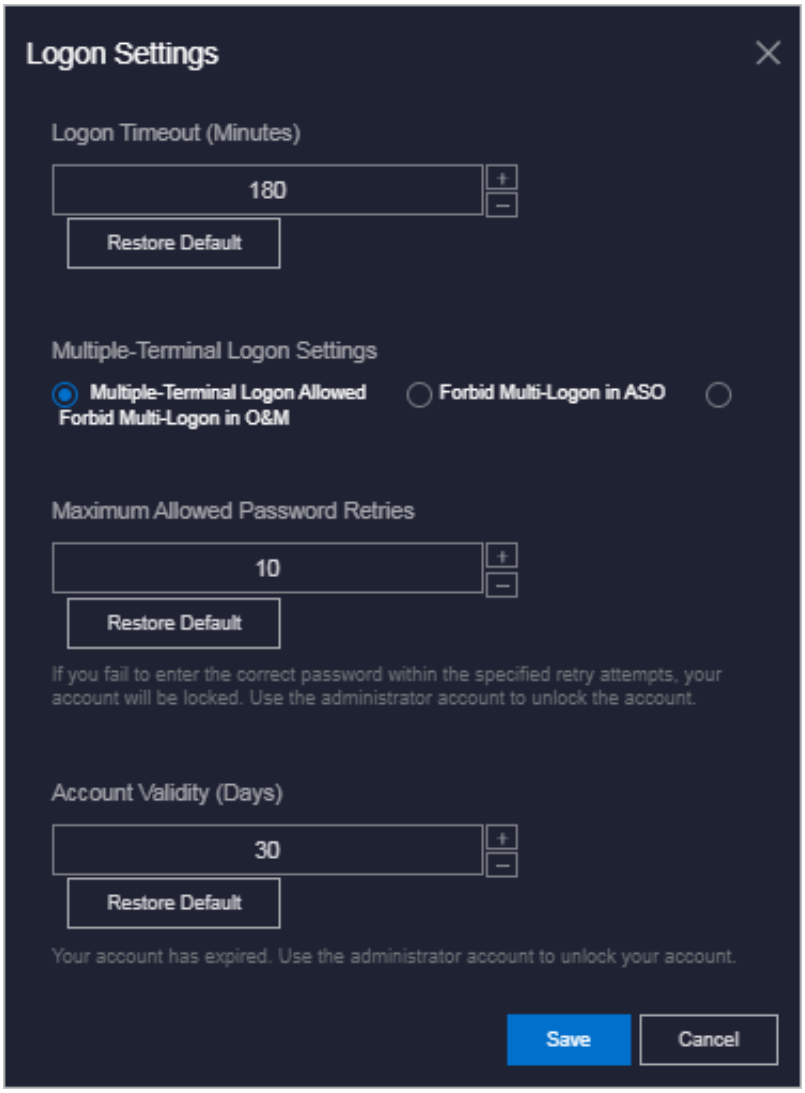
dialog box, click to upload the custom system logo image and system name image and then click Upload.




- Logon settings

  In the upper-right corner, click the down-arrow button next to the logon username and then select Logon Settings. In the displayed Logon Settings dialog box, configure the logon timeout, multiple-terminal logon settings,

maximum allowed password retries, account validity, and logon policy. Then, click Save.




## 1.1.9.5 Two factor authentication

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

**Context**

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

- **Google two-factor authentication**

  **This authentication method uses the password and mobile phone to provide double protection for accounts. You can obtain the logon key after configurin g users in ASO, and then enter the key in the Google authenticator app of your**

**mobile phone. The app dynamically generates a verification code based on the time and key for logon.**

- **USB key authentication**

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

  **Upon logon, if the account enables the USB key authentication, the ASO frontend calls the browser controls, reads the certificate in the 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**

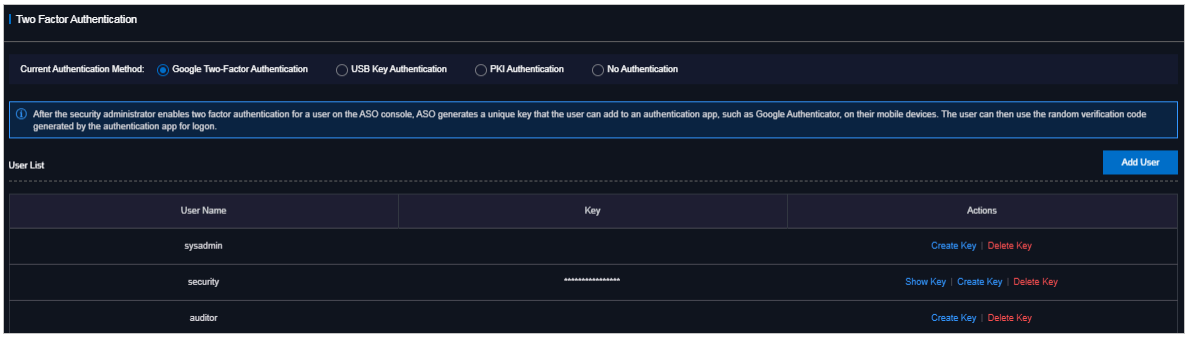
  **Enable the ASO HTTPS mutual authentication and change the certificate provided by the user if you select this authentication method. The third-party manufacturer makes the certificate and provides the service that the backend verifies the certificate. After the mutual HTTPS authentication is enabled, 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 name and ID card number of a user. Therefore, bind the name and ID card number with a user account when you configure the authentication method in ASO.**

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

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

## Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Two Factor Authentication.




3. On the Two Factor Authentication page, you can:
   - Google two-factor authentication
     a. Select Google Two-Factor Authentication as the Current Authentication Method.
     b. Click Add User in the upper-right corner. The added user is displayed in the user list.
     c. Find the user that you are about to enable the Google two-factor authentication, and then click Create Key in the Actions column. After the key is created, you can click Show Key in the Actions column to display the key in plain text.
     d. Enter the key in the Google authenticator app of your mobile phone. The app dynamically generates a verification code based on the time and key for logon. With the two-factor authentication enabled, you are required to enter the verification code on your app when logging on to the system.

     **Note:**
     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.

e. To disable the two-factor authentication, click Delete Key in the Actions column.

- USB key authentication

a. Select USB Key Authentication as the Current Authentication Method.

b. In the Authentication Server Configuration section, click Add Server. In the displayed dialog box, enter the IP Address and Port of the server, and then click OK. The added server is displayed in the server list. Click Test to test the connectivity of the authentication server.

c. In the User List section, click Add User. The added user is displayed in the user list.

d. Find the user that you are about to enable the USB key authentication, and then click Bind Serial Number in the Actions column. In the displayed dialog box, enter the serial number to bind the user account with this serial number.

Note:

When adding an authentication in ASO, ASO calls the browser controls to automatically enter the serial number. If the serial number fails to be entered, you must enter it manually. The serial number of USB key authentication is written in the USB key hardware. Therefore, you must insert the USB key, install the drive and browser controls, and then read the serial number by calling the browser controls.

e. Then, click Enable Authentication in the Actions column.

- PKI authentication

a. Select PKI Authentication as the Current Authentication Method.

b. In the Authentication Server Configuration section, click Add Server. In the displayed dialog box, enter the IP Address and Port of the server, and then

click OK. The added server is displayed in the server list. Click Test to test the connectivity of the authentication server.

c. In the User List section, click Add User. Enter the Username, Full Name, and ID Card Number, and then click OK. The added user is displayed in the user list.

d. Find the user that you are about to enable the PKI authentication, and then click Bind in the Actions column. Enter the full name and ID card number of the user to bind the user account with the name and ID card number.

e. Then, click Enable Authentication in the Actions column.

- 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.

### 1.1.9.6 Application whitelist

The system administrator can add, modify, or delete an application whitelist.

**Context**

The application whitelist permissions consist of read-only and read/write. The configured value is the logon user permission. With the whitelist function enabled, the application can be accessed by all users who have successfully logged on.

The application whitelist is managed by the system administrator. You can access this page after logging on as a system 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 Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Application Whitelist.

3. On the Application Whitelist page, you can:

   - Add a whitelist

     In the upper-right corner, click Add to Whitelist. In the displayed Add to Whitelist dialog box, select the service and permission, and then click OK.
   - Modify the permission

     In the Permission drop-down list, modify the permission of the service to Read/Write or Read-only.
   - Delete a whitelist

     Find the whitelist to be deleted, and then click Delete in the Actions column. Click OK in the displayed dialog box.

### 1.1.9.7 Server password management

**The Server Password module allows you to configure and manage server passwords and search for history passwords in the Apsara Stack environment.**

**Context**

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

**The Server Password module has the following functions:**

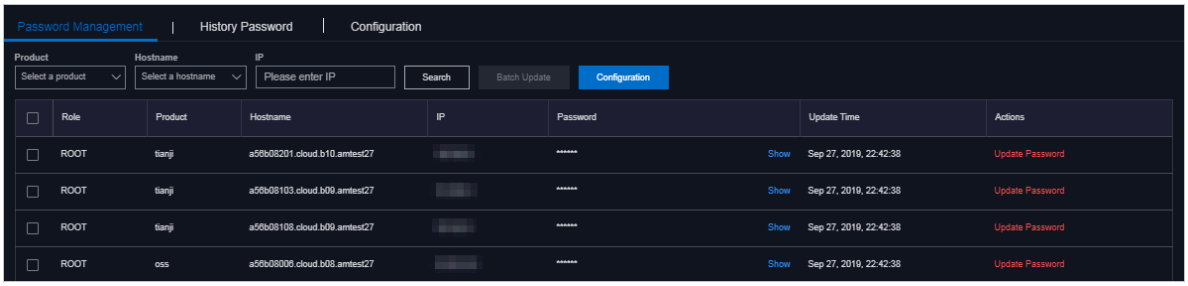
- **Supports viewing the information of all servers in the Apsara Stack environment.**
- **Supports searching for server passwords by product, hostname, or IP address.**
- **Supports configuring the password expiration period and password length.**
- **Supports manually updating the passwords of one or more servers at a time.**
- **Supports viewing the history of server password updates.**

**Procedure**

1. *Log on to Apsara Stack Operations*.

2. In the left-side navigation pane, choose System Management > Server Password.

   The Password Management tab displays the passwords of all the servers in the Apsara Stack environment.



3. On this tab, you can:

   - Search for servers

     On the Password Management tab, configure the product, hostname, or IP address, and then click Search to search for specific servers.

   - Show passwords

     a. On the Password Management tab, find a server.
     b. Click Show in the Password column, and then the system displays the host password in plain text, which turns into cipher text after 10 seconds. Alternatively, directly click Hide to display the cipher text.

   - Update passwords

     a. On the Password Management tab, find a server.
     b. Click Update Password in the Actions column.
     c. In the displayed Update Password dialog box, enter the Password and Confirm Password, and then click OK.

        Then, the server password is updated.

   - Update multiple passwords at a time

     a. On the Password Management tab, select multiple servers.
     b. Click Batch Update.
     c. Enter the Password and Confirm Password, and then click OK.

        Then, the passwords of the selected servers are updated.

   - Configure the password expiration period

     a. On the Password Management tab, select one or more servers.
     b. Click Configuration.
     c. In the displayed Configuration Item dialog box, enter the Password Expiration Period and select the Unit, and then click OK.

        Server passwords are updated immediately after the configuration and will be updated again after an expiration period.

   - View the history of server password updates

     Click the History Password tab. Configure the history product, history hostname, or history IP address and then click Search to view the history of server password updates in the search results.

- **Show history passwords of servers**

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

  b. **Click Show in the Password column, and then the system displays the host password in plain text, which turns into cipher text after 10 seconds. Alternatively, directly click Hide to display the cipher text.**

- **View and modify the password configuration policy**

  **Click the Configuration tab. View the metadata, including the initial password, password length, and retry times, of server password management. Where,**

  - **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 update the password of a server in the Apsara Stack environment.**
  - **The password length is the length of passwords automatically updated by the system.**
  - **Retry times is the number of retries when the password fails to be updated.**

  **To modify the configurations, click Modify Configurations in the Actions column. In the displayed dialog box, enter the Initial Password, Password Length, and Retry Times, and then click OK.**

### 1.1.9.8 Operation logs

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

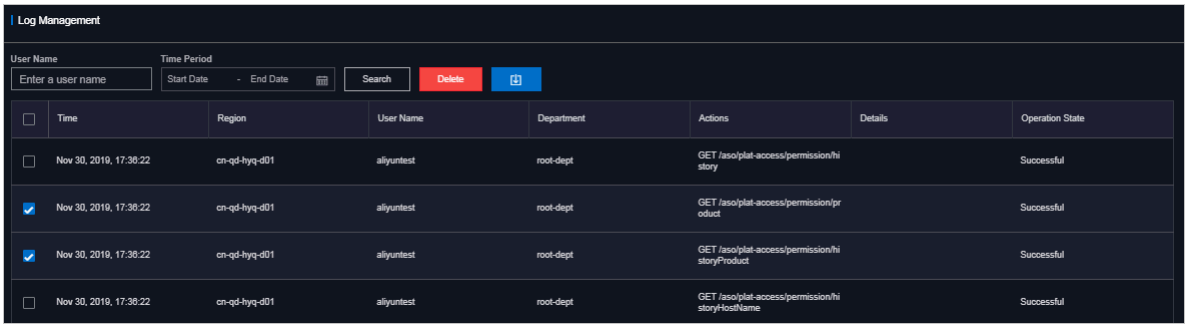
**Context**

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

**Procedure**

1. *Log on to Apsara Stack Operations*.

2. In the left-side navigation pane, choose System Management > Operation Logs.




3. On the Log Management page, you can:

   - Search for logs

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

   - Delete logs

     Select one or more logs to be deleted. Click Delete and then click OK in the displayed dialog box.

   - Export logs

     Click  to export the logs of the current page.

## 1.1.9.9 View the authorization information

The Authorization page allows customers, field engineers, or operations engineers to quickly view the service with an authorization problem and then troubleshoot the problem.

### Prerequisites

Make sure that the current logon user has the permissions of an administrator. Only a user with the administrator permissions can view the trial authorization information or enter the authorization code to view the formal authorization information on the Authorization Details page.

If you do not have the permissions of an administrator, a message indicating that you do not have sufficient permissions is displayed when you access this page.

### Procedure

1. *Log on to Apsara Stack Operations*.
2. In the left-side navigation pane, choose System Management > Authorization.

3. View the authorization information on the Authorization Details page.

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

You can view the authorization information, including authorization version , customer information, authorization type, Elastic Compute Service (ECS) instance ID, the start date and end date of software license update and tech support, and service authorizations, of all services in the current Apsara Stack environment.

See the detailed authorization information and the corresponding description in the following table.

| Authorization information | Description |
| --- | --- |
| Authorization Version | You can use the BP number in the version to associate with a project or contract.<br>Where,<br>· TRIAL in the version indicates that the authorization is a trial one. The trial authorization is valid within 90 days from the date of deployment.<br>· FORMAL in the version indicates that the authorization is a formal one. The authorization information of the service comes from the signed contract. |
| Authorization Type | Indicates the current authorization type and authorization status. |
| Customer information | Includes the customer name, customer ID, and customer user ID. |
| ECS Instance ID | The ECS instance ID in the Deployment Planner of the field environment. |
| Cloud Platform Version | The Apsara Stack version of the current cloud platform. |

| Authorization information | Description |
| --- | --- |
| Authorization Created At | The start time of the authorization. |
| Authorization information of a service | Includes the service name, service content, authorization mode, service authorizations, software license update and tech support start date, software license update and tech support end date, and real-time authorization status.<br>If the following information appears in the Authorization Status column of a service:<br>· RENEW Service Expired<br>Indicates that the customer must renew the subscription as soon as possible. Otherwise, the field operations services, including ticket processing, are to be terminated.<br>· Specifications Above Quota<br>Indicates that the specifications deployed in the field for a service have exceeded the quota signed in the contract, and the customer must scale up the service as soon as possible. |

# 1.2 Operation Access Manager (OAM)

## 1.2.1 OAM introduction

Overview

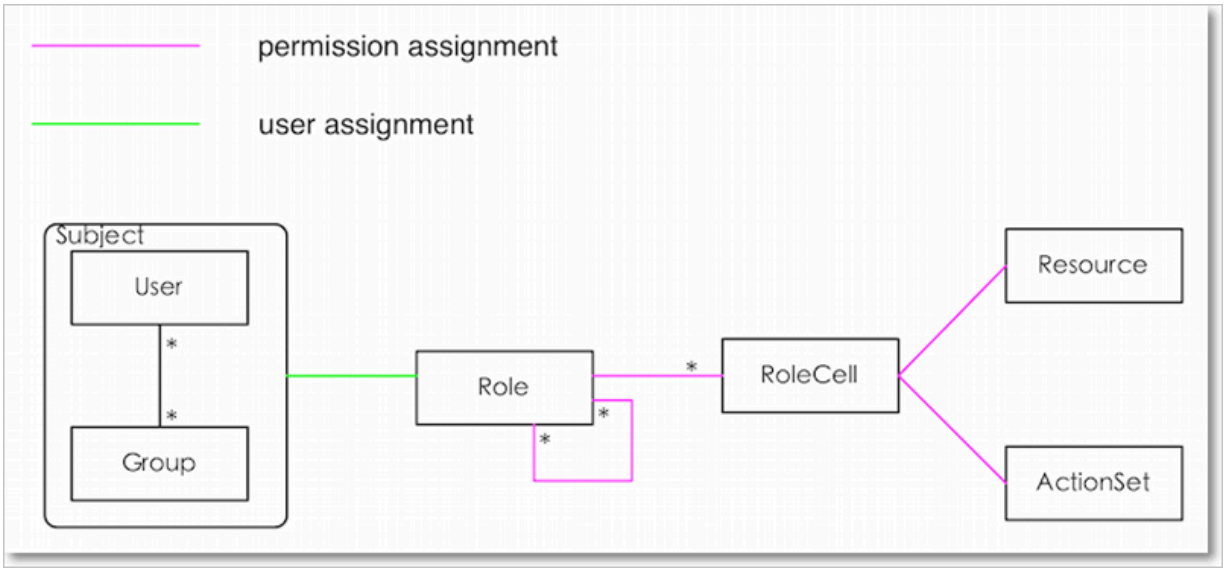
**Operation Access Manager (OAM) is a centralized permission management platform of Apsara Stack Operations (ASO). OAM uses a simplified role-based access control (RBAC) model. Administrators can use OAM to assign roles to operations personnel, granting them corresponding operation permissions to operations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

OAM permission model

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

**See the *OAM permission model* as follows.**

Figure 1-2: Permission model




## 1.2.2 Instructions

**Before using Operation Access Manager (OAM), you must know the following basic concepts about permission management.**

subject

**Operators of the access control system. OAM has two types of subjects: users and groups.**

user

**Administrators and operators of operations systems.**

group

**A collection of users.**

role

**The core of the role-based access control (RBAC) system.**

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

RoleHierarchy

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

RoleCell

**The specific description of a permission. A RoleCell consists of resources, ActionSets, and available authorizations.**

resource

**The description of an authorized object. For more information about resources of operations platforms, see** *Permission lists of operations platforms*.

ActionSet

**The description of authorized actions. An ActionSet can contain multiple actions. For more information about actions of operations platforms, see** *Permission lists of operations platforms*.

available authorizations

**The maximum number of authorizations in the 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 Available Authorizations 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 Available Authorizations cannot be greater than 4. If Available Authorizations is set to 0 when administrator B grants the permission to operator D, operator D can only use the permission but cannot grant it to others.**

**Note:**

**Currently, OAM does not support the cascaded revocation for cascaded authorization. Therefore, administrator C and operator D still have the permission even if the permission is revoked for administrator B.**

## 1.2.3 Quick start

**This topic describes how to add and assign roles quickly.**

### 1.2.3.1 Log on to OAM

**This topic describes how to log on to Operation Access Manager (OAM).**

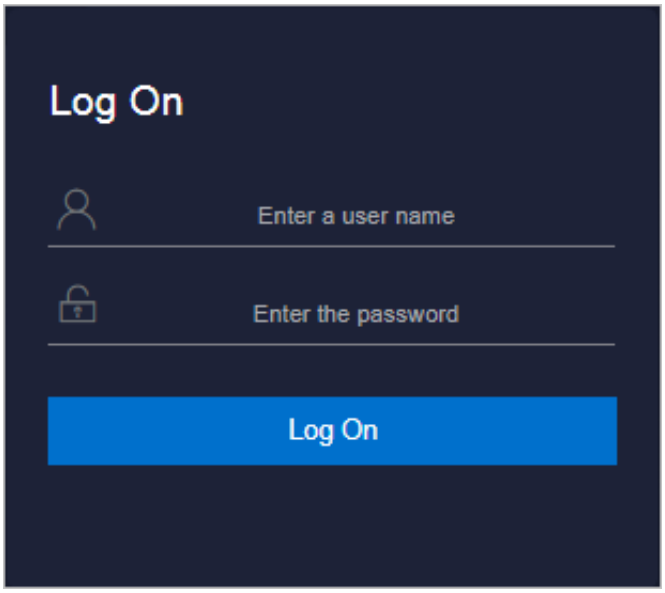
**Prerequisites**

- **ASO access address in the format of http://*region-id*.aso.*intranet-domain-id*.com.**
- **Google Chrome browser (recommended).**

**Procedure**

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

Figure 1-3: Log on to ASO




**Note:**
**You can select the language from the drop-down list in the upper-right corner to change the language of ASO.**

3. Enter the correct username and password.
   - The system has three default users:
     - Security officer: manages other users or roles.
     - Auditor officer: views audit logs.
     - System administrator: used for other functions except those of the security officer and auditor officer.
   - You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.
4. Click Log On to log on to ASO.
5. In the left-side navigation pane, select Products.
6. Click OAM under Apsara Stack O&M.

### 1.2.3.2 Create a group

Create a user group for centralized management.

**Procedure**

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

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

### 1.2.3.3 Add group members

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

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Group Management > Owned Groups.
3. Find the group and then click Manage in the Actions column.

4. Click Add Member in the Group Member section.
5. Select the search mode, enter the corresponding information, and then click Details. The user details are displayed.

   Three search modes are available:

   - RAM User Account: Search for the user in the format of *RAM username@primary account ID*.
   - Account Primary Key: Search for the user by using the unique ID of the user's cloud account.
   - Logon Account Name: Search for the user by using the logon name of the user's cloud account.
6. Click Add.
7. You can repeat the preceding steps to add more group members.

   To remove a member from the group, click Remove in the Actions column at the right of the member.

### 1.2.3.4 Add group roles

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

**Prerequisites**

- The role to be added is created. For more information about how to create a role, see *Create a role*.
- You are the owner of the group and the role.

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Group Management > Owned Groups.
3. Find the group and then click Manage in the Actions column.
4. Click Add Role in the Role List section.
5. Search for roles by Role Name. Select one or more roles and then configure the expiration time.
6. Then, click Confirm.

   To remove a role from the group, click Remove in the Actions column at the right of the role in the Role List section.

### 1.2.3.5 Create a role

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Role Management > Owned Roles.
3. In the upper-right corner of the Owned Roles page, click Create Role.
4. In the displayed dialog box, enter the Role Name and Description, and then select the Role Type.
5. Optional: Configure the role tags, which can be used to filter roles.
   a) Click Edit Tag.
   b) In the displayed Edit Tags dialog box, click Create.
   c) Enter the Key and the corresponding Value of the tag and then click Confirm.
   d) Repeat the preceding step to create more tags.

      The created tags are displayed in the dotted box.
   e) Click Confirm to create the tags.
6. Click Confirm to create the role.

### 1.2.3.6 Add inherited roles to a role

**Add inherited roles to a role to grant the permissions of the former 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 search for your owned roles, see *Search for roles*.**

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Role Management > Owned Roles.
3. Find the role and then click Manage in the Actions column.
4. Click the Inherited Role tab.
5. Click Add Role. Search for roles by Role Name and then select one or more roles.
6. Click Confirm.

### 1.2.3.7 Add resources to a role

**You must add resources to a created role.**

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Role Management > Owned Roles.
3. Find the role and then click Manage in the Actions column.
4. Click the Resource List tab.
5. Click Add Resource.
6. Complete the configurations. For more information, see *Table 1-1: Configurations*.

   Table 1-1: Configurations

| Configuration item | Description |
| --- | --- |
| BID | The deployment region ID. |
| Product | The cloud product to be added, for example, rds.<br>**Note:**<br>The cloud product name must be lowercase. For example, enter rds, instead of RDS. |
| Resource Path | For more information about resources of cloud products and operations platforms, see *Permission lists of operations platforms*. |
| Actions | An ActionSet, which can contain multiple actions.<br>For more information about actions of operations platforms, see *Permission lists of operations platforms*. |
| Available Authorizations | The maximum number of authorizations in the 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 | The description of the resource. |

7. Click Add.

## 1.2.3.8 Add authorized users to a role

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

**Prerequisites**

The corresponding users or user groups are created. Users are created in the Apsara Stack console. For more information about how to create user groups, see *Create a group*.

## Procedure

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Role Management > Owned Roles.
3. Find the role and then click Manage in the Actions column.
4. Click the Authorized Users tab.
5. Click Add User.
6. Select the search mode and enter the corresponding information.

   Four search modes are available:

   - RAM User Account: search in the format of `RAM username@primary account ID`.
   - Account Primary Key: search by using the unique ID of the user's cloud account.
   - Logon Account Name: search by using the logon name of the user's cloud account.
   - Group Name: search by group name.

   > **Note:**
   > You can search for a single user or user group. For more information about how to create a user group, see *Create a group*.

7. Configure the expiration time.

   After the expiration time is reached, the user does not have the permissions of the role. To authorize the user again, the role creator must click Renew at the right of the authorized user on the Authorized Users tab, and then configure the new expiration time.

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

   To cancel the authorization, click Remove at the right of the authorized user on the Authorized Users tab.

## 1.2.4 Manage groups

**Group Management allows you to view, modify, or delete groups.**

### 1.2.4.1 Modify the group information

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

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Group Management > Owned Groups.**
3. **Find the group and then click Manage in the Actions column.**
4. **Click Modify in the upper-right corner.**
5. **In the displayed Modify Group dialog box, modify the Group Name and Description.**
6. **Click Confirm.**

### 1.2.4.2 View group role details

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

**Prerequisites**

**A role is added to the group.**

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Group Management > Owned Groups.**
3. **Find the group and then click Manage in the Actions column.**
4. **In the Role List section, click Details at the right of a role.**

5. On the Role Information page, you can:
   - Click the Inherited Role tab to view the information about the inherited roles.

     To view the detailed information of an inherited role, click Details in the Actions column at the right of the inherited role.
   - Click the Resource List tab to view the resource information of the role.

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

### 1.2.4.3 Delete a group

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

**Prerequisites**

The group to be deleted does not contain members.

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Group Management > Owned Groups.
3. Find the group to be deleted and then click Delete in the Actions column.

### 1.2.4.4 View authorized groups

You can view the groups to which you are added on the Authorized Groups page.

**Context**

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

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Group Management > Authorized Groups.
3. On the Authorized Groups page, view the name, owner, description, and modified time of the group to which you belong.

## 1.2.5 Manage roles

**Role Management allows you to view, modify, transfer, or delete roles.**

### 1.2.5.1 Search for roles

**You can view your owned roles on the Owned Roles page.**

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Role Management > Owned Roles.**
3. **Optional: Enter the role name.**
4. **Click Search to search for roles that meet the search condition.**

> **Note:**
> **If the role you want to search for has a tag, you can click Tag and select the tag key to search for the role based on the tag.**

### 1.2.5.2 Modify the role information

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

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Role Management > Owned Roles.**
3. **Find the role and then click Manage in the Actions column.**
4. **Click Modify in the upper-right corner.**
5. **In the displayed Modify Role dialog box, modify the Role Name, Description, Role Type, and Tag.**
6. **Then, click Confirm.**

### 1.2.5.3 View the role inheritance tree

**You can view the role inheritance tree to know the basic information and resource information of a role and its inherited roles.**

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Role Management > Owned Roles.**
3. **Find the role and then click Manage in the Actions column.**

4. Click the Inheritance Tree tab.

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

### 1.2.5.4 Transfer roles

You can transfer roles to other groups or users according to business requirements.

**Procedure**

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

   Four search modes are available:

   - RAM User Account: search in the format of *RAM username@primary account ID*.
   - Account Primary Key: search by using the unique ID of the user's cloud account.
   - Logon Account Name: search by using the logon name of the user's cloud account.
   - Group Name: search by group name.
6. Click Transfer to transfer the roles to the user or group.

### 1.2.5.5 Delete a role

You can delete a role that is no longer in use according to business requirements.

**Prerequisites**

The role to be deleted does not contain inherited roles, resources, or authorized users.

**Procedure**

1. *Log on to OAM*.
2. In the left-side navigation pane, choose Role Management > Owned Roles.
3. At the right of the role to be deleted and then click Delete.

