ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

apsara base

Apsara Uni-manager Operations Console User Guide

Product Version: v3.16.2

Document Version: 20240715

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

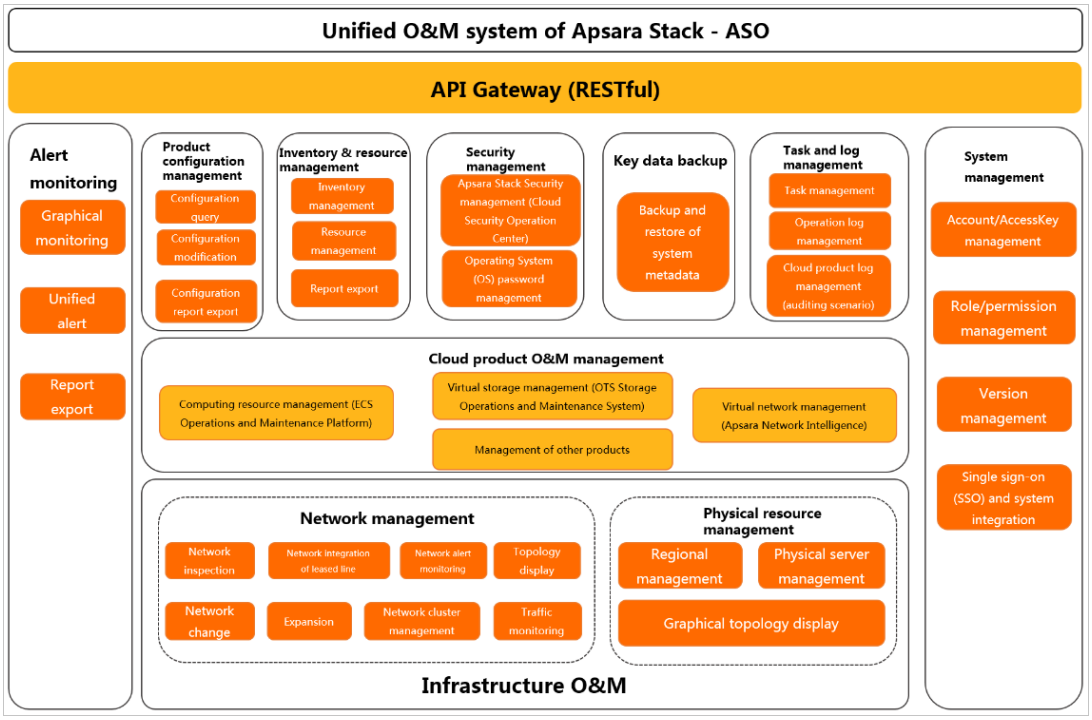
1.Overview

This topic describes the management framework of the Apsara Uni-manager Operations Console.

Management framework of the Apsara Uni-manager Operations Console

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

Figure 1. Apsara Uni-manager Operations Console



Based on ITIL and ISO 20000, the management framework of the Apsara Uni-manager Operations Console uses management support tools to adapt to various management modes in a process-oriented, normalized, and standardized manner. This has implemented the systematic management of the overall process of operations services The management framework of the Apsara Uni-manager Operations Console provides the full lifecycle management methods, management standards, management modes, management supporting tools, management objects, and process-based management methods of IT operations services.

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

Apsara Uni-manager Operations Console

The Apsara Uni-manager Operations Console is a unified and intelligent O&M platform. In accordance with the Information Technology Infrastructure Library (ITIL) and IT Service Management (ITSM) standards, the operations processes and requirements must be abstract, and automation is implemented by using intelligent operations tools. For customized operations, interfaces and multi-level approval must be used to reduce risks.

In the Apsara Uni-manager Operations Console, cloud operations is classified into the following layers: infrastructure, cloud service, and business operations.

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

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

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

O&M support services

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

2.Get started

2.1. Prepare an operations account

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console as a system administrator.
2. Create a role that has the necessary O&M permissions. For more information, see Role management.
3. Create an operations account and assign the created role to the account. For more information, see User management.

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

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

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

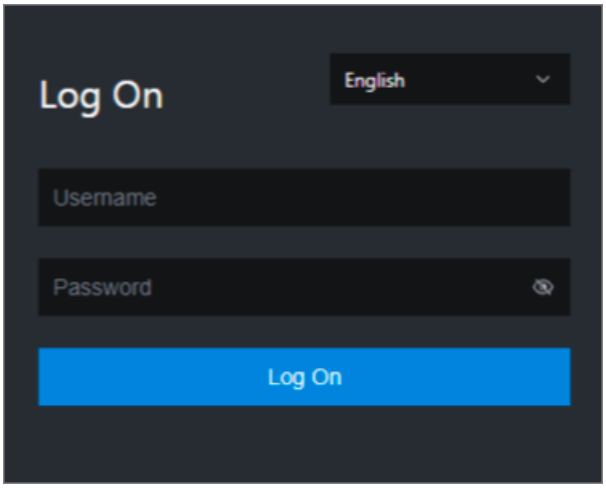
Prerequisites

- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

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

Procedure

1. Open your Chrome browser.
2. In the address bar, enter the endpoint of the Apsara Uni-manager Operations Console. Press the Enter key.



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

3. Enter your username and password.

   > **Note**
   >
   > Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

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

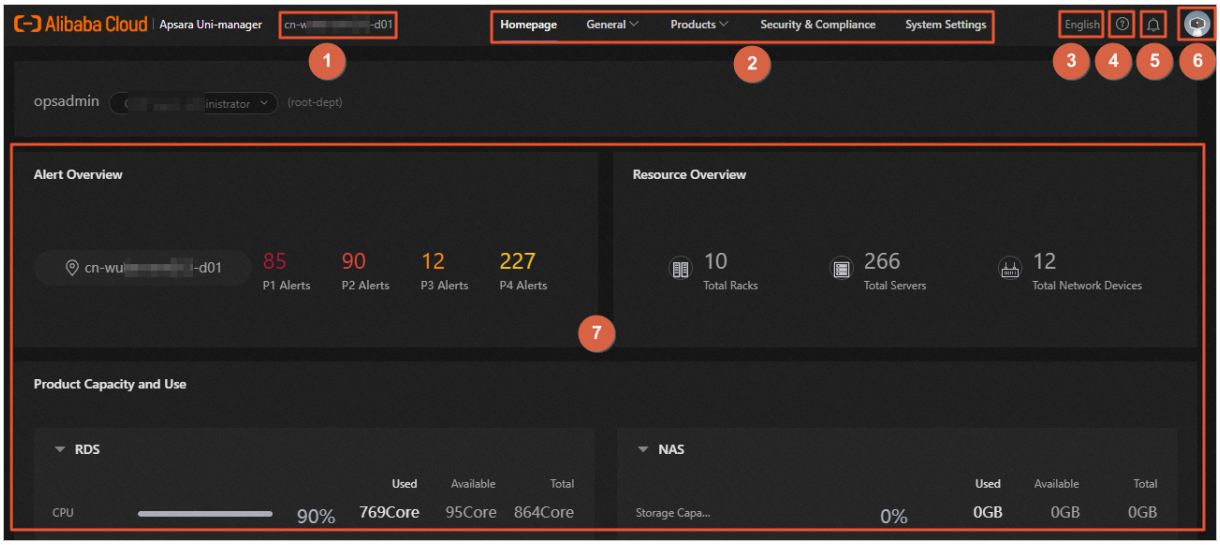
   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains the following special characters: ! @ # $ %
   - The password must be 10 to 20 characters in length.

4. Click **Log On**.

2.3. Apsara Uni-manager Operations Console homepage

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



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

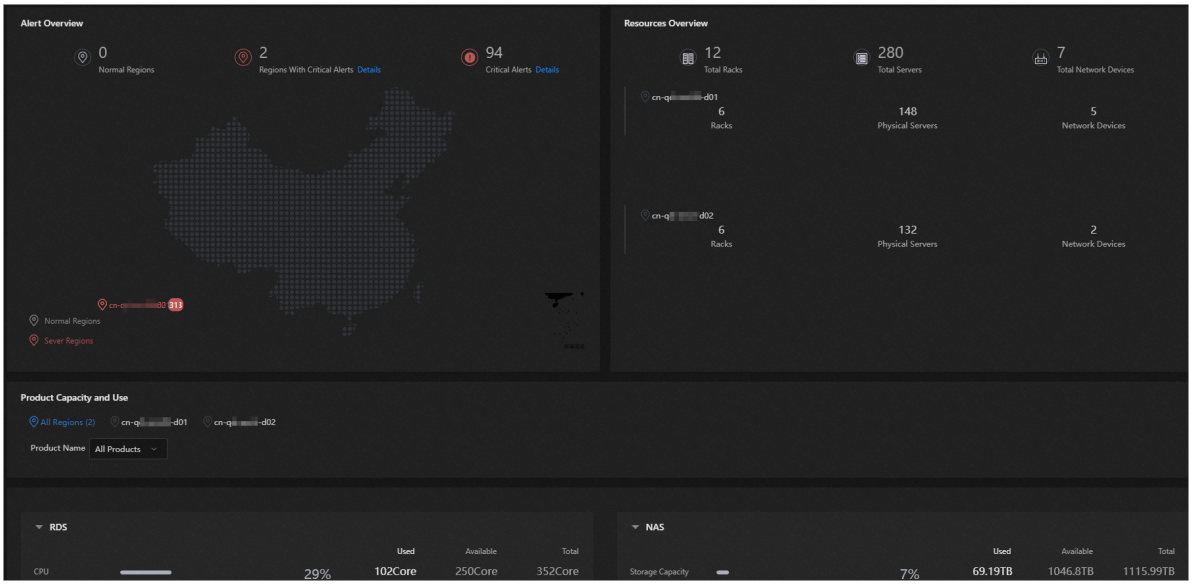
No.	Section	Description
1	Region selector	Select a region from the drop-down list to switch the region. This feature helps you manage all regions in a centralized manner.
2	Top navigation bar	Hover or click for more options.
3	Language	Click to switch the language of the console.
4	Help center	Click to enter the alert knowledge base.
5	Alert	Click to view unhandled critical alerts.
6	Account information and logon settings	Click for options including Personal information, Logon settings, View version information, and Exit.
7	Dashboard	View information and perform operations related to alerts, resources, and resource usage.