### 1.2.5.6 View authorized roles

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

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, choose Role Management > Authorized Roles.**
3. **On the Authorized Roles page, you can view the name, owner, description, modified time, and expiration time of the role assigned to you.**

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

### 1.2.5.7 View all roles

**You can view all the roles in Operation Access Manager (OAM) on the All Roles page.**

**Procedure**

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

   **You can search for roles by Role Name on this page.**
4. **At the right of a role, click Details to view the inherited roles, resources, and inheritance tree information of the role.**

## 1.2.6 Search for resources

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

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, select Search Resource.**
3. **Enter the Resource and Action in the search boxes, and then click Search to search for roles that meet the conditions.**
4. **At the right of a role, click Details in the Actions column to view the inherited roles, resources, and inheritance tree information of the role.**

## 1.2.7 View the personal information

**You can view the personal information of the current user and test the permissions on the Personal Information page.**

**Procedure**

1. *Log on to OAM*.
2. **In the left-side navigation pane, select Personal Information.**
3. **In the Basic Information section, you can view the username, user type, created time, AccessKey ID, and AccessKey Secret of the current user.**

   **Note:**
   **Click Show or Hide to show or hide the AccessKey Secret.**
4. **In the Test Permission section, test if the current user has a certain permission.**
   a) **Enter the resource information in the Resource field.**

      **Note:**
      **Use the English input method when entering values in the Resource and Action fields.**
   b) **Enter the permissions in the Action field, such as create, read, and write. Separate multiple permissions with commas (,).**

## 1.2.8 Appendix

### 1.2.8.1 Default roles and their functions

**This topic describes the default roles in Operation Access Manager (OAM) and their functions.**

#### 1.2.8.1.1 Default role of OAM

**This topic describes the default role of Operation Access Manager (OAM) and the corresponding available authorizations.**

| Role name | Role description | Resource | Actions | Available authorizations |
|---|---|---|---|---|
| Super administrator | An administrator with root permissions | *:* | * | 10 |

# 1.2.8.1.2 Default roles of Apsara Infrastructure Management Framework

**This topic describes the default roles of Apsara Infrastructure Management Framework and the corresponding available authorizations.**

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

| Role name | Role description | Resource | Actions | Available authorizations |
| --- | --- | --- | --- | --- |
| Tianji_Service read-only | Has the read-only permission to Apsara Infrastructure Management Framework services, which allows you to view the configurations and templates of all services | *:tianji:services | ["read"] | 0 |
| Tianji_Service administrator | Has all the permissions to Apsara Infrastructure Management Framework services, which allows you to view and modify the configurations and templates of all services | *:tianji:services | ["*"] | 0 |
| Tianji_IDC administrator | Has all the permissions to Apsara Infrastructure Management Framework data centers, which allows you to view and modify the data center information | *:tianji:idcs | ["*"] | 0 |

| Role name | Role description | Resource | Actions | Available authorizations |
| --- | --- | --- | --- | --- |
| Tianji administrator | Has all the permissions to Apsara Infrastructure Management Framework, which allows you to perform operations on all Apsara Infrastructure Management Framework configurations | *:tianji | ["*"] | 0 |

### 1.2.8.1.3 Default role of Tianjimon

**This topic describes the default role of Tianjimon and the corresponding available authorizations.**

| Role name | Role description | Resource | Actions | Available authorizations |
| --- | --- | --- | --- | --- |
| Tianjimon operations | Has all Tianjimon permissions, which allows you to perform basic monitoring and operations | 26842: tianjimon:* | ["*"] | 0 |

## 1.2.8.2 Permission lists of operations platforms

**This topic describes the permissions of operations platforms.**

## 1.2.8.2.1 Permission list of Apsara Infrastructure Management Framework

**This topic describes the permissions of Apsara Infrastructure Management Framework.**

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:services:[sname]:tjmontemplates:[tmplname] | delete | DeleteServiceTjmonTmpl |
| *:tianji:services:[sname]:tjmontemplates:[tmplname] | write | PutServiceTjmonTmpl |
| *:tianji:services:[sname]:templates:[tmplname] | write | PutServiceConfTmpl |
| *:tianji:services:[sname]:templates:[tmplname] | delete | DeleteServiceConfTmpl |
| *:tianji:services:[sname]:serviceinstances:[siname]:tjmontemplate | read | GetServiceInstanceTjmonTmpl |
| *:tianji:services:[sname]:serviceinstances:[siname]:tssessions | terminal | CreateTsSessionByService |
| *:tianji:services:[sname]:serviceinstances:[siname]:template | write | SetServiceInstanceTmpl |
| *:tianji:services:[sname]:serviceinstances:[siname]:template | delete | DeleteServiceInstanceTmpl |
| *:tianji:services:[sname]:serviceinstances:[siname]:template | read | GetServiceInstanceTmpl |
| *:tianji:services:[sname]:serviceinstances:[siname]:tags:[tag] | delete | DeleteServiceInstanceProductTagInService |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:services:[sname]:serviceinstances:[siname]:tags:[tag] | write | AddServiceInstanceProductTagInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:resources | read | GetServerroleResourceInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | write | OperateSRMachineInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | read | GetMachineSRInfoInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | delete | DeleteSRMachineActionInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | read | GetMachinesSRInfoInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | delete | DeleteSRMachinesActionInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | write | OperateSRMachinesInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:resources | read | GetAppResourceInService |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:machines:[machine]:tianjilogs | read | TianjiLogsInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:serverroles | read | GetServiceInstanceServerrolesInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:schema | write | SetServiceInstanceSchema |
| *:tianji:services:[sname]:serviceinstances:[siname]:schema | delete | DeleteServiceInstanceSchema |
| *:tianji:services:[sname]:serviceinstances:[siname]:rollings:[version] | write | OperateRollingJobInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:rollings | read | ListRollingJobInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:resources | read | GetInstanceResourceInService |
| *:tianji:services:[sname]:serviceinstances:[siname]:machines:[machine] | read | GetMachineAllSRInfoInService |
| *:tianji:services:[sname]:serviceinstances:[siname] | write | DeployServiceInstanceInService |
| *:tianji:services:[sname]:serviceinstances:[siname] | read | GetServiceInstanceConf |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:name | read | GetMachineAppFileListInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:download | read | GetMachineAppFileDownloadInService |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:content | read | GetMachineAppFileContentInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:filelist | read | GetMachineFileListInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:dockerlogs | read | DockerLogsInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:debuglog | read | GetMachineDebugLogInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps | read | GetMachineAppListInService |
| *:tianji:services:[sname]:serverroles:[serverrole]:apps:[app]:dockerinspect | read | DockerInspect |
| *:tianji:services:[sname]:schemas:[schemaname] | write | PutServiceSchema |
| *:tianji:services:[sname]:schemas:[schemaname] | delete | DeleteServiceSchema |
| *:tianji:services:[sname]:resources | read | GetResourceInService |
| *:tianji:services:[sname] | delete | DeleteService |
| *:tianji:services:[sname] | write | CreateService |
| *:tianji:projects:[pname]:machinebuckets:[bname]:machines:[machine] | read | GetMachineBucketMachineInfo |
| *:tianji:projects:[pname]:machinebuckets:[bname]:machines | read | GetMachineBucketMachines |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:projects:[pname]:machinebuckets:[bname] | write | CreateMachineBucket |
| *:tianji:projects:[pname]:machinebuckets:[bname] | write | OperateMachineBucketMachines |
| *:tianji:projects:[pname]:machinebuckets:[bname] | delete | DeleteMachineBucket |
| *:tianji:projects:[pname]:machinebuckets:[bname] | read | GetMachineBucketMachinesLegacy |
| *:tianji:projects:[pname]:machinebuckets | read | GetMachineBucketList |
| *:tianji:projects:[pname]:projects:[pname]:clusters:[cname]:tssessions:[tssessionname]:tsses | terminal | UpdateTsSessionTssByCluster |
| *:tianji:projects:[pname]:projects:[pname]:clusters:[cname]:tssessions | terminal | CreateTsSessionByCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tjmontemplate | read | GetServiceInstanceTjmonTmplInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template | delete | DeleteServiceInstanceTmplInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template | write | SetServiceInstanceTmplInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template | read | GetServiceInstanceTmplInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tags:[tag] | write | AddServiceInstanceProductTagInCluster |

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

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:debuglog | read | GetMachineDebugLog |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps | read | GetMachineAppList |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | read | GetMachineSRInfoInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | write | OperateSRMachineInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine] | delete | DeleteSRMachineActionInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | write | OperateSRMachinesInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | delete | DeleteSRMachinesActionInCluster |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines | read | GetAllMachineSRInfoInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:resources | read | GetAppResourceInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:machines:[machine]:tianjilogs | read | TianjiLogsInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:dockerinspect | read | DockerInspectInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles | read | GetServiceInstanceServerrolesInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema | delete | DeleteServiceInstanceSchemaInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema | write | SetServiceInstanceSchemaInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:resources | read | GetInstanceResourceInCluster |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname] | delete | DeleteServiceInstance |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname] | write | CreateServiceInstance |
| *:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname] | read | GetServiceInstanceConfInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:rollings:[version] | write | OperateRollingJob |
| *:tianji:projects:[pname]:clusters:[cname]:rollings | read | ListRollingJob |
| *:tianji:projects:[pname]:clusters:[cname]:resources | read | GetResourceInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:quota | write | SetClusterQuotas |
| *:tianji:projects:[pname]:clusters:[cname]:machinesinfo | read | GetClusterMachineInfo |
| *:tianji:projects:[pname]:clusters:[cname]:machines:[machine] | read | GetMachineAllSRInfo |
| *:tianji:projects:[pname]:clusters:[cname]:machines:[machine] | write | SetMachineAction |
| *:tianji:projects:[pname]:clusters:[cname]:machines:[machine] | delete | DeleteMachineAction |
| *:tianji:projects:[pname]:clusters:[cname]:machines | write | OperateClusterMachines |
| *:tianji:projects:[pname]:clusters:[cname]:difflist | read | GetVersionDiffList |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:projects:[pname]:clusters:[cname]:diff | read | GetVersionDiff |
| *:tianji:projects:[pname]:clusters:[cname]:deploylogs:[version] | read | GetDeployLogInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:deploylogs | read | GetDeployLogListInCluster |
| *:tianji:projects:[pname]:clusters:[cname]:builds:[version] | read | GetBuildJob |
| *:tianji:projects:[pname]:clusters:[cname]:builds | read | ListBuildJob |
| *:tianji:projects:[pname]:clusters:[cname] | write | OperateCluster |
| *:tianji:projects:[pname]:clusters:[cname] | delete | DeleteCluster |
| *:tianji:projects:[pname]:clusters:[cname] | read | GetClusterConf |
| *:tianji:projects:[pname]:clusters:[cname] | write | DeployCluster |
| *:tianji:projects:[pname] | write | CreateProject |
| *:tianji:projects:[pname] | delete | DeleteProject |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit] | write | CreateRackunit |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit] | write | SetRackunitAttr |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit] | delete | DeleteRackunit |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack] | write | SetRackAttr |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack] | write | CreateRack |

| Resource | Action | Description |
| --- | --- | --- |
| *:tianji:idcs:[idc]:rooms:[room]:racks:[rack] | delete | DeleteRack |
| *:tianji:idcs:[idc]:rooms:[room] | write | CreateRoom |
| *:tianji:idcs:[idc]:rooms:[room] | delete | DeleteRoom |
| *:tianji:idcs:[idc]:rooms:[room] | write | SetRoomAttr |
| *:tianji:idcs:[idc] | delete | DeleteIdc |
| *:tianji:idcs:[idc] | write | SetIdcAttr |
| *:tianji:idcs:[idc] | write | CreateIdc |

#### 1.2.8.2.2 Permission list of Tianjimon

**This topic describes the permission of Tianjimon.**

| Resource | Action | Description |
| --- | --- | --- |
| 26842:tianjimon:monitor-manage | manage | Monitoring and operations |

## 1.3 Apsara Infrastructure Management Framework

## 1.3.1 Old version

### 1.3.1.1 What is Apsara Infrastructure Management Framework?

**This topic describes what Apsara Infrastructure Management Framework is from the aspects of core functions and basic concepts.**

#### 1.3.1.1.1 Overview

**Apsara Infrastructure Management Framework is a distributed data center management system, which manages applications on clusters containing multiple machines and provides the basic functions such as deployment, upgrade, expansion, contraction, and configuration changes.**

**Apsara Infrastructure Management Framework also supports monitoring data and analyzing reports, which facilitates users to perform one-stop Operation &**

**Maintenance (O&M) control. Based on the Apsara Infrastructure Management Framework services, automated O&M is implemented in the large-scale distributed environment, which greatly improves the operations efficiency and enhances the system availability.**

**Apsara Infrastructure Management Framework is mainly composed of TianjiMaster and TianjiClient. Apsara Infrastructure Management Framework installs TianjiClient as the agent on machines it manages. Then, TianjiMaster accepts and issues the upper-layer instructions to TianjiClient for execution. In the upper layer, Apsara Infrastructure Management Framework is divided into different components based on different functions, and then provides API server and portal for external use.**

Core functions

- **Network initialization in data centers**
- **Server installation and maintenance process management**
- **Deployment, expansion, and upgrade of cloud products**
- **Configuration management of cloud products**
- **Automatic application for cloud product resources**
- **Automatic repair of software and hardware faults**
- **Basic monitoring and business monitoring of software and hardware**

#### 1.3.1.1.2 Basic concepts

**Before using Apsara Infrastructure Management Framework, you must know the following basic concepts for a better understanding.**

project

**A collection of clusters, which provides service capabilities for external entities.**

cluster

**A collection of physical machines, which logically provides services and is used to deploy project software.**

- **A cluster can only belong to one project.**
- **Multiple services can be deployed on a cluster.**

service

**A set of software, which provides relatively independent functions. A service is composed of one or more server roles and can be deployed on multiple clusters**

**to form multiple sets of services and provide the corresponding service capabilities. For example, Apsara Distributed File System, Job Scheduler, and Apsara Name Service and Distributed Lock Synchronization System are all services.**

service instance

**A service that is deployed on a cluster.**

server role

**One or more indivisible deployment units into which a service can be divided based on functions. A server role is composed of one or more specific applications. If a service is deployed on a cluster, all the server roles of the service must be deployed to machines of this cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same server.**

server role instance

**A server role that is deployed on a machine. A server role can be deployed on multiple machines.**

application

**Applications correspond to each process-level service component in a server role and each application works independently. The application is the minimum unit for deployment and upgrade in Apsara Infrastructure Management Framework, and can be deployed to each machine. Generally, an application is an executable software or Docker container.**

**If a server role is deployed on a machine, all applications in the server role must be deployed to this machine.**

rolling

**Each time when a user updates configurations, Apsara Infrastructure Management Framework upgrades services and modifies the cluster configurations based on the updated configurations. This process is called rolling.**

service configuration template

**Some configurations are the same when services are deployed on clusters. A service configuration template can be created to quickly write the same configurations to different clusters. The service configuration template is basically used for large-scale deployment and upgrade.**

associated service template

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

final status

**If a cluster is in this status, all hardware and software on each of its machines are normal and all software are in the target version.**

dependency

**The dependency between server roles in a service defines that server roles with dependencies run tasks or are upgraded based on the dependency order. For example, if A depends on B, B is upgraded first. A starts to be downloaded after B is downloaded successfully, and upgraded after B is successfully upgraded. (By default, the dependency does not take effect for configuration upgrade.)**

upgrade

**A way of aligning the current status with the final status of a service. After a user submits the version change, Apsara Infrastructure Management Framework upgrades the service version to the target version. With the server role as the processing unit, upgrade aims to update the versions of all machines to the target version.**

**At the beginning, the final status and current status of the cluster are the same. When a user submits the change, the final status is changed, whereas the current status is not. A rolling task is generated and has the final status as the target version . During the upgrade, the current status is continuously approximating to the final status. Finally, the final status and the current status are the same when the upgrade is finished.**

### 1.3.1.2 Log on to Apsara Infrastructure Management Framework

**This topic describes how to log on to Apsara Infrastructure Management Framework.**

**Prerequisites**

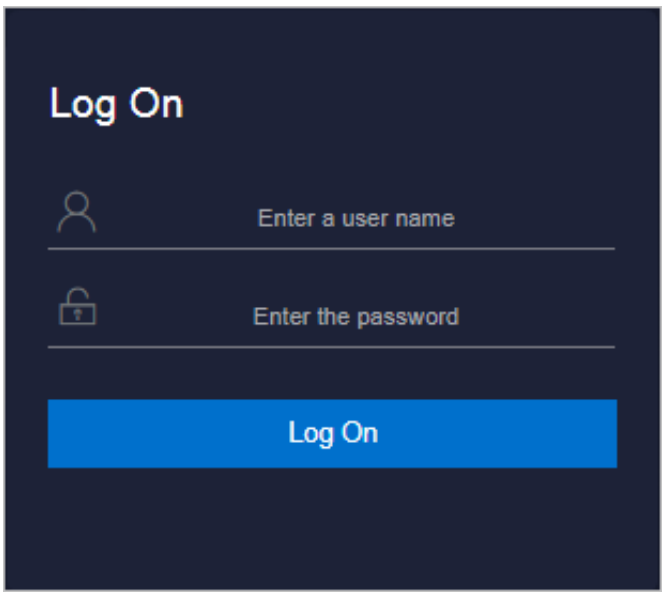
- **ASO access address in the format of http://*region-id*.aso.*intranet-domain-id*.com.**

- Google Chrome browser (recommended).

**Procedure**

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

   Figure 1-4: Log on to ASO




   **Note:**
   You can select the language from the drop-down list in the upper-right corner to change the language of ASO.

3. Enter the correct username and password.
   - The system has three default users:
     - Security officer: manages other users or roles.
     - Auditor officer: views audit logs.
     - System administrator: used for other functions except those of the security officer and auditor officer.
   - You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!),

at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.

4. Click Log On to log on to ASO.
5. In the left-side navigation pane, select Products.
6. In the product list, select Apsara Infrastructure Management Framework.

## 1.3.1.3 Web page introduction

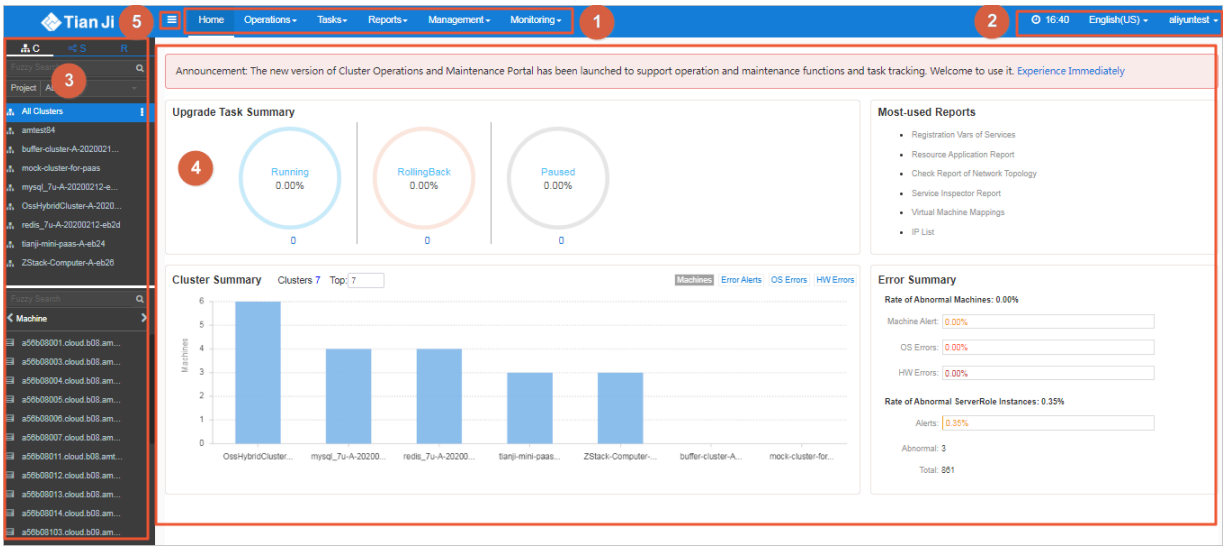
Before performing Operation & Maintenance (O&M) operations on Apsara Infrastructure Management Framework, you must have a general understanding of the Apsara Infrastructure Management Framework page.

### 1.3.1.3.1 Introduction on the home page

After you log on to Apsara Infrastructure Management Framework, the home page appears. This topic allows you to get a general understanding of the basic operations and functions of Apsara Infrastructure Management Framework.

*Log on to Apsara Infrastructure Management Framework*. The home page appears, as shown in *Figure 1-5: Home page of Apsara Infrastructure Management Framework*.

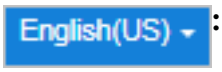
Figure 1-5: Home page of Apsara Infrastructure Management Framework




For more information about the descriptions of functional areas on the home page, see *Table 1-2: Descriptions of functional areas*.

Table 1-2: Descriptions of functional areas

| Area | | Description |
| --- | --- | --- |
| 1 | Top navigation bar | · Operations: the quick entrance of Operations & Maintenance (O&M) operations, which allows operations engineers to quickly find the corresponding operations and operation objects. This menu consists of the following sections:<br>- Cluster Operations: performs O&M operations on and manages clusters with the project permissions, such as viewing the cluster status.<br>- Service Operations: manages services with the service permissions, such as viewing the service list information.<br>- Machine Operations: maintains and manages all the machines in Apsara Infrastructure Management Framework, such as viewing the machine status.<br>· Tasks: A rolling task is generated after you modify the configurations in the system. In this menu, you can view running tasks, history tasks, and the deployment summary of clusters, services, and server roles in all projects.<br>· Reports: displays the monitoring data in tables and provides the function of searching for different reports.<br>· Monitoring: effectively monitors metrics in the process of system operation and sends alert notifications for abnormal conditions. This menu includes the functions of displaying alert status, modifying alert rules, and searching for the alert history. |

| Area | | Description |
| --- | --- | --- |
| 2 | Function buttons in the upper-right corner | ·  :<br>- TJDB Synchronization Time: the generated time of the data that is displayed on the current page.<br>- Final Status Computing Time: the computing time of the final-status data that is displayed on the current page.<br>After data is generated, the system processes the data at maximum speed. As an asynchronous system, Apsara Infrastructure Management Framework has some latency. The time helps explain why the current data results are generated and determine whether the current system has a problem.<br>·  : In the English environment, click this drop-down list to switch to another language.<br>·  : The logon account information. Click this drop-down list and select Logout to log out of Apsara Infrastructure Management Framework. |
| 3 | Left-side navigation pane | In the left-side navigation pane, you can directly view the logical structure of the Apsara Infrastructure Management Framework model.<br>You can view the corresponding detailed data analysis and operations by selecting different levels of nodes in the left-side navigation pane. For more information, see *Introduction on the left-side navigation pane*. |

| Area | | Description |
| --- | --- | --- |
| 4 | Home page | Displays the summary of related tasks or information as follows:<br>· Upgrade Task Summary: the numbers and proportions of running, rolling back, and paused upgrade tasks.<br>· Cluster Summary: the numbers of machines, error alerts, operating system errors, and hardware errors for different clusters.<br>· Error Summary: the metrics for the rate of abnormal machines and the rate of abnormal server role instances.<br>· Most-used Reports: links of the most commonly used statistics reports, which facilitates you to view the report information. |
| 5 | Button used to collapse /expand the left -side navigation pane | If you are not required to use the left-side navigation pane when performing O&M operations, click this button to collapse the left-side navigation pane and increase the space of the content area. |

### 1.3.1.3.2 Introduction on the left-side navigation pane

**The left-side navigation pane has three common tabs: C (cluster), S (service), and R (report). With some operations, you can view the related information quickly.**

Cluster

**Fuzzy search is supported to search for the clusters in a project, and you can view the cluster status, cluster operations information, service final status, and logs.**

**In the left-side navigation pane, click the C tab. Then, you can:**

- **Enter the cluster name in the search box to search for the cluster quickly. Fuzzy search is supported.**
- **Select a project from the Project drop-down list to display all the clusters in the project.**
- **Move the pointer over  at the right of a cluster and then perform operations on the cluster as instructed.**

- **Click a cluster and all the machines and services in this cluster are displayed in the lower-left corner. Move the pointer over  at the right of a machine or service and then perform operations on the machine or service as instructed.**
- **Click the Machine tab in the lower-left corner. Double-click a machine to view all the server roles in the machine. Double-click a server role to view the applications and then double-click an application to view the log files.**
- **Click the Service tab in the lower-left corner. Double-click a service to view all the server roles in the service. Double-click a server role to view the machines, double-click a machine to view the applications, and double-click an application to view the log files.**
- **Double-click a log file. Move the pointer over  at the right of the log file and then select Download to download the log file.**

  **Move the pointer over a log file and then click View at the right of the log file to view the log details based on time. On the Log Viewer page, enter the keyword to search for logs.**

Service

**Fuzzy search is supported to search for services and you can view services and service instances.**

**In the left-side navigation pane, click the S tab. Then, you can:**

- **Enter the service name in the search box to search for the service quickly. Fuzzy search is supported.**
- **Move the pointer over  at the right of a service and then perform operations on the service as instructed.**
- **Click a service and all the service instances in this service are displayed in the lower-left corner. Move the pointer over  at the right of a service instance and then perform operations on the service instance as instructed.**

Report

**Fuzzy search is supported to search for reports and you can view the report details.**

**In the left-side navigation pane, click the R tab. Then, you can:**

- Enter the report name in the search box to search for the report quickly. Fuzzy search is supported.
- Click All Reports or Favorites to display groups of different categories in the lower-left corner. Double-click a group to view all the reports in this group. Double-click a report to view the report details on the right pane.

### 1.3.1.4 Cluster operations

This topic describes the actions about cluster operations.

#### 1.3.1.4.1 View cluster configurations

By viewing the cluster configurations, you can view the basic information, deployment plan, and configurations of a cluster.

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Operations > Cluster Operations.

   The Cluster Operations page displays the following information:

   - Cluster

     The cluster name. Click the cluster name to go to the *Cluster Dashboard* page.
   - Scale-Out/Scale-In

     The number of machines or server roles that are scaled out or in. Click the link to go to the *Cluster Operation and Maintenance Center* page.
   - Abnormal Machine Count

     The statistics of machines whose status is not Good in the cluster. Click the link to go to the *Cluster Operation and Maintenance Center* page.
   - Final Status of Normal Machines

     Displays whether the cluster reaches the final status. Select Clusters Not Final to display clusters that do not reach the final status. Click the link to go to the *Service Final Status Query* page.
   - Rolling

     Displays whether the cluster has a running rolling task. Select Rolling Tasks to display clusters that have rolling tasks. Click the link to go to the *Rolling Task* page.

3. **Select a project from the Project drop-down list and/or enter the cluster name in the Cluster field to search for clusters.**
4. **Find the cluster whose configurations you are about to view and then click Cluster Configuration in the Actions column. The Cluster Configuration page appears.**

   **For more information about the Cluster Configuration page, see** *Table 1-3: Cluster configurations* **.**

   Table 1-3: Cluster configurations

| Category | Item | Description |
| --- | --- | --- |
| Basic Information | Cluster | The cluster name. |
| | Project | The project to which the cluster belongs. |
| | Clone Switch | · Mock Clone: The system is not cloned when a machine is added to the cluster.<br>· Real Clone: The system is cloned when a machine is added to the cluster. |
| | Machines | The number of machines in the cluster. Click View Clustering Machines to view the machine list. |
| | Security Verification | The access control among processes. Generally, the non-production environment uses the default configurations and does not perform the verification. In other cases, customize the configurations based on actual requirements to enable or disable the verification. |
| | Cluster Type | · RDS<br>· NETFRAME<br>· T4: a special type that is required by the mixed deployment of e-commerce.<br>· Default: other conditions. |
| Deployment Plan | Service | The service deployed in the cluster. |

| Category | Item | Description |
| --- | --- | --- |
| | Dependency Service | The service that the current service depends on. |
| Service Information | Service Information | Select a service from the Service Information drop-down list and then the configurations of this service are displayed. |
| | Service Template | The template used by the service. |
| | Monitoring Template | The monitoring template used by the service. |
| | Machine Mappings | The machines included in the server role of the service. |
| | Software Version | The software version of the server role in the service. |
| | Availability Configuration | The availability configuration percentage of the server role in the service. |
| | Deployment Plan | The deployment plan of the server role in the service. |
| | Configuration Information | The configuration file used in the service. |
| | Role Attribute | Server roles and the corresponding parameters. |

5. Click Operation Logs in the upper-right corner to view the release changes. For more information, see *View operation logs*.

## 1.3.1.4.2 View the cluster dashboard

**The cluster dashboard allows you to view the basic information and related statistics of a cluster.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.

2. You have two ways to go to the Cluster Dashboard page:
   - In the left-side navigation pane, click the C tab. Move the pointer over  at the right of a cluster and then select Dashboard.
   - In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, click the cluster name.
3. On the Cluster Dashboard page, you can view the cluster information, including the basic information, final status information, rolling job information, dependencies, resource information, virtual machines, and monitoring information. For more information about the descriptions, see the following table.

| Item | Description |
| --- | --- |
| Basic Cluster Information | Displays the basic information of the cluster as follows:<br>· Project Name: the project name.<br>· Cluster Name: the cluster name.<br>· IDC: the data center to which the cluster belongs.<br>· Final Status Version: the latest version of the cluster.<br>· Cluster in Final Status: whether the cluster reaches the final status.<br>· Machines Not In Final Status: the number of machines that do not reach the final status in the cluster when the cluster does not reach the final status.<br>· Real/Pseudo Clone: whether to clone the system when a machine is added to the cluster.<br>· Expected Machines: the number of expected machines in the cluster.<br>· Actual Machines: the number of machines in the current environment.<br>· Machines Not Good: the number of machines whose status is not Good in the cluster.<br>· Actual Services: the number of services that are actually deployed in the cluster.<br>· Actual Server Roles: the number of server roles that are actually deployed in the cluster.<br>· Cluster Status: whether the cluster is starting or shutting down machines. |

| Item | Description |
| --- | --- |
| Machine Status Overview | The statistical chart of the machine status in the cluster . |
| Machines in Final Status | The numbers of machines that reach the final status and those that do not reach the final status in each service of the cluster. |
| Load-System | The system load chart of the cluster. |
| CPU-System | The CPU load chart. |
| Mem-System | The memory load chart. |
| Disk_usage-System | The statistical table of the disk usage. |
| Traffic-System | The system traffic chart. |
| TCP State-system | The TCP request status chart. |
| TCP Retrans-System | The chart of TCP retransmission amount. |
| Disk_IO-System | The statistical table of the disk input and output. |
| Service Instances | Displays the service instances deployed in the cluster and the related final status information.<br>· Service Instance: the service instance deployed in the cluster.<br>· Final Status: whether the service instance reaches the final status.<br>· Expected Server Roles: the number of server roles that the service instance expects to deploy.<br>· Server Roles In Final Status: the number of server roles that reach the final status in the service instance.<br>· Server Roles Going Offline: the number of server roles that are going offline in the service instance.<br>· Actions: Click Details to go to the Service Instance Information Dashboard page. For more information about the service instance dashboard, see *View the service instance dashboard*. |

| Item | Description |
| --- | --- |
| Upgrade Tasks | Displays the upgrade tasks related to the cluster.<br>· Cluster Name: the name of the upgrade cluster.<br>· Type: the type of the upgrade task. The options include app (version upgrade) and config (configuration change).<br>· Git Version: the change version to which the upgrade task belongs.<br>· Description: the description about the change.<br>· Rolling Result: the result of the upgrade task.<br>· Submitted By: the person who submits the change.<br>· Submitted At: the time when the change is submitted.<br>· Start Time: the time to start the rolling.<br>· End Time: the time to finish the upgrade.<br>· Time Used: the time used for the upgrade.<br>· Actions: Click Details to go to the Rolling Task page. For more information about the rolling task, see *View rolling tasks*. |
| Cluster Resource Request Status | · Version: the resource request version.<br>· Msg: the exception message.<br>· Begintime: the start time of the resource request analysis.<br>· Endtime: the end time of the resource request analysis.<br>· Build Status: the build status of resources.<br>· Resource Process Status: the resource request status in the version. |

| Item | Description |
| --- | --- |
| Cluster Resource | · Service: the service name.<br>· Server Role: the server role name.<br>· App: the application of the server role.<br>· Name: the resource name.<br>· Type: the resource type.<br>· Status: the resource request status.<br>· Error Msg: the exception message.<br>· Parameters: the resource parameters.<br>· Result: the resource request result.<br>· Res: the resource ID.<br>· Reprocess Status: the status of interaction with Business Foundation System during the VIP resource request.<br>· Reprocess Msg: the exception message of interaction with Business Foundation System during the VIP resource request.<br>· Reprocess Result: the result of interaction with Business Foundation System during the VIP resource request.<br>· Refer Version List: the version that uses the resource. |
| VM Mappings | The information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.<br>· VM: the hostname of the virtual machine.<br>· Currently Deployed On: the hostname of the physical machine where the virtual machine is currently deployed.<br>· Target Deployed On: the hostname of the physical machine where the virtual machine is expected to be deployed. |

| Item | Description |
| --- | --- |
| Service Dependencies | The dependencies of service instances and server roles in the cluster, and the final status information of the dependent service or server role.<br>· Service: the service name.<br>· Server Role: the server role name.<br>· Dependent Service: the service on which the server role depends.<br>· Dependent Server Role: the server role on which the server role depends.<br>· Dependent Cluster: the cluster to which the dependent server role belongs.<br>· Dependency in Final Status: whether the dependent server role reaches the final status. |

### 1.3.1.4.3 View the cluster operation and maintenance center

**The cluster operation and maintenance center allows you to view the status or statistics of services or machines in the cluster.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **You have three ways to go to the Cluster Operation and Maintenance Center page:**
   - **In the left-side navigation pane, click the C tab. Move the pointer over**  **at the right of a cluster and then select Cluster Operation and Maintenance Center.**
   - **In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, choose Monitoring > Cluster Operation and Maintenance Center in the Actions column at the right of a cluster.**
   - **In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, click a cluster name. On the Cluster Dashboard page, choose Operations Menu > Cluster Operation and Maintenance Center.**

3. View the information on the Cluster Operation and Maintenance Center page.

| Item | Description |
| --- | --- |
| SR not in Final Status | Displays all the server roles that do not reach the final status in the cluster.<br>Click the number to expand a server role list, and click a server role in the list to display the information of machines included in the server role. |
| Running Tasks | Displays whether the cluster has running rolling tasks.<br>Click Rolling to go to the Rolling Task page. For more information about the rolling task, see *View rolling tasks*. |
| Head Version Submitted At | The time when the head version is submitted.<br>Click the time to view the submission details. |
| Head Version Analysis | The head version analysis is the process that Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to detailed change contents. The head version analysis has the following statuses:<br>· Preparing: No new version is available now.<br>· Waiting: The latest version is found. The analysis module has not started up yet.<br>· Doing: The module is analyzing the application that requires change.<br>· done: The head version analysis is successfully completed.<br>· Failed: The head version analysis failed. The change contents cannot be parsed.<br>If the status is not done, Apsara Infrastructure Management Framework cannot detect the change contents of server roles in the latest version.<br>Click the status to view the relevant information. |

| Item | Description |
| --- | --- |
| Service | Select a service deployed in the cluster from the drop-down list. |
| Server Role | Select a server role of a service in the cluster from the drop-down list.<br>  Note:<br>After you select the service and server role, the information of machines related to the service or server role is displayed in the list. |
| Total Machines | The total number of machines in the cluster, or the total number of machines included in a specific server role of a specific service. |
| Scale-in/Scale-out | The number of machines or server roles that are scaled in or out. |
| Abnormal Machines | The number of abnormal machines that encounter each type of the following faults.<br>· Ping Failed: A ping_monitor error is reported, and TianjiMaster cannot successfully ping the machine.<br>· No Heartbeat: TianjiClient on the machine does not regularly report data to indicate the status of this machine, which may be caused by the TianjiClient problem or network problem.<br>· Status Error: The machine has an error reported by the monitor or a fault of the critical or fatal level. Check the alert information and accordingly solve the issue. |

| Item | Description |
| --- | --- |
| Abnormal Services | The number of machines with abnormal services. To determine if a service reaches the final status, see the following rules:<br>· The server role on the machine is in the GOOD status.<br>· Each application of the server role on the machine must keep the actual version the same as the head version.<br>· Before the Image Builder builds an application of the head version, Apsara Infrastructure Management Framework cannot determine the value of the head version and the service final status is unknown. This process is called the change preparation process. The service final status cannot be determined during the preparation process or upon a preparation failure. |

| Item | Description |
| --- | --- |
| Machines | Displays all the machines in the cluster or the machines included in a specific server role of a specific service.<br>· Machine search: Click the search box to enter the machine in the displayed dialog box. Fuzzy or batch search is supported.<br>· Click the machine name to view the physical information of the machine in the displayed Machine Information dialog box. Click DashBoard to go to the Machine Details page. For more information about the machine details, see *View the machine dashboard*.<br>· Move the pointer over the blank area in the Final Status column or the Final SR Status column and then click Details to view the machine status, system service information, server role status on the machine, and exception message.<br>· If no service or server role is selected from the drop-down list, move the pointer over the blank area in the Running Status column and then click Details to view the running status information or exception message of the machine.<br>If a service and a server role are selected from the corresponding drop-down lists, move the pointer over the blank area in the SR Running Status column and then click Details to view the running status information or exception message of the server role on the machine.<br>· Click Error, Warning, or Good in the Monitoring Statistics column to view the monitored items of machines and monitored items of server roles.<br>· Click Terminal in the Actions column to log on to the machine and perform related operations.<br>· Click Machine Operation in the Actions column to restart, out-of-band restart, or clone the machine again. |

## 1.3.1.4.4 View the service final status

**The Service Final Status Query page allows you to view if a service in a cluster reaches the final status and the final status information.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.