2.4. Homepage

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

Procedure

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



The homepage consists of the **Alert Overview**, **Resources Overview**, and **Product Capacity and Use** sections.

- In the **Alert Overview** section, you can view the numbers of regions with no alerts and critical alerts. You can view the names of the regions. You can also view the total number of critical alerts and their distribution among regions.
- In the **Resources Overview** section, you can view the total numbers of racks, servers, and network devices.
- In the **RProduct Capacity and Use** section, you can view the resource quotas and usage of cloud services.

  Cloud service-related metrics are displayed in the following dimensions: total, used, available resources, and their usage.

Cloud service	Metric
ECS	CPU (cores)
	Disk (GB)
	Memory (GB)
RDS	CPU (cores)
	Disk (GB)
	Memory (GB)
SLB	Internal IP Address
	Public IP Address
OSS	Storage Capacity
SLS	SLS-INNER
	SLS-PUBLIC
OTS	Memory (GB)

NAS	Memory (GB)

3.General O&M

3.1. Alert management

3.1.1. Alert overview

You can view alert statistics by region and service. You can also view alerts of a specific region and time point.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Overview**.
3. View alert details in each section.

   The Alert Overview page consists of five sections to provide alert statistics and analysis from different perspectives.

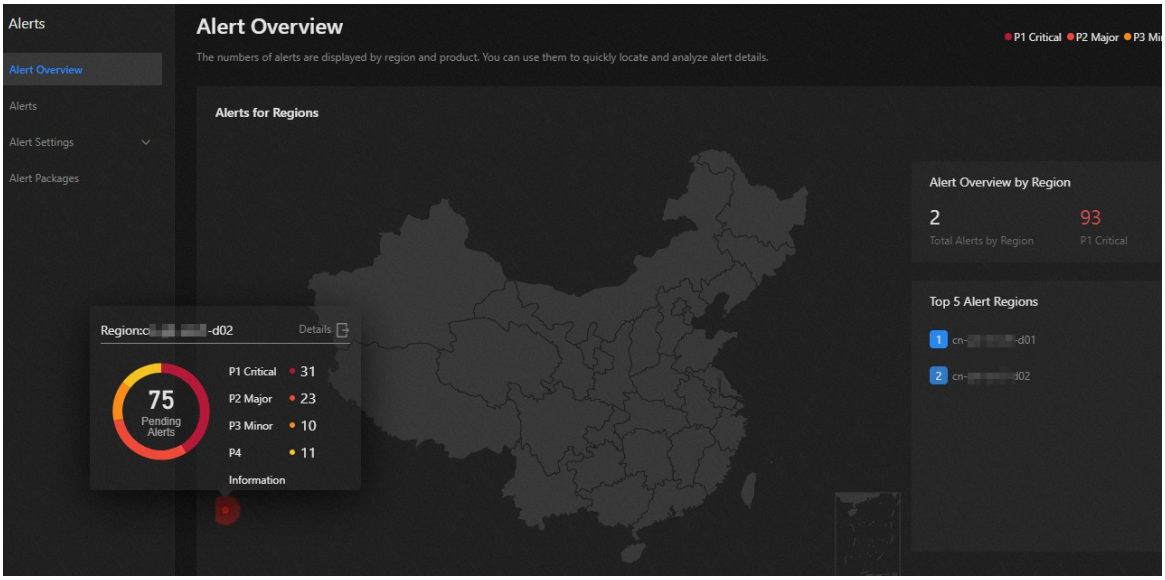
   - The **Alerts for Regions** section shows the number of alerts by level for each region.

     The following figure shows an example for one region.

     - Different colors indicate different levels from P1 to P4.
     - The more the alerts of a level, the larger the corresponding color takes up the ring chart.

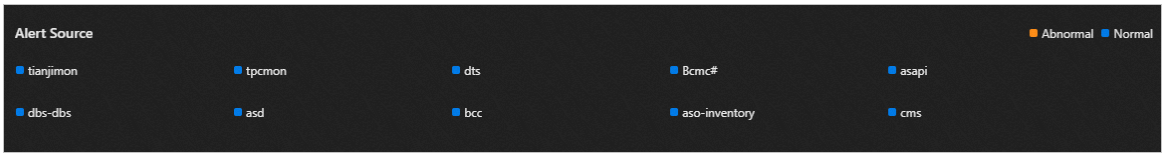
     The following figure shows an example for multiple regions.

     - Bright dots indicate that there are alerts in the regions.

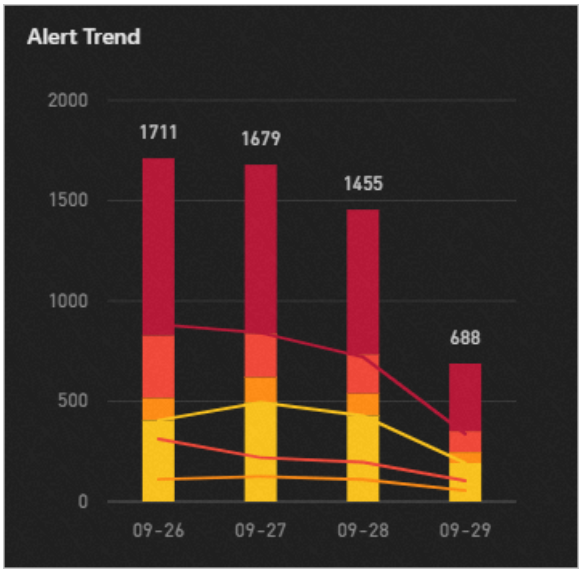
- The colors of the dots indicate different levels of the alerts. The darker the color, the higher the level.
- A larger dot indicates more alerts in the region.
- On the right of the map, the total number of regions that have alerts, the total number of P1 alerts, and the top five abnormal regions are displayed.

- The **Alert Source** section shows the status of each alert source.



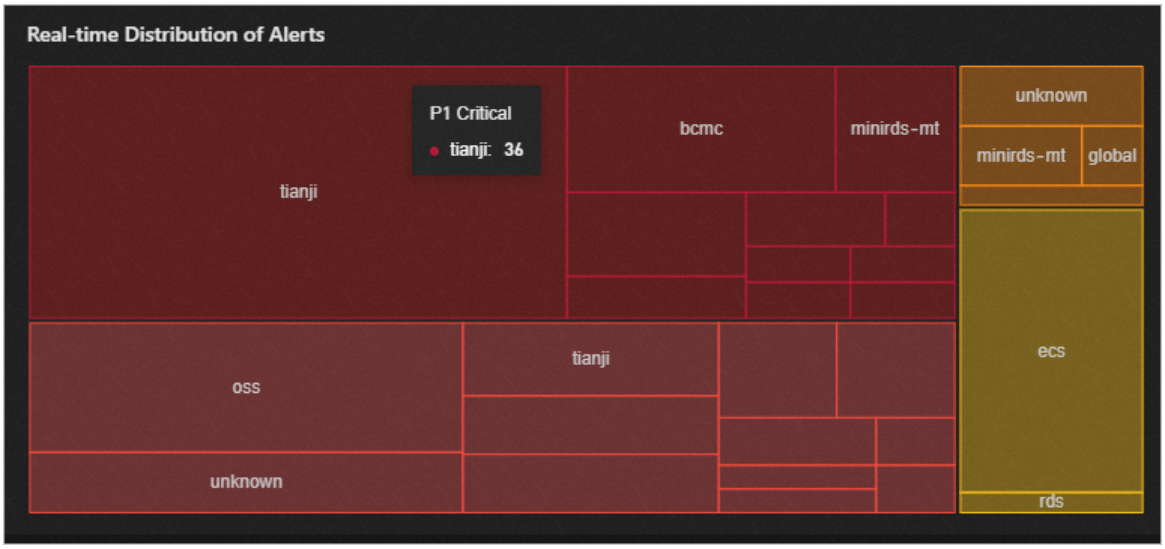
> **Note**
>
> Orange indicates that the alert source is abnormal. Blue indicates that the alert source is normal.

- The **Alert Trend** section shows the number of alerts by day.



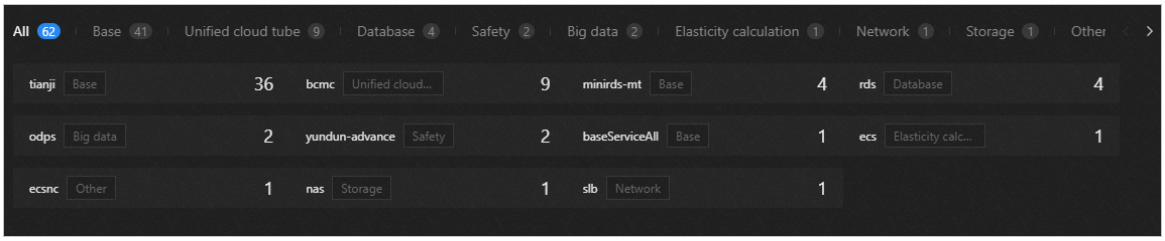
- The bar chart shows changes in the numbers of alerts on different days.
- Colors on each bar represent the alert levels. The darker the color, the higher the alert level.
- A larger area of each bar indicates more alerts of the corresponding levels.
- When you move the pointer over a bar, the system displays the numbers of alerts of all levels for the day.
- The line charts shows the trends of the numbers of alerts of different levels.

- The **Real-time Distribution of Alerts** section shows the alerts and alert levels of different products in real time.



  - The darker the color, the higher the alert level.
  - A larger color block indicates more alerts.
  - When you move the pointer over a color block, the system displays the alert level and quantity.

- The **P1 Alert Statistics** section shows the cloud platforms that have P1 alerts.



> **Note**
> Each tab is a product category. Click a tab to view the products that have P1 alerts under the category.

3.1.2. Alert list

You can view and handle all current alerts, set custom conditions to search for specific alerts, and export the list of alerts in XLSX format.

3.1.2.1. View the alert list

You can view all current alerts, set custom conditions to search for specific alerts, and export the list of alerts in XLSX format.

Procedure

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

By default, the **Not Disabled** tab is displayed. You can click the **Disabled** tab to view disabled alerts.

3. (Optional)

   In the upper-right corner of the page, click the icon to set the information items that you want to view.

4. In the upper-left corner of the page, enter a keyword and click the icon to perform a fuzzy search. The keyword can be part of an alert ID or a field in the Details in the Resource With Alerts column.

   You can also click **Advanced Search** to filter alert data by alert ID, alert source, product, alert status, alert level, and time range.

5. View the details of alerts, including the alert IDs, alert resources, alert levels, alert information, products, alert statuses, last generation time and duration, numbers of alerts, and alert sources.

   > **Note**
   >
   > Move the pointer over Details in the **Resource With Alerts** column. The details of an alert are displayed.

6. (Optional)In the upper-left corner of the page, click **Export Report**. The alerts are exported to your computer in XLSX format automatically.
7. Click the ID of an alert or click **Details** in the **Operation** column to view the details of the alert on the **Alert Details** page. For more information, see View the details of an alert.

3.1.2.2. View the details of an alert

You can view the details of an alert.

Procedure

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

   By default, the **Not Disabled** tab page is displayed. You can click the **Disabled** tab to view the details of disabled alerts.

3. In the alert list, find the alert whose details you want to view, and click **Details** in the **Operation** column. You can also click the alert ID in the **Alert ID** column to go to the Alert Details page.
4. In the **Alert Information** section, view the alert ID, alert level, product, alert information, alert time, alert status, number of times the alert is triggered, alert rule, current value, monitoring metrics, alert source, and alert details.
5. In the **Alert View** section, view the alert monitoring metrics in charts.
   - **1 Day**: shows the alert monitoring metrics of the day before the alert is triggered.
   - **1 Week**: shows the alert monitoring metrics of the week before the alert is triggered.
6. In the **Alert Impact** section, view the impact of the alert. You can view the server roles that may be affected by the alert and their statuses. In addition, the services, clusters, products, and physical machines to which the server roles belong are displayed.
7. In the **Suggestions** section, view the handling suggestions for the alert. The ID, title, and link of the corresponding KB document are displayed. Click the link to read suggestions .

3.1.2.3. Change the states of alerts

You can change the state to Processing or Disabled for one or more alerts.

Procedure

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

   By default, the **Not Disabled** tab is displayed.
3. Change the states of alerts.
   - Set to Processing: Find the alert that you want to manage, and click **Handle** in the **Operation** column. You can also select the alert or alerts that you want to manage and click **Batch Handle** in the lower part of the page.
   - Set to Disabled: Find the alert that you want to manage, and click **Disable** in the **Operation** column. You can also select the alert or alerts that you want to disable and click **Batch Disable** in the lower part of the page. The disabled alerts are displayed on the Disabled tab.

3.1.3. Alert settings

3.1.3.1. Policy management

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

3.1.3.1.1. Alert contacts

You can query, add, modify, or delete alert contacts based on your business requirements.

Procedure

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

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

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

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

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

3.1.3.1.2. Alert contact groups

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

Procedure

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

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

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

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

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

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

3.1.3.1.3. Configure static parameters

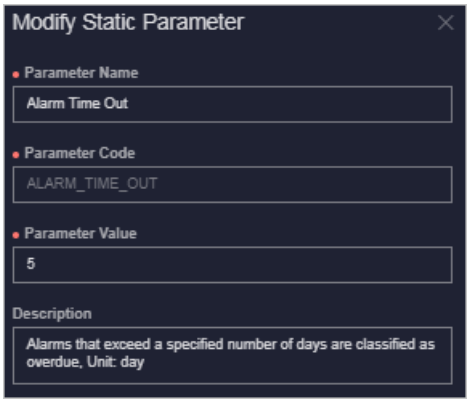
You can configure alert-related static parameters to suit your business needs. Only parameters related to timeout alerts can be configured.

Context

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

Procedure

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



Parameter	Description
Parameter Name	Enter a parameter name related to the configuration.
Parameter Value	Enter a parameter value. The default value is 5, indicating five days.
Description	Enter a description for the configuration.

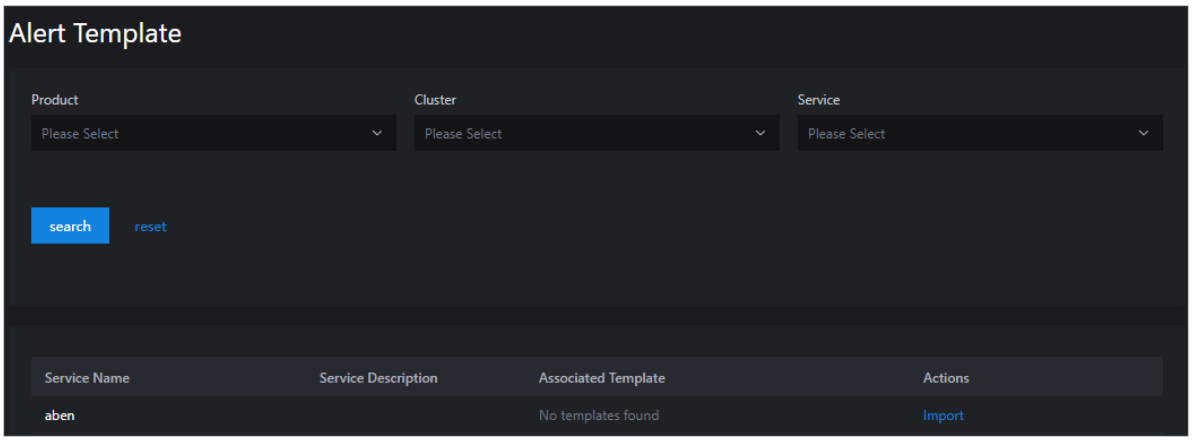
8. Click **OK**.

3.1.3.2. Alert templates

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

Procedure

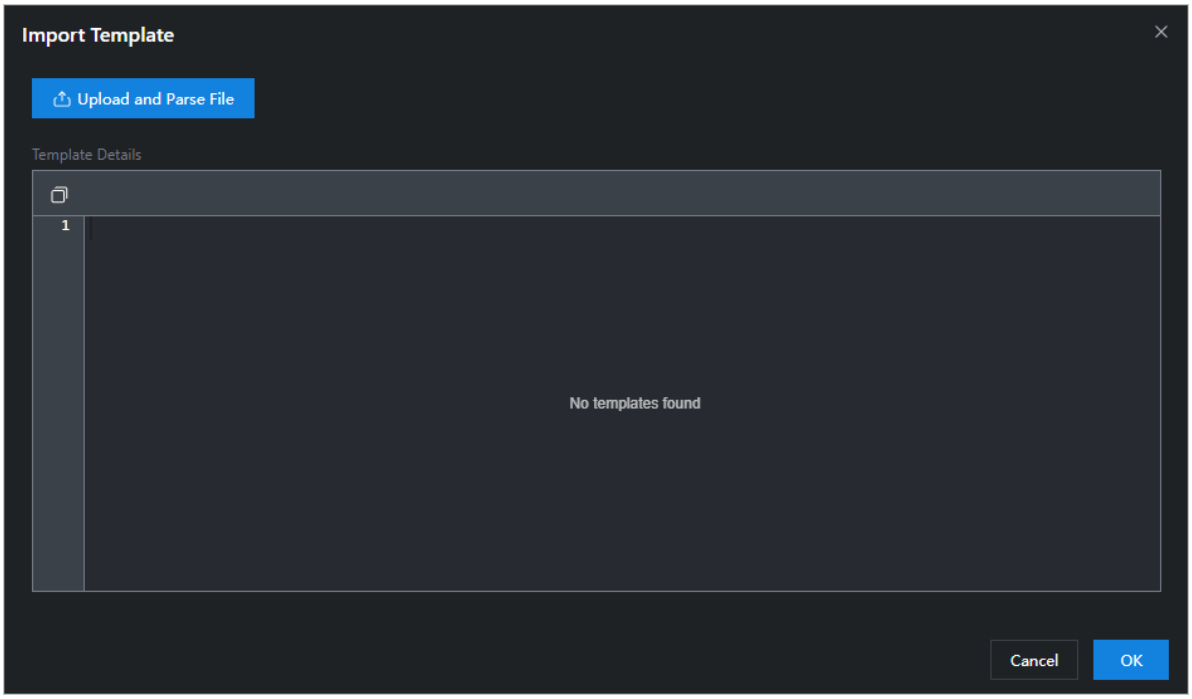
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Settings**.
3. Click **Alert Templates**. On the Alert Template page, specify the **Product**, **Cluster**, and **Service** parameters by using the drop-down lists, and click **Search** to view the details of the service.



4. (Optional) Click **Reset** to clear the search conditions.
5. Download Alert Templates.

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

6. Click **Import** in the Actions column corresponding to an entry. In the **Import Template** dialog box, click **Upload and Parse File**. Select the template and click **Open**. After the template is uploaded, click **OK**.



3.1.3.3. Notification management

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Settings**.
3. In the left-side navigation pane, click **Notifications**.
4. On the **Subscribe** tab, click **Add Channel**.
5. In the **Add Subscription** panel, configure the parameters described in the following table.

Parameter	Description
Channel Name	The name of the subscription channel.
Subscribed Language	The language in which you want to receive notifications. Valid values: Chinese and English.
Subscription Region	The region where the subscription is located.