2. You have two ways to go to the Service Final Status Query page:
   - In the left-side navigation pane, click the C tab. Move the pointer over  at the right of a cluster and then choose Monitoring > Service Final Status Query.
   - In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, choose Monitoring > Service Final Status Query in the Actions column at the right of a cluster.
3. View the information on the Service Final Status Query page.

| Item | Description |
| --- | --- |
| Project Name | The name of the project to which the cluster belongs. |
| Cluster Name | The cluster name. |
| Head Version Submitted At | The time when the head version is submitted. |
| Head Version Analysis | The head version analysis is the process that Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to detailed change contents. The head version analysis has the following statuses:<br>· Preparing: No new version is available now.<br>· Waiting: The latest version is found. The analysis module has not started up yet.<br>· Doing: The module is analyzing the application that requires change.<br>· done: The head version analysis is successfully completed.<br>· Failed: The head version analysis failed. The change contents cannot be parsed.<br>If the status is not done, Apsara Infrastructure Management Framework cannot detect the change contents of server roles in the latest version. |
| Cluster Rolling Status | Displays the information of the current rolling task in the cluster, if any. The rolling task may not be of the head version. |

| Item | Description |
| --- | --- |
| Cluster Machine Final Status Statistics | The status of all machines in the cluster. Click View Details to go to the Cluster Operation and Maintenance Center page and view the detailed information of all machines. For more information about the cluster operation and maintenance center, see *View the cluster operation and maintenance center*. |
| Final Status of Cluster SR Version | The final status of cluster service version.<br>**Note:**<br>Take statistics of services that do not reach the final status, which is caused by version inconsistency or status exceptions. If services do not reach the final status because of machine problems, go to Cluster Machine Final Status Statistics to view the statistics. |
| Final Status of SR Version | The number of machines that do not reach the final status when a server role has tasks. |

### 1.3.1.4.5 View operation logs

**By viewing operation logs, you can obtain the differences between different Git versions.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. You have two ways to go to the Cluster Operation Logs page:
   - In the left-side navigation pane, click the C tab. Move the pointer over at the right of a cluster and then choose Monitoring > Operation Logs.
   - In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, choose Monitoring > Operation Logs in the Actions column at the right of a cluster.
3. On the Cluster Operation Logs page, click Refresh. View the Git version, description, submitter, submitted time, and task status.

4. Optional: Complete the following steps to view the differences between versions on the Cluster Operation Logs page.
   a) Find the log in the operation log list and then click View Release Changes in the Actions column.
   b) On the Version Difference page, complete the following configurations:
      - Select Base Version: Select a base version.
      - Configuration Type: Select Extended Configuration or Cluster Configuration. Extended 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.
   c) Click Obtain Difference.

      The differential file list is displayed.
   d) Click each differential file to view the detailed differences.

## 1.3.1.5 Service operations

This topic describes the actions about service operations.

### 1.3.1.5.1 View the service list

The service list allows you to view the list of all services and the related information.

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Operations > Service Operations.
3. View the information on the Service Operations page.

| Item | Description |
| --- | --- |
| Service | The service name. |
| Service Instances | The number of service instances in the service. |
| Service Configuration Templates | The number of service configuration templates. |
| Monitoring Templates | The number of monitoring templates. |

| Item | Description |
| --- | --- |
| Service Schemas | The number of service configuration validation templates. |
| Actions | Click Management to view the service instances, service templates, monitoring templates, monitoring instances, service schemas, and detection scripts. |

### 1.3.1.5.2 View the service instance dashboard

**The service instance dashboard allows you to view the basic information and statistics of a service instance.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, click the S tab.
3. Enter the service name in the search box. Services that meet the search condition are displayed.
4. Click a service name and then service instances in the service are displayed in the lower-left corner.
5. Move the pointer over  at the right of a service instance and then select Dashboard.

6. View the information on the Service Instance Information Dashboard page.

| Item | Description |
| --- | --- |
| Service Instance Summary | Displays the basic information of the service instance as follows:<br>· Cluster Name: the name of the cluster to which the service instance belongs.<br>· Service Name: the name of the service to which the service instance belongs.<br>· Actual Machines: the number of machines in the current environment.<br>· Expected Machines: the number of machines that the service instance expects.<br>· Target Total Server Roles: the number of server roles that the service instance expects.<br>· Actual Server Roles: the number of server roles in the current environment.<br>· Template Name: the name of the service template used by the service instance.<br>· Template Version: the version of the service template used by the service instance.<br>· Schema: the name of the service schema used by the service instance.<br>· Monitoring System Template: the name of the monitoring system template used by the service instance. |
| Server Role Statuses | The statistical chart of the current status of server roles in the service instance. |
| Machine Statuses for Server Roles | The status statistics of machines where server roles are located. |
| Service Monitoring Information | · Monitored Item: the name of the monitored item.<br>· Level: the level of the monitored item.<br>· Description: the description of the monitored contents.<br>· Updated At: the time when the data is updated. |

| Item | Description |
| --- | --- |
| Service Alert Status | · Alert Name<br>· Instance Information<br>· Alert Start<br>· Alert End<br>· Alert Duration<br>· Severity Level<br>· Occurrences: the number of times the alert is triggered. |
| Server Role List | · Server Role<br>· Current Status<br>· Expected Machines<br>· Machines In Final Status<br>· Machines Going Offline<br>· Rolling Task Status<br>· Time Used: the time used for running the rolling task.<br>· Actions: Click Details to go to the *Server Role Dashboard* page. |
| Service Alert History | · Alert Name<br>· Alert Time<br>· Instance Information<br>· Severity Level<br>· Contact Group |
| Service Dependencies | The dependencies of service instances and server roles in the service instance, and the final status information of the dependent service or server role.<br>· Server Role: the server role name.<br>· Dependent Service: the service on which the server role depends.<br>· Dependent Server Role: the server role on which the server role depends.<br>· Dependent Cluster: the cluster to which the dependent server role belongs.<br>· Dependency in Final Status: whether the dependent server role reaches the final status. |

## 1.3.1.5.3 View the server role dashboard

**The server role dashboard allows you to view the statistics of a server role.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, click the S tab.**
3. **Enter the service name in the search box. Services that meet the search condition are displayed.**
4. **Click a service name and then service instances in the service are displayed in the lower-left corner.**
5. **Move the pointer over  at the right of a service instance and then select Dashboard.**
6. **In the Server Role List section of the Service Instance Information Dashboard page, click Details in the Actions column.**

7. View the information on the Server Role Dashboard page.

| Item | Description |
| --- | --- |
| Server Role Summary | Displays the basic information of the server role as follows:<br>· Project Name: the name of the project to which the server role belongs.<br>· Cluster Name: the name of the cluster to which the server role belongs.<br>· Service Instance: the name of the service instance to which the server role belongs.<br>· Server Role: the server role name.<br>· In Final Status: whether the server role reaches the final status.<br>· Expected Machines: the number of expected machines.<br>· Actual Machines: the number of actual machines.<br>· Machines Not Good: the number of machines whose status is not Good.<br>· Machines with Role Status Not Good: the number of server roles whose status is not Good.<br>· Machines Going Offline: the number of machines that are going offline.<br>· Rolling: whether a running rolling task exists.<br>· Rolling Task Status: the current status of the rolling task.<br>· Time Used: the time used for running the rolling task. |
| Machine Final Status Overview | The statistical chart of the current status of the server role. |
| Server Role Monitoring Information | · Updated At: the time when the data is updated.<br>· Monitored Item: the name of the monitored item.<br>· Level: the level of the monitored item.<br>· Description: the description of the monitored item. |

| Item | Description |
| --- | --- |
| Machine Information | · Machine Name: the hostname of the machine.<br>· IP: the IP address of the machine.<br>· Machine Status: the machine status.<br>· Machine Action: the action that the machine is performing.<br>· Server Role Status: the status of the server role.<br>· Server Role Action: the action that the server role is performing.<br>· Current Version: the current version of the server role on the machine.<br>· Target Version: the expected version of the server role on the machine.<br>· Error Message: the exception message.<br>· Actions:<br>- Click Terminal to log on to the machine and perform operations.<br>- Click Restart to restart the server roles on the machine.<br>- Click Details to go to the Machine Details page. For more information about the machine details, see *View the machine dashboard*.<br>- Click Machine System View to go to the Machine Info Report page. For more information about the machine info report, see *Machine info report*.<br>- Click Machine Operation to restart, out of band restart, or clone the machine again. |
| Server Role Monitoring Information of Machines | · Updated At: the time when the data is updated.<br>· Machine Name: the machine name.<br>· Monitored Item: the name of the monitored item.<br>· Level: the level of the monitored item.<br>· Description: the description of the monitored item. |

| Item | Description |
| --- | --- |
| VM Mappings | The information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.<br>· VM: the hostname of the virtual machine.<br>· Currently Deployed On: the hostname of the physical machine where the virtual machine is currently deployed.<br>· Target Deployed On: the hostname of the physical machine where the virtual machine is expected to be deployed. |
| Service Dependencies | The dependencies of service instances and server roles in the service instance, and the final status information of the dependent service or server role.<br>· Dependent Service: the service on which the server role depends.<br>· Dependent Server Role: the server role on which the server role depends.<br>· Dependent Cluster: the cluster to which the dependent server role belongs.<br>· Dependency in Final Status: whether the dependent server role reaches the final status. |

## 1.3.1.6 Machine operations

**This topic describes the actions about machine operations.**

## 1.3.1.6.1 View the machine dashboard

**The machine dashboard allows you to view the statistics of a machine.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, click the C tab.
3. On the Machine tab in the lower-left corner, enter the machine name in the search box. Machines that meet the search condition are displayed.
4. Move the pointer over  at the right of a machine and then select Dashboard.

5. On the Machine Details page, view all the information of this machine. For more information, see the following table.

| Item | Description |
| --- | --- |
| Load-System | The system load chart of the cluster. |
| CPU-System | The CPU load chart. |
| Mem-System | The memory load chart. |
| DISK Usage-System | The statistical table of the disk usage. |
| Traffic-System | The system traffic chart. |
| TCP State-System | The TCP request status chart. |
| TCP Retrans-System | The chart of TCP retransmission amount. |
| DISK IO-System | The statistical table of the disk input and output. |
| Machine Summary | · Project Name: the name of the project to which the machine belongs.<br>· Cluster Name: the name of the cluster to which the machine belongs.<br>· Machine Name: the machine name.<br>· SN: the serial number of the machine.<br>· IP: the IP address of the machine.<br>· IDC: the data center of the machine.<br>· Room: the room in the data center where the machine is located.<br>· Rack: the rack where the machine is located.<br>· Unit in Rack: the location of the rack.<br>· Warranty: the warranty of the machine.<br>· Purchase Date: the date when the machine is purchased.<br>· Machine Status: the running status of the machine.<br>· Status: the hardware status of the machine.<br>· CPUs: the number of CPUs for the machine.<br>· Disks: the disk size.<br>· Memory: the memory size.<br>· Manufacturer: the machine manufacturer.<br>· Model: the machine model.<br>· os: the operating system of the machine.<br>· part: the disk partition. |
| Server Role Status of Machine | The distribution of the current status of all server roles on the machine. |

| Item | Description |
| --- | --- |
| Machine Monitoring Information | · Monitored Item: the name of the monitored item.<br>· Level: the level of the monitored item.<br>· Description: the description of the monitored contents.<br>· Updated At: the time when the monitoring information is updated. |
| Machine Server Role Status | · Service Instance<br>· Server Role<br>· Server Role Status<br>· Server Role Action<br>· Error Message<br>· Target Version<br>· Current Version<br>· Actual Version Update Time<br>· Actions:<br>- Click Details to go to the Server Role Dashboard page. For more information about the server role dashboard, see *View the server role dashboard*.<br>- Click Restart to restart the server roles on the machine. |
| Application Status in Server Roles | · Application Name: the application name.<br>· Process Number<br>· Status: the application status.<br>· Current Build ID: the ID of the current package version.<br>· Target Build ID: the ID of the expected package version.<br>· Git Version<br>· Start Time<br>· End Time<br>· Interval: the interval between the time when Apsara Infrastructure Management Framework detects that the process exits and the time when Apsara Infrastructure Management Framework repairs the process.<br>· Information Message: the normal output logs.<br>· Error Message: the abnormal logs. |

## 1.3.1.7 Monitoring center

**You can view the alert status, alert rules, and alert history in the monitoring center.**

## 1.3.1.7.1 Modify an alert rule

**You can modify an alert rule based on the actual business requirements.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Operations > Service Operations.
3. Enter the service name in the search box.
4. Find the service and then click Management in the Actions column.
5. Click the Monitoring Template tab.
6. Find the monitoring template that you are about to edit and then click Edit in the Actions column.
7. Configure the monitoring parameters based on actual conditions.
8. Click Save Change.

   Wait about 10 minutes. The monitoring instance is automatically deployed. If the status becomes `Successful` and the deployment time is later than the modified time of the template, the changes are successfully deployed.

## 1.3.1.7.2 View the status of a monitoring instance

**After a monitoring instance is deployed, you can view the status of the monitoring instance.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Operations > Service Operations.
3. Enter the service name in the search box.
4. Find the service and then click Management in the Actions column.
5. Click the Monitoring Instance tab.

   In the Status column, view the current status of the monitoring instance.

### 1.3.1.7.3 View the alert status

**The Alert Status page allows you to view the alerts generated in different services and the corresponding alert details.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the top navigation bar, choose Monitoring > Alert Status.**
3. **You can configure the service name, cluster name, alert name, and/or the time range when the alert is triggered to search for alerts.**
4. **View the alert details on the Alert Status page. See the following table for the alert status descriptions.**

| Item | Description |
| --- | --- |
| Service | The service name. |
| Cluster | The name of the cluster where the service is located. |
| Instance | The name of the service instance being monitored.<br>Click the instance to view the alert history of this instance. |
| Alert Status | Alerts have two statuses: Restored and Alerting. |
| Alert Level | Alerts have the following four levels, from high to low, according to the effect on services.<br>· P1<br>· P2<br>· P3<br>· P4 |
| Alert Name | The name of the generated alert.<br>Click the alert name to view the alert rule details. |
| Alert Time | The time when the alert is triggered and how long the alert has lasted. |
| Actions | Click Show to show the data before and after the alert time. |

### 1.3.1.7.4 View alert rules

**The Alert Rules page allows you to view the configured alert rules.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.

2. In the top navigation bar, choose Monitoring > Alert Rules.
3. You can configure the service name, cluster name, and/or alert name to search for alert rules.
4. View the detailed alert rules on the Alert Rules page. See the following table for the alert rule descriptions.

| Item | Description |
| --- | --- |
| Service | The service name. |
| Cluster | The name of the cluster where the service is located. |
| Alert Name | The name of the generated alert. |
| Alert Conditions | The conditions met when the alert is triggered. |
| Periods | The frequency (in seconds) with which an alert rule is run. |
| Alert Contact | The groups and members that are notified when an alert is triggered. |
| Status | The current status of the alert rule.<br>· Running: Click to stop this alert rule.<br>· Stopped: Click to run this alert rule. |

### 1.3.1.7.5 View the alert history

**The Alert History page allows you to view all the history alerts generated in different services and the corresponding alert details.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Monitoring > Alert History.
3. You can configure the service name, cluster name, time range, and/or period to search for alerts.
4. View the history alerts on the Alert History page. See the following table for the history alert descriptions.

| Item | Description |
| --- | --- |
| Service | The name of the service to which the alert belongs. |
| Cluster | The name of the cluster where the service is located. |
| Alert Instance | The name of the resource where the alert is triggered. |
| Status | Alerts have two statuses: Restored and Alerting. |

| Item | Description |
| --- | --- |
| Alert Level | Alerts have the following four levels, from high to low, according to the effect on services.<br>· P1<br>· P2<br>· P3<br>· P4 |
| Alert Name | The name of the generated alert.<br>Click the alert name to view the alert rule details. |
| Alert Time | The time when the alert is triggered. |
| Alert Contact | The groups and members that are notified when an alert is triggered. |
| Actions | Click Show to show the data before and after the alert time. |

## 1.3.1.8 Tasks and deployment summary

**This topic describes how to view rolling tasks, running tasks, history tasks, and deployment summary on Apsara Infrastructure Management Framework.**

### 1.3.1.8.1 View rolling tasks

**You can view running rolling tasks and the corresponding status.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Operations > Cluster Operations.
3. Select Rolling Tasks to display clusters with rolling tasks.
4. In the search results, click rolling in the Rolling column.
5. On the displayed Rolling Task page, view the information in the Change Task list and Change Details list.

Table 1-4: Change Task list

| Item | Description |
| --- | --- |
| Change Version | The version that triggers the change of the rolling task. |
| Description | The description about the change. |

| Item | Description |
| --- | --- |
| Head Version Analysis | The head version analysis is the process that Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to detailed change contents. The head version analysis has the following statuses:<br>· Preparing: No new version is available now.<br>· Waiting: The latest version is found. The analysis module has not started up yet.<br>· Doing: The module is analyzing the application that requires change.<br>· done: The head version analysis is successfully completed.<br>· Failed: The head version analysis failed. The change contents cannot be parsed.<br>If the status is not done, Apsara Infrastructure Management Framework cannot detect the change contents of server roles in the latest version. |
| Blocked Server Role | Server roles blocked in the rolling task. Generally, server roles are blocked because of dependencies. |
| Submitter | The person who submits the change. |
| Submitted At | The time when the change is submitted. |
| Actions | Click View Difference to go to the Version Difference page. For more information, see *View operation logs*.<br>Click Stop to stop the rolling task.<br>Click Pause to pause the rolling task. |

Table 1-5: Change Details list

| Item | Description |
| --- | --- |
| Service Name | The name of the service where a change occurs. |

| Item | Description |
| --- | --- |
| Status | The current status of the service.<br>The rolling status of the service is an aggregated result, which is calculated based on the rolling status of the server role.<br>· succeeded: The task is successfully run.<br>· blocked: The task is blocked.<br>· failed: The task failed. |
| Server Role Status | The server role status. Click > at the left of the service name to expand and display the rolling task status of each server role in the service.<br>Server roles have the following statuses:<br>· Downloading: The task is being downloaded.<br>· Rolling: The rolling task is running.<br>· RollingBack: The rolling task failed and is rolling back. |
| Depend On | The services that this service depends on or server roles that this server role depends on. |
| Actions | Click Stop to stop the change of the server role.<br>Click Pause to pause the change of the server role. |

## 1.3.1.8.2 View running tasks

**By viewing running tasks, you can know the information of all the running tasks.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.

2. In the top navigation bar, choose Tasks > Running Tasks.
3. You can configure the cluster name, role name, task status, task submitter, Git version, and/or the start time and end time of the task to search for running tasks.
4. Find the task that you are about to view the details and then click View Tasks in the Rolling Task Status column. The Rolling Task page appears. For more information about the rolling task, see *View rolling tasks*.

### 1.3.1.8.3 View history tasks

**You can view the historical running conditions of completed tasks.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Tasks > History Tasks.
3. You can configure the cluster name, Git version, task submitter, and/or the start time and end time of the task to search for history tasks.
4. Find the task that you are about to view the details and then click Details in the Actions column. The Rolling Task page appears. For more information about the rolling task, see *View rolling tasks*.

### 1.3.1.8.4 View the deployment summary

**On the Deployment Summary page, you can view the deployment conditions of clusters, services, and server roles in all projects on Apsara Infrastructure Management Framework.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the top navigation bar, choose Tasks > Deployment Summary.
   - View the deployment status and the duration of a certain status for each project.
     - Gray: wait to be deployed. It indicates that some services of the project depend on server roles or service instances that are being deployed, and

other service instances or server roles in the project have already been deployed.

- Blue: being deployed. It indicates that the project has not reached the final status for one time yet.
- Green: has reached the final status. It indicates that all clusters in the project have reached the final status.
- Orange: not reaches the final status. It indicates that a server role does not reach the final status for some reason after the project reaches the final status for the first time.

· Configure the global clone switch.

- normal: Clone is allowed.
- block: Clone is forbidden.

· Configure the global dependency switch.

- normal: All configured dependencies are checked.
- ignore: The dependency is not checked.
- ignore_service: None of the service-level dependencies, including the server role dependencies across services, are checked, and only the server role-level dependencies are checked.

3. Click the Deployment Details tab to view the deployment details.

   For more information, see the following table.

| Item | Description |
| --- | --- |
| Status Statistics | The general statistics of deployment conditions, including the total number of projects that are currently available. Click each status to display the projects in the corresponding status in the list. The projects have five deployment statuses:<br>· Final: All the clusters in the project have reached the final status.<br>· Deploying: The project has not reached the final status for one time yet.<br>· Waiting: Some services of the project depend on server roles or service instances that are being deployed, and other service instances or server roles in the project have already been deployed.<br>· Non-final: A server role does not reach the final status for some reason after the project reaches the final status for the first time.<br>· Inspector Warning: An error is detected on service instances in the project during the inspection. |
| Start Time | The time when Apsara Infrastructure Management Framework starts the deployment. |
| Progress | The proportion of server roles that reach the final status to all the server roles in the current environment. |
| Deployment Status | The time indicates the deployment duration for the following statuses: Final, Deploying, Waiting, and Inspector Warning.<br>The time indicates the duration before the final status is reached for the Non-final status.<br>Click the time to view the details. |

| Item | Description |
| --- | --- |
| Deployment Progress | The proportion of clusters, services, and server roles that reach the final status to the total clusters, services, and server roles in the project.<br>Move the pointer over the blank area at the right of the data of roles and then click Details to view the deployment statuses of clusters, services, and server roles. The deployment statuses are indicated by icons, which are the same as those used for status statistics. |
| Resource Application Progress | Total indicates the total number of resources related to the project.<br>· Done: the number of resources that have been successfully applied for.<br>· Doing: the number of resources that are being applied for and retried. The number of retries (if any) is displayed next to the number of resources.<br>· Block: the number of resources whose applications are blocked by other resources.<br>· Failed: the number of resources whose applications failed. |
| Inspector Error | The number of inspection alerts for the current project. |
| Monitoring Information | The number of alerts generated for the machine monitor and the machine server role monitor in the current project. |
| Dependency | Click the icon to view the project services that depend on other services, and the current deployment status of the services that are depended on. |

## 1.3.1.9 Reports

The system allows you to search for and view reports based on your business needs, and add commonly used reports to your favorites.

### 1.3.1.9.1 View reports

The Reports menu allows you to view the statistical data.

**Context**

You can view the following reports on Apsara Infrastructure Management Framework.

· System reports: default and common reports in the system.

- All reports: includes the system reports and custom reports.

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. You can go to the report list in the following three ways:
   - In the top navigation bar, choose Reports > System Reports.
   - In the top navigation bar, choose Reports > All Reports.
   - In the left-side navigation pane, click the R tab. Move the pointer over  at the right of All Reports and then select View.

   See the following table for the report descriptions.

| Item | Description |
| --- | --- |
| Report | The report name.<br>Move the pointer over  next to Report to search for reports by report name. |
| Group | The group to which the report belongs.<br>Move the pointer over  next to Group to filter reports by group name. |
| Status | Indicates whether the report is published. |
| Public | Indicates whether the report is public. |
| Created By | The person who creates the report. |
| Published At | The published time and created time of the report. |
| Actions | Click Add to Favorites to add this report to your favorites. Then, you can view the report by choosing Reports > Favorites in the top navigation bar or moving the pointer over  at the right of Favorites on the R tab in the left-side navigation pane and then selecting View. |

3. Optional: Enter the name of the report that you are about to view in the search box.
4. Click the report name to go to the corresponding report details page.

   For more information about the reports, see *Appendix*.

### 1.3.1.9.2 Add a report to favorites

**You can add common reports to favorites. Then, find them quickly on the Favorites page.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **You can go to the report list in the following three ways:**
   - **In the top navigation bar, choose Reports > System Reports.**
   - **In the top navigation bar, choose Reports > All Reports.**
   - **In the left-side navigation pane, click the R tab. Move the pointer over  at the right of All Reports and then select View.**
3. **Enter the name of the report that you are about to add to favorites in the search box.**
4. **At the right of the report, click Add to Favorites in the Actions column.**
5. **In the displayed Add to Favorites dialog box, enter tags for the report.**
6. **Click Add to Favorites.**

## 1.3.1.10 Metadata operations

**In this version, you can only use command lines to perform metadata operations.**

### 1.3.1.10.1 Common parameters

**Common parameters consist of the common request parameters and the common response parameters.**

Common request parameters

**Common request parameters are request parameters that you must use when you call each API.**

Table 1-6: Parameter descriptions

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The API name. For more information about the valid values, see *APIs on the control side* and *APIs on the deployment side*. |

Common response parameters

**Each time you send a request to call an API, the system returns a unique identifier, regardless of whether the call is successful.**

Table 1-7: Parameter descriptions

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| RequestID | String | Yes | The request ID.<br>The request ID is returned, regardless of whether the API call is successful. |
| Code | String | No | The error code. |
| Message | String | No | The reason of failure, which appears when the API call fails. |
| Result | The type varies with the request, which is subject to the returned result of the specific API. | No | The request result , which appears when the API call is successful. |

**Note:**

- **If the API call is successful, RequestID is returned and the HTTP return code is 200.**
- **If the API call fails, RequestID, Code, and Message are returned and the HTTP return code is 4xx or 5xx.**

Instance types

```
{
    "rds.mys2.small":{
        "cpu":2,
        "memory":4096,
        "disk":51200,
        "max_connections":60
    },
    "rds.mys2.mid":{
        "cpu":4,
        "memory":4096,
        "disk":51200,
        "max_connections":150
    },
    "rds.mys2.standard":{
        "cpu":6,
        "memory":4096,
        "disk":51200,
        "max_connections":300
    },
    "rds.mys2.large":{
        "cpu":8,
        "memory":7200,
        "disk":102400,
        "max_connections":600
    },
    "rds.mys2.xlarge":{
        "cpu":9,
        "memory":12000,
        "disk":204800,
        "max_connections":1500
    },
    "rds.mys2.2xlarge":{
        "cpu":10,
        "memory":20000,
        "disk":512000,
        "max_connections":2000
    }
}
```

## 1.3.1.10.2 Access APIs

**This topic describes how to access APIs on the control side and the deployment side.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Operations > Machine Operations.**

3. **Select a project or enter the cluster name or machine name to search for the corresponding machine.**

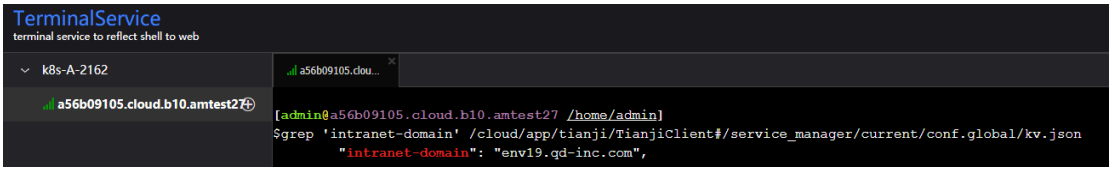
4. Access APIs.

   - Access an API on the control side

     a. Find the machine that you are about to access and then click Terminal in the Actions column to log on to the machine.

     b. In the command window, enter the following command and then press Enter to obtain the intranet-domain.

     ```
     grep 'intranet-domain' /cloud/app/tianji/TianjiClient#/
     service_manager/current/conf.global/kv.json
     ```

     c. You can log on to the API on the control side in the following ways. Here, take `ListInstance` as an example.

     - Get request

       ```
       curl 'xdb-master.xdb.{intranet-domain}:15678?
        Action=ListInstance'
       ```

     - Post request

       ```
       curl 'xdb-master.xdb.{intranet-domain}:15678' -X POST -d
        '{"Action":"ListInstance"}'
       ```

   - Access an API on the deployment side

     a. Find the machine that you are about to access and record the IP address in the Hostname column.

     b. You can log on to the API on the deployment side in the following ways. Here, take `CheckState` as an example.

     Assume that the IP address of the target machine is 127.0.0.1.

     - Get request

       ```
       curl '127.0.0.1:18765? Action=CheckState&Port=3606'
       ```

     - Post request

       ```
       curl '127.0.0.1:18765' -X POST -d '{"Action":"CheckState","
       Port":3606}'
       ```

## 1.3.1.10.3 APIs on the control side

### *1.3.1.10.3.1 DescribeInstance*

**Views instances.**

Description

**Views the detailed information of an instance.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: DescribeInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| InstanceID | Integer | Yes | The instance ID. |
| InstanceName | String | Yes | The instance name. |
| Domain | String | Yes | The domain name. |
| Port | Integer | Yes | The instance port. |
| PaxosPort | Integer | Yes | The communication port between instance nodes. |
| InstanceDir | String | Yes | The instance directory. |
| Level | String | Yes | The instance specifications. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Config | String | No | The custom my.cnf configuration of the instance, which is in the JSON format. |
| LeaderIP | String | No | The IP address of the primary node. |
| ActionName | String | Yes | The action name. |
| ActionStatus | String | Yes | The action status. |
| Description | String | Yes | The description. |
| IsDeleted | Integer | No | Whether the instance is deleted. 0 indicates No and 1 indicates Yes. |
| NodeList | []NodeInfo | Yes | The information of the instance nodes. |

**The structure of NodeInfo is as follows.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| InstanceID | Integer | Yes | The instance ID. |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the instance node. |
| NodeID | Integer | Yes | The ID of the instance node. |
| ActionName | String | Yes | The action name. |
| ActionStatus | String | Yes | The action status. |
| Description | String | Yes | The description. |
| IsDeleted | Integer | No | Whether the node is deleted. 0 indicates No and 1 indicates Yes. |

Examples

### Sample requests

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeInstance&
InstanceName=xdb-meta'
```

### Sample responses


```
{
    "Result": {
        "ActionName": "",
        "Level": "rds.mys2.standard",
        "InstanceID": 1,
        "LeaderIP": "10.39.XX.XX",
        "Config": "{}",
        "Description": "",
        "ActionStatus": "",
        "Domain": "xdb-meta.xdb.env8c-inc.com",
        "PaxosPort": 11606,
        "InstanceName": "xdb-meta",
        "User": "xdb",
        "Password": "xdb",
        "Port": 3606,
        "IsDeleted": 0,
        "InstanceDir": "/apsarapangu/disk1/xdb/xdb_instance_3606",
        "NodeList": [
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.38.XX.XX",
                "InstanceName": "xdb-meta",
                "NodeID": 1,
                "IsDeleted": 0
            },
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.39.XX.XX",
                "InstanceName": "xdb-meta",
                "NodeID": 2,
                "IsDeleted": 0
            },
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.39.145.20",
                "InstanceName": "xdb-meta",
                "NodeID": 3,
                "IsDeleted": 0
            }
        ]
    },
    "RequestID": "3CFCBA07-3D87-4A99-B8C1-E861A7D1A573"
```

```
}
```

### *1.3.1.10.3.2 ListInstance*

**Lists instances.**

Description

**Lists the basic information of instances.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: ListInstance |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
|---|---|---|---|
| InstanceNames | String | Yes | The list of instance names. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ListInstance'
```

**Sample responses**

```
{
    "Result": {
        "InstanceNames": [
            "xdb-meta",
            "xdb-instance-1",
            "xdb-instance-2",
            "xdb-instance-3"
        ]
    },
    "RequestID": "A921B8C7-C833-417C-B46A-E0CE129EBE48"
```

```
}
```

### 1.3.1.10.3.3 CreateInstance

**Creates an instance.**

Description

**Creates an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: CreateInstance |
| InstanceName | String | Yes | The instance name. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |
| Level | String | Yes | *Instance types* |
| Config | String | No | The custom my.cnf configuration of the instance, which is in the JSON format. The key must be the same as the value of the field in my.cnf, which is of the string type. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=CreateInstance&
InstanceName=xdb-instance-1&User=admin&password=xdb&Level=rds.mys2.
small'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "8BCB3B39-6140-459F-B283-F83C03ADC3CA"
}
```

### *1.3.1.10.3.4 DeleteInstance*

**Deletes an instance.**

Description

**Deletes an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: DeleteInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl '127.0.0.1:15678? Action=DeleteInstance&InstanceName=xdb-instance
-1'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "9C40CCB3-4FAB-4242-9B87-792E8154E5CD"
}
```

### *1.3.1.10.3.5 RestartInstance*

**Restarts an instance.**

Description

**Restarts an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: RestartInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=RestartInstance&
InstanceName=xdb-instance-2'
```

**Sample responses**

```
{
```

```
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "47277A23-5FFE-4A46-B65F-E6F2569F44E5"
}
```

### *1.3.1.10.3.6 UpgradeInstance*

**Performs a minor upgrade of an instance.**

Description

**Performs a minor upgrade of an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: UpgradeInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=UpgradeInstance&
InstanceName=xdb-instance-2'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "95E8B098-B04A-4BCA-BEBE-DA1D11BBAD4A"
```

```
}
```

### *1.3.1.10.3.7 DescribeTaskProgress*

**Views the task progress.**

Description

**Views the task progress.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value : DescribeTaskProgress |
| RequestID | String | Yes | The request ID. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Progress | String | Yes | The instance progress, including pending, doing, done, and failed. |
| Description | String | Yes | The description of the instance progress. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeTaskProgress&
RequestID=47277A23-5FFE-4A46-B65F-E6F2569F44E5'
```

**Sample responses**

```
{
    "Result": {
        "Progress": "done",
        "Description": "Success"
    },
    "RequestID": "AC535130-F40E-4D45-BC05-0F45C8473346"
}
```

## *1.3.1.10.3.8 ChangeLeaderTo*

**Changes the leader role of an instance to another node.**

Description

**Changes the leader role of an instance to another node.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: ChangeLeaderTo |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the machine where the new leader node is located. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ChangeLeaderTo&
InstanceName=xdb-instance-1&IP=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "37638DE5-14C1-4D2E-984F-FEA1F29C9F84"
}
```

## *1.3.1.10.3.9 ModifyInstanceLevel*

**Modifies the instance specifications.**

Description

**Modifies the instance specifications. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value : ModifyInstanceLevel |
| InstanceName | String | Yes | The instance name. |
| Level | String | Yes | The new instance specifications. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ModifyInstanceLevel&
InstanceName=xdb-instance-1&Level=rds.mys2.mid'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "21B91211-BB09-4665-835D-9471A6F07F24"
}
```

## *1.3.1.10.3.10 DescribeLeader*

**Views the primary node information of an instance.**

Description

**Views the primary node information of an instance.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: DescribeLeader |
| InstanceName | String | Yes | The instance name. |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| LeaderIP | String | Yes | The IP address of the primary node. |
| Port | Integer | Yes | The instance port. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeLeader&
InstanceName=xdb-meta'
```