Parameter	Description
Filtering Condition	The filter conditions used to filter alerts. Valid values: ◦ **Basic** ◦ **Critical** ◦ **Important** ◦ **Minor** ◦ Custom filter
Protocol	The protocol that is used to push alerts. Only HTTP is supported.
Push Interface Address	The IP address of the push interface.
Port Number	The port number of the push interface.
URI	The URI of the push interface.
HTTP Method	The request method that is used to push alerts. Only the POST method is supported.
Push Cycle (Minutes)	The interval at which alerts are pushed. Unit: minutes.
Pushed Alerts	The number of alerts pushed each time.
Push Mode	The mode in which alerts are pushed. Valid values: ◦ **ALL**: All alerts are pushed in each push cycle. ◦ **TOP**: Only high priority alerts are pushed in each push cycle.
Push Template	The template that is used to push alerts. Valid values: ◦ ASO: the default template. ◦ ANS: Select this template to push alerts by DingTalk or emails. You can configure only one channel of this type. **Note** A preset ANS template exists if the system is already connected to ANS. To restore the initial configurations of the template, click **Reset** in the **Actions** column corresponding to the channel.
Custom JSON Fields	The push receiver can use this field to customize an identifier. The field must be in the JSON format.

Parameter	Description
Push Switch	Specifies whether to push alerts. If the switch in this panel is not turned on, you can enable the push feature in the **Push Switch** column after you configure the subscription channel.

6. Click **OK**.

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

   > **Note** For an ANS push channel, you must enter the email address or DingTalk account to which the alerts are pushed after you click **Test** in the Actions column.
8. After you configure the push channel and turn on Push Switch, you can click the **Push** tab to view the push records.

3.1.3.4. Alert blocking

3.1.3.4.1. Create an alert blocking rule

Alert blocking allows you to block alerts reported during a specified period of time, and block alerts by product, cluster, service, server role, and machine.

Prerequisites

You have obtained permissions on the alert blocking menu.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Settings**.
3. In the left-side navigation pane, click **Alert Blocking**.
4. In the upper-left corner of the page, click **Create Blocking Rule**.
5. In the dialog box that appears, configure the filters to block alerts.

Parameter	Description
Resource	Optional. The name of the product to which the alerts to be blocked belong.
Cluster	Optional. The name of the cluster to which the alerts to be blocked belong.
Machine	Optional. The hostname of the ECS instance to be blocked.
Service	Optional. The name of the service to which the alerts to be blocked belong.
Server Role	Optional. The server role to which the alerts to be blocked belong.

Parameter	Description
Alert ID	Optional. The IDs of the alerts to be blocked.
Alert Level	Optional. The level of the alerts to be blocked. Valid values: ◦ **P1**: indicates critical alerts. The **Alert Level** of these alerts is **P1** in **Monitoring > Alert History** of Apsara Infrastructure Management. ◦ **P2**: indicates major alerts. The **Alert Level** of these alerts is **P2** in **Monitoring > Alert History** of Apsara Infrastructure Management. ◦ **P3**: indicates minor alerts. The **Alert Level** of these alerts is **P3** in **Monitoring > Alert History** of Apsara Infrastructure Management. ◦ **P4**: indicates reminder alerts. The **Alert Level** of these alerts is **P4** in **Monitoring > Alert History** of Apsara Infrastructure Management.
Alert Source	Optional. The source of the alerts to be blocked.
Alert Occurrence Time	Optional. The time period during which the alerts to be blocked occur.
Effective Status	Required. Specifies whether the blocking rule takes effect.

6. Click **OK**.

3.1.3.4.2. View an alert blocking rule

You can view an alert blocking rule in the list or search for a rule by using filter conditions.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Settings**.
3. In the left-side navigation pane, click **Alert Blocking**.
4. You can view an alert blocking rule in the list. To find a rule more quickly, you can specify the product, cluster, machine, and service, and click Search. Fuzzy match is supported.
5. **Optional:**You can also click **Advanced** and search for an alert item to help you locate a rule quickly.

3.1.3.4.3. Modify an alert blocking rule

You can modify an alert blocking rule based on your business requirements.

Prerequisites

You have obtained permissions on the alert blocking menu.

Procedure

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

4. Find the alert blocking rule that you want to manage, and click **Edit** in the **Operation** column. In the dialog box that appears, modify the parameters and click **OK**.

> **Note** You can enable or disable the alert blocking rule by turning on or off the switch in the **Status** column.

3.1.3.4.4. Delete an alert blocking rule

You can delete an alert blocking rule that you no longer need.

Prerequisites

You have obtained permissions on the alert blocking menu.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Settings**.
3. In the left-side navigation pane, click **Alert Blocking**.
4. Find the blocking rule that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

3.1.3.5. Blocked alerts

You can view an effective alert blocking rule and the alerts that are blocked by the rule.

Prerequisites

- You have obtained the permission to view blocked alerts.
- You have created at least one alert blocking rule and the rule is effective.

Procedure

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

> **Note** The Blocked Alerts page displays alert IDs, resources with alerts, alert levels, alert information, owning resources, alert occurrence time, sources, and associated blocking rules.

4. You can enter a keyword, such as an alert ID, source, or owning resource, to search for alerts. Fuzzy search is supported.
5. (Optional)Click **Advanced Search**, specify more filter conditions, and then click **Search**.
6. Move the pointer over **Details** in the **Resources with Alerts** column of an alert to view the alert details, including the product, cluster, service, server role, and host.
7. In the row of an alert, click **Blocking Rule** in the **Operation** column. A dialog box appears:
   - If the blocking rule is not deleted, the details of the blocking rule are displayed in the dialog box. You can modify the parameters in the dialog box and click **OK**.
   - If the blocking rule is deleted, message **The alert blocking rule has been deleted** appears.

3.1.4. Alert package configuration

You can upload an alert package to support hot replacement of alert data.

Context

This operation allows you to implement incremental configuration without suspending services. Acceptable package contents include alert text localization file and alert handling suggestion KB file. The package must be prepared and generated according to certain rules. Packages that are not prepared and generated in this manner are not accepted. This prevents alert configurations from being tampered with.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Alerts > Alert Packages**.
3. Click **Import Alert Package**. In the dialog box that appears, import a package. Then wait for the result. The system shows a message indicating whether the import succeeds or fails.

> **Important** The system supports TAR packages that are no larger than 200 MB in size. The system verifies the data of the package. Therefore, the alert package must be prepared and generated by Alibaba Cloud O&M engineers.

3.2. Inspection management

3.2.1. One-click inspection

You can perform one-click inspections for various scenarios to help maintain system and product health.

3.2.1.1. Preset inspection

You can start preset inspection tasks for various scenarios based on your business requirements.

Background information

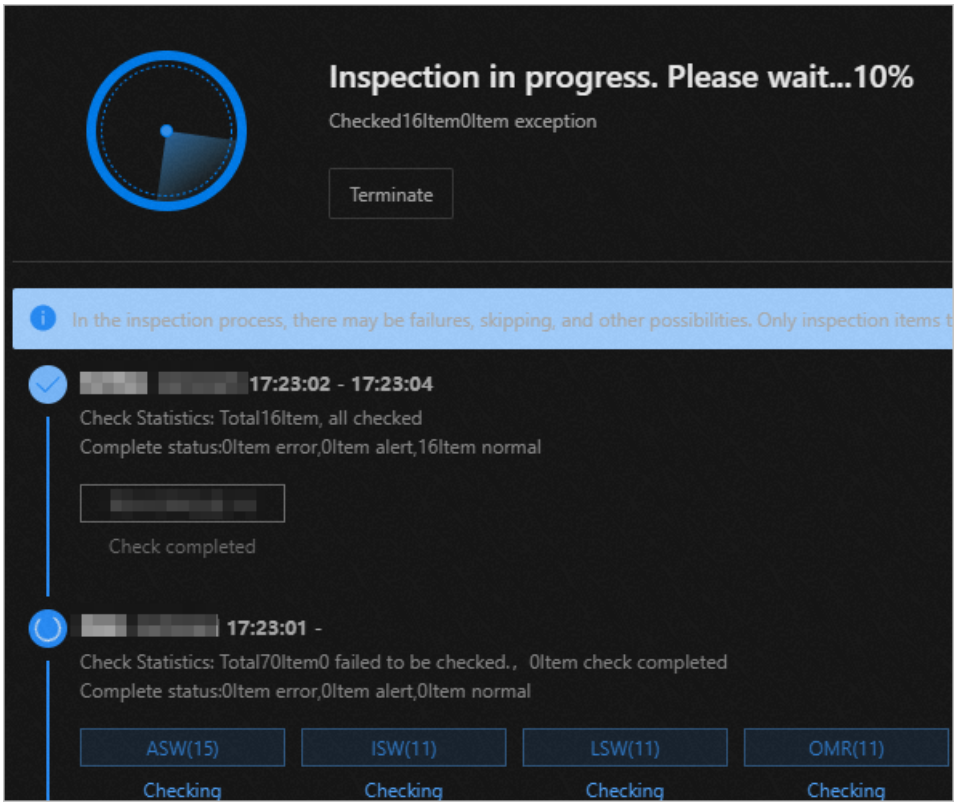
The system provides four preset inspection scenarios:

- One-click inspection: general inspection for all products.
- Physical machine inspection: deep inspection for physical machines.
- Network inspection: deep inspection for basic networks.
- OS inspection: deep inspection for OSs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > All Inspections**.
3. Click one of the four preset scenarios and start an inspection task:
   - If this is the first time the inspection is performed, click **Check now**.
   - If this is not the first time the inspection is performed, click **Re-check**.

After the inspection is started, the system displays the inspection progress in detail. If you need to stop the inspection, click **Terminate**. In the message that appears, click **OK**.



4. After the inspection is complete, view the inspection results on the page. You can also click **View the complete report** to view the detailed inspection report.

3.2.1.2. Custom inspection

If you have configured a custom inspection scenario, you can start a custom inspection task based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > All Inspections**.
3. Click **Custom inspection**.
4. Select an inspection scenario and click **Immediate inspection**.
5. After the inspection is complete, click **View the complete report** to view the detailed inspection report.

3.2.1.3. View the result of a recent inspection

You can view the result of a recent inspection for a preset scenario or the custom scenario.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > All Inspections**.
3. Select a preset inspection scenario or the custom inspection scenario.
4. Move the pointer over the inspection result of the scenario to view the number of errors,

warnings, and passed items.

5. Click **View the complete report** to view the detailed report.

3.2.2. Inspection dashboard

The inspection dashboard displays recent inspection tasks, data overview, distribution and trends of exceptions, task records, issues, and latest inspection reports.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Dashboard**.
3. In the upper part of the page, view:
   - The execution status of the inspection task, the numbers of issues, and the inspection capability (the numbers of inspection scenarios and items).
   - The rankings of inspection items and sub-items by the numbers of errors and warnings.

     > **Note** You can move the pointer over a row to view the numbers of errors and warnings for the corresponding item or sub-item.

   - You can select an inspection scenario from the drop-down list to view the trend charts of the numbers of errors, warnings, and inspection items of the scenario

4. In the middle of the page, view the inspection task records and issue details for the past seven days.
   i. Click the number in the **Inspection item results** column to view the details of the inspection item.
   ii. (Optional)Move the pointer over **Analysis** in the **Actions** column to view the details of the inspection result.
5. In the **Latest inspection report** section, view the latest inspection results.

i. Move the pointer over the inspection results of a scenario to view the numbers of errors, warnings, and passed items.

ii. Click **View the complete report** to view the detailed report.

3.2.3. Inspection report

You can view all recent inspection reports to learn about the problems or faults of the system.

Context

By default, the system displays the report of the latest successful inspection. You can search for the inspection report that you need by scenario or time in the upper right corner of the Inspection Report page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Reports**.
3. In the **Basic Information** section, you can view the scenario, start time, end time, initiator, and result recommendations of the inspection.
4. In the **Overview of inspection results** section, you can view the overall pass rate, total number of inspection items, numbers of passed items, warnings, and errors, and details of a specific scenario.
5. In the **Inspection Result Details** section, you can view the details of each inspection item.

   > **Note**
   > - You can use the filter feature to search for specific inspection items.
   > - Move the pointer over **Details** in the **Inspection parameters** and **Inspection content** columns to view the details.

6. Click the number in the **Inspection results** column to view the details of the inspection task.

   > **Note** Move the pointer over **Analyze** in the **Actions** column to view the details of the inspection result.

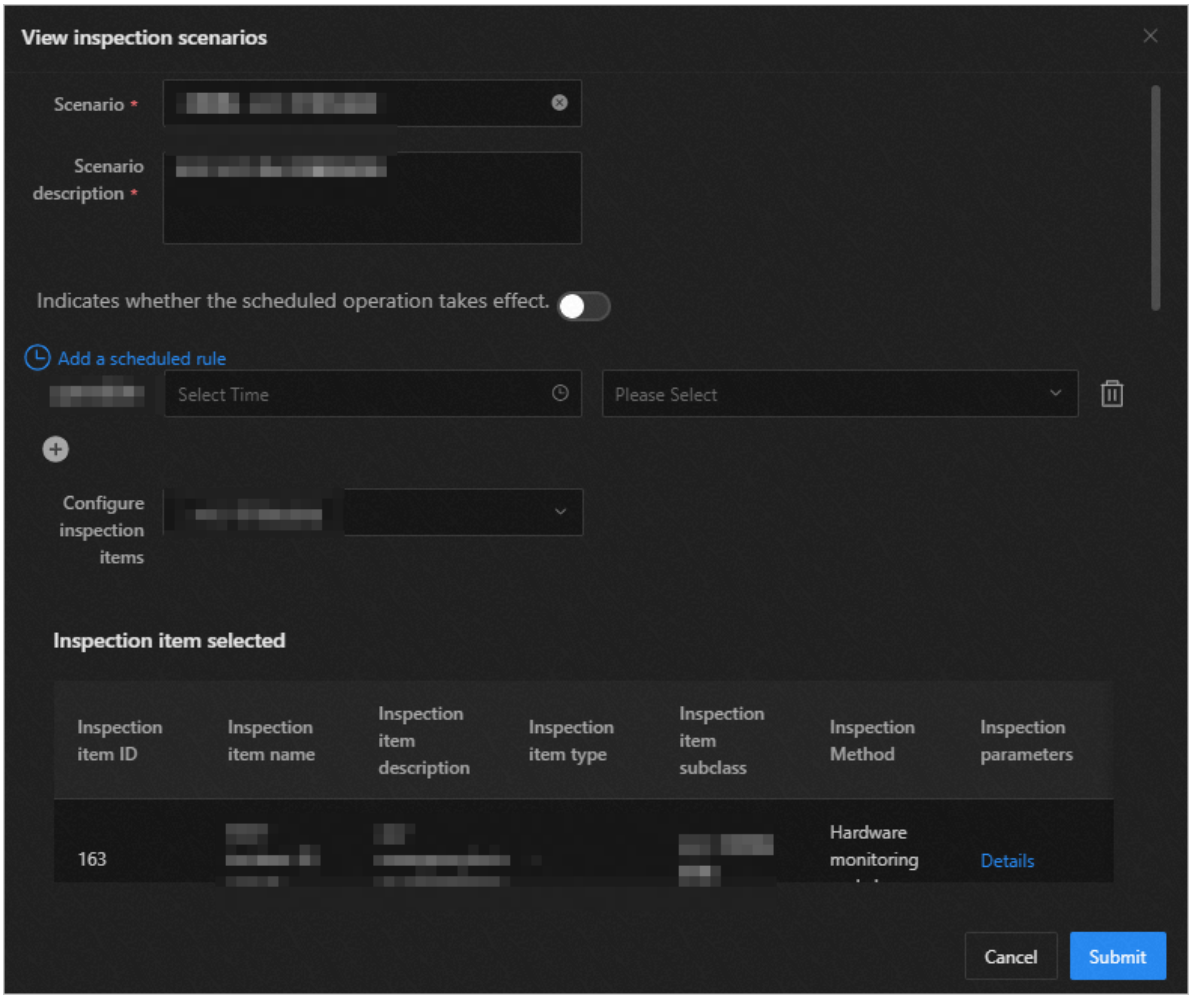
3.2.4. Inspection scenario configuration

3.2.4.1. View the configurations of an inspection scenario

You can view a configured inspection scenario and its inspection items.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Scenarios**.
3. You can view all the configured inspection scenarios. You can also view a specific scenario by using the filter conditions.
4. In the row of the scenario that you want to manage, click **Details** in the **Operation** column. In the dialog box that appears, view the configurations.



5. Move the pointer over **Details** in the **Inspection parameters** column to view the detailed inspection parameters.

3.2.4.2. Create an inspection scenario

You can create an inspection scenario based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Scenarios**.
3. Click **Create an inspection scenario**.
4. In the dialog box that appears, set the parameters and click **Submit**.

3.2.4.3. Modify an inspection scenario

You can modify the configurations of an inspection scenario based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Scenarios**.
3. In the row of the scenario that you want to manage, click **Details** in the **Operation** column.
4. In the dialog box that appears, modify the parameters and click **Submit**.

> **Note** You can modify only schedule-related parameters for a preset scenarios. You can modify all parameters for a custom scenario.

3.2.4.4. Delete an inspection scenario

You can delete an inspection scenario that you no longer need.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Scenarios**.
3. In the row of the scenario that you want to manage, click **Delete** in the **Operation** column.

> **Note** Preset inspection scenarios cannot be deleted.

3.2.5. Query inspection records

3.2.5.1. View inspection records

You can view the records of system inspections and the report of each inspection.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Records**.
3. You can view the records of all system inspections. You can also filter inspection records by using filter conditions.
4. Find the inspection record whose report you want to view, and click **Inspection Report** in the **Operation** column.

3.2.5.2. Stop an inspection

You can stop an ongoing inspection task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Records**.
3. Find the inspection record that you want to manage, and click **Stop** in the **Operation** column.

3.2.6. Query inspection items

You can view the information about all inspection items.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Items**.
3. You can view all inspection items. You can also view specific items by using the filter conditions.
4. Move the pointer over **Details** in the **Inspection parameters** and **Inspection content** columns to view the details.

3.2.7. Inspection packages

3.2.7.1. Import an inspection data package

You can import an inspection data package for preset scenarios.

Context

This feature supports only packages that are provided by the Alibaba Cloud support team. Other packages will fail the validation.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Packages**.
3. Click **Import inspection data packets**. In the dialog box that appears, select your package, and click **Open**.

3.2.7.2. Export an inspection data package

You can export inspection data packages for preset scenarios.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Inspections > Inspection Packages**.
3. Click **Export**. The data package is downloaded to your computer automatically.

3.3. Resource management

3.3.1. Products

3.3.1.1. View the product management dashboard

You can view all resources in the product dimension, including the details of products, clusters, services, and server roles.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Products**.
3. View the total numbers of products, clusters, services, server roles, and their statuses in the upper part of the page.

   In the **Architecture** section, click a product category on the left to view the final states of the products.

> **Note** The red dot next to a category indicates that some products have not reached the final state in this category.

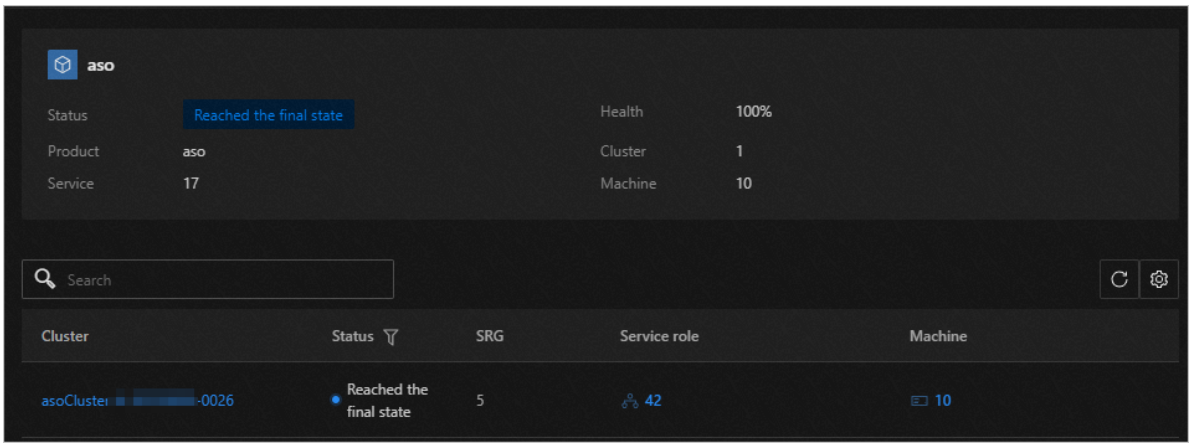
3.3.1.2. View the resources of a product

You can view the resource details of a product, such as its associated clusters, services, service roles, and virtual machines.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Products**.
3. In the **Architecture** section, click the icon of a product to view its details and the clusters

to which it belongs.