**Sample responses**

```
{
    "Result": {
        "LeaderIP": "10.27.0.1",
        "Password": "xdb",
        "Port": 3606,
        "User": "xdb"
    },
    "RequestID": "2F05EE81-DC47-478E-9CA9-9AE8CA809151"
}
```

### *1.3.1.10.3.11 RecreateNode*

**Recreates an instance node.**

Description

**Uses other available nodes to recreate an instance node by backup and recovery. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: RecreateNode |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the instance node to be recreated. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=RecreateNode&
InstanceName=xdb-instance-1&IP=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "7F079E11-1DE9-4148-A9FA-683E4C58F9C2"
}
```

## *1.3.1.10.3.12 CreateDatabase*

**Creates a database and a user.**

Description

**Creates a database and a user.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: CreateDatabase |
| InstanceName | String | Yes | The instance name. |
| DBName | String | Yes | The database name. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=CreateDatabase&
InstanceName=xdb-instance-1&DBName=xdb&User=admin&Password=xdb_passwo
rd'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "A2BEF74F-5C3A-4CEF-A2B8-C14C71E36569"
}
```

## *1.3.1.10.3.13 DeleteDatabase*

**Deletes a database.**

Description

**Deletes a database.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: DeleteDatabase |
| InstanceName | String | Yes | The instance name. |
| DBName | String | Yes | The name of the database to be deleted. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DeleteDatabase&
InstanceName=xdb-instance-1&DBName=xdb'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "23F75A0A-B1D6-4341-BD5B-1A5F3FD45848"
}
```

## *1.3.1.10.3.14 DeleteUser*

**Deletes a user.**

Description

**Deletes a user.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: DeleteUser |
| InstanceName | String | Yes | The instance name. |
| User | String | Yes | The username. |
| Host | String | No | The source address range. If not configured, the user account is deleted in all of the source addresses by default. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DeleteUser&InstanceNa
me=xdb-instance-1&User=admin&Host=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "6A82AFF6-2B4D-48EF-868D-BBA54667D846"
}
```

## 1.3.1.10.4 APIs on the deployment side

### *1.3.1.10.4.1 CheckHealth*

**Checks if an instance node is of the leader role and whether the status is readable and writeable.**

Description

**Checks if an instance node is of the leader role. An instance node is regarded as healthy only if it is of the leader role and is readable and writeable.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `Action` | **String** | **Yes** | **The parameter specified by the system. Value: CheckHealth** |
| `Port` | **Integer** | **Yes** | **The port of the instance node.** |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `health` | **Boolean** | **Yes** | **The health status.** |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=CheckHealth&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "health": true
    },
    "RequestID": "304B69CE-1566-4E87-B618-233F40238FFF"
}
```

```
{
    "Message":"{\"health\": false}",
    "Code":"NodeNotHealth",
    "RequestID":"E939DB9B-4337-4B1C-8680-F62BEDD645DC"
}
```

### *1.3.1.10.4.2 CheckState*

**Checks whether the status of an instance node is normal.**

Description

**Checks whether the status of an instance node is normal. Generally, you have the following two situations:**

- **The node is of the leader role and is readable and writeable.**
- **The node is of the follower role and is readable.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: CheckState |
| Port | Integer | Yes | The port of the instance node. |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| IP | String | Yes | The IP address of the instance node. |
| Port | Integer | Yes | The instance port. |
| Role | String | Yes | The role of the instance node. |
| Writeable | String | Yes | Whether the instance node is writeable. |
| Readable | String | Yes | Whether the instance node is readable. |
| State | String | Yes | The status of the instance node. If the status is normal, the value is GOOD. Otherwise, the value is ERROR. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=CheckState&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "Readable": true,
        "State": "GOOD",
        "Role": "Follower",
        "Port": 3606,
        "IP": "10.39.145.10"
    },
    "RequestID": "45A59426-46D3-4709-8DD6-CD9F243336E0"
```

```
}
```

### 1.3.1.10.4.3 DescribeNodeStatus

**Views the status of an instance node.**

Description

**Views the status of an instance node. A leader node is readable and writeable, while a follower node is readable.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value : DescribeNodeStatus |
| Port | Integer | Yes | The port of the instance node. This parameter is required if the instance mode is single_machine. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| IP | String | Yes | The IP address of the instance node. |
| Port | Integer | Yes | The port of the instance node. |
| Role | String | Yes | The instance role. |
| Writeable | String | Yes | Whether the instance node is writeable. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Readable | String | Yes | Whether the instance node is readable. |
| ConnectionCount | Integer/String | Yes | The number of connections. If the retrieval fails, the value is unknown. |
| MaxConnectionCount | Integer/String | Yes | The maximum number of connections. If the retrieval fails, the value is unknown. |
| ConnectionPercent | Integer/String | Yes | The percentage of connections. If the retrieval fails, the value is unknown. |
| QPS | Integer/String | Yes | Queries per second (QPS). If the retrieval fails, the value is unknown. |
| CpuPercent | Integer/String | Yes | The CPU usage. If the retrieval fails, the value is unknown. |
| MemoryPercent | Integer/String | Yes | The memory usage. If the retrieval fails, the value is unknown. |
| DiskPercent | Integer/String | Yes | The disk usage. If the retrieval fails, the value is unknown. |
| State | String | Yes | The status of the instance node. If the status is normal, the value is GOOD. Otherwise, the value is ERROR. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=DescribeNodeStatus&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "CpuPercent": 2.74,
        "IP": "10.39.XX.XX",
        "Readable": true,
        "MemoryPercent": 56.13,
        "State": "GOOD",
        "Role": "Follower",
        "MaxConnectionCount": 500,
        "ActiveThreadCount": 34,
        "Writeable": false,
        "ConnectionCount": 37,
        "DiskPercent": 3.0,
        "ConnectionPercent": 7.4,
        "QPS": 15.95,
        "Port": 3606
    },
    "RequestID": "D18328B1-78A9-4F3E-BB2E-B27AB7683C19"
}
```

## *1.3.1.10.4.4 ListNode*

**Lists instance nodes.**

Description

**Lists the basic information of instance nodes.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: ListNode |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Nodes | String | Yes | The list of instance names. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=ListNode'
```

**Sample responses**

```
{
    "Result": {
        "Nodes": [
            "xdb-instance-1",
            "xdb-instance-2",
            "xdb-instance-3",
            "xdb-meta"
        ]
    },
    "RequestID": "3F7BB536-FA3F-4597-A3DF-E5830F5A3A21"
}
```

### *1.3.1.10.4.5 BackupNode*

**Backs up data of an instance node and transmits the data to a specified location (Use the nc command to transmit data to the port of a specified IP address).**