4. Click a cluster to view its details, the services that are deployed on the cluster, and the role groups.
5. Click a service to view its details and the service roles.

> **Note** You can also click the **Role groups** tab and click a role group to view information about the role group.

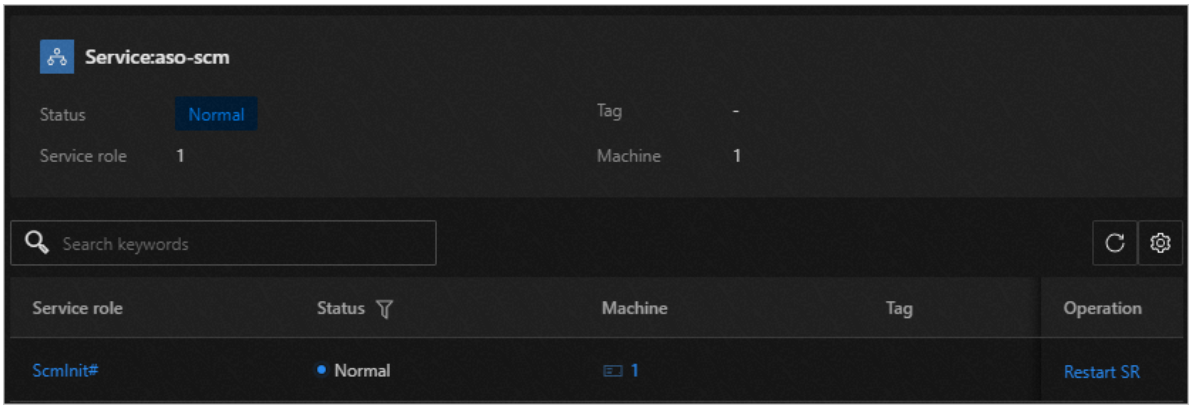
6. Click a service role to view its details and the virtual machines that it resides.
7. Click a virtual machine to view its details and the service roles that are deployed on the virtual machine.
8. **Optional:**After you click the icon of a product, you can expand the left-side tree and click a related node of any product to view the details of the node. You can also search for a specific node to view its details.

3.3.1.3. Restart a server role

You can restart a service role (SR) based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Products**.
3. Click a product. On the Cloud Product Details page, click a cluster. On the cluster details page, click a service. (You can also expand the left-side tree to find a service.) On the service details page, find an SR and click **Restart SR** in the **Operation** column. In the message that appears, click **OK**.



> **Note** You can also restart an SR on the **Role groups** tab of the cluster details page or on the VM details page.

3.3.1.4. Perform security O&M on a VM

You can log on to a virtual machine (VM) remotely to perform O&M operations.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Products**.
3. Click the icon of the product that you want to manage. On the Cloud Product Details page, expand the left-side structure tree to find the service role that you want to use. Click the service role. Find the VM and click **Security O&M** in the **Operation** column.
4. Perform the following steps:
   i. After you log on to the VM, enter Linux commands in the command-line interface (CLI) to perform O&M operations.
   ii. Click **Upload File**. The **Upload File** dialog box appears. You can upload a file in one of the following ways:
      - Click the dotted box. In the dialog box that appears, select the file to be uploaded and click **Open**. Then click **Upload** in the **Upload File** dialog box.
      - Drag the file to the dotted box and then click **Upload**.
   iii. Click **File Download**. The **File Download** dialog box appears. Set **File Directory** and **File Name** and then click **Download** to download the file to the configured directory. If you do not set the directory, the file is downloaded to the download folder of the local browser by default.

> **Note**
> - You cannot upload a folder.
> - The maximum size of an uploaded file is 200 MB.
> - If the file to be uploaded is larger than 200 MB, use the `split` and `cat` commands to split and merge the file.

3.3.2. Data centers

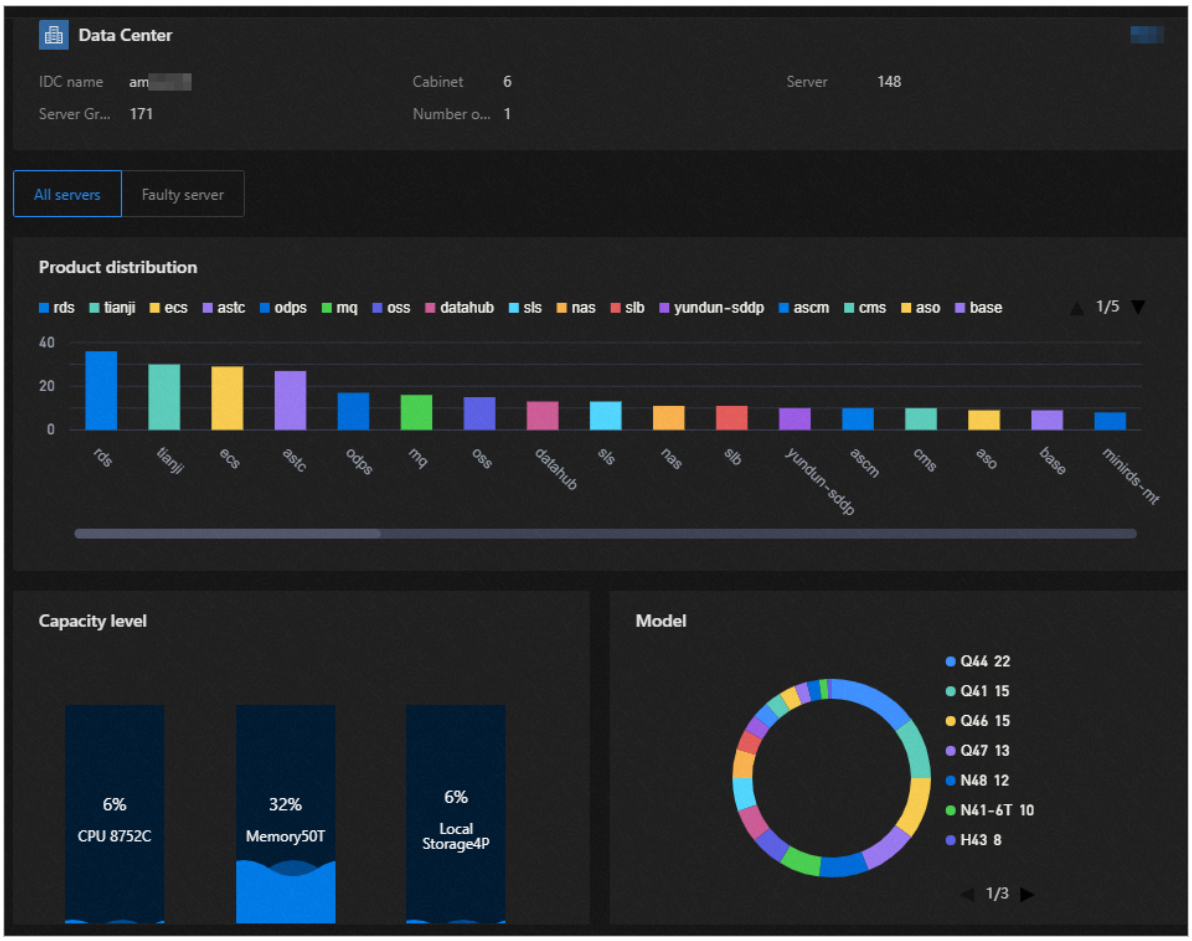
3.3.2.1. View the details of a data center

You can view information about cabinets, servers, and server roles in data centers.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Data Centers**.
3. View the information, including:
   - Basic information of the data center: such as its name, the number of cabinets, and the number of servers.
   - Server distribution by product: the distributions of all servers and faulty servers among products.

- Capacity level: the CPU, memory, and local storage usages of all servers.
- Server distribution by model: the distribution of all servers by model.