Description

**Backs up data of an instance node and transmits the data to a specified location.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: BackupNode |
| Port | Integer | Yes | The instance port. |
| TargetIP | String | Yes | The IP address of the target location. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| TargetPort | Integer | Yes | The port of the target location. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=BackupNode&Port=3606&TargetIP=10.39.XX.
XX&TargetPort='
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "6A82AFF6-2B4D-48EF-868D-BBA54667D846"
}
```

## 1.3.1.11 Appendix

### 1.3.1.11.1 IP list

**This report displays the IP addresses of physical machines and Docker applications.**

IP List of Physical Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The hostname of the machine. |
| IP | The IP address of the machine. |

IP List of Docker Applications

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The hostname of the machine. |

| Item | Description |
| --- | --- |
| Docker Host | The Docker hostname. |
| Docker IP | The Docker IP address. |

## 1.3.1.11.2 Project component info report

**This report displays the name and status for each type of project components, including services, server roles, and machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The name of a cluster in the project. |
| Service | The name of a service in the cluster. |
| Server Role | The name of a server role in the service. |
| Server Role Status | The running status of the server role on the machine. |
| Server Role Action | The action that the server role performs on the machine. Data is available only when Apsara Infrastructure Management Framework asks the server role to perform certain actions, such as rolling and restart actions. |
| Machine Name | The hostname of the machine. |
| IP | The IP address of the machine. |
| Machine Status | The running status of the machine. |
| Machine Action | The action that Apsara Infrastructure Management Framework asks the machine to perform, such as the clone action. |

## 1.3.1.11.3 Machine info report

**This report displays the statuses of machines and server roles on the machines.**

Machine Status

**Displays all the machines currently managed by Apsara Infrastructure Management Framework and their corresponding statuses. In the Global Filter section at the top of the page, select the project, cluster, and machine from the project, cluster, and machine drop-down lists, and then click Filter on the right to filter the data.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |

| Item | Description |
| --- | --- |
| IP | The IP address of the machine. |
| Machine Status | The machine status. |
| Machine Action | The action currently performed by the machine. |
| Machine Action Status | The action status. |
| Status Description | The description about the machine status. |

Expected Server Role List

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The name of the expected server role on the machine. |

Abnormal Monitoring Status

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Monitored Item | The name of the monitored item. |
| Level | The level of the monitored item. |
| Description | The description of the monitored item contents. |
| Updated At | The updated time of the monitored item. |

Server Role Version and Status on Machine

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The server role name. |

| Item | Description |
| --- | --- |
| Server Role Status | The status of the server role. |
| Target Version | The expected version of the server role on the machine. |
| Current Version | The current version of the server role on the machine. |
| Status Description | The description about the status. |
| Error Message | The exception message of the server role. |

Monitoring Status

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The server role name. |
| Monitored Item | The name of the monitored item. |
| Level | The level of the monitored item. |
| Description | The description of the monitored item contents. |
| Updated At | The updated time of the monitored item. |

## 1.3.1.11.4 Rolling info report

**This report displays the running and completed rolling tasks and the task-related status.**

Choose a rolling action

**This list only displays the running rolling tasks. If no rolling task is running, no data is available in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Git Version | The version of change that triggers the rolling task. |
| Description | The description about the change entered by a user when the user submits the change. |
| Start Time | The start time of the rolling task. |

| Item | Description |
| --- | --- |
| End Time | The end time of the rolling task. |
| Submitted By | The ID of the user who submits the change. |
| Rolling Task Status | The current status of the rolling task. |
| Submitted At | The time when the change is submitted. |

Server Role in Job

**Select a rolling task in the Choose a rolling action section to display the rolling status of server roles related to the selected task. If no rolling task is selected, the server role statuses of all historical rolling tasks are displayed.**

| Item | Description |
| --- | --- |
| Server Role | The server role name. |
| Server Role Status | The rolling status of the server role. |
| Error Message | The exception message of the rolling task. |
| Git Version | The version of change to which the rolling task belongs. |
| Start Time | The start time of the rolling task. |
| End Time | The end time of the rolling task. |
| Approve Rate | The proportion of machines that have the rolling task approved by the decider. |
| Failure Rate | The proportion of machines that have the rolling task failed. |
| Success Rate | The proportion of machines that have the rolling task succeeded. |

Server Role Rolling Build Information

**The source version and target version of each application under the server role in the rolling process.**

| Item | Description |
| --- | --- |
| App | The name of the application that requires rolling in the server role. |

| Item | Description |
| --- | --- |
| Server Role | The server role to which the application belongs. |
| From Build | The version before the upgrade. |
| To Build | The version after the upgrade. |

Server Role Statuses on Machines

**Select a server role in the Server Role in Job section to display the deployment status of this server role on the machine.**

| Item | Description |
| --- | --- |
| Machine Name | The name of the machine on which the server role is deployed. |
| Expected Version | The target version of the rolling. |
| Actual Version | The current version. |
| State | The status of the server role. |
| Action Name | The Apsara Infrastructure Management Framework action currently performed by the server role. |
| Action Status | The action status. |

## 1.3.1.11.5 Machine RMA approval pending list

**Some Apsara Infrastructure Management Framework actions (such as restart) on machines and server roles can be triggered by users, but this type of actions must be reviewed and approved. This report is used to process the actions that must be reviewed and approved.**

Machine

**Displays the basic information of pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| IP | The IP address of the machine. |

| Item | Description |
| --- | --- |
| State | The running status of the machine. |
| Action Name | The action on the machine. |
| Action Status | The status of the action on the machine. |
| Actions | The approval button. |

Machine Serverrole

**Displays the information of server roles on the pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| IP | The IP address of the machine. |
| Serverrole | The server role name. |
| State | The running status of the server role. |
| Action Name | The action on the server role. |
| Action Status | The status of the action on the server role. |
| Actions | The approval button. |

Machine Component

**Displays the hard disk information of pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| Component | The hard disk on the machine. |
| State | The running status of the hard disk. |
| Action Name | The action on the hard disk. |
| Action Status | The status of the action on the hard disk. |
| Actions | The approval button. |

### 1.3.1.11.6 Registration vars of services

**This report displays values of all service registration variables.**

| Item | Description |
|---|---|
| Service | The service name. |
| Service Registration | The service registration variable. |
| Cluster | The cluster name. |
| Update Time | The updated time. |

### 1.3.1.11.7 Virtual machine mappings

**Use the global filter to display the virtual machines of a specific cluster.**

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

| Item | Description |
|---|---|
| Project | The project name. |
| Cluster | The cluster name. |
| VM | The hostname of the virtual machine. |
| Currently Deployed On | The hostname of the physical machine on which the virtual machine is currently deployed. |
| Target Deployed On | The hostname of the physical machine on which the virtual machine is expected to be deployed. |

### 1.3.1.11.8 Service inspector report

**Use the global filter to display the service inspection reports of a specific cluster.**

**Service Inspector: Data is available only for services with inspection configured.**

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

## 1.3.1.11.9 Resource application report

**In the Global Filter section, select the project, cluster, and machine from the project, cluster, and machine drop-down lists and then click Filter on the right to display the corresponding resource application data.**

Change Mappings

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Version | The version where the change occurs. |
| Resource Process Status | The resource application status in the version. |
| Msg | The exception message. |
| Begintime | The start time of the change analysis. |
| Endtime | The end time of the change analysis. |

Changed Resource List

| Item | Description |
| --- | --- |
| Res | The resource ID. |
| Type | The resource type. |
| Name | The resource name. |
| Owner | The application to which the resource belongs. |
| Parameters | The resource parameters. |
| Ins | The resource instance name. |
| Instance ID | The resource instance ID. |

Resource Status

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| APP | The application of the server role. |

| Item | Description |
| --- | --- |
| Name | The resource name. |
| Type | The resource type. |
| Status | The resource application status. |
| Parameters | The resource parameters. |
| Result | The resource application result. |
| Res | The resource ID. |
| Reprocess Status | The status of the interaction with Business Foundation System during the VIP resource application. |
| Reprocess Msg | The error message of the interaction with Business Foundation System during the VIP resource application. |
| Reprocess Result | The result of the interaction with Business Foundation System during the VIP resource application. |
| Refer Version List | The version that uses the resource. |
| Error Msg | The exception message. |

## 1.3.1.11.10 Statuses of project components

**This report displays the status of all server roles in an abnormal status on machines of the project, and the monitoring information (alert information reported by the server role to Apsara Infrastructure Management Framework monitor) of server roles and machines.**

Error State Component Table

**Only displays the information of server roles that are not in GOOD status and server roles to be upgraded.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Need Upgrade | Whether the current version reaches the final status. |

| Item | Description |
| --- | --- |
| Server Role Status | The current status of the server role. |
| Machine Status | The current status of the machine. |

Server Role Alert Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

Machine Alert Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

Service Inspector Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

## 1.3.1.11.11 Relationship of service dependency

**This report displays the dependencies among server roles. Use the global filter to display the data of a specific cluster in the list.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Dependent Service | The service on which the server role depends. |
| Dependent Server Role | The server role on which the server role depends. |
| Dependent Cluster | The cluster to which the dependent server role belongs. |
| Dependency in Final Status | Whether the dependent server role reaches the final status. |

## 1.3.1.11.12 Check report of network topology

**This report checks if network devices and machines have wirecheck alerts.**

Check Report of Network Topology

**Checks if network devices have wirecheck alerts.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Network Instance | The name of the network device. |

| Item | Description |
| --- | --- |
| Level | The alert level. |
| Description | The description about the alert information. |

Check Report of Server Topology

**Checks if servers (machines) have wirecheck alerts.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The server (machine) name. |
| Level | The alert level. |
| Description | The description about the alert information. |

## 1.3.1.11.13 Clone report of machines

**This report displays the clone progress and status of machines.**

Clone Progress of Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Machine Status | The running status of the machine. |
| Clone Progress | The progress of the current clone process. |

Clone Status of Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Machine Action | The action performed by the machine, such as the clone action. |
| Machine Action Status | The status of the action performed by the machine. |
| Machine Status | The running status of the machine. |

| Item | Description |
| --- | --- |
| Level | Whether the clone action performed by the machine is normal. |
| Clone Status | The current status of the clone action performed by the machine. |

## 1.3.1.11.14 Auto healing/install approval pending report

**The list structure is the same as the machine RMA approval pending list, whereas this view is used for the approval during the installation. For more information, see** *Machine RMA approval pending list*.

## 1.3.1.11.15 Machine power on or off statuses of clusters

**After a cluster starts or shuts down machines, you can view the related information in this report.**

Cluster Running Statuses

**If a cluster is starting or shutting down machines, the corresponding data is available in this list. No data indicates that no cluster has machines shut down.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Action Name | The startup or shutdown action that is being performed by the cluster. |
| Action Status | The status of the action. |

Server Role Power On or Off Statuses

**Displays the power on or off statuses of server roles in the cluster selected in the Cluster Running Statuses section.**

**Select a row in the Cluster Running Statuses section to display the information of the corresponding cluster in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Server Role | The server role name. |
| Action Name | The startup or shutdown action that is being performed by the server role. |
| Action Status | The status of the action. |

Statuses on Machines

**Displays the running status of the selected server role on machines.**

**Select a row in the Server Role Power On or Off Statuses section to display the information of the corresponding server role in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Server Role Status | The running status of the server role. |
| Server Role Action | The action currently performed by the server role. |
| Server Role Action Status | The status of the action. |
| Error Message | The exception message. |

Machine Statuses

**Displays the running statuses of machines in the selected cluster.**

**Select a row in the Statuses on Machines section to display the information of the corresponding machine in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| IP | The IP address of the machine. |
| Machine Status | The running status of the machine. |
| Machine Action | The action currently performed by the machine. |
| Machine Action Status | The action status of the machine. |
| Error Message | The exception message. |

## 1.3.2 New version

# 1.3.2.1 What is Apsara Infrastructure Management Framework?

**This topic describes what Apsara Infrastructure Management Framework is from the aspects of core functions and basic concepts.**

## 1.3.2.1.1 Introduction

**Apsara Infrastructure Management Framework is a distributed data center management system, which manages applications on clusters containing multiple machines and provides the basic functions such as deployment, upgrade, expansion, contraction, and configuration changes.**

### Overview

**Apsara Infrastructure Management Framework also supports monitoring data and analyzing reports, which facilitates users to perform one-stop Operation & Maintenance (O&M) control. Based on the Apsara Infrastructure Management Framework services, automated O&M is implemented in the large-scale distributed environment, which greatly improves the operations efficiency and enhances the system availability.**

**Apsara Infrastructure Management Framework is mainly composed of TianjiMaster and TianjiClient. Apsara Infrastructure Management Framework installs TianjiClient as the agent on machines it manages. Then, TianjiMaster accepts and issues the upper-layer instructions to TianjiClient for execution. In the upper layer, Apsara Infrastructure Management Framework is divided into different components based on different functions, and then provides API server and portal for external use.**

### Core functions

- **Network initialization in data centers**
- **Server installation and maintenance process management**
- **Deployment, expansion, and upgrade of cloud products**
- **Configuration management of cloud products**
- **Automatic application for cloud product resources**
- **Automatic repair of software and hardware faults**
- **Basic monitoring and business monitoring of software and hardware**

#### 1.3.2.1.2 Basic concepts

**Before using Apsara Infrastructure Management Framework, you must know the following basic concepts for a better understanding.**

project

**A collection of clusters, which provides service capabilities for external entities.**

cluster

**A collection of physical machines, which logically provides services and is used to deploy project software.**

- **A cluster can only belong to one project.**
- **Multiple services can be deployed on a cluster.**

service

**A set of software, which provides relatively independent functions. A service is composed of one or more server roles and can be deployed on multiple clusters to form multiple sets of services and provide the corresponding service capabilities. For example, Apsara Distributed File System, Job Scheduler, and Apsara Name Service and Distributed Lock Synchronization System are all services.**

service instance

**A service that is deployed on a cluster.**

server role

**One or more indivisible deployment units into which a service can be divided based on functions. A server role is composed of one or more specific applications. If a service is deployed on a cluster, all the server roles of the service must be deployed to machines of this cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same server.**

server role instance

**A server role that is deployed on a machine. A server role can be deployed on multiple machines.**

application

**Applications correspond to each process-level service component in a server role and each application works independently. The application is the minimum unit for deployment and upgrade in Apsara Infrastructure Management Framework,**

**and can be deployed to each machine. Generally, an application is an executable software or Docker container.**

**If a server role is deployed on a machine, all applications in the server role must be deployed to this machine.**

rolling

**Each time when a user updates configurations, Apsara Infrastructure Management Framework upgrades services and modifies the cluster configurations based on the updated configurations. This process is called rolling.**

service configuration template

**Some configurations are the same when services are deployed on clusters. A service configuration template can be created to quickly write the same configurations to different clusters. The service configuration template is basically used for large-scale deployment and upgrade.**

associated service template

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

desired state

**If a cluster is in this state, all hardware and software on each of its machines are normal and all software are in the target version.**

dependency

**The dependency between server roles in a service defines that server roles with dependencies run tasks or are upgraded based on the dependency order. For example, if A depends on B, B is upgraded first. A starts to be downloaded after B is downloaded successfully, and upgraded after B is successfully upgraded. (By default, the dependency does not take effect for configuration upgrade.)**

upgrade

**A way of aligning the current state with the desired state of a service. After a user submits the version change, Apsara Infrastructure Management Framework upgrades the service version to the target version. With the server role as the**

**processing unit, upgrade aims to update the versions of all machines to the target version.**

**At the beginning, the desired state and current state of the cluster are the same. When a user submits the change, the desired state is changed, whereas the current state is not. A rolling task is generated and has the desired state as the target version. During the upgrade, the current state is continuously approximating to the desired state. Finally, the desired state and the current state are the same when the upgrade is finished.**

### 1.3.2.2 Log on to Apsara Infrastructure Management Framework

**This topic describes how to log on to Apsara Infrastructure Management Framework.**

**Prerequisites**

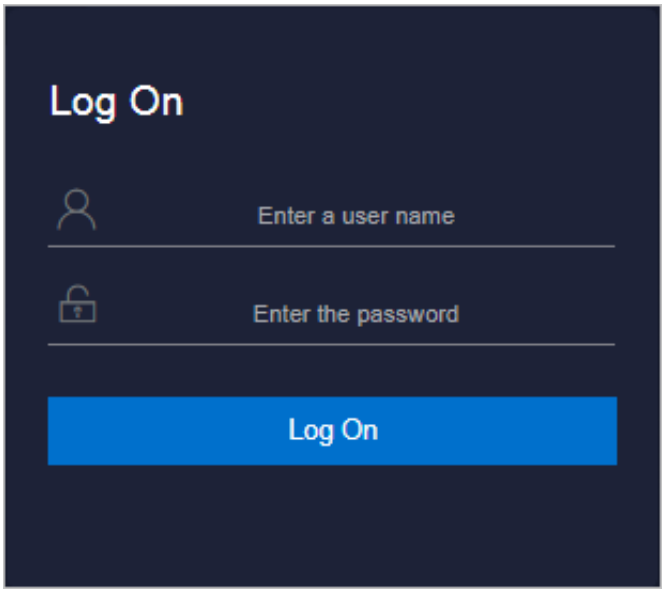
- **ASO access address in the format of http://***region-id***.aso.***intranet-domain-id***.com.**
- **Google Chrome browser (recommended).**

**Procedure**

1. **Open the browser.**

2. **Enter the ASO access address http://*region-id*.aso.*intranet-domain-id*.com in the address bar and then press Enter.**

   Figure 1-6: Log on to ASO




   **Note:**
   **You can select the language from the drop-down list in the upper-right corner to change the language of ASO.**

3. **Enter the correct username and password.**
   - **The system has three default users:**
     - **Security officer: manages other users or roles.**
     - **Auditor officer: views audit logs.**
     - **System administrator: used for other functions except those of the security officer and auditor officer.**
   - **You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.**
4. **Click Log On to log on to ASO.**
5. **In the left-side navigation pane, select Products.**

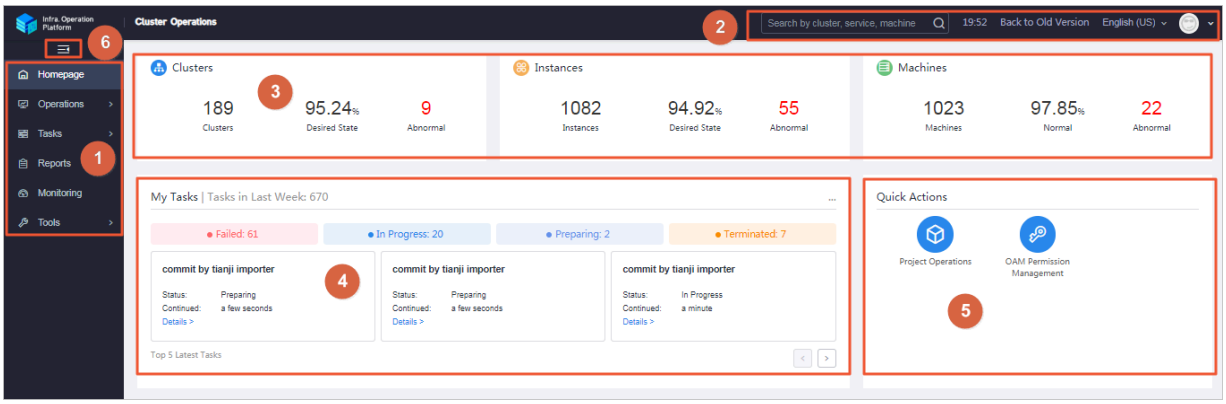
6. In the Product List, select Apsara Infrastructure Management Framework.

## 1.3.2.3 Homepage introduction

After you log on to Apsara Infrastructure Management Framework, the homepage appears. This topic allows you to get a general understanding of the basic operations and functions of Apsara Infrastructure Management Framework.

*Log on to Apsara Infrastructure Management Framework*. The homepage appears, as shown in the following figure.

Figure 1-7: Homepage of Apsara Infrastructure Management Framework




For more information about the descriptions of functional areas on the homepage, see the following table.

Table 1-8: Descriptions of functional areas

| Area | | Description |
| --- | --- | --- |
| 1 | Left-side navigation pane | · Operations: the quick entrance of Operation & Maintenance (O&M) operations, which allows operations engineers to quickly find the corresponding operations and operation objects. This menu consists of the following sections:<br>- Project Operations: manages projects with the project permissions.<br>- Cluster Operations: performs O&M operations on and manages clusters with the project permissions, such as viewing the cluster status.<br>- Service Operations: manages services with the service permissions, such as viewing the service list information.<br>- Machine Operations: maintains and manages all the machines in Apsara Infrastructure Management Framework, such as viewing the machine status.<br>· Tasks: A rolling task is generated after you modify the configurations in the system. In this menu, you can view running tasks, history tasks, and the deployment summary of clusters, services, and server roles in all projects.<br>· Reports: displays the monitoring data in tables and provides the function of searching for different reports.<br>· Monitoring: effectively monitors metrics in the process of system operation and sends alert notifications for abnormal conditions. This menu includes the functions of displaying alert status, modifying alert rules, and searching for the alert history.<br>· Tools: provides the machine tools and the IDC shutdown function. |

| Area | | Description |
| --- | --- | --- |
| 2 | Function buttons in the upper-right corner | · Search box: Supports global search. Enter a keyword in the search box to search for clusters, services, and machines.<br>· Move the pointer over the time and then you can view:<br>- TJDB Sync Time: the generated time of the data that is displayed on the current page.<br>- Desired State Calc Time: the calculation time of the desired-state data that is displayed on the current page.<br>After data is generated, the system processes the data at maximum speed. As an asynchronous system, Apsara Infrastructure Management Framework has some latency. The time helps explain why the current data results are generated and determine whether the current system has a problem.<br>· English (US): In the English environment, click this drop-down list to switch to another language.<br>· Click the avatar of the logon user and then select Exit to log out of Apsara Infrastructure Management Framework. |
| 3 | Status section of global resources | Displays the overview of global resources.<br>· Clusters: displays the total number of clusters, the percentage of clusters that reach the desired state, and the number of abnormal clusters.<br>· Instances: displays the total number of instances, the percentage of instances that reach the desired state, and the number of abnormal instances.<br>· Machines: displays the total number of machines, the percentage of machines with the Normal state, and the number of abnormal machines.<br>Move the pointer over the section and then click Show Detail to go to the Cluster Operations page, Service Operations page, or Machine Operations page. |

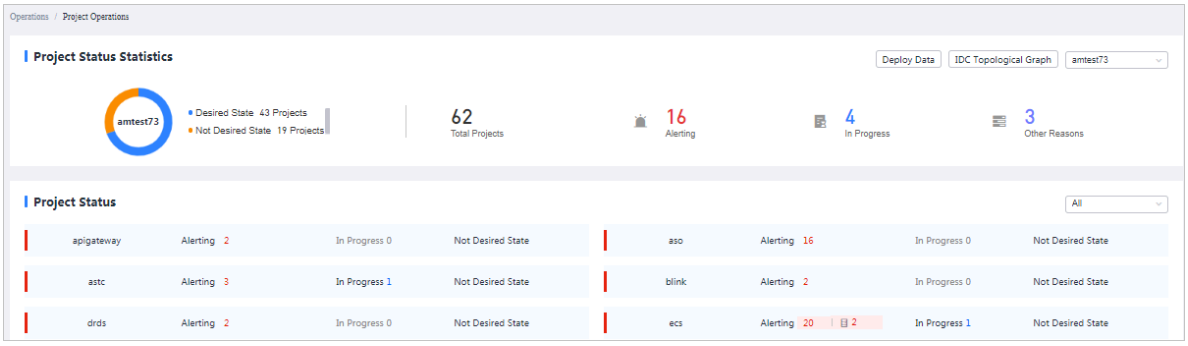
| Area | | Description |
| --- | --- | --- |
| 4 | Task status section | Displays the information of tasks submitted in the last week. Click the number at the right of a task status to go to the My Tasks page and then view tasks of the corresponding status.<br>The top 5 latest tasks are displayed at the bottom of this section and you can click Details to view the task details. |
| 5 | Quick actions | Displays links of common quick actions, which allows you to perform operations quickly. |
| 6 | Expand/ collapse button | If you are not required to use the left-side navigation pane when performing O&M operations, click this button to collapse the left-side navigation pane and increase the space of the content area. |

## 1.3.2.4 Project operations

**The Project Operations module allows you to search for and view details of a project.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Operations > Project Operations.**




3. **On this page, you can:**
   - **Search for a project**

     **Click the drop-down list in the upper-right corner of the Project Status section. Enter a project name in the search box, and then select the name to**

search for the project. You can view the numbers of alerts and running tasks for the project and whether the project reaches the desired state.

- View the details of a project
  - Find the project whose details you are about to view. Click the number at the right of Alerting. In the displayed Alert Information dialog box, view the specific monitoring metrics, monitoring types, and alert sources. Click the value in the Alert Source column to view the service details.
  - Find the project whose details you are about to view. Click the number at the right of In Progress. In the displayed Tasks dialog box, view the details of Upgrade Service and Machine Change.

## 1.3.2.5 Cluster operations

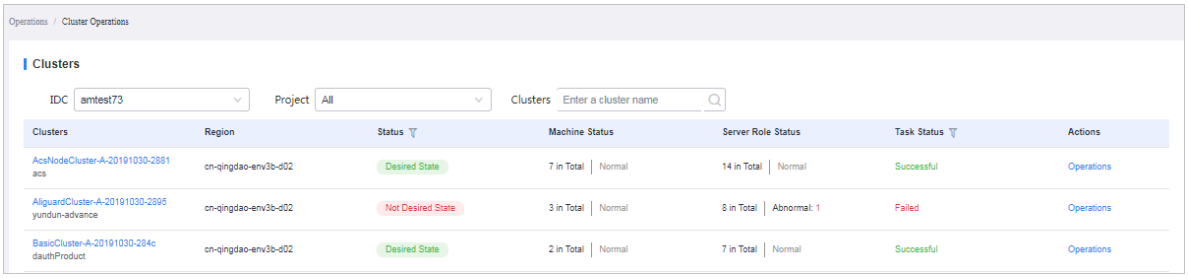
This topic describes the actions about cluster operations.

### 1.3.2.5.1 View the cluster list

The cluster list allows you to view all of the clusters and the corresponding information.

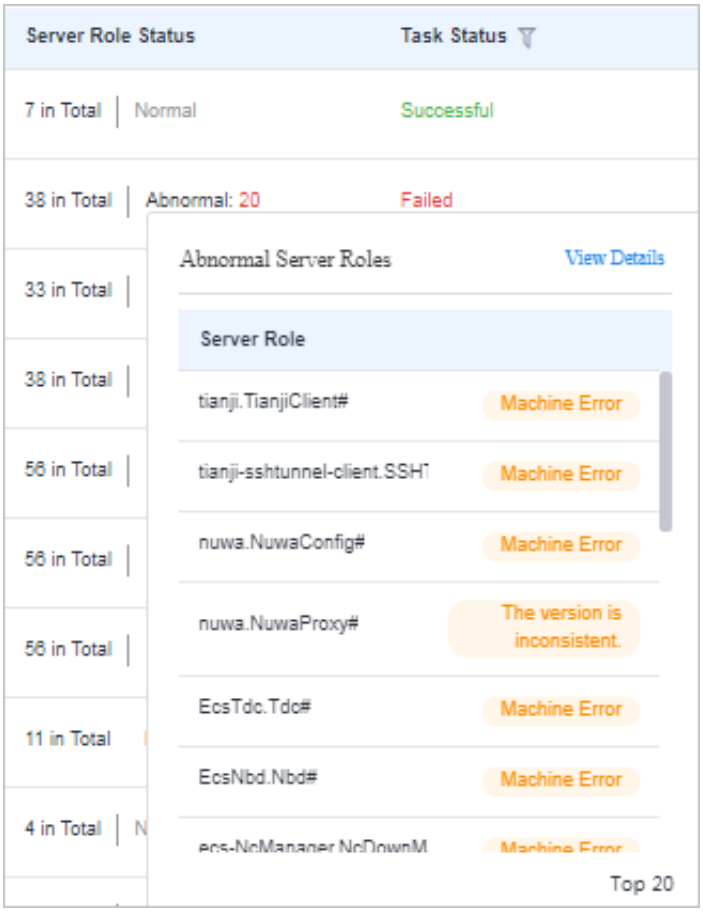
**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. To view the cluster list, you can:
   - On the Homepage, move the pointer over the Clusters section and then click Show Detail in the upper-right corner.
   - In the left-side navigation pane, choose Operations > Cluster Operations.




On this page, you can view the following information.

| Item | Description |
| --- | --- |
| Clusters | The cluster name. Click the cluster name to view the cluster details. |
| Region | The name of the region where the cluster is located. |

| Item | Description |
| --- | --- |
| Status | Indicates whether the cluster reaches the desired state. Use  to filter the clusters.<br>· Desired State: All the clusters of a project reach the desired state.<br>· Not Desired State: After a project reaches the desired state for the first time, a server role does not reach the desired state because of undefined reasons. |
| Machine Status | The number of machines and the corresponding status in the cluster. Click the status to go to the Machines tab of the Cluster Details page. |
| Server Role Status | The number of server roles and the corresponding status in the cluster. Click the status to go to the Services tab of the Cluster Details page. Click Abnormal in the Server Role Status column to view all the abnormal server roles in the cluster in the displayed dialog box. Click View Details in the upper-right corner of the dialog box to go to the Services tab of the Cluster Details page.<br>  |

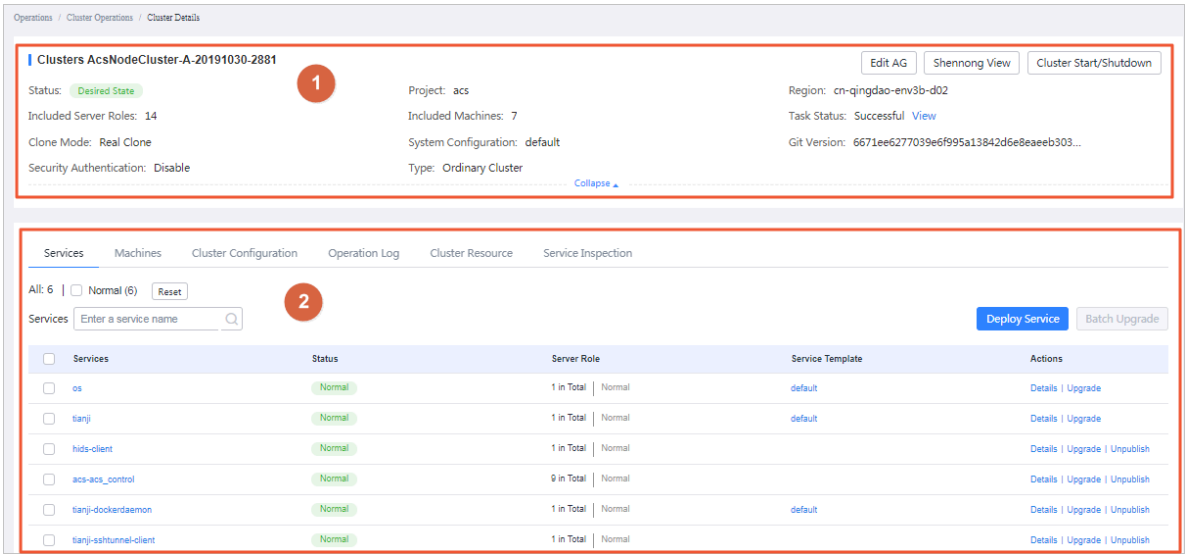
| Item | Description |
| --- | --- |
| Task Status | The status of the task submitted to the cluster. Use to filter the clusters. Click the status to view the task details. |

### 1.3.2.5.2 View the cluster details

**You can view the cluster statistics by viewing the cluster details.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Operations > Cluster Operations.
3. Select a project from the Project drop-down list or enter the cluster name in the Clusters field to search for the corresponding cluster.
4. Find the cluster whose configurations you are about to view. Click the cluster name or Operations in the Actions column at the right of the cluster to go to the Cluster Details page.




| Area | Item | Description |
| --- | --- | --- |
| 1 | Status | · Desired State: All the clusters of this project reach the desired state.<br>· Not Desired State: After the project reaches the desired state for the first time, a server role does not reach the desired state because of undefined reasons. |
| | Project | The project to which the cluster belongs. |
| | Region | The region to which the cluster belongs. |

| Area | Item | Description |
| --- | --- | --- |
| | Included Server Roles | The number of server roles included in the cluster. |
| | Included Machines | The number of machines included in the cluster. |
| | Task Status | The status of the current task. Click View to view the task details.<br>· Successful: indicates the task is successful.<br>· Preparing: indicates data is being synchronized and the task is not started yet.<br>· In Progress: indicates the cluster has a changing task.<br>· Paused: indicates the task is paused<br>· Failed: indicates the task failed.<br>· Terminated: indicates the task is manually terminated. |
| | Clone Mode | · Mock Clone: The system is not cloned when a machine is added to the cluster.<br>· Real Clone: The system is cloned when a machine is added to the cluster. |
| | System Configuration | The name of the system service template used by the cluster. |
| | Git Version | The change version to which the cluster belongs. |
| | Security Authentication | The access control among processes. Generally , the non-production environment uses the default configurations and does not perform the verification. In other cases, customize the configurations based on actual requirements to enable or disable the verification. |

| Area | Item | Description |
| --- | --- | --- |
| | Type | · Ordinary Cluster: an operations unit facing to machine groups, where multiple services can be deployed.<br>· Virtual Cluster: an operations unit facing to services, which can centrally manage software versions of machines of multiple physical clusters.<br>· RDS: a type of cluster that renders special cgroup configurations according to a certain rule.<br>· NETFRAME: a type of cluster that renders special configurations for the special scenario of Server Load Balancer (SLB).<br>· T4: a type of cluster that renders special configurations for the mixed deployment of e-commerce.<br>Currently, Alibaba Cloud Apsara Stack only has ordinary clusters. |
| 2 | Services | View the statuses of all the services in this cluster. You can also upgrade or unpublish a service.<br>· Normal: The service works properly.<br>· Not Deployed: No machine is deployed on the service.<br>· Changing: Some server roles in the service are changing.<br>· Operating: No server role is changing, but the machine where server roles are installed is performing the Operation and Maintenance (O&M) operations.<br>· Abnormal: No server role is changing or the machine where server roles are installed is not performing the O&M operations, but the server role status is not GOOD or the version that the service runs on the machine and the version configured in the configurations are different. |

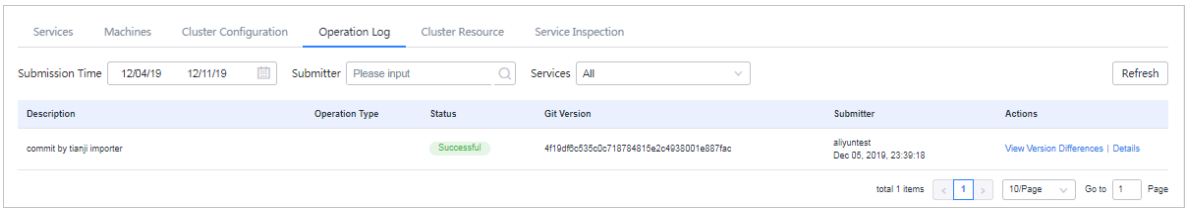
| Area | Item | Description |
| --- | --- | --- |
| | Machines | View the running statuses and monitoring statuses of all the machines in this cluster. You can also view the details of server roles to which the machine belongs. |
| | Cluster Configuration | The configuration file used in the cluster. |
| | Operation Log | View the version differences. |
| | Cluster Resource | Filter the resource whose details you are about to view according to certain conditions. |
| | Service Inspection | View the inspection information of each service in the cluster. |

## 1.3.2.5.3 View operation logs

**By viewing operation logs, you can obtain the differences between Git versions.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. To view the operation logs of a cluster, you can:
   - Enter a cluster name in the search box in the upper-right corner of the page. Click Operations at the right of the cluster to go to the Cluster Details page. Click the Operation Log tab.
   - In the left-side navigation pane, choose Operations > Cluster Operations. On the Cluster Operations page, click Operations in the Actions column at the right of a cluster to go to the Cluster Details page. Click the Operation Log tab.




3. On the Operation Log tab, view the version differences.
   a) Click View Version Differences in the Actions column at the right of a log.
   b) On the Version Differences page, select a basic version from the Versus drop-down list. Then, the contents of the different file are automatically displayed.
   c) Select each different file from the Different File drop-down list to view the detailed differences.

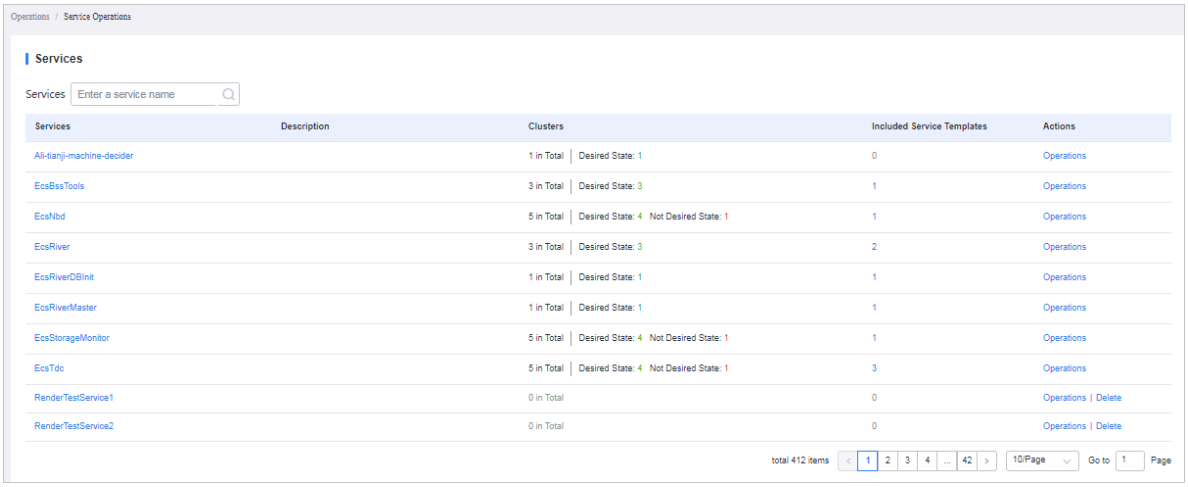
# 1.3.2.6 Service operations

## 1.3.2.6.1 View the service list

**The service list allows you to view all of the services and the corresponding information.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. To view the service list, you can:
   - On the Homepage, move the pointer over the Instances section and then click Show Detail in the upper-right corner.
   - In the left-side navigation pane, choose Operations > Service Operations.




On this page, you can view the following information.

| Item | Description |
| --- | --- |
| Services | The service name. Click the service name to view the service details. |
| Clusters | The number of clusters where the service is located and the corresponding cluster status. |
| Included Service Templates | The number of service templates this service includes. |
| Actions | Click Operations to go to the Service Details page. |

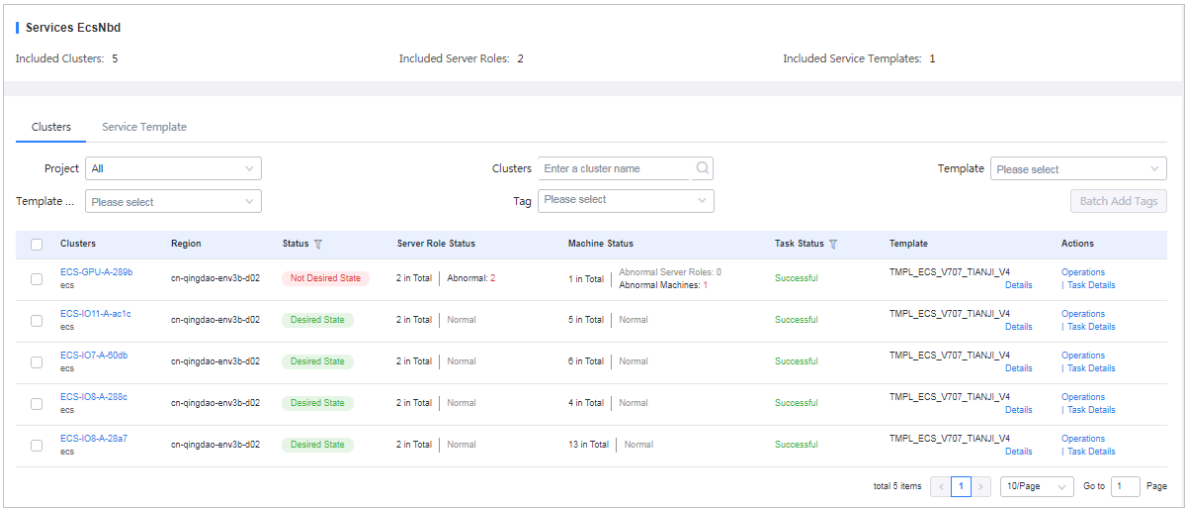
3. Enter a service name in the search box and then the service that meets the condition is displayed in the list.

# 1.3.2.6.2 View the server role details

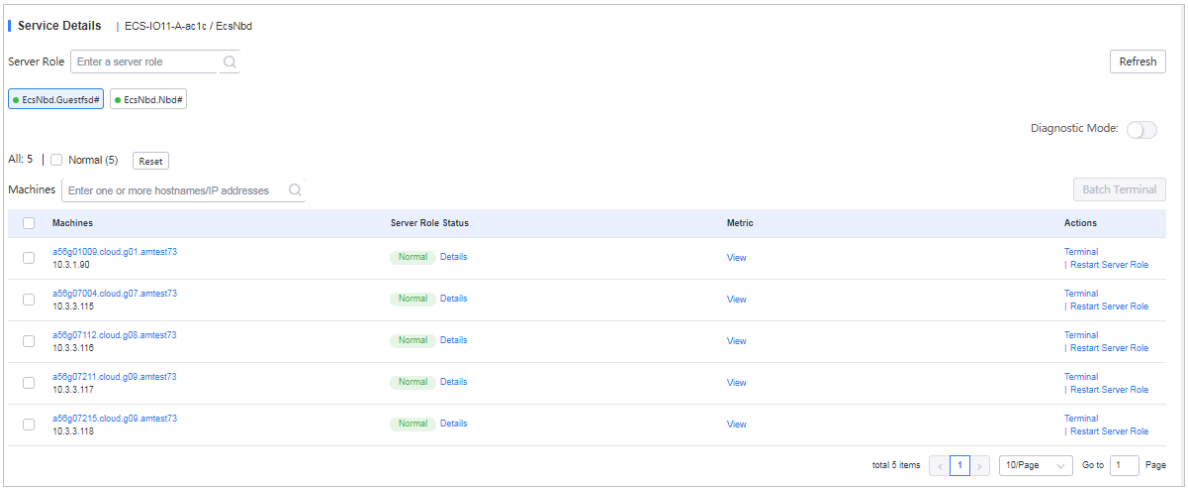
**You can view the server role statistics by viewing the server role details.**

## Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Operations > Service Operations.**
3. **Enter a service name in the search box and then the service that meets the condition is displayed in the list.**
4. **Click the service name or click Operations in the Actions column.**




5. **On the Clusters tab, click the status in the Server Role Status column to view the server roles included in a cluster.**



6. Enter a keyword in the search box to search for a server role. Then, the details of the corresponding server role are displayed in the list.

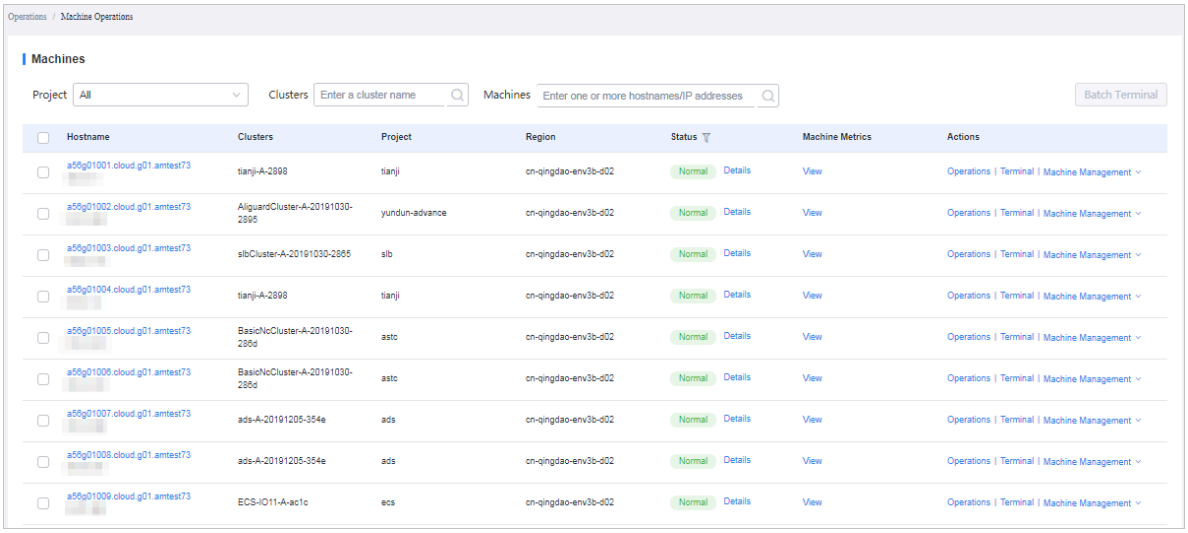
| Item | Description |
| --- | --- |
| Machines | The machine to which the server role belongs. Click the machine name to view the machine details. |
| Server Role Status | The status of the server role. Click Details to view the basic information, application version information, application process information, and resources of the server role. |
| Metric | Click View to view the statuses of server role metrics and machine metrics. |
| Actions | · Click Terminal to log on to the machine and perform operations.<br>· Click Restart Server Role to restart the server role. |

## 1.3.2.7 Machine operations

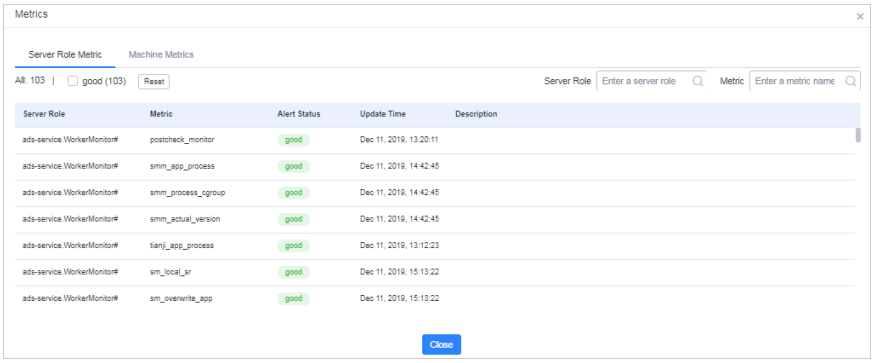
**You can view the machine statistics by viewing the machine list.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. To view the machine list, you can:
   - On the Homepage, move the pointer over the Machines section and then click Show Detail in the upper-right corner.
   - In the left-side navigation pane, choose Operations > Machine Operations.



3. Select a project or enter the cluster name or machine name to search for the corresponding machine.

| Item | Description |
| --- | --- |
| Hostname | Click the hostname to go to the Machine Details page. |
| Status | The current status of the machine. Use  to filter the machines. Click Details and then the Status Details of Machine dialog box appears. |
| Machine Metrics | Click View and then the Metrics dialog box appears.<br>  <br>The Server Role Metric tab and Machine Metrics tab display the corresponding metrics, and you can view the specific alert status and updated time.<br>Enter a keyword in the search box in the upper-right corner to search for a server role or metric. You can also select the status to filter metrics. |
| Actions | · Click Operations to go to the Machine Details page.<br>· Click Terminal to log on to the machine and perform operations. You can select multiple machines and then click Batch Terminal in the upper-right corner to log on to multiple machines at a time.<br>· Click Machine Management to perform an out-of-band restart operation on the machine. |

## 1.3.2.8 Monitoring center

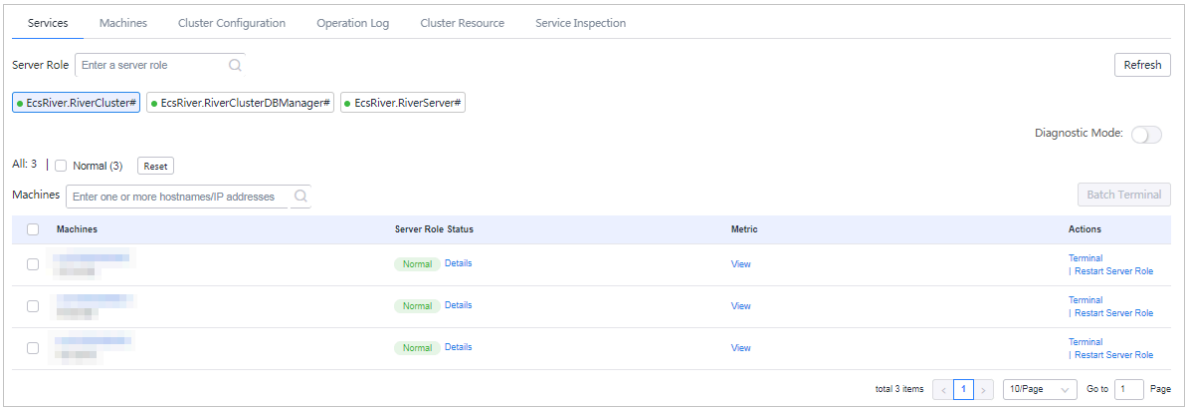
You can view the alert status, alert rules, and alert history in the monitoring center.

### 1.3.2.8.1 View the monitoring instance status

You can view the status of a monitoring instance after it is deployed.

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Operations > Service Operations.
3. Enter a service name in the search box to search for the corresponding service.
4. Click Operations in the Actions column at the right of the service.
5. On the Clusters tab, configure the conditions and then search for the cluster. Click Operations in the Actions column.
6. On the Cluster Details page, select the server role you are about to view and then click View in the Metric column. Then, view the statuses of server role metrics and machine metrics.

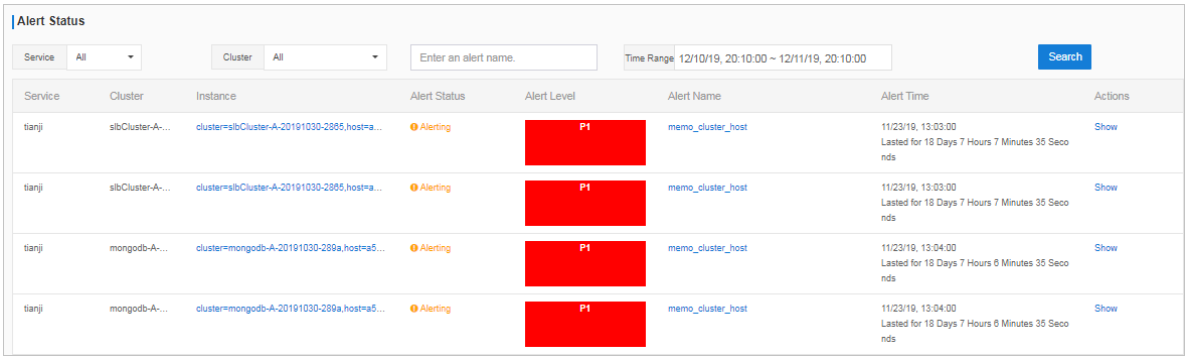



## 1.3.2.8.2 View the alert status

**The Alert Status page allows you to view the alerts generated in different services and the corresponding alert details.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Monitoring. On the Monitoring page, click Go to open the target page.
3. In the top navigation bar, choose Monitoring > Alert Status.



4. You can configure the service name, cluster name, alert name, or the time range when the alert is triggered to search for alerts.
5. On the Alert Status page, view the alert details. For more information about the alert status descriptions, see the following table.

| Item | Description |
| --- | --- |
| Service | The service name. |
| Cluster | The name of the cluster where the service is located. |
| Instance | The name of the service instance being monitored.<br>Click the instance to view the alert history of this instance. |
| Alert Status | Alerts have two statuses: Restored and Alerting. |
| Alert Level | Alerts have the following four levels, from high to low, according to the effect on services.<br>· P1<br>· P2<br>· P3<br>· P4 |
| Alert Name | The name of the generated alert.<br>Click the alert name to view the alert rule details. |
| Alert Time | The time when the alert is triggered and how long the alert has lasted. |
| Actions | Click Show to show the data before and after the alert time. |

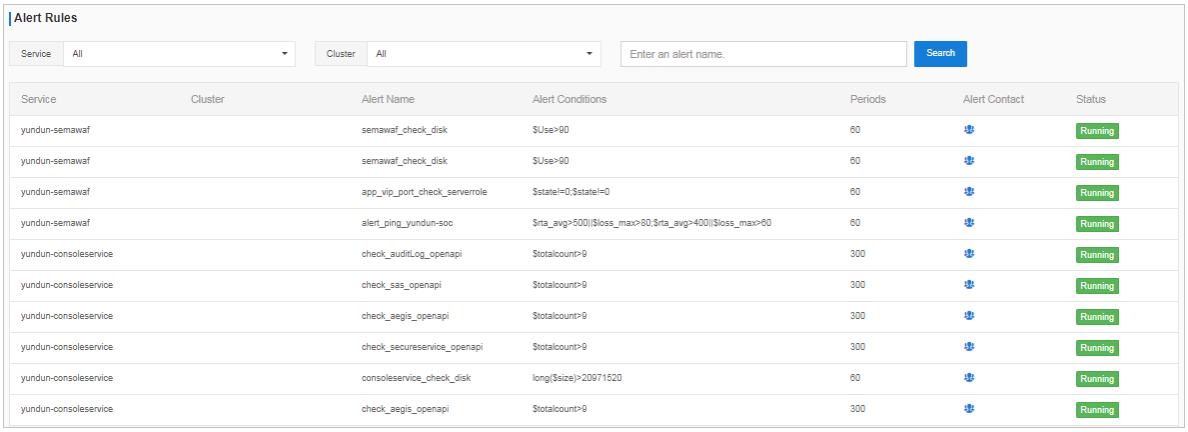
## 1.3.2.8.3 View alert rules

The Alert Rules page allows you to view the configured alert rules.

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Monitoring. On the Monitoring page, click Go to open the target page.

3. In the top navigation bar, choose Monitoring > Alert Rules.




4. You can configure the service name, cluster name, or alert name to search for alert rules.
5. On the Alert Rules page, view the detailed alert rules. For more information about the alert rule descriptions, see the following table.

| Item | Description |
| --- | --- |
| Service | The service name. |
| Cluster | The name of the cluster where the service is located. |
| Alert Name | The name of the generated alert. |
| Alert Conditions | The conditions met when the alert is triggered. |
| Periods | The frequency (in seconds) with which an alert rule is run. |
| Alert Contact | The groups and members that are notified when an alert is triggered. |
| Status | The current status of the alert rule.<br>· Running: Click to stop the alert rule.<br>· Stopped: Click to run the alert rule. |

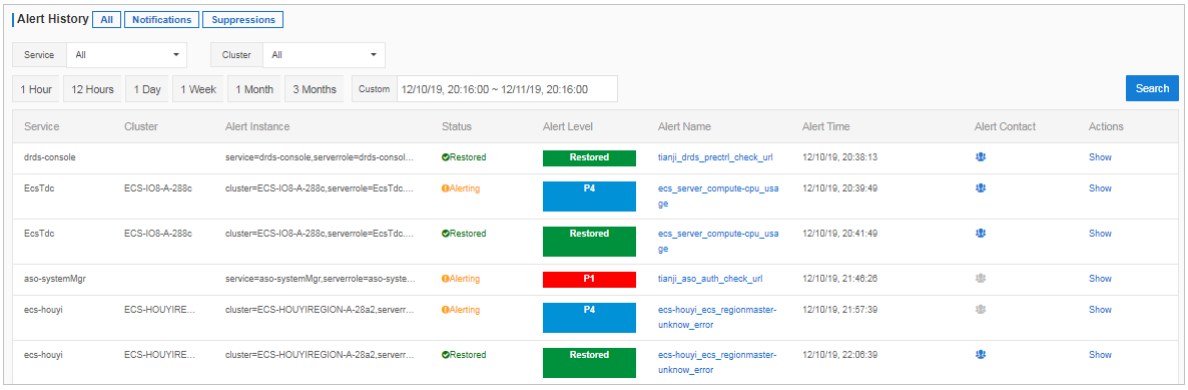
## 1.3.2.8.4 View the alert history

The Alert History page allows you to view all the history alerts generated in different services and the corresponding alert details.

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Monitoring. On the Monitoring page, click Go to open the target page.

3. In the top navigation bar, choose Monitoring > Alert History.




4. You can configure the service name, cluster name, time range, or period to search for alerts.
5. On the Alert History page, view the history alerts. For more information about the history alert descriptions, see the following table.

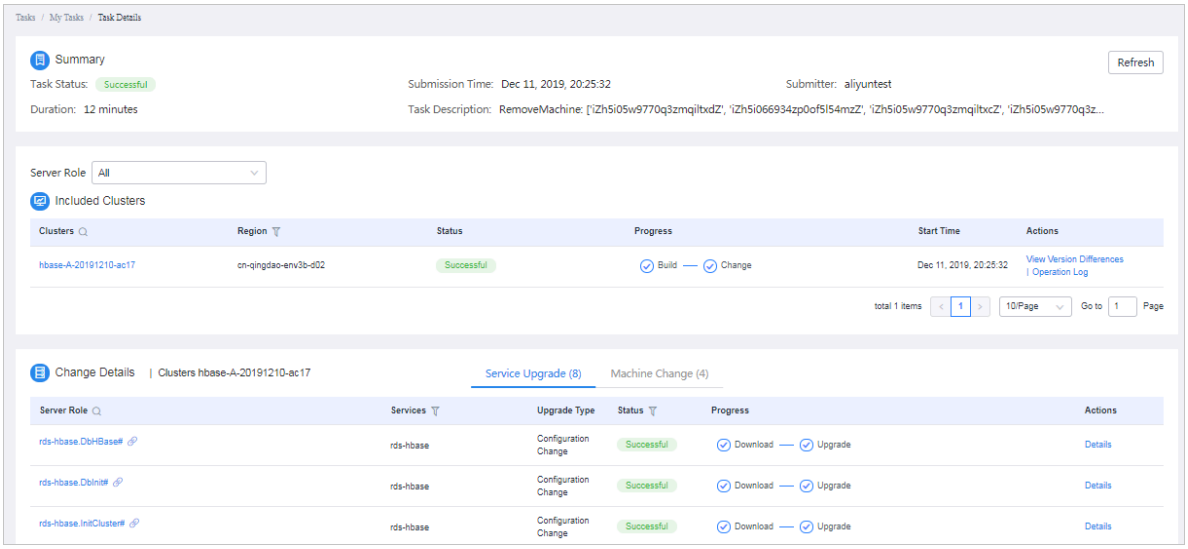
| Item | Description |
| --- | --- |
| Service | The name of the service to which the alert belongs. |
| Cluster | The name of the cluster where the service is located. |
| Alert Instance | The name of the resource where the alert is triggered. |
| Status | Alerts have two statuses: Restored and Alerting. |
| Alert Level | Alerts have the following four levels, from high to low, according to the effect on services.<br>· P1<br>· P2<br>· P3<br>· P4 |
| Alert Name | The name of the generated alert.<br>Click the alert name to view the alert rule details. |
| Alert Time | The time when the alert is triggered. |
| Alert Contact | The groups and members that are notified when an alert is triggered. |
| Actions | Click Show to show the data before and after the alert time. |

## 1.3.2.9 View tasks

**The task list allows you to view the submitted tasks and the corresponding status.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*
2. **To view the task list, you can:**
   - **In the left-side navigation pane, choose Tasks > My Tasks.**
   - **In the left-side navigation pane, choose Tasks > Related Tasks.**
3. **You can use**  **to filter tasks in the Status column.**
4. **Find the task whose details you are about to view and then click the task name or click Details in the Actions column.**
5. **On the Task Details page, view the status and progress of each cluster and server role.**




## 1.3.2.10 Reports

## 1.3.2.10.1 View reports

**The Reports module allows you to view the statistical data.**

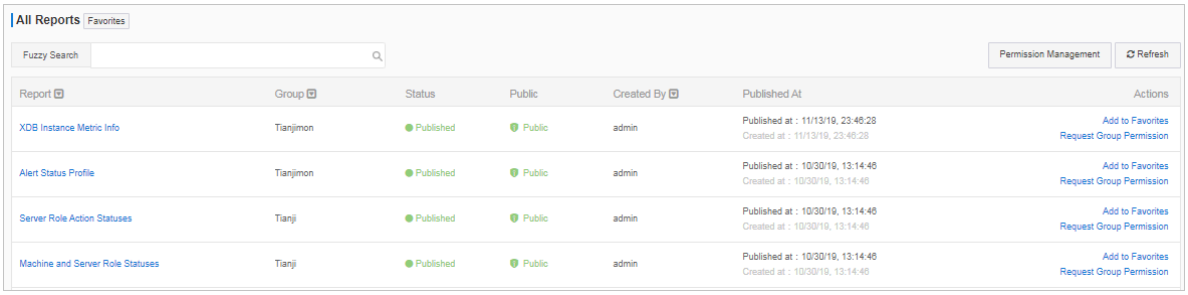
### Context

**You can view the following reports on Apsara Infrastructure Management Framework.**

- **System reports: default and common reports in the system.**
- **All reports: includes the system reports and custom reports.**

## Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Reports. On the Reports page, click Go to open the target page.




For more information about the report descriptions, see the following table.

| Item | Description |
| --- | --- |
| Report | The report name.<br>Move the pointer over the down-arrow button next to Report to search for reports by report name. |
| Group | The group to which the report belongs.<br>Move the pointer over the down-arrow button next to Group to filter reports by group name. |
| Status | Indicates whether the report is published.<br>· Published<br>· Not published |
| Public | Indicates whether the report is public.<br>· Public: All of the logon users can view the report.<br>· Not public: Only the current logon user can view the report. |
| Created By | The person who creates the report. |
| Published At | The time when the report is published and created. |
| Actions | Click Add to Favorites to add this report to your favorites. Then, you can view the report by choosing Reports > Favorites in the top navigation bar. |

3. Optional: Enter the name of the report that you are about to view in the search box.

4. **Click the report name to go to the corresponding report details page.**

   **For more information about the reports, see Appendix.**

#### 1.3.2.10.2 Add a report to favorites

**You can add common reports to favorites. Then, find them quickly on the Favorites page.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Reports. On the Reports page, click Go to open the target page.**
3. **Enter the name of the report that you are about to add to favorites in the search box.**
4. **At the right of the report, click Add to Favorites in the Actions column.**
5. **In the displayed Add to Favorites dialog box, enter tags for the report.**
6. **Click Add to Favorites.**

### 1.3.2.11 Tools

#### 1.3.2.11.1 Machine tools

**The Machine Tools module guides operations personnel to perform Operation & Maintenance (O&M) operations in common scenarios.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Tools > Operation Tools > Machine Tools. On the Machine Tools page, click Go to open the target page.**

3. Select the operation scene according to actual situations.

| Operation scene | Description | Action |
| --- | --- | --- |
| Scene 1: NC Scale-out ( with existing machines) | Scales out an SRG of the worker type. | Select a target cluster and a target SRG. Select the machines to be scaled out in the left-side section and then click Select> to add them to the right-side section. Click Submit and then click Confirm in the displayed dialog box. |
| Scene 2: Host Scale-out ( with existing machines) | Scales out the DockerHost#Buffer of an Apsara Infrastructure Management Framework cluster. | Select a target cluster. Select the machines to be scaled out in the left-side section and then click Select> to add them to the right-side section. Click Submit and then click Confirm in the displayed dialog box. |
| Scene 3: NC Scale-in | Scales in an SRG of the worker type. | Select a target cluster and a target SRG. Select the machines to be scaled in in the left-side section and then click Select> to add them to the right-side section. Click Submit and then click Confirm in the displayed dialog box. |
| Scene 4: Host Scale-in | Scales in the DockerHost #Buffer of an Apsara Infrastructure Management Framework cluster. | Select a target cluster. Select the machines to be scaled in in the left-side section and then click Select> to add them to the right-side section. Click Submit and then click Confirm in the displayed dialog box. |

| Operation scene | Description | Action |
| --- | --- | --- |
| Scene 5: VM Migration | Migrates virtual machines (VMs) from a host to another host. | Select a source host and a destination host. Select the VMs to be migrated in the left-side section and then click Select> to add them to the right-side section. Click Submit and then click Confirm in the displayed dialog box. |
| Scene 6: Host Switching | Switches from a standby host to a primary host. | Select a source host and a destination host. Click Submit and then click Confirm in the displayed dialog box. |

### 1.3.2.11.2 IDC shutdown

**If you are about to maintain the IDC or shut down all of the machines in the IDC, you must shut down the IDC.**

**Prerequisites**

**Warning:**

**This is a high-risk operation, so proceed with caution.**

**Procedure**

1. *Log on to Apsara Infrastructure Management Framework*.
2. **In the left-side navigation pane, choose Tools > IDC Shutdown, and then click Go to open the target page.**
3. **On the Clusters Shutdown page, click Start Shutdown to shut down all of the machines in the IDC with one click.**

### 1.3.2.12 Metadata operations

**In this version, you can only use command lines to perform metadata operations.**

# 1.3.2.12.1 Common parameters

**Common parameters consist of the common request parameters and the common response parameters.**

Common request parameters

**Common request parameters are request parameters that you must use when you call each API.**

Table 1-9: Parameter descriptions

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `Action` | **String** | **Yes** | **The API name. For more information about the valid values, see** *APIs on the control side* **and** *APIs on the deployment side*. |

Common response parameters

**Each time you send a request to call an API, the system returns a unique identifier, regardless of whether the call is successful.**

Table 1-10: Parameter descriptions

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `RequestID` | **String** | **Yes** | **The request ID.**<br>**The request ID is returned, regardless of whether the API call is successful.** |
| `Code` | **String** | **No** | **The error code.** |
| `Message` | **String** | **No** | **The reason of failure, which appears when the API call fails.** |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Result | The type varies with the request, which is subject to the returned result of the specific API. | No | The request result , which appears when the API call is successful. |

**Note:**

- **If the API call is successful, RequestID is returned and the HTTP return code is 200.**
- **If the API call fails, RequestID, Code, and Message are returned and the HTTP return code is 4xx or 5xx.**

Instance types

```
{
    "rds.mys2.small":{
        "cpu":2,
        "memory":4096,
        "disk":51200,
        "max_connections":60
    },
    "rds.mys2.mid":{
        "cpu":4,
        "memory":4096,
        "disk":51200,
        "max_connections":150
    },
    "rds.mys2.standard":{
        "cpu":6,
        "memory":4096,
        "disk":51200,
        "max_connections":300
    },
    "rds.mys2.large":{
        "cpu":8,
        "memory":7200,
        "disk":102400,
        "max_connections":600
    },
    "rds.mys2.xlarge":{
        "cpu":9,
        "memory":12000,
        "disk":204800,
        "max_connections":1500
    },
    "rds.mys2.2xlarge":{
        "cpu":10,
        "memory":20000,
        "disk":512000,
        "max_connections":2000
    }
```

```
}
```

## 1.3.2.12.2 Access APIs

**This topic describes how to access APIs on the control side and the deployment side.**

### Procedure

1. *Log on to Apsara Infrastructure Management Framework*.
2. In the left-side navigation pane, choose Operations > Machine Operations.
3. Select a project or enter the cluster name or machine name to search for the corresponding machine.

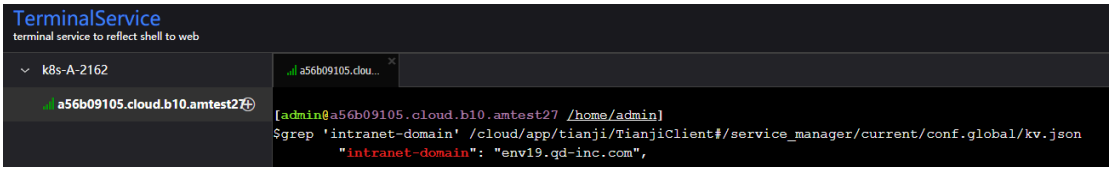
4. Access APIs.

   - Access an API on the control side

     a. Find the machine that you are about to access and then click Terminal in the Actions column to log on to the machine.

     b. In the command window, enter the following command and then press Enter to obtain the intranet-domain.

     ```
     grep 'intranet-domain' /cloud/app/tianji/TianjiClient#/
     service_manager/current/conf.global/kv.json
     ```

     c. You can log on to the API on the control side in the following ways. Here, take `ListInstance` as an example.

     - Get request

       ```
       curl 'xdb-master.xdb.{intranet-domain}:15678?
        Action=ListInstance'
       ```

     - Post request

       ```
       curl 'xdb-master.xdb.{intranet-domain}:15678' -X POST -d
        '{"Action":"ListInstance"}'
       ```

   - Access an API on the deployment side

     a. Find the machine that you are about to access and record the IP address in the Hostname column.

     b. You can log on to the API on the deployment side in the following ways. Here, take `CheckState` as an example.

     Assume that the IP address of the target machine is 127.0.0.1.

     - Get request

       ```
       curl '127.0.0.1:18765? Action=CheckState&Port=3606'
       ```

     - Post request

       ```
       curl '127.0.0.1:18765' -X POST -d '{"Action":"CheckState","
       Port":3606}'
       ```

## 1.3.2.12.3 APIs on the control side

### *1.3.2.12.3.1 DescribeInstance*

**Views instances.**

Description

**Views the detailed information of an instance.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: DescribeInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| InstanceID | Integer | Yes | The instance ID. |
| InstanceName | String | Yes | The instance name. |
| Domain | String | Yes | The domain name. |
| Port | Integer | Yes | The instance port. |
| PaxosPort | Integer | Yes | The communication port between instance nodes. |
| InstanceDir | String | Yes | The instance directory. |
| Level | String | Yes | The instance specifications. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Config | String | No | The custom my.cnf configuration of the instance, which is in the JSON format. |
| LeaderIP | String | No | The IP address of the primary node. |
| ActionName | String | Yes | The action name. |
| ActionStatus | String | Yes | The action status. |
| Description | String | Yes | The description. |
| IsDeleted | Integer | No | Whether the instance is deleted. 0 indicates No and 1 indicates Yes. |
| NodeList | []NodeInfo | Yes | The information of the instance nodes. |

**The structure of NodeInfo is as follows.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| InstanceID | Integer | Yes | The instance ID. |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the instance node. |
| NodeID | Integer | Yes | The ID of the instance node. |
| ActionName | String | Yes | The action name. |
| ActionStatus | String | Yes | The action status. |
| Description | String | Yes | The description. |
| IsDeleted | Integer | No | Whether the node is deleted. 0 indicates No and 1 indicates Yes. |

Examples

### Sample requests

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeInstance&
InstanceName=xdb-meta'
```

### Sample responses


```
{
    "Result": {
        "ActionName": "",
        "Level": "rds.mys2.standard",
        "InstanceID": 1,
        "LeaderIP": "10.39.XX.XX",
        "Config": "{}",
        "Description": "",
        "ActionStatus": "",
        "Domain": "xdb-meta.xdb.env8c-inc.com",
        "PaxosPort": 11606,
        "InstanceName": "xdb-meta",
        "User": "xdb",
        "Password": "xdb",
        "Port": 3606,
        "IsDeleted": 0,
        "InstanceDir": "/apsarapangu/disk1/xdb/xdb_instance_3606",
        "NodeList": [
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.38.XX.XX",
                "InstanceName": "xdb-meta",
                "NodeID": 1,
                "IsDeleted": 0
            },
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.39.XX.XX",
                "InstanceName": "xdb-meta",
                "NodeID": 2,
                "IsDeleted": 0
            },
            {
                "ActionStatus": "",
                "ActionName": "",
                "Description": "",
                "InstanceID": 1,
                "IP": "10.39.145.20",
                "InstanceName": "xdb-meta",
                "NodeID": 3,
                "IsDeleted": 0
            }
        ]
    },
    "RequestID": "3CFCBA07-3D87-4A99-B8C1-E861A7D1A573"
```

```
}
```

### *1.3.2.12.3.2 ListInstance*

**Lists instances.**

Description

**Lists the basic information of instances.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: ListInstance |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
|---|---|---|---|
| InstanceNames | String | Yes | The list of instance names. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ListInstance'
```

**Sample responses**

```
{
    "Result": {
        "InstanceNames": [
            "xdb-meta",
            "xdb-instance-1",
            "xdb-instance-2",
            "xdb-instance-3"
        ]
    },
    "RequestID": "A921B8C7-C833-417C-B46A-E0CE129EBE48"
```

```
}
```

### 1.3.2.12.3.3 CreateInstance

**Creates an instance.**

Description

**Creates an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: CreateInstance |
| InstanceName | String | Yes | The instance name. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |
| Level | String | Yes | *Instance types* |
| Config | String | No | The custom my.cnf configuration of the instance, which is in the JSON format. The key must be the same as the value of the field in my.cnf, which is of the string type. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=CreateInstance&
InstanceName=xdb-instance-1&User=admin&password=xdb&Level=rds.mys2.
small'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "8BCB3B39-6140-459F-B283-F83C03ADC3CA"
}
```

### *1.3.2.12.3.4 DeleteInstance*

**Deletes an instance.**

Description

**Deletes an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: DeleteInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl '127.0.0.1:15678? Action=DeleteInstance&InstanceName=xdb-instance
-1'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "9C40CCB3-4FAB-4242-9B87-792E8154E5CD"
}
```

### *1.3.2.12.3.5 RestartInstance*

**Restarts an instance.**

Description

**Restarts an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: RestartInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=RestartInstance&
InstanceName=xdb-instance-2'
```

**Sample responses**

```
{
```

```
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "47277A23-5FFE-4A46-B65F-E6F2569F44E5"
}
```

### *1.3.2.12.3.6 UpgradeInstance*

**Performs a minor upgrade of an instance.**

Description

**Performs a minor upgrade of an instance. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: UpgradeInstance |
| InstanceName | String | Yes | The instance name. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=UpgradeInstance&
InstanceName=xdb-instance-2'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "95E8B098-B04A-4BCA-BEBE-DA1D11BBAD4A"
```

```
}
```

### 1.3.2.12.3.7 DescribeTaskProgress

**Views the task progress.**

Description

**Views the task progress.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value : DescribeTaskProgress |
| RequestID | String | Yes | The request ID. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Progress | String | Yes | The instance progress, including pending, doing, done, and failed. |
| Description | String | Yes | The description of the instance progress. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeTaskProgress&
RequestID=47277A23-5FFE-4A46-B65F-E6F2569F44E5'
```

**Sample responses**

```
{
    "Result": {
        "Progress": "done",
        "Description": "Success"
    },
    "RequestID": "AC535130-F40E-4D45-BC05-0F45C8473346"
}
```

## *1.3.2.12.3.8 ChangeLeaderTo*

**Changes the leader role of an instance to another node.**

Description

**Changes the leader role of an instance to another node.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: ChangeLeaderTo |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the machine where the new leader node is located. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ChangeLeaderTo&
InstanceName=xdb-instance-1&IP=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "37638DE5-14C1-4D2E-984F-FEA1F29C9F84"
}
```

### *1.3.2.12.3.9 ModifyInstanceLevel*

**Modifies the instance specifications.**

Description

**Modifies the instance specifications. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value : ModifyInstanceLevel |
| InstanceName | String | Yes | The instance name. |
| Level | String | Yes | The new instance specifications. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=ModifyInstanceLevel&
InstanceName=xdb-instance-1&Level=rds.mys2.mid'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "21B91211-BB09-4665-835D-9471A6F07F24"
}
```

## *1.3.2.12.3.10 DescribeLeader*

**Views the primary node information of an instance.**

Description

**Views the primary node information of an instance.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: DescribeLeader |
| InstanceName | String | Yes | The instance name. |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| LeaderIP | String | Yes | The IP address of the primary node. |
| Port | Integer | Yes | The instance port. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DescribeLeader&
InstanceName=xdb-meta'
```

**Sample responses**

```
{
    "Result": {
        "LeaderIP": "10.27.0.1",
        "Password": "xdb",
        "Port": 3606,
        "User": "xdb"
    },
    "RequestID": "2F05EE81-DC47-478E-9CA9-9AE8CA809151"
}
```

### *1.3.2.12.3.11 RecreateNode*

**Recreates an instance node.**

Description

**Uses other available nodes to recreate an instance node by backup and recovery. This is an asynchronous task. You can view the task result by calling the DescribeTaskProgress API based on the RequestID in the responses.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters***.**

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: RecreateNode |
| InstanceName | String | Yes | The instance name. |
| IP | String | Yes | The IP address of the instance node to be recreated. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=RecreateNode&
InstanceName=xdb-instance-1&IP=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Task has created, you can use api(DescribeTaskProgress
) to get task progress.",
    "RequestID": "7F079E11-1DE9-4148-A9FA-683E4C58F9C2"
}
```

## *1.3.2.12.3.12 CreateDatabase*

**Creates a database and a user.**

Description

**Creates a database and a user.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: CreateDatabase |
| InstanceName | String | Yes | The instance name. |
| DBName | String | Yes | The database name. |
| User | String | Yes | The username. |
| Password | String | Yes | The password. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=CreateDatabase&
InstanceName=xdb-instance-1&DBName=xdb&User=admin&Password=xdb_passwo
rd'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "A2BEF74F-5C3A-4CEF-A2B8-C14C71E36569"
}
```

## *1.3.2.12.3.13 DeleteDatabase*

**Deletes a database.**

Description

**Deletes a database.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: DeleteDatabase |
| InstanceName | String | Yes | The instance name. |
| DBName | String | Yes | The name of the database to be deleted. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DeleteDatabase&
InstanceName=xdb-instance-1&DBName=xdb'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "23F75A0A-B1D6-4341-BD5B-1A5F3FD45848"
}
```

### *1.3.2.12.3.14 DeleteUser*

**Deletes a user.**

Description

**Deletes a user.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: DeleteUser |
| InstanceName | String | Yes | The instance name. |
| User | String | Yes | The username. |
| Host | String | No | The source address range. If not configured, the user account is deleted in all of the source addresses by default. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl 'xdb-master.xdb.env8c-inc.com:15678? Action=DeleteUser&InstanceNa
me=xdb-instance-1&User=admin&Host=10.39.XX.XX'
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "6A82AFF6-2B4D-48EF-868D-BBA54667D846"
}
```

## 1.3.2.12.4 APIs on the deployment side

### *1.3.2.12.4.1 CheckHealth*

**Checks if an instance node is of the leader role and whether the status is readable and writeable.**

Description

**Checks if an instance node is of the leader role. An instance node is regarded as healthy only if it is of the leader role and is readable and writeable.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `Action` | **String** | **Yes** | **The parameter specified by the system. Value: CheckHealth** |
| `Port` | **Integer** | **Yes** | **The port of the instance node.** |

Response parameters

**For more information about the common response parameters, see** *Common response parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| `health` | **Boolean** | **Yes** | **The health status.** |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=CheckHealth&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "health": true
    },
    "RequestID": "304B69CE-1566-4E87-B618-233F40238FFF"
}
```

```
{
    "Message":"{\"health\": false}",
    "Code":"NodeNotHealth",
    "RequestID":"E939DB9B-4337-4B1C-8680-F62BEDD645DC"
}
```

### *1.3.2.12.4.2 CheckState*

**Checks whether the status of an instance node is normal.**

Description

**Checks whether the status of an instance node is normal. Generally, you have the following two situations:**

- **The node is of the leader role and is readable and writeable.**
- **The node is of the follower role and is readable.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
|---|---|---|---|
| Action | String | Yes | The parameter specified by the system. Value: CheckState |
| Port | Integer | Yes | The port of the instance node. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| IP | String | Yes | The IP address of the instance node. |
| Port | Integer | Yes | The instance port. |
| Role | String | Yes | The role of the instance node. |
| Writeable | String | Yes | Whether the instance node is writeable. |
| Readable | String | Yes | Whether the instance node is readable. |
| State | String | Yes | The status of the instance node. If the status is normal, the value is GOOD. Otherwise, the value is ERROR. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=CheckState&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "Readable": true,
        "State": "GOOD",
        "Role": "Follower",
        "Port": 3606,
        "IP": "10.39.145.10"
    },
    "RequestID": "45A59426-46D3-4709-8DD6-CD9F243336E0"
```

```
}
```

### 1.3.2.12.4.3 DescribeNodeStatus

**Views the status of an instance node.**

Description

**Views the status of an instance node. A leader node is readable and writeable, while a follower node is readable.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value : DescribeNodeStatus |
| Port | Integer | Yes | The port of the instance node. This parameter is required if the instance mode is single_machine. |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| IP | String | Yes | The IP address of the instance node. |
| Port | Integer | Yes | The port of the instance node. |
| Role | String | Yes | The instance role. |
| Writeable | String | Yes | Whether the instance node is writeable. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Readable | String | Yes | Whether the instance node is readable. |
| ConnectionCount | Integer/String | Yes | The number of connections. If the retrieval fails, the value is unknown. |
| MaxConnectionCount | Integer/String | Yes | The maximum number of connections. If the retrieval fails, the value is unknown. |
| ConnectionPercent | Integer/String | Yes | The percentage of connections. If the retrieval fails, the value is unknown. |
| QPS | Integer/String | Yes | Queries per second (QPS). If the retrieval fails, the value is unknown. |
| CpuPercent | Integer/String | Yes | The CPU usage. If the retrieval fails, the value is unknown. |
| MemoryPercent | Integer/String | Yes | The memory usage. If the retrieval fails, the value is unknown. |
| DiskPercent | Integer/String | Yes | The disk usage. If the retrieval fails, the value is unknown. |
| State | String | Yes | The status of the instance node. If the status is normal, the value is GOOD. Otherwise, the value is ERROR. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=DescribeNodeStatus&Port=3606'
```

**Sample responses**

```
{
    "Result": {
        "CpuPercent": 2.74,
        "IP": "10.39.XX.XX",
        "Readable": true,
        "MemoryPercent": 56.13,
        "State": "GOOD",
        "Role": "Follower",
        "MaxConnectionCount": 500,
        "ActiveThreadCount": 34,
        "Writeable": false,
        "ConnectionCount": 37,
        "DiskPercent": 3.0,
        "ConnectionPercent": 7.4,
        "QPS": 15.95,
        "Port": 3606
    },
    "RequestID": "D18328B1-78A9-4F3E-BB2E-B27AB7683C19"
}
```

## *1.3.2.12.4.4 ListNode*

**Lists instance nodes.**

Description

**Lists the basic information of instance nodes.**

Request parameters

**For more information about the common request parameters, see *Common request parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: ListNode |

Response parameters

**For more information about the common response parameters, see *Common response parameters*.**

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Nodes | String | Yes | The list of instance names. |

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=ListNode'
```

**Sample responses**

```
{
    "Result": {
        "Nodes": [
            "xdb-instance-1",
            "xdb-instance-2",
            "xdb-instance-3",
            "xdb-meta"
        ]
    },
    "RequestID": "3F7BB536-FA3F-4597-A3DF-E5830F5A3A21"
}
```

### *1.3.2.12.4.5 BackupNode*

**Backs up data of an instance node and transmits the data to a specified location (Use the nc command to transmit data to the port of a specified IP address).**

Description

**Backs up data of an instance node and transmits the data to a specified location.**

Request parameters

**For more information about the common request parameters, see** *Common request parameters*.

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| Action | String | Yes | The parameter specified by the system. Value: BackupNode |
| Port | Integer | Yes | The instance port. |
| TargetIP | String | Yes | The IP address of the target location. |

| Name | Type | Required | Description |
| --- | --- | --- | --- |
| TargetPort | Integer | Yes | The port of the target location. |

Response parameters

*Common response parameters*

Examples

**Sample requests**

```
curl '127.0.0.1:18765? Action=BackupNode&Port=3606&TargetIP=10.39.XX.
XX&TargetPort='
```

**Sample responses**