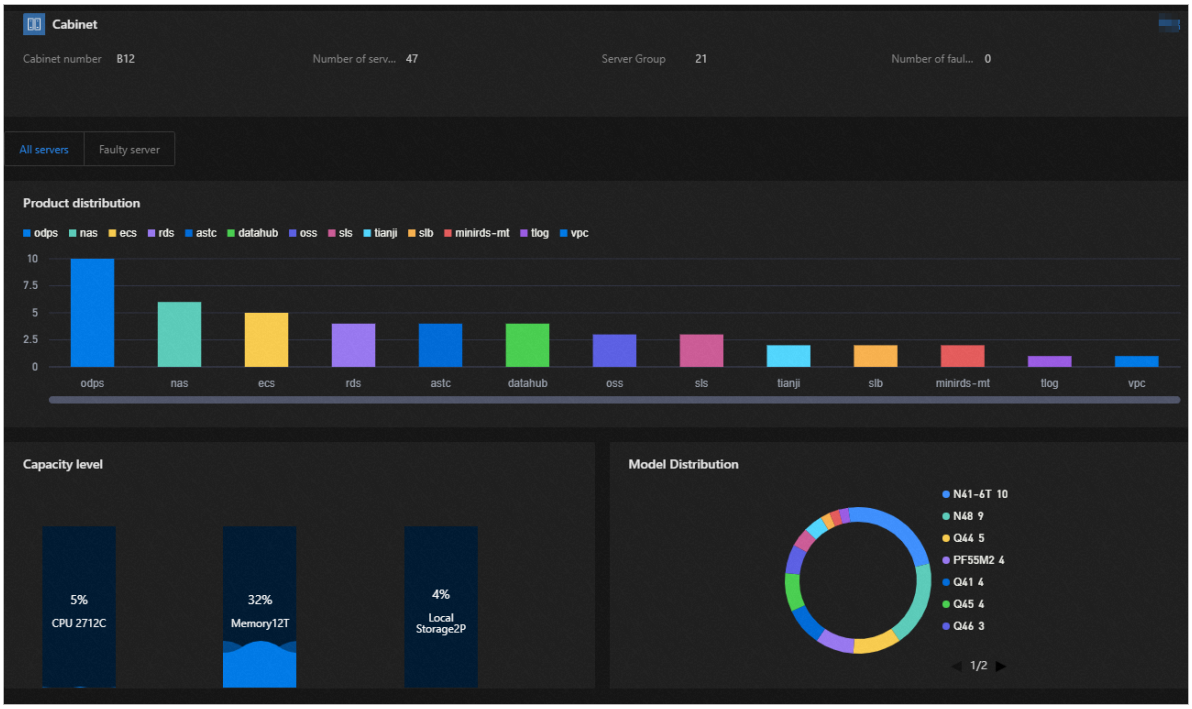


3.3.2.2. View the details of a cabinet

You can view the details of a cabinet, such as its server and service role information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Data Centers**.
3. Expand the left-side tree and click the cabinet whose details you want to view.
4. View the following information about the cabinet:
   - Basic information: the cabinet number and the numbers of servers, server groups, and faulty servers.
   - Server distribution by product: the distributions of all servers and faulty servers among products.
   - Capacity level: the CPU, memory, and local storage usages of all servers.
   - Server distribution by model: the distributions of all servers by model.

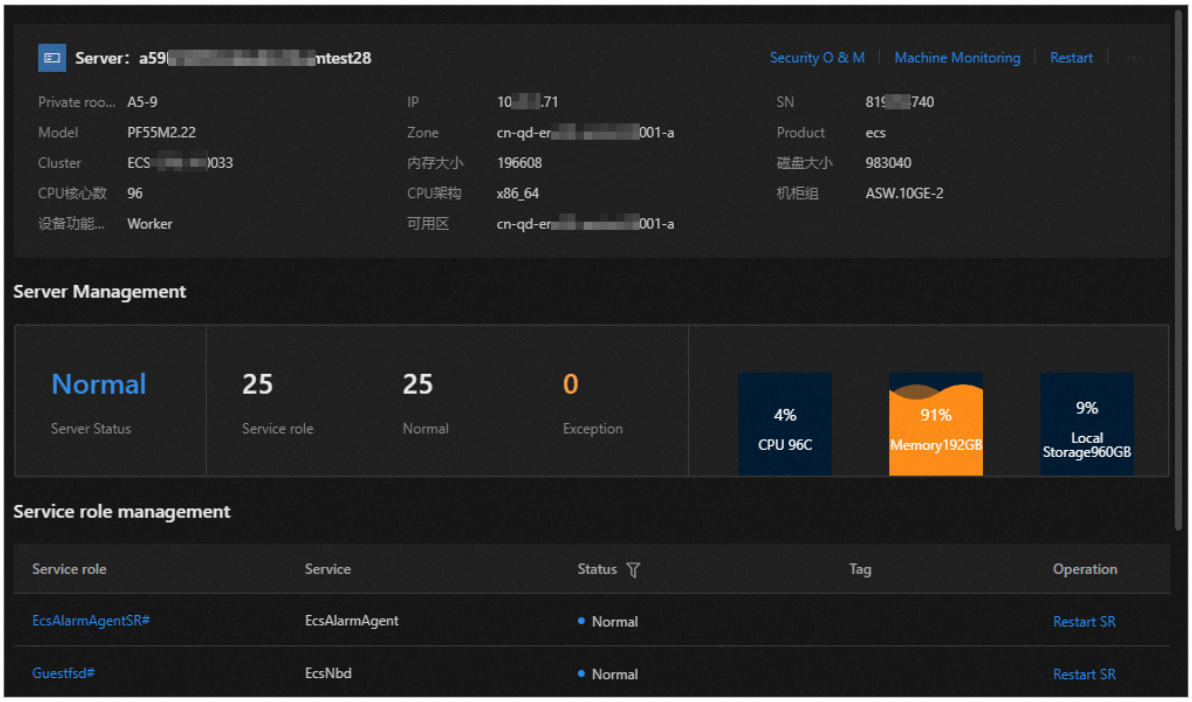


3.3.2.3. View the details of a server

You can view the detailed information about a server.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Data Centers**.
3. Expand the tree on the left and click the server that you want to view.
4. You can view the details of the server, including:
   - Its basic information, such as its private room, IP address, and SN.
   - Its management information, such as its status, number of service roles, CPU usage, memory usage, and local storage usage.
   - The management information about its service roles, such as the services they belong to, the statuses, and the tags of the service roles.



5. Click a service role. In the dialog box that appears, you can view the details of the servers where the service role is deployed.

3.3.2.4. Restart a server

You can restart a server based on your business requirements.

Procedure

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

> **Note** You can also restart a server in the server details dialog box on the **Products** page.

3. Expand the tree on the left and click the server that you want to manage.
4. In the upper-right corner of the page, click **Restart**. In the message that appears, click **OK**.

3.3.2.5. Restart a service role

You can restart a service role (SR) based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Data Centers**.
3. Expand the tree on the left and click the server that you want to view.
4. In the lower part of the page, find the SR that you want to restart, and click **Restart SR** in the **Operation** column. In the message that appears, click **OK**.

3.3.2.6. Security O&M

You can log on to a virtual machine (VM) remotely to perform O&M operations.

Procedure

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

   > **Note** You can also access the security O&M feature from a server details page. Choose General > Resources > **Products** and select a server to go to the server details page.

3. Expand the tree on the left and click the server that you want to manage.
4. In the upper-right corner of the page, click **Security O&M**.

   > **Note** If you want to perform O&M operations on the server of a service role, click the service role in the lower part of the page. In the dialog box that appears, find the server that you want to manage and click **Security O&M** in the **Operation** column.

5. Perform the following steps:
   i. After you log on to the VM, enter Linux commands in the command-line interface (CLI) to perform O&M operations.
   ii. Click **Upload File** in the CLI window. The **Upload File** dialog box appears. You can upload a file in one of the following ways:
      - Click the dotted box. In the dialog box that appears, select the file to be uploaded and click **Open**. Click **Upload** in the **Upload File** dialog box.
      - Drag the file to the dotted box and then click **Upload**.
   iii. Click **Download File**. The **Download File** dialog box appears. Set **File Directory** and **File Name** and then click **Download** to download the file to the configured directory. If you do not set the directory, the file is downloaded to the download folder of the local browser by default.

   > **Note**
   > - You cannot upload a folder.
   > - The maximum size of an uploaded file is 200 MB.
   > - If the file to be uploaded is larger than 200 MB, use the `split` and `cat` commands to split and merge the file.

3.3.2.7. Monitor a server

You can view the monitoring information of physical machines, and view and fix alerts.

Procedure

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

   > **Note** You can also access the machine monitoring feature from a server details page. Choose General > Resources > **Products** and select a server to go to the server details page.

3. Expand the tree on the left and click the server that you want to view.

4. In the upper-right corner of the page, click **Machine Monitoring**.
   The **Monitoring Information** tab is displayed by default. Select a metric from the drop-down list in the upper-right corner of the chart, set a time range, and then click the icon.

   You can view the monitoring charts of CPU usage, system load, disk usage, memory usage, host traffic, and disk I/O.

   > **Note** Move the pointer over the monitoring chart. The metric value at the corresponding point in time appears.

5. Click the **Alert information** tab to view, handle, or delete alerts.
   - View: Set a time range and click **Search** to view the alerts of service hosts.
   - Handle: Find the alert that you want to handle, and click **Repair** in the **Operation** column. The status of the alert changes to **Handled**.
   - Delete: Find the alert that you want to delete and click **Delete** in the **Operation** column. In the message that appears, click **OK**.

3.3.2.8. System brain

You can use the system brain feature to diagnose the operating system of a server to discover risks before they cause impact. You can also use the feature to collect error information to help you troubleshoot.

Procedure

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

   > **Note** Alternatively, you can choose General > Resources > **Products**, expand the tree on the left, click a service role, and click System brain in the Operation column or click a machine name and click System brain in the Server details dialog box that appears.

3. Expand the tree on the left and click the server that you want to diagnose.
4. In the upper-right corner of the page, click **System brain**.
5. **Optional:**Click **Update Diagnostic tools** to install the latest diagnostic tool.

   > **Note** Updating the diagnostic tool terminates ongoing tasks. If the current tool is the latest, the version number does not change after the update.

6. Select an operation from the drop-down list. The system displays the diagnosis results and details accordingly.

   > **Note**
   > - If no diagnostic information is displayed, click **Implementation**.
   > - If you select **System Log collection**, you must click the icon to download the diagnosis details.

3.3.3. Network

3.3.3.1. View the reference topology

The reference topology is the baseline topology of all network devices in the cloud platform.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the final state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Network**.
3. Select **Reference topology** from the **Topology type** drop-down list. The reference topology is displayed.

> **Note**
>
> The **Alert refresh** switch is turned on by default if **Topology type** is set to **Reference topology**. You can turn this switch off or on again based on your business requirements.
>
> - If the switch is turned on, the statuses of devices and links are updated when an alert is generated.
> - If the switch is turned off, the statuses of devices and links are not updated when an alert is generated.

3.3.3.2. View the real-time topology

The real-time topology is the current topology of all network devices in the cloud platform.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Network**.
3. Select **Real-time topology** from the **Topology type** drop-down list. The real-time topology is displayed.