```
{
    "Result": "Success",
    "RequestID": "6A82AFF6-2B4D-48EF-868D-BBA54667D846"
}
```

## 1.3.2.13 Appendix

### 1.3.2.13.1 Project component info report

**This report displays the name and status for each type of project components, including services, server roles, and machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The name of a cluster in the project. |
| Service | The name of a service in the cluster. |
| Server Role | The name of a server role in the service. |
| Server Role Status | The running status of the server role on the machine. |
| Server Role Action | The action that the server role performs on the machine. Data is available only when Apsara Infrastructure Management Framework asks the server role to perform certain actions, such as rolling and restart actions. |
| Machine Name | The hostname of the machine. |
| IP | The IP address of the machine. |
| Machine Status | The running status of the machine. |

| Item | Description |
| --- | --- |
| Machine Action | The action that Apsara Infrastructure Management Framework asks the machine to perform, such as the clone action. |

### 1.3.2.13.2 IP list

**This report displays the IP addresses of physical machines and Docker applications.**

IP List of Physical Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The hostname of the machine. |
| IP | The IP address of the machine. |

IP List of Docker Applications

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The hostname of the machine. |
| Docker Host | The Docker hostname. |
| Docker IP | The Docker IP address. |

### 1.3.2.13.3 Machine info report

**This report displays the statuses of machines and server roles on the machines.**

Machine Status

**Displays all the machines currently managed by Apsara Infrastructure Management Framework and their corresponding statuses. In the Global Filter section at the top of the page, select the project, cluster, and machine from the project, cluster, and machine drop-down lists, and then click Filter on the right to filter the data.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |

| Item | Description |
| --- | --- |
| IP | The IP address of the machine. |
| Machine Status | The machine status. |
| Machine Action | The action currently performed by the machine. |
| Machine Action Status | The action status. |
| Status Description | The description about the machine status. |

Expected Server Role List

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The name of the expected server role on the machine. |

Abnormal Monitoring Status

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Monitored Item | The name of the monitored item. |
| Level | The level of the monitored item. |
| Description | The description of the monitored item contents. |
| Updated At | The updated time of the monitored item. |

Server Role Version and Status on Machine

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The server role name. |

| Item | Description |
| --- | --- |
| Server Role Status | The status of the server role. |
| Target Version | The expected version of the server role on the machine. |
| Current Version | The current version of the server role on the machine. |
| Status Description | The description about the status. |
| Error Message | The exception message of the server role. |

Monitoring Status

**Select a row in the Machine Status section to display the corresponding information in this list.**

| Item | Description |
| --- | --- |
| Machine Name | The machine name. |
| Server Role | The server role name. |
| Monitored Item | The name of the monitored item. |
| Level | The level of the monitored item. |
| Description | The description of the monitored item contents. |
| Updated At | The updated time of the monitored item. |

## 1.3.2.13.4 Rolling info report

**This report displays the running and completed rolling tasks and the task-related status.**

Choose a rolling action

**This list only displays the running rolling tasks. If no rolling task is running, no data is available in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Git Version | The version of change that triggers the rolling task. |
| Description | The description about the change entered by a user when the user submits the change. |
| Start Time | The start time of the rolling task. |

| Item | Description |
| --- | --- |
| End Time | The end time of the rolling task. |
| Submitted By | The ID of the user who submits the change. |
| Rolling Task Status | The current status of the rolling task. |
| Submitted At | The time when the change is submitted. |

Server Role in Job

**Select a rolling task in the Choose a rolling action section to display the rolling status of server roles related to the selected task. If no rolling task is selected, the server role statuses of all historical rolling tasks are displayed.**

| Item | Description |
| --- | --- |
| Server Role | The server role name. |
| Server Role Status | The rolling status of the server role. |
| Error Message | The exception message of the rolling task. |
| Git Version | The version of change to which the rolling task belongs. |
| Start Time | The start time of the rolling task. |
| End Time | The end time of the rolling task. |
| Approve Rate | The proportion of machines that have the rolling task approved by the decider. |
| Failure Rate | The proportion of machines that have the rolling task failed. |
| Success Rate | The proportion of machines that have the rolling task succeeded. |

Server Role Rolling Build Information

**The source version and target version of each application under the server role in the rolling process.**

| Item | Description |
| --- | --- |
| App | The name of the application that requires rolling in the server role. |

| Item | Description |
| --- | --- |
| Server Role | The server role to which the application belongs. |
| From Build | The version before the upgrade. |
| To Build | The version after the upgrade. |

Server Role Statuses on Machines

**Select a server role in the Server Role in Job section to display the deployment status of this server role on the machine.**

| Item | Description |
| --- | --- |
| Machine Name | The name of the machine on which the server role is deployed. |
| Expected Version | The target version of the rolling. |
| Actual Version | The current version. |
| State | The status of the server role. |
| Action Name | The Apsara Infrastructure Management Framework action currently performed by the server role. |
| Action Status | The action status. |

## 1.3.2.13.5 Machine RMA approval pending list

**Some Apsara Infrastructure Management Framework actions (such as restart) on machines and server roles can be triggered by users, but this type of actions must be reviewed and approved. This report is used to process the actions that must be reviewed and approved.**

Machine

**Displays the basic information of pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| IP | The IP address of the machine. |

| Item | Description |
| --- | --- |
| State | The running status of the machine. |
| Action Name | The action on the machine. |
| Action Status | The status of the action on the machine. |
| Actions | The approval button. |

Machine Serverrole

**Displays the information of server roles on the pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| IP | The IP address of the machine. |
| Serverrole | The server role name. |
| State | The running status of the server role. |
| Action Name | The action on the server role. |
| Action Status | The status of the action on the server role. |
| Actions | The approval button. |

Machine Component

**Displays the hard disk information of pending approval machines.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Hostname | The hostname of the machine. |
| Component | The hard disk on the machine. |
| State | The running status of the hard disk. |
| Action Name | The action on the hard disk. |
| Action Status | The status of the action on the hard disk. |
| Actions | The approval button. |

### 1.3.2.13.6 Registration vars of services

**This report displays values of all service registration variables.**

| Item | Description |
|---|---|
| Service | The service name. |
| Service Registration | The service registration variable. |
| Cluster | The cluster name. |
| Update Time | The updated time. |

### 1.3.2.13.7 Virtual machine mappings

**Use the global filter to display the virtual machines of a specific cluster.**

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

| Item | Description |
|---|---|
| Project | The project name. |
| Cluster | The cluster name. |
| VM | The hostname of the virtual machine. |
| Currently Deployed On | The hostname of the physical machine on which the virtual machine is currently deployed. |
| Target Deployed On | The hostname of the physical machine on which the virtual machine is expected to be deployed. |

### 1.3.2.13.8 Service inspector report

**Use the global filter to display the service inspection reports of a specific cluster.**

**Service Inspector: Data is available only for services with inspection configured.**

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

## 1.3.2.13.9 Resource application report

**In the Global Filter section, select the project, cluster, and machine from the project, cluster, and machine drop-down lists and then click Filter on the right to display the corresponding resource application data.**

Change Mappings

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Version | The version where the change occurs. |
| Resource Process Status | The resource application status in the version. |
| Msg | The exception message. |
| Begintime | The start time of the change analysis. |
| Endtime | The end time of the change analysis. |

Changed Resource List

| Item | Description |
| --- | --- |
| Res | The resource ID. |
| Type | The resource type. |
| Name | The resource name. |
| Owner | The application to which the resource belongs. |
| Parameters | The resource parameters. |
| Ins | The resource instance name. |
| Instance ID | The resource instance ID. |

Resource Status

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| APP | The application of the server role. |

| Item | Description |
| --- | --- |
| Name | The resource name. |
| Type | The resource type. |
| Status | The resource application status. |
| Parameters | The resource parameters. |
| Result | The resource application result. |
| Res | The resource ID. |
| Reprocess Status | The status of the interaction with Business Foundation System during the VIP resource application. |
| Reprocess Msg | The error message of the interaction with Business Foundation System during the VIP resource application. |
| Reprocess Result | The result of the interaction with Business Foundation System during the VIP resource application. |
| Refer Version List | The version that uses the resource. |
| Error Msg | The exception message. |

## 1.3.2.13.10 Statuses of project components

**This report displays the status of all server roles in an abnormal status on machines of the project, and the monitoring information (alert information reported by the server role to Apsara Infrastructure Management Framework monitor) of server roles and machines.**

Error State Component Table

**Only displays the information of server roles that are not in GOOD status and server roles to be upgraded.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Need Upgrade | Whether the current version reaches the final status. |

| Item | Description |
| --- | --- |
| Server Role Status | The current status of the server role. |
| Machine Status | The current status of the machine. |

Server Role Alert Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

Machine Alert Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

Service Inspector Information

**Select a row in the Error State Component Table section to display the corresponding information in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Monitored Item | The monitored item name of the server role. |
| Level | The alert level. |
| Description | The description about the alert contents. |
| Updated At | The updated time of the alert information. |

## 1.3.2.13.11 Relationship of service dependency

**This report displays the dependencies among server roles. Use the global filter to display the data of a specific cluster in the list.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Service | The service name. |
| Server Role | The server role name. |
| Dependent Service | The service on which the server role depends. |
| Dependent Server Role | The server role on which the server role depends. |
| Dependent Cluster | The cluster to which the dependent server role belongs. |
| Dependency in Final Status | Whether the dependent server role reaches the final status. |

## 1.3.2.13.12 Check report of network topology

**This report checks if network devices and machines have wirecheck alerts.**

Check Report of Network Topology

**Checks if network devices have wirecheck alerts.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Network Instance | The name of the network device. |

| Item | Description |
| --- | --- |
| Level | The alert level. |
| Description | The description about the alert information. |

Check Report of Server Topology

**Checks if servers (machines) have wirecheck alerts.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The server (machine) name. |
| Level | The alert level. |
| Description | The description about the alert information. |

## 1.3.2.13.13 Clone report of machines

**This report displays the clone progress and status of machines.**

Clone Progress of Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Machine Status | The running status of the machine. |
| Clone Progress | The progress of the current clone process. |

Clone Status of Machines

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| Machine Action | The action performed by the machine, such as the clone action. |
| Machine Action Status | The status of the action performed by the machine. |
| Machine Status | The running status of the machine. |

| Item | Description |
| --- | --- |
| Level | Whether the clone action performed by the machine is normal. |
| Clone Status | The current status of the clone action performed by the machine. |

## 1.3.2.13.14 Auto healing/install approval pending report

**The list structure is the same as the machine RMA approval pending list, whereas this view is used for the approval during the installation. For more information, see** *Machine RMA approval pending list*.

## 1.3.2.13.15 Machine power on or off statuses of clusters

**After a cluster starts or shuts down machines, you can view the related information in this report.**

Cluster Running Statuses

**If a cluster is starting or shutting down machines, the corresponding data is available in this list. No data indicates that no cluster has machines shut down.**

| Item | Description |
| --- | --- |
| Project | The project name. |
| Cluster | The cluster name. |
| Action Name | The startup or shutdown action that is being performed by the cluster. |
| Action Status | The status of the action. |

Server Role Power On or Off Statuses

**Displays the power on or off statuses of server roles in the cluster selected in the Cluster Running Statuses section.**

**Select a row in the Cluster Running Statuses section to display the information of the corresponding cluster in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Server Role | The server role name. |
| Action Name | The startup or shutdown action that is being performed by the server role. |
| Action Status | The status of the action. |

Statuses on Machines

**Displays the running status of the selected server role on machines.**

**Select a row in the Server Role Power On or Off Statuses section to display the information of the corresponding server role in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Server Role | The server role name. |
| Machine Name | The machine name. |
| Server Role Status | The running status of the server role. |
| Server Role Action | The action currently performed by the server role. |
| Server Role Action Status | The status of the action. |
| Error Message | The exception message. |

Machine Statuses

**Displays the running statuses of machines in the selected cluster.**

**Select a row in the Statuses on Machines section to display the information of the corresponding machine in the list.**

| Item | Description |
| --- | --- |
| Cluster | The cluster name. |
| Machine Name | The machine name. |
| IP | The IP address of the machine. |
| Machine Status | The running status of the machine. |
| Machine Action | The action currently performed by the machine. |
| Machine Action Status | The action status of the machine. |
| Error Message | The exception message. |

# 2 Product operations

## 2.1 Operations of basic cloud products

### 2.1.1 ApsaraDB for RDS

#### 2.1.1.1 Architecture

#### 2.1.1.1.1 System architecture

##### *2.1.1.1.1.1 Backup system*

**ApsaraDB for RDS can back up databases at any time and restore them to any point in time based on the backup policy, making the data more traceable.**

Automatic backup

**ApsaraDB RDS for MySQL supports both physical and logical backup.**

**You can flexibly configure the backup start time based on the service off-peak hours. All backup files are retained for seven days.**

Log management

**ApsaraDB RDS for MySQL automatically generates binlogs and allows you to download them for local incremental backup.**

Instance cloning

**A cloned instance is a new instance with the same content as the primary instance , including data and settings. This feature allows you to restore data of the primary instance or create multiple instances that are the same as the primary instance.**

##### *2.1.1.1.1.2 Monitoring system*

**RDS provides multi-dimensional monitoring services across the physical, network, and application layers to ensure business availability.**

Performance monitoring

**RDS provides nearly 20 metrics for system performance monitoring, such as disk capacity, IOPS, connections, CPU utilization, network traffic, TPS, QPS, and cache**

**hit rate. You can obtain the running status information for any instances within the past year.**

SQL auditing

**The system records the SQL statements and related information sent to RDS instances, such as the connection IP address, database name, access account, execution time, and number of records returned. You can use SQL auditing to check instance security and locate problems.**

Threshold alerts

**RDS provides alert SMS notifications if status or performance exceptions occur in the instance.**

**These exceptions can be involved in instance locking, disk capacity, IOPS, connections, and CPU. You can configure alert thresholds and up to 50 alert recipients (of which five are effective at a time). When an instance exceeds the threshold, an SMS notification is sent to the alert recipients.**

Web operation logs

**The system logs all modification operations in the RDS console for administrators to check. These logs are retained for a maximum of 30 days.**

#### *2.1.1.1.1.3 Control system*

**If a host or instance does not respond, the RDS high-availability (HA) component checks for exceptions and fails over services within 30 seconds to guarantee that applications run normally.**

#### *2.1.1.1.1.4 Task scheduling system*

**You can use the RDS console or API operations to create and delete instances, or switch instances between the internal network and Internet. All instance operations are scheduled, traced, and displayed as tasks.**

### 2.1.1.2 Log on to the Apsara Stack Operations console

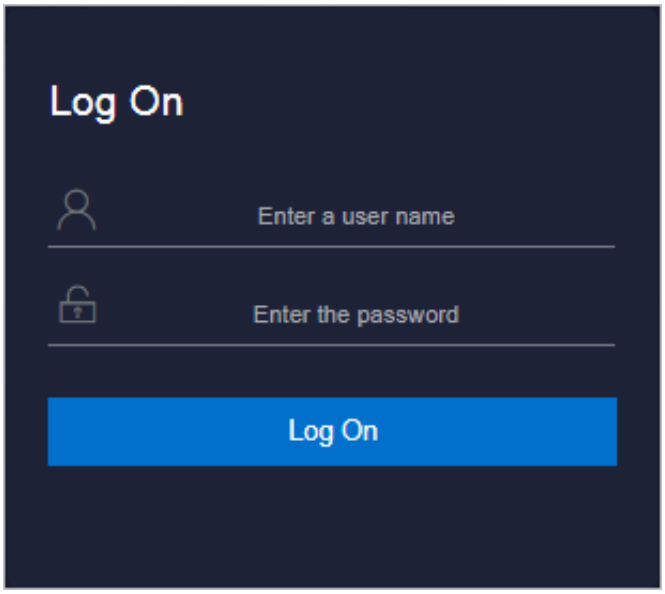
**Prerequisites**

- **ASO access address in the format of http://***region-id***.aso.***intranet-domain-id***.com.**
- **Google Chrome browser (recommended).**

**Procedure**

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

   Figure 2-1: Log on to ASO

   **Note:**
   **You can select the language from the drop-down list in the upper-right corner to change the language of ASO.**
3. **Enter the correct username and password.**
   - **The system has three default users:**
     - **Security officer: manages other users or roles.**
     - **Auditor officer: views audit logs.**
     - **System administrator: used for other functions except those of the security officer and auditor officer.**
   - **You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.**
4. **Click Log On to log on to ASO.**

## 2.1.1.3 Instance management

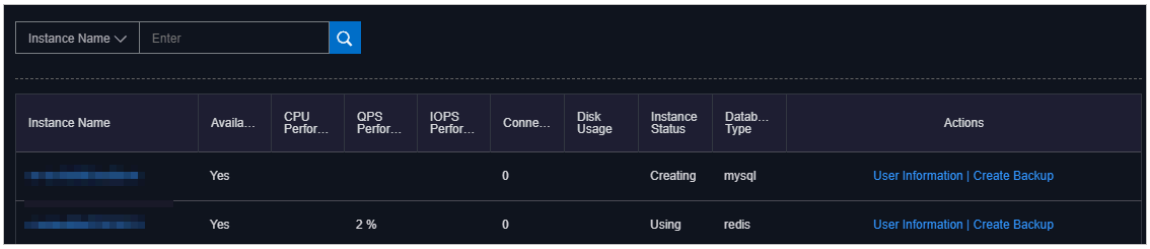
**You can view instance details, logs, and user information.**

### Procedure

1. *Log on to the Apsara Stack Operations console*.
2. **In the left-side navigation pane, choose Products > RDS.**
3. **On the Instance Management tab of RDS, you can perform the following operations:**
   - **View instances**

     **View instances that belong to the account on the Instance Management tab, as shown in *Figure 2-2: Instances*.**

     Figure 2-2: Instances

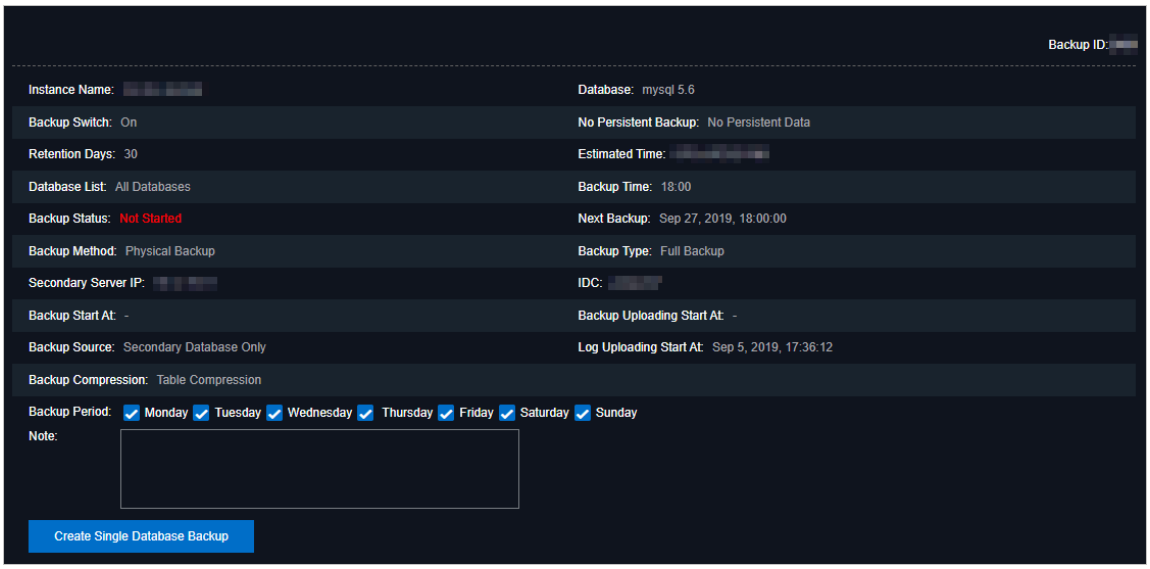
   - **View instance details**

     **Click the ID of an instance to view details, as shown in *Figure 2-3: Instance details*. You can switch your service between primary and secondary instances and query history operations on this page.**

     **Note:**

**If data is not synchronized between the primary and secondary instances, a forced switchover may result in data loss. Proceed with caution.**

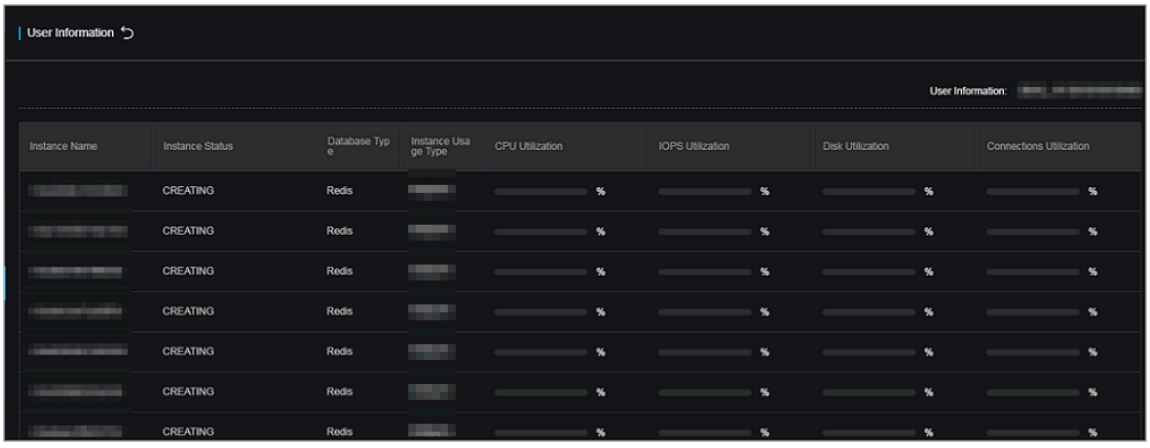
Figure 2-3: Instance details




- **View user information**

  **On the Instance Management tab, click User Information in the Actions column corresponding to an instance, as shown in *Figure 2-4: User information*.**

  Figure 2-4: User information

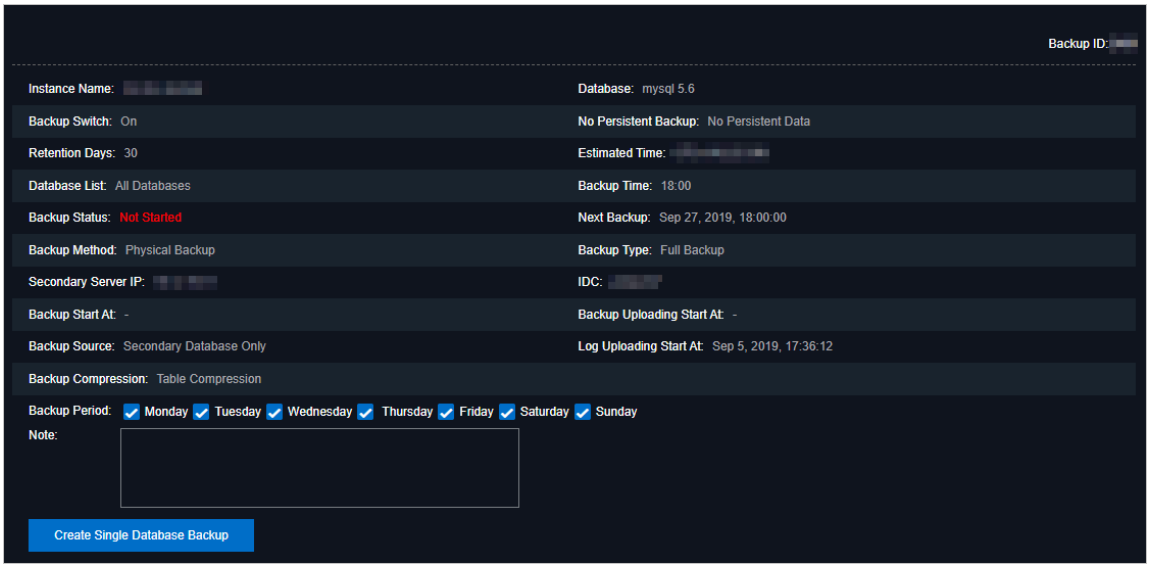



- **Create backups**

  **For ApsaraDB RDS for MySQL instances, click Create Backup in the Actions column to view the backup information, as shown in *Figure 2-5: Backup information*.**

**You can also click Create Single Database Backup on the Backup Information page to back up a single database.**

Figure 2-5: Backup information

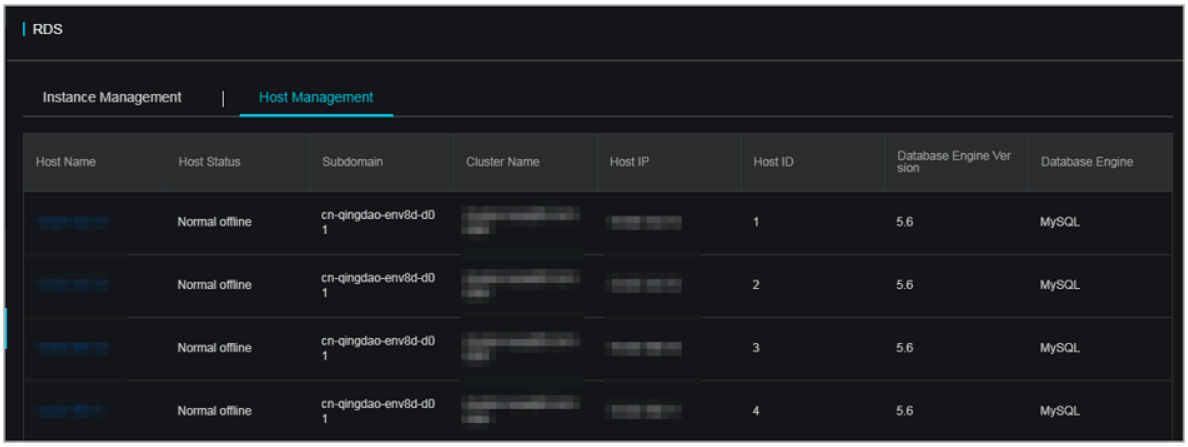



## 2.1.1.4 Manage hosts

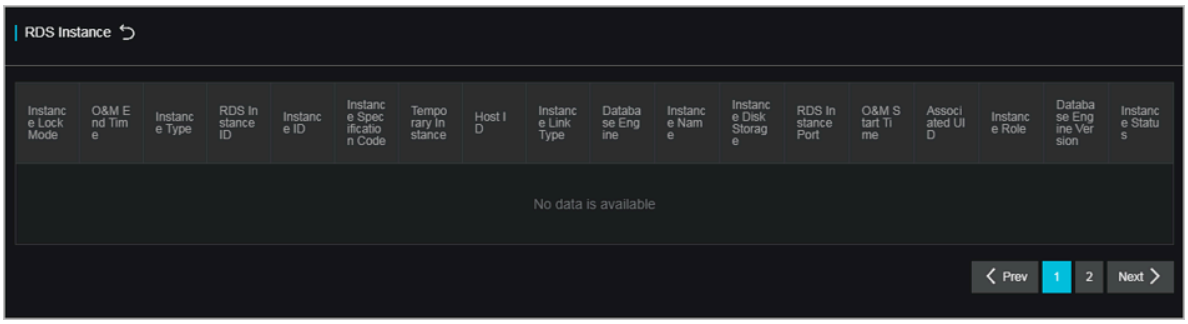
**You can view and manage hosts.**

### Procedure

1. *Log on to the Apsara Stack Operations console*.
2. **In the left-side navigation pane, choose Products > RDS.**
3. **On the Host Management tab of RDS, you can view all host information.**



4. **Click a hostname to go to the RDS Instance page. You can view all instances on this host.**




## 2.1.1.5 Security maintenance

### 2.1.1.5.1 Network security maintenance

**Network security maintenance consists of device and network security maintenance.**

Device security

**Check network devices and enable their security management protocols and configurations of devices.**

**Check for timely updates to secure versions of network device software.**

**For more information about the security maintenance method, see the device documentation.**

Network security

**Based on your network considerations, select the intrusion detection system (IDS ) or intrusion prevention system (IPS) to detect abnormal Internet and Intranet traffic and protect against attacks.**

### 2.1.1.5.2 Account password maintenance

**Account passwords include RDS system passwords and device passwords.**

**To ensure account security, you must periodically change the system and device passwords, and use passwords with high complexity.**

## 2.1.2 AnalyticDB for PostgreSQL

## 2.1.2.1 Overview

Purpose

**This guide summarizes possible problems that you may encounter during O&M operations and provides solutions for you.**

**If you encounter system problems not covered in this guide, you can submit a ticket to Alibaba Cloud for technical support.**

Requirements

**You must possess IT skills including computer network knowledge, computer operation knowledge, problem analysis, and troubleshooting.**

**Additionally, you must pass the pre-job training of the Alibaba Cloud system to learn necessary Alibaba Cloud system knowledge, including but not limited to system principles, networking, features, and the use of maintenance tools.**

**Note that during maintenance operations, you must comply with operating procedures to ensure personal and system security. User data must be kept strictly confidential and must not be copied or disseminated without the written consent of the users.**

Precautions

**To ensure a stable system and avoid unexpected events, you must follow the following guidelines.**

- **Hierarchical permission management**

  **Permissions on networks, devices, systems, and data are granted based on the services and roles of the O&M personnel to prevent system faults caused by unauthorized operations.**
- **System security**

  **Before performing any system operations, you must be aware of their impacts.**

  **You must record all problems encountered during operations for problem analysis and troubleshooting.**

- **Personal and data security**
  - **You must take safety measures in accordance with the device manuals when operating electrical equipment.**
  - **You must use secure devices to access the business network.**
  - **Unauthorized data replication and dissemination are prohibited.**

Support

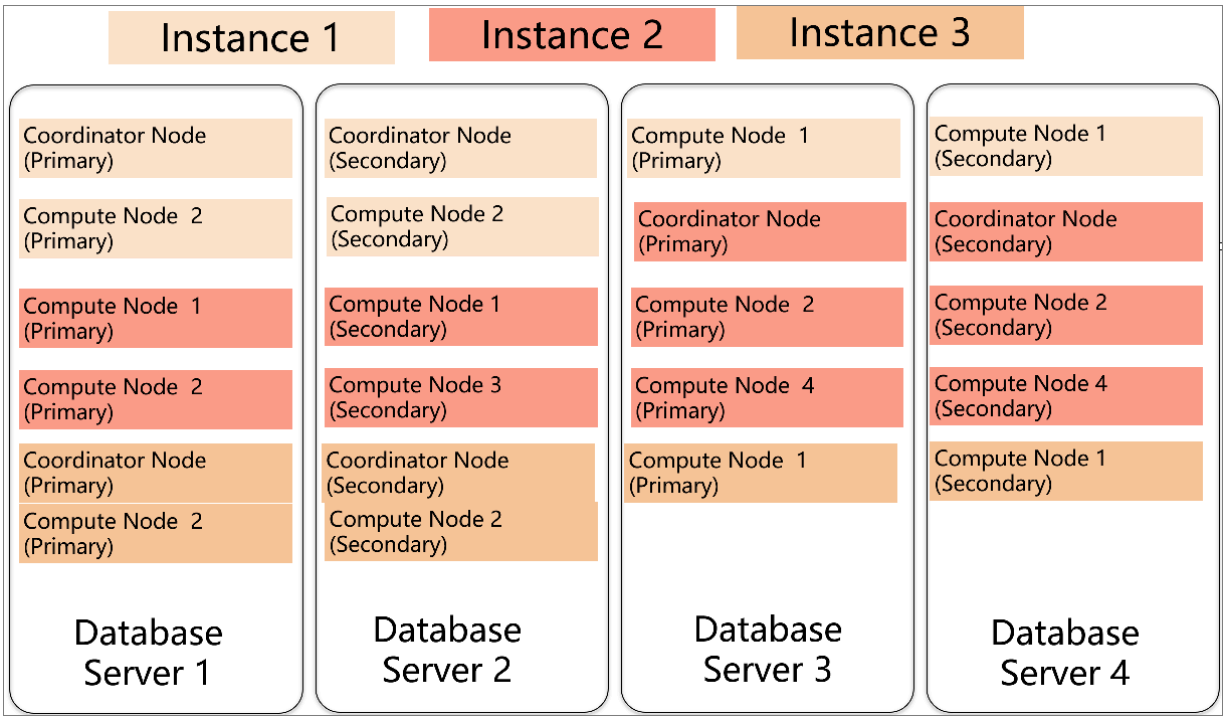
**You can contact Alibaba Cloud technical support for help.**

## 2.1.2.2 Architecture

Physical cluster architecture

**The following figure shows the physical cluster architecture of AnalyticDB for PostgreSQL.**

Figure 2-6: Physical cluster architecture




**You can create multiple instances within a physical cluster of AnalyticDB for PostgreSQL. Each cluster includes two components: the coordinator node and the compute node.**

- **The coordinator node is used for access from applications. It receives connection requests and SQL query requests from clients and dispatches computing tasks to compute nodes. The cluster deploys a secondary node of the coordinator node**

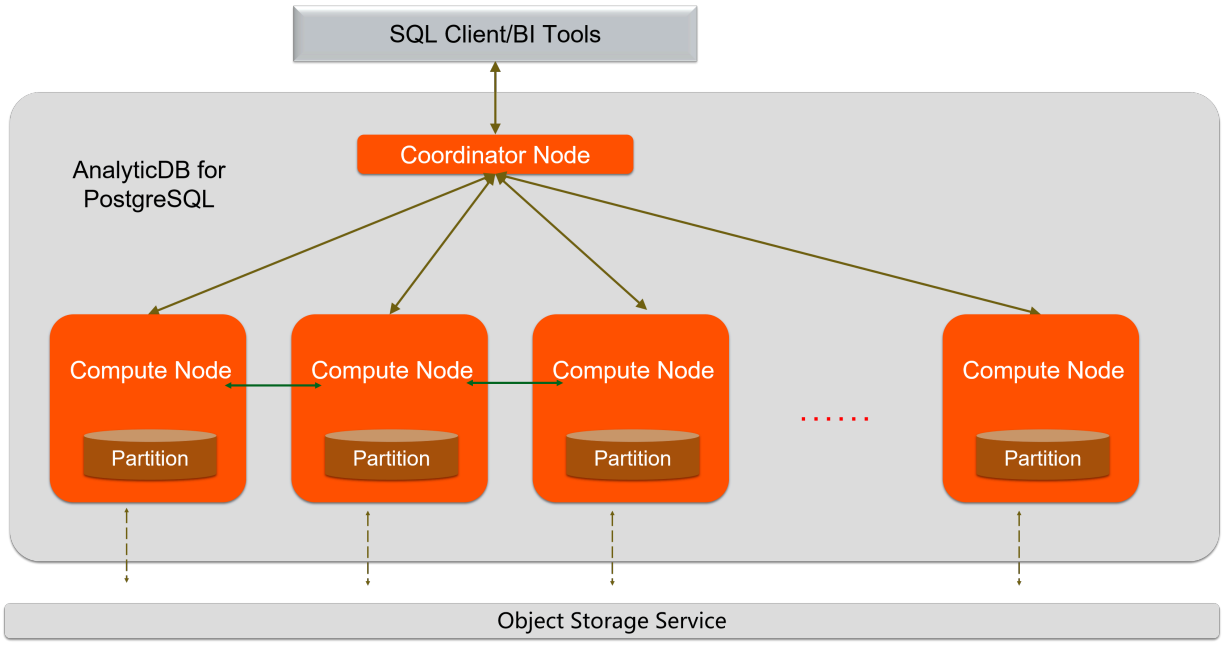
on an independent physical server and replicates data from the primary node to the secondary node for failover. The secondary node does not accept external connections.

- Compute nodes are independent instances in AnalyticDB for PostgreSQL. Data is evenly distributed across compute nodes by hash value or RANDOM function , and is analyzed and computed in parallel. Each compute node consists of a primary node and a secondary node for automatic failover.

Logical architecture of an instance

You can create multiple instances within a cluster of AnalyticDB for PostgreSQL. The following figure shows the logical architecture of an instance.

Figure 2-7: Logical architecture of an instance




Data is distributed across compute nodes by hash value or RANDOM function of a specified distributed column. Each compute node consists of a primary node and a secondary node to ensure dual-copy storage. High-performance network communication is supported across nodes. When the coordinator node receives a request from the application, the coordinator node parses and optimizes SQL statements to generate a distributed execution plan. After the coordinator node sends the execution plan to the compute nodes, the compute nodes will perform an MPP execution of the plan.

## 2.1.2.3 Routine maintenance

## 2.1.2.3.1 Check for data skew on a regular basis

**You must check for data skew on a regular basis during maintenance to prevent the instance from being read-only due to excessive data in some compute nodes.**

**You can use the following methods to locate data skew. The procedure is as follows.**

1. **For a single table or database, you can view the space occupied within each compute node to determine whether data has been skewed.**
   a. **Execute the following statement to determine whether the data in a database has been skewed:**

      ```
      SELECT pg_size_pretty(pg_database_size('postgres')) FROM
      gp_dist_random('gp_id');
      ```

      **You can view the space occupied by the dbname database in each compute node after the statement is executed. If the space occupied in one or more compute nodes is significantly greater than that of other compute nodes, it indicates the data in this database is skewed.**
   b. **Execute the following statement to determine whether the data in a table has been skewed:**

      ```
      SELECT pg_size_pretty(pg_relation_size('tblname')) FROM gp_dist_ra
      ndom('gp_id');
      ```

      **Using the preceding statement, you can view the space occupied by the tblname table within each compute node after the statement is executed. If the space occupied within one or more compute nodes is significantly greater than that of other compute nodes, it indicates the data in this table is skewed. You must modify the partition key to redistribute the data.**

2. You can use the system views to determine whether data has been skewed.
   a. Execute the following statement to check whether the storage space is skewed. The principle of this method is similar to that of the preceding space-viewing method:

      ```
      SELECT * FROM gp_toolkit.gp_skew_coefficients
      ```

      You can use the view to check the data volume of rows in a table. The larger the table, the more time it will take for the check to complete.
   b. Use the gp_toolkit.gp_skew_idle_fractions view to calculate the percentage of idle system resources during a table scan to check whether the data is skewed:

      ```
      SELECT * FROM gp_toolkit.gp_skew_idle_fractions
      ```

      For more information, see *Checking for Uneven Data Distribution*.

#### 2.1.2.3.2 Execute VACUUM and ANALYZE statements

You can execute `VACUUM` and `ANALYZE` statements on a regular basis for frequently updated tables and databases. You can also execute `VACUUM` and `ANALYZE` statements after you have performed a large number of update or write operations to prevent the operations from consuming excessive resources and storage space.

### 2.1.2.4 Security maintenance

#### 2.1.2.4.1 Network security maintenance

Regular maintenance will help ensure the security of networks and devices.

Device security

Check network devices and enable the security management protocols and configurations for the devices you want to secure. Check for up-to-date versions of network device software and update the software to more secure versions in a timely manner. For more information about security maintenance methods, see the product documentation of each device.

Network security

You can select the intrusion detection system (IDS) or intrusion prevention system (IPS) based on the network status to check public and internal traffic, and defend the network against abnormal behaviors and attacks.

#### 2.1.2.4.2 Account password maintenance

**Account passwords include the superuser password of AnalyticDB for PostgreSQL and the password of the host operating system.**

**To ensure account security, use complex passwords and periodically change the passwords of systems and devices.**

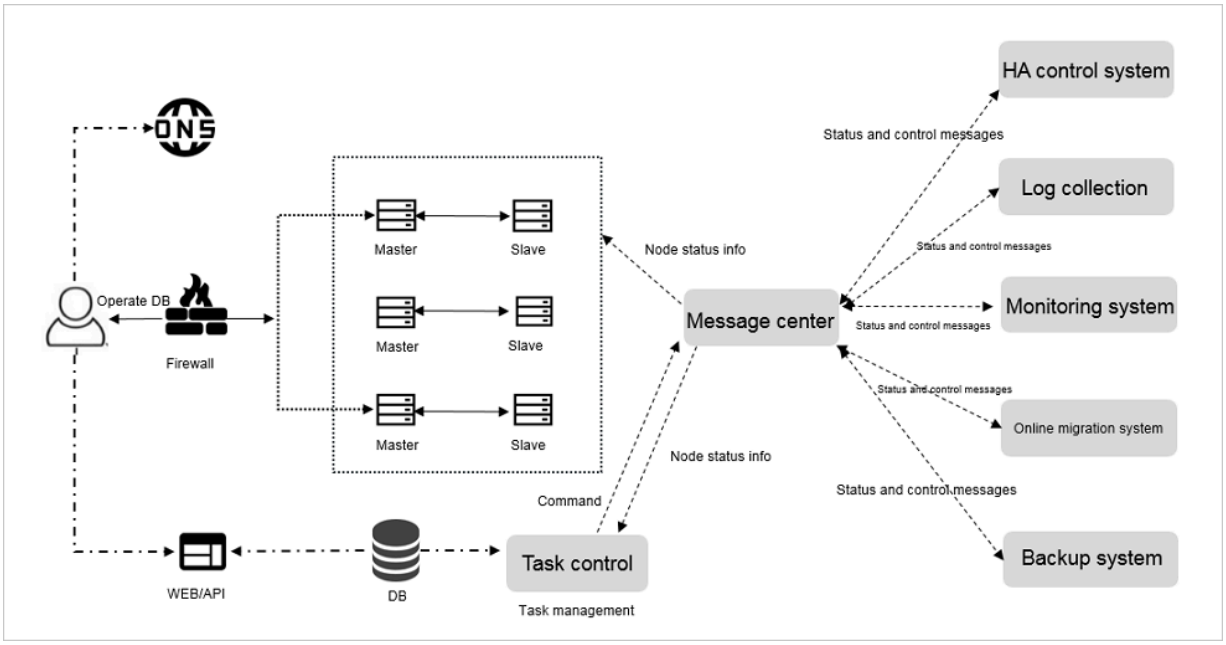
## 2.1.3 KVStore for Redis

### 2.1.3.1 O&M tool

**The Apsara Stack Operation console provides the following operations and maintenance (O&M) features for KVStore for Redis:**

- **Instance management: allows you to view instance details, instance logs, and user information.**
- **Host management: allows you to view and manage hosts.**

### 2.1.3.2 Architecture diagram




### 2.1.3.3 Architecture

#### 2.1.3.3.1 Architecture

#### 2.1.3.3.1.1 Backup system

Automatic backup

**KVStore for Redis supports full backup. You can flexibly configure backup start time based on off-peak hours of your business. The system retains backup files for seven days or fewer.**

Temporary backup

**You can create temporary backups as needed. The system retains backup files for seven days or fewer.**

#### 2.1.3.3.1.2 Data migration system

Migrate data to and from KVStore for Redis

**KVStore for Redis provides professional tools and migration wizards to help you migrate data to or out of KVStore for Redis.**

Download backup files

**KVStore for Redis retains backup files for seven days or fewer. During this period, you can log on to the KVStore for Redis console to download the files.**

#### 2.1.3.3.1.3 Monitoring system

Performance monitoring

**KVStore for Redis provides a variety of system performance metrics, including disk capacity, memory usage, connections, CPU usage, network traffic, QPS, and request command operations. You can check the running status information within a period of one year for an instance.**

Threshold alerts

**KVStore for Redis can notify you of alerts by means of SMS messages in the case of exceptions in instance status or performance.**

**These exceptions involve instance locked status, disk capacity, input/output operations per second (IOPS), connections, and CPU usage. You can customize alert thresholds and configure 50 alert contacts or fewer. Five of these alert contacts can take effect at the same time. When an instance exceeds the threshold, the system sends SMS messages to the corresponding alert contacts.**

Web operation logs

**The system keeps logs for all changes in the KVStore for Redis console. Therefore, the administrator can check these logs. The system retains logs for 30 days or fewer .**

#### *2.1.3.3.1.4 Control system*

**After a host or instance crashes, the KVStore for Redis high-availability (HA) component checks for the exception and performs the failover operation within 30 seconds. This guarantees that applications run normally and the KVStore for Redis service is highly available.**

#### *2.1.3.3.1.5 Task scheduling system*

**You can use the KVStore for Redis console or KVStore for Redis API operations to create and delete instances or switch instances between the internal and public networks. The backend schedules, traces, and displays all instance operations as tasks.**

### 2.1.3.4 Log on to the Apsara Stack Operations console

**Prerequisites**

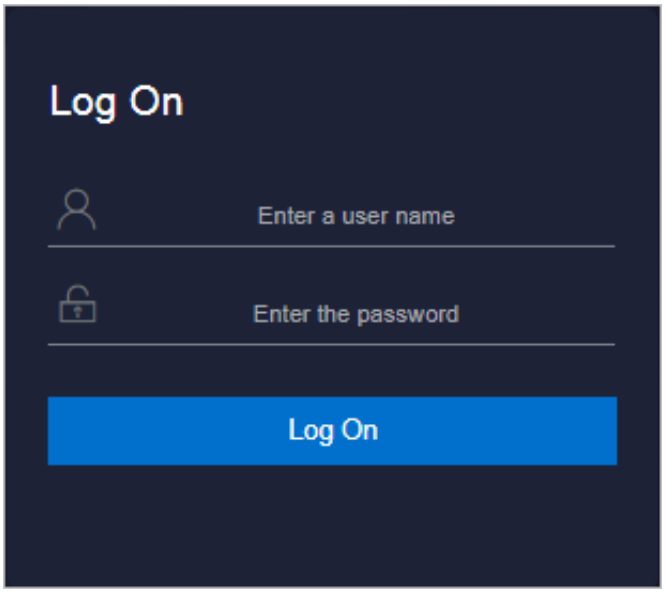
- **ASO access address in the format of http://***region-id***.aso.***intranet-domain-id***.com.**
- **Google Chrome browser (recommended).**

**Procedure**

1. **Open the browser.**

2. **Enter the ASO access address http://*region-id*.aso.*intranet-domain-id*.com in the address bar and then press Enter.**

   Figure 2-8: Log on to ASO




   **Note:**
   **You can select the language from the drop-down list in the upper-right corner to change the language of ASO.**

3. **Enter the correct username and password.**
   - **The system has three default users:**
     - **Security officer: manages other users or roles.**
     - **Auditor officer: views audit logs.**
     - **System administrator: used for other functions except those of the security officer and auditor officer.**
   - **You must modify the password of your username as instructed when you log on to ASO for the first time. To improve security, the password must be 10-20 characters long and can contain English uppercase/lowercase letters (A-Z or a-z), numbers (0-9), and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%), which meets the minimum complexity requirements.**
4. **Click Log On to log on to ASO.**

## 2.1.3.5 Instance management

**You can view instance details, logs, and user information.**

**Procedure**

1. *Log on to the Apsara Stack Operations console*.
2. **In the left-side navigation pane, choose Products > RDS to go to the RDS page. Click the Instance Management tab. On the Instance Management tab, you can perform these operations:**
   - **View the list of instances.**

     **On the Instance Management tab, you can view the instances under your account.**
   - **View the details of an instance.**

     **Click the ID of a target instance to view the details of the instance.**
   - **View user information.**

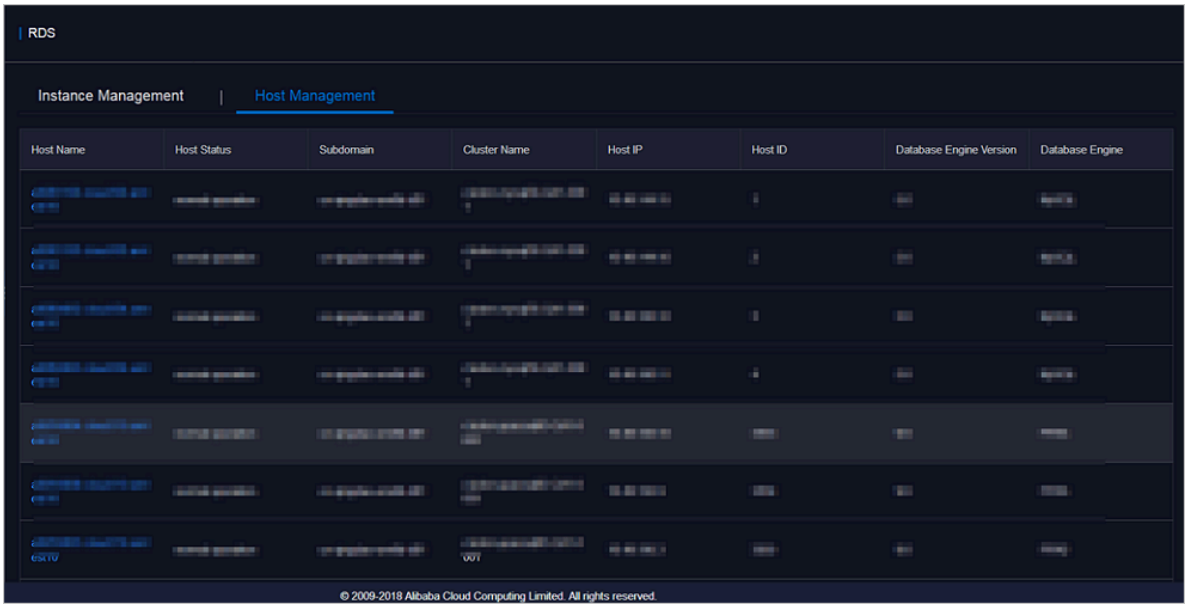
     **Click User Information in the Actions column.**

## 2.1.3.6 Host management

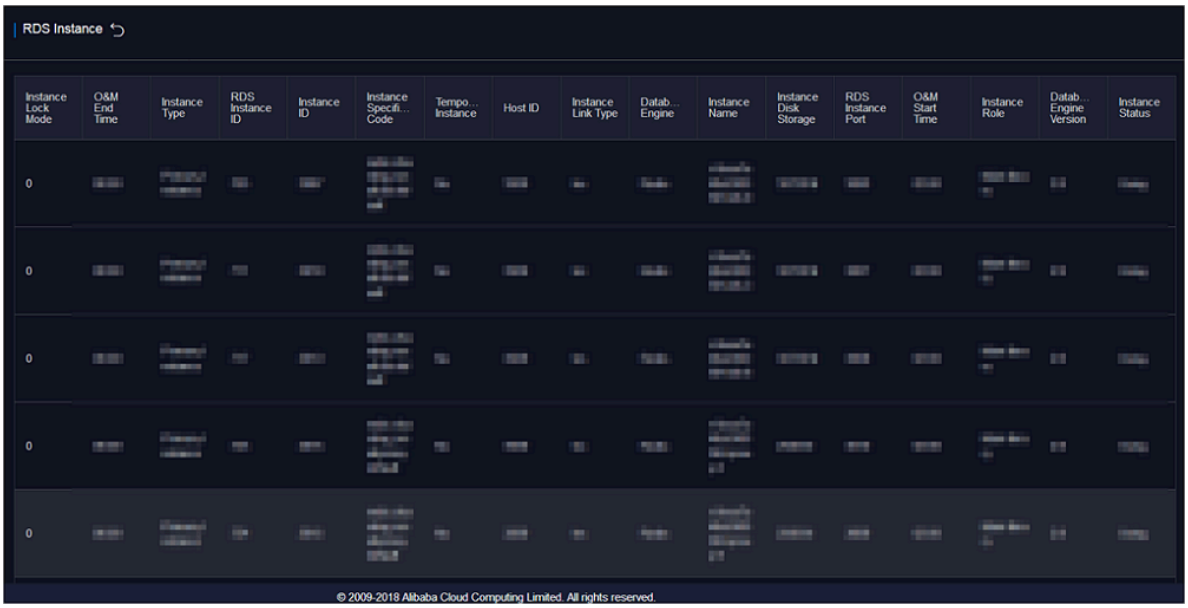
**Host management allows you to view and manage hosts.**

**Procedure**

1. *Log on to the Apsara Stack Operations console*.
2. **In the left-side navigation pane, choose Products > RDS to go to the RDS page. Click the Host Management tab to view the information about all hosts.**



3. **Click a host name to go to the RDS Instance page. You can view all instances on this host.**




## 2.1.3.7 Security maintenance

## 2.1.3.7.1 Network security maintenance

**Network security maintenance involves device security and network security.**

Device security

**Check network devices, and enable security management protocols and configurations for these devices.**

**Check software versions of network devices and update them to more secure versions in time.**

**For more information about security maintenance methods, see documents of related devices.**

Network security

**Based on your network conditions, select the intrusion detection system (IDS) or intrusion prevention system (IPS) to detect abnormal Internet and intranet traffic and protect against abnormal behavior and attacks in real time.**

## 2.1.3.7.2 Password maintenance

**Passwords include system passwords and device passwords in KVStore for Redis.**

**To secure your account, you must periodically change the system and device passwords, and use complex passwords.**

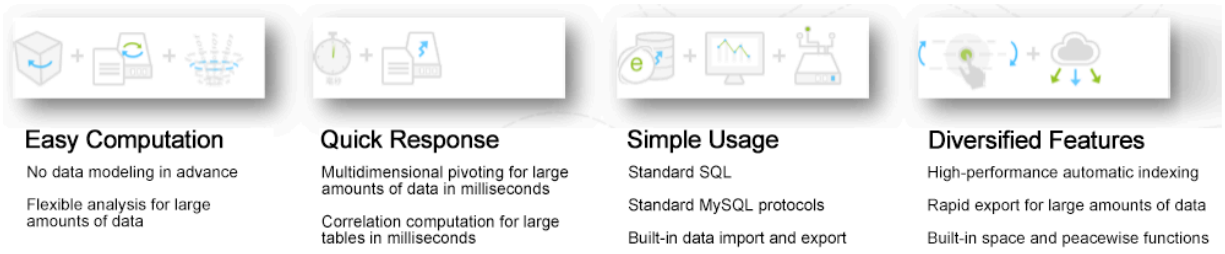
# 2.2 Operations of big data products

## 2.2.1 AnalyticDB for MySQL

### 2.2.1.1 What is AnalyticDB for MySQL?

**AnalyticDB for MySQL (originally named ADS) is an Alibaba Cloud developed real-time online analytical processing (RT-OLAP) service that enables online analytics of large amounts of data at high concurrency. It can analyze hundreds of billions of data records from multiple dimensions at millisecond-level timing to provide you with data-driven insights into your business.**

**Able to compute large amounts of data with quick response, AnalyticDB for MySQL enables you to instantly and agilely explore and find data value. You can also embed AnalyticDB for MySQL into a business system to provide end users with analysis services.**




**AnalyticDB for MySQL can perform low latency, high concurrency, and real-time online processing and retrieval for large amounts of data. AnalyticDB for MySQL is widely used by enterprises for real-time multidimensional analysis, by businesses for customer group selection and analysis, and by government agencies for flexible big data retrieval and statistics. AnalyticDB for MySQL has been used in Internet business systems that have hundreds of thousands to tens of millions of users, such as Data Cube, Taobao Index, Kuaidi Dache, Alimama DMP, and Taobao Groceries.**

Key technology: storage

**AnalyticDB for MySQL provides two storage modes:**

- **High-performance storage: delivers good query and concurrent processing performance but requires high storage costs with SSDs. This storage mode is**

**suitable for scenarios where large amounts of data is flexibly analyzed or queried with high concurrency.**

- **Large-capacity storage: features low storage costs, but provides lower query and concurrent processing performance than high-performance storage. This storage mode is suitable for scenarios where details are queried from large amounts of data or low concurrency and high latency analysis are required.**

**AnalyticDB for MySQL uses column store to store data of tables. Each table can consist of over 1,000 columns. Column store has the following features:**

- **Advantage: Only a few I/O resources are required when data analysis or statistics is performed or when a small number of columns are queried within a wide table.**
- **Disadvantage: Highly distributed data requires excessive I/O resources when many columns are queried.**
- **Unique feature: Data presorting of aggregate columns can help mitigate the downsides.**

Scenarios

- **Application type**

  **This type of business provides simple queries which do not require joins of multiple tables and only return small amounts of data.**

- **BI type**

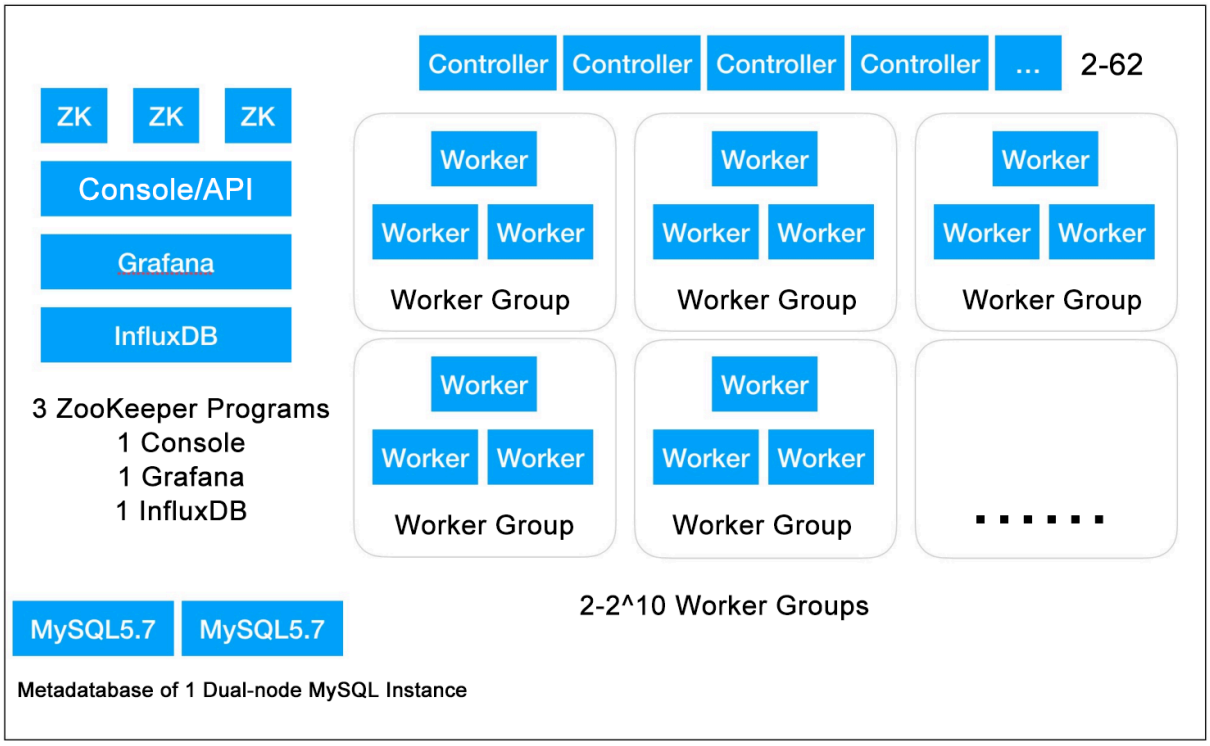
  **This type of business provides a real-time data warehouse where real-time tables are joined with multiple dimension tables to sort and divide data into many groups.**

- **Ad-hoc type**

  **This type of business provides complex analysis by joining multiple real-time tables to sort and group data or return over 500 data records.**

## 2.2.1.2 Architecture

### 2.2.1.2.1 System architecture



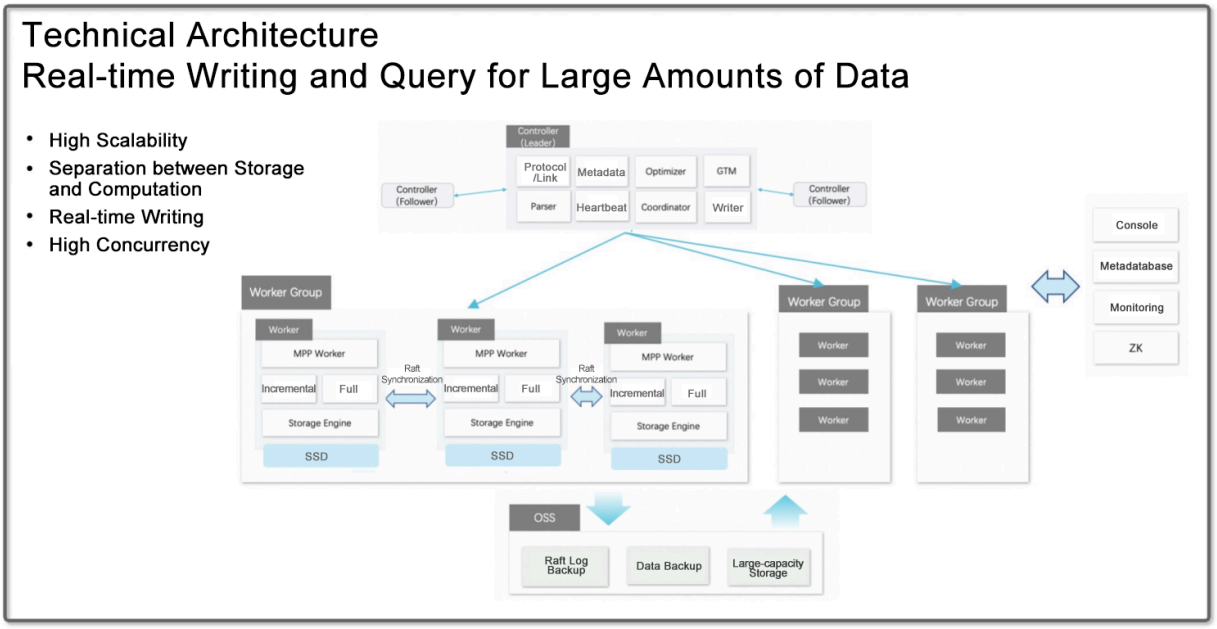

- **AnalyticDB for MySQL is compatible with the MySQL protocol and supports JDBC , ODBC, and RESTful APIs. It is compatible with third-party user data analysis applications, Apsara Stack Quick BI and DataV, and commercial BI tools such as Tableau and QlikView.**
- **AnalyticDB for MySQL can exchange data with MaxCompute, ApsaraDB for RDS, and OSS in Apsara Stack.**
- **Controllers parse, plan, and optimize SQL statements. Server Load Balancer (SLB) can be deployed at the frontend for load balancing.**

  **Workers compute and store data. A worker group is composed of three workers. Each cluster can consist of more than two worker groups.**
- **AnalyticDB for MySQL functional modules include controllers, worker groups, Zookeeper, InfluxDB, Grafana, console, and MySQL.**
- **AnalyticDB for MySQL clusters store metadata for control and scheduling.**
- **ZooKeeper manages the configurations of AnalyticDB for MySQL modules and elects primary and secondary nodes of the modules.**
- **DMS provides access to the data management console.**

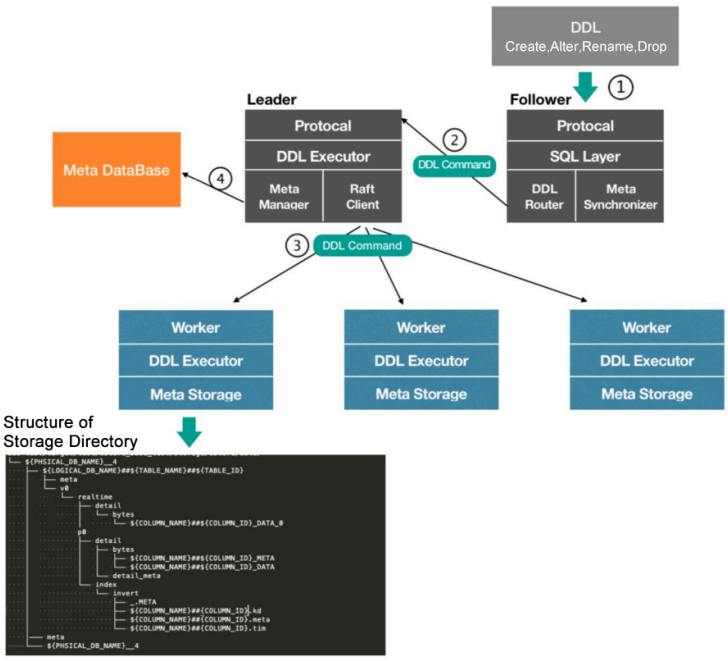
# 2.2.1.2.2 Components and features

Online resource scheduling module

**The online resource scheduling module is an online service module of Job Scheduler. This module provides cluster application, management, and scheduling for online services.**




Kernel: SQL Execution



- **Cluster application: applies for computing and storage resources from the resource pool based on cluster specifications.**
- **Cluster management: starts, stops, restarts, or deletes workers.**
- **Cluster scheduling: handles worker failover and backs up data and logs.**

AnalyticDB for MySQL functional modules

**AnalyticDB for MySQL functional modules enable you to query, write, modify, and batch import data.**

**Controller**

- **Authenticates database users.**
- **Supports JDBC and ODBC protocols. The controller proxy service supports RESTful APIs.**
- **Reads table schemas from RDS when creating or querying tables.**
- **Parses SQL statements, delivers statements for other functional modules to execute, aggregates query results, and returns them to clients.**
- **Delivers the CREATE and DROP operations of databases and tables for the resource manager (RM) to execute.**
- **Reads the configuration from ZooKeeper upon startup and uses ZooKeeper to select the primary discovery server in MPP mode.**
- **Parses, plans, optimizes, and executes SELECT statements, reads indexes and data from a local file system, and returns results.**
- **Extracts worker-imported data or worker-created indexes from the worker cache or file system.**

**Worker**

- **Works in a mode with one primary/secondary coordinator and multiple workers.**
- **Processes data imported in real time. A worker processes one or more table partitions.**
- **Executes INSERT statements from controllers, logs INSERT operations into the file system for primary/secondary replication and disaster recovery, and pushes inserted data to the primary compute node so that data is visible in real time.**
- **Reads the ZooKeeper configuration upon startup and uses ZooKeeper to select the primary coordinator.**

- **Uses MaxCompute MapReduce to import offline data and creates partitions, row groups, metadata, and indexes for imported data.**
- **Uses AnalyticDB for MySQL MapReduce to periodically merge the baselines of imported data and creates partitions, row groups, metadata, and indexes for imported data.**

**RM**

- **Schedules resources through Gallardo APIs to:**
  - **Assign or cancel the controller and worker services for new and deleted databases.**
  - **Start or stop services.**
  - **Isolate resources such as CPU and memory.**
- **Schedules data to allocate partition metadata for real-time tables of workers and saves the data to RDS.**
- **Checks system health status.**
- **Upgrades or rolls back the system online.**
- **Scales the system in or out.**
- **Reads the configurations from ZooKeeper upon startup and uses ZooKeeper to select the primary RM.**

## 2.2.1.2.3 Node group specifications

**Node groups are the basic unit to distribute storage and computing resources in AnalyticDB for MySQL. Node groups provide the following resources:**

- **CPU: the available CPU cores.**
- **Memory: the available memory size.**
- **Disk space: the available disk space.**

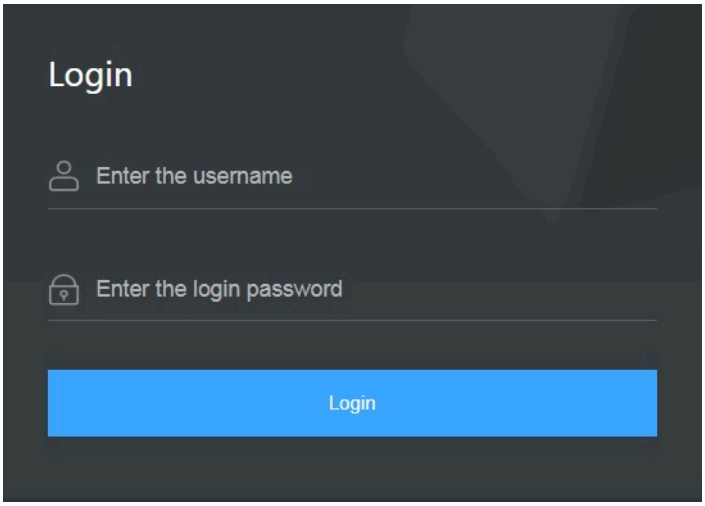
## 2.2.1.3 AnalyticDB for MySQL console

**The AnalyticDB for MySQL console allows you to create or delete database clusters, change specifications of clusters, and manage database accounts.**

## 2.2.1.3.1 Cluster management

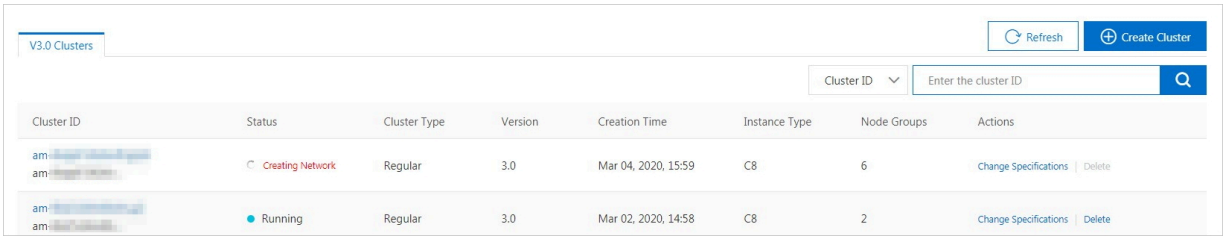
### *2.2.1.3.1.1 Log on to the console*

**Enter a username and password to log on to the console, as shown in the following figure.**




## 2.2.1.3.1.2 Manage a cluster

**In the top navigation bar, choose Products > Database Services > AnalyticDB for MySQL to log on to the AnalyticDB for MySQL console. You can view the list of clusters and their statuses.**




**The console contains the following information:**

- **Clusters: lists all clusters and their statuses.**
- **Create Cluster: allows you to create a database cluster.**
- **Actions: allows you to change specifications of a cluster or delete a cluster.**

## 2.2.1.3.1.3 Create a database cluster

**This topic describes how to create an AnalyticDB for MySQL cluster.**

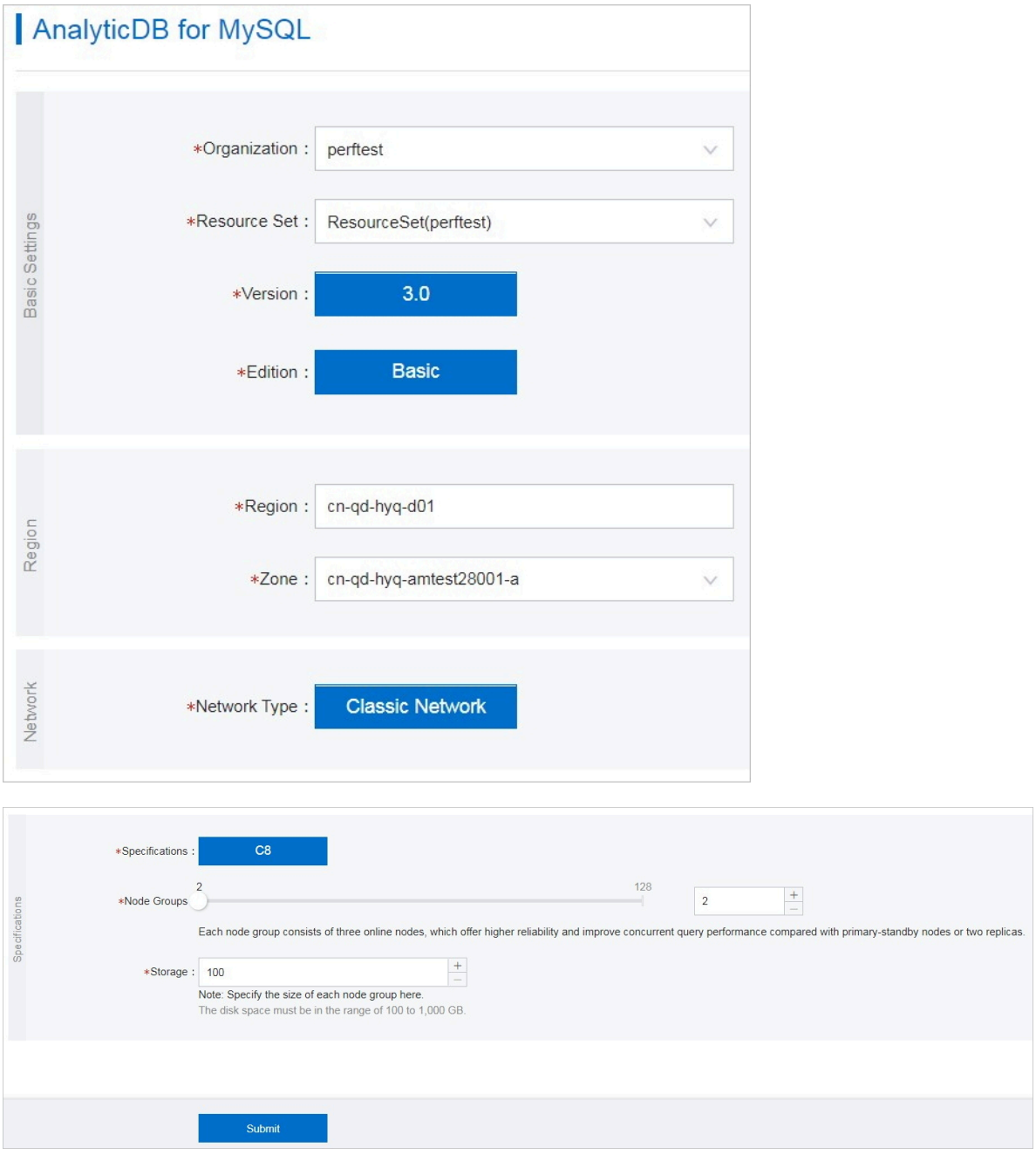
**Procedure**

1. *Log on to the console*.

2. Click Create Cluster in the upper-right corner of the Clusters page and configure parameters as prompted.

| Parameter | Description |
| --- | --- |
| Region | The region where the cluster resides. You cannot change the region after the cluster is created. We recommend that you select a region that is closest to the geographic area of your business to improve access speed and stability. |
| Zone | The zone of the cluster. A zone is an independent physical area located within a region. There are no substantive differences between zones. |
| Organization | The organization to which the cluster belongs. |
| Resource Set | The resource set of the cluster. |
| Version | Only version 3.0 is supported. |
| Edition | Only Basic is supported. |
| Network Type | AnalyticDB for MySQL only supports classic networks.<br>Cloud services in a classic network are not isolated. Access control to cloud services in a classic network is implemented by the security groups or whitelist policies of the services. |
| Specifications | The ECU specifications. |
| Node Groups | The number of node groups. By default, each node group consists of three replicas. |

| Parameter | Description |
| --- | --- |
| Storage | The storage space of a node group. |




3. After you have configured the preceding parameters, click Submit.

## 2.2.1.3.1.4 View monitoring information

You can view cluster monitoring information in real time in the AnalyticDB for MySQL console.

### Procedure

1. *Log on to the console*.

2. **In the upper-left corner of the page, select the region where the cluster resides.**
3. **On the Clusters page, click Cluster ID corresponding to the cluster.**
4. **In the left-side navigation pane, click Monitoring Information to view the cluster monitoring information.**

   **The monitoring information includes CPU utilization, cluster connections, QPS, and query response time.**

## 2.2.1.3.2 Account management

### *2.2.1.3.2.1 Create a database account*

**This topic describes types of database accounts and how to create accounts in AnalyticDB for MySQL.**

Types of database accounts

**AnalyticDB for MySQL provides two types of database accounts: privileged account and standard account.**

Table 2-1: Types of database accounts

| Type of database account | Description |
| --- | --- |
| **Privileged account** | · **You can only create and manage privileged accounts through the console.**<br>· **You can only create one privileged account for each cluster. Privileged accounts have permissions to manage all standard accounts and databases within a cluster.**<br>· **You can use the privileged account to disconnect any standard accounts from the cluster. You can use the privileged account to manage fine-grained permissions to suit your business needs. For example, you can grant each standard account permissions to query specific tables.**<br>· **A privilege account in AnalyticDB for MySQL is equivalent to a root account in MySQL.** |

| Type of database account | Description |
| --- | --- |
| Standard account | · You can only create and manage standard accounts through SQL statements.<br>· You can create up to 256 standard accounts for a cluster.<br>· You must manually grant specific database permissions to standard accounts.<br>· You cannot use a standard account to disconnect other accounts from the cluster. |

Create a privileged account

1. Log on to the AnalyticDB for MySQL console.
2. In the upper-left corner of the page, select the region where the target cluster is located.
3. On the Clusters page, find the target cluster and click its ID. In the left-side navigation pane, click Accounts. On the Accounts page, click Create Account.
4. In the Create Account dialog box that appears, configure the following parameters.

| Parameter | Description |
| --- | --- |
| Database Account | The name of the privileged account.<br>The name must be 2 to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a lowercase letter and end with a lowercase letter or digit. |
| Account Type | The privileged account, which cannot be modified. |

| Parameter | Description |
| --- | --- |
| Password | The password of the privileged account.<br>The password must be 8 to 32 characters in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. Special characters include ! @ # $ % ^ & * ( ) _ + - = |
| Confirm Password | Re-enter the password of the privileged account. |
| Description | Optional. The description of the database account. |

5. Click OK.

Create a standard account

For information about how to create a standard account and grant permissions, see `CREATE USER` in *User Guide*.

## *2.2.1.3.2.2 Manage database accounts and permissions*

- For more information about how to create a RAM user, see `CREATE USER.`
- For more information about how to grant permissions to a RAM user, see `GRANT`.
- For more information about how to revoke the permissions of a RAM user, see `REVOKE`.
- For more information about how to modify the name of a database account, see `RENAME USER`.
- For more information about how to delete a database account, see `DROP USER`.

## 2.2.1.4 Security maintenance

### 2.2.1.4.1 Network security maintenance

**Network security maintenance helps you ensure device and network security.**

Device security

**Check network devices and enable security management protocols and configurations of devices.**

**Check frequently for up-to-date versions of network device software and update to more secure versions in a timely manner.**

**For more information about the security maintenance method, see the product documentation of each device.**

Network security

**You can select the intrusion detection system (IDS) or intrusion prevention system (IPS) based on the network status to check public and internal traffic, and defend the network against abnormal behaviors and attacks.**

### 2.2.1.4.2 Account password maintenance

**Account passwords include AnalyticDB for MySQL system and device passwords.**

**To ensure account security, you must use complex passwords for your systems and devices and change these passwords on a regular basis.**