> **Note** If **Topology type** is set to **Real-time topology**, the **Alert refresh** feature is unavailable.

3.3.4. Resource tags

The Resource Tags page shows and manages resources that you have added to favorites in a unified manner.

3.3.4.1. Add a node to favorites

You can add nodes to favorites. The added nodes are displayed on the **Resource Tags** page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Products**.
3. In the **Architecture** section, click the icon of the product that you want to manage.
4. In the left-side structure tree, click the star next to the node that you want to add to favorites. You can expand the tree for lower-level nodes.

   > **Note** You can also add nodes to favorites in the same way on the **Data Centers** page.

5. View the added nodes on the **Resource Tags** page. You can click a node to view its details.

3.3.4.2. View resource tags

You can view the list of resources to which you have bound tags.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Resource Tags**.
3. You can view the list of resources to which tags are bound. You can also search for resources and tags by resource name, type, or tag.

3.3.4.3. Bind tags to resources

You can bind tags to resources based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Resource Tags**.
3. Click **Bind tags**. In the wizard that appears, select one or more tags and click **Next**.

   > **Note** You can add or delete tags based on your business requirements:
   > - Add a tag: click **Add Tags**. In the dialog box that appears, enter a tag value and click **OK**.
   > - Delete a tag: Find the tag that you want to delete, and click **Delete** in the **Operation** column. In the message that appears, click **OK**.

4. Select the resources to which you want to bind tags and click **Next**.

   > **Note** You can select resources from the product view or data center view. You can select multiple resources, but the resources must be at the same level.

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

3.3.4.4. Unbind tags from resources

You can unbind tags from resources based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Resource Tags**.
3. Select resources and click **Unbind tags**. In the message that appears, click **OK**.

3.3.4.5. Modify a resource tag

You can delete resource tags that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Resource Tags**.
3. Find the resource that you want to manage and click **Modify tags** in the **Operation** column. In the dialog box that appears, click the icon next to the tag that you want to delete, and click **OK**.

3.3.4.6. Export resource tags

You can export resource tags based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Resources > Resource Tags**.
3. Click **Export**. In the dialog box that appears, click **Download**. All resource tags displayed on the page are downloaded.

> **Note** If you do not want to export all the resource tags, select the resource tags that you want to export, and click **Export**. In the dialog box that appears, click **Download**.

3.4. Capacity management

3.4.1. Capacity analysis dashboard

The Inventory Analysis module allows you to predict capacity trends and perform operations based on the available product capacity and usage habits.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > Capacity Analytics**.
3. On the **Inventory Analysis** page, view the cloud product capacity.

- At the top of the page, view the average available capacity, trend, and core product usages.
- In the **Product Available Capacity Forecast** section, view the capacity of items related to a single product.
  - Click **Days**, **Weeks**, or **Months** to view the predicted available capacity of the product within the specified time range.
  - Click an item under a product name to view the corresponding capacity.
  - Move the pointer over a curve. Capacity information at a specific time point is displayed.

3.4.2. View ECS capacity

You can view ECS capacity to learn the resource usage and availability of ECS instances and perform O&M operations accordingly.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > ECS Capacity**.
3. Select a date in the upper part of the page and view the ECS capacity.

> **Note** You can click the icon in the upper-right corner of the page to specify a zone and configure thresholds.

   - The **CPU Inventory Details (Cores)** and **Memory Inventory Details (TB)** sections show the usage and availability of CPU (core) and memory (TB) resources of all ECS instance families for the last five days.
   - The **ECS Inventory Details** section shows the capacity details of a specified ECS instance type on the specified date on multiple pages by **Zone**, **Instance Type**, and **Date**, as well as the CPU and memory configurations corresponding to each instance of this type.
4. (Optional)Query data by specifying the **Zone**, **Instance Type**, and **Date** in the **ECS Inventory Details** section, and then click **Export** to export the ECS capacity details to your computer.

3.4.3. View SLB capacity

You can view SLB capacity to learn the resource usage and availability of SLB instances and perform O&M operations accordingly.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > SLB Capacity**.

   > **Note** You can click the icon in the upper-right corner to configure thresholds.

3. Select a cluster from the **Cluster** drop-down list in the upper-left corner and click **Query** to view the SLB capacity data of the cluster.

   > **Note**
   > - The clusters that have **slbCluster** in their names are default clusters.
   > - The clusters that have **slbExtraCluster** in their names are expanded clusters.

4. View the SLB capacity.
   - The Internal VIP Usage and Public VIP Usage sections show the amount and percentage of internal and public VIP capacities that are being used.
   - The NIC traffic section shows the inbound and outbound NIC traffic.

     > **Note**
     > - By default, both inbound traffic and outbound traffic are displayed. You can click the icon for inbound traffic or outbound traffic in the upper-left corner of the **NIC traffic** section to view the traffic data of a specific direction.
     > - **_ifin**: inbound traffic (KByte/s).
     > - **_ifout**: outbound traffic (KByte/s).

   - In the **SLB Inventory Details** section, you can query SLB capacity by **Type** and **Date** on multiple pages.
5. (Optional)In the upper-right corner of the **SLB Inventory Details** section, click **Export**. In the dialog box that appears, click **Download** to export the data.

3.4.4. View RDS capacity

You can view the Relational Database Service (RDS) inventory to query the usage and availability of RDS resources. This way, you can perform O&M operations in an efficient manner.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity**.
3. View the RDS inventory on the page that appears.

> **Note** You can click the icon in the upper-right corner to configure thresholds for each engine.

- The **RDS Inventory** section shows the inventories of different types of RDS instances within the last five days. Different colors indicate different types of RDS instances.
- The **RDS Inventory Details** section shows the RDS inventory details by **Engine** and **Date** on multiple pages.

3.4.5. View OSS capacity

You can view the Object Storage Service (OSS) capacity to learn more about the usage and availability of OSS resources and perform O&M operations more efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > OSS Capacity**.

> **Note** You can click the icon in the upper-right corner to configure the thresholds.

3. View the OSS capacity.
   - The **Historical Available Inventory (TB)** section shows the availability of OSS resources over the last five days.
   - The **Used Inventory (TB)** section shows the amount and percentage of OSS resources that are being used.
   - The **OSS Bucket Inventory Details** section shows the OSS capacity details on multiple pages by **Date**.

3.4.6. View Tablestore capacity

By viewing the Tablestore capacity, you can query the usage and availability of Tablestore resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > Tablestore Capacity**.

> **Note** You can click the icon in the upper-right corner and configure the global quota.

3. View the Tablestore capacity.
   - The **Historical Available Inventory (TB)** section shows the Tablestore capacity availability in the last five days.
   - The **Used Inventory (TB)** section shows the amount and percentage of Tablestore capacity that are being used.
   - You can query Tablestore capacity details on multiple pages by **Date**.

3.4.7. View Log Service capacity

By viewing the Log Service capacity, you can query the usage and availability of Log Service resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > Log Service Capacity**.

   > **Note** You can click the icon in the upper-right corner of the page to configure the capacity thresholds and global quota.

3. On the **SLS-Inner** tab, view the Log Service capacity details.
   - The **Historical Inventory Records (TB)** section shows the available and total Log Service capacity for the last five days.
   - The **Quota Details (GB)** section shows the amount and percentage of Log Service capacity that are being used.
   - The **Log Service Inventory Details** section shows the Log Service capacity details on multiple pages by **Date**.
4. Click the **PublicBasicCluster-XXX** tab to view details about the Log Service capacity for which you have applied.
   - The **Inventory Availability History (TB)** section shows the available Log Service capacity for the last five days.
   - The **Used Inventory (TB)** section shows the amount and percentage of Log Service capacity that are being used.
   - The **SLS Inventory Details** section shows the Log Service capacity details on multiple pages by **Date**.

3.4.8. View EBS capacity

By viewing the Elastic Block Storage (EBS) capacity, you can query the usage and availability of EBS resources to efficiently perform O&M operations.

Context

> **Note** EBS is the Apsara Distributed File System storage provided for ECS by the base, and ECS IO clusters are used for Apsara Distributed File System storage. Therefore, you can view the EBS capacity in ECS IO clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > EBS Capacity**.
3. If multiple ECS IO clusters exist in the environment, click the tab of each ECS IO cluster to view the EBS capacity.
   - The **Historical Available Inventory (TB)** section shows the available EBS capacity for the last five days.
   - The **Used Inventory (TB)** section shows the amount and percentage of EBS capacity that are being used.

- You can query EBS capacity details on multiple pages by date.

3.4.9. View NAS capacity

You can view NAS capacity to learn the resource usage and availability of NAS and perform O&M operations accordingly.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Capacity > NAS Capacity**.
3. View NAS capacity on the page that appears.
   - The **Historical Available Inventory (TB)** section shows NAS capacity for the last five days.
   - The **Used Inventory (TB)** section shows the amount and percentage of NAS capacity that is being used.
   - You can query NAS capacity details by date.

3.5. Changes

3.5.1. Operation Orchestration Service

The Operation Orchestration Service feature automates O&M for data centers. A web-based method is provided to implement O&M operations for resources at scale, simplify O&M management of IT resources, and support full-stack automated O&M of the infrastructure, the Apsara Stack environment, operating systems, and the application layer.

3.5.1.1. View host resources

You can view the information about hosts such as physical machines or Docker virtual machines.

Background information

Before you execute a script or an O&M job on a host, you can view the specific information about the host to ensure that the script or job can be effectively executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
   By default, the **Host Resources** page appears.
3. Enter a hostname, project name, or cluster name in the search box, and click **Search**.
   Fuzzy search is supported.
   You can view the information about the hosts that meet the filter conditions, including the hostname, IP address, project name, cluster name, operating system, and data center.
4. (Optional) Click **Reset** to clear the filter conditions.

3.5.1.2. View Docker resources

You can view the information about Docker containers.

Background information

Before you execute a script or an O&M job on a Docker container, you can view the specific information about the Docker container to ensure that the script or job can be effectively executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Docker Resources**.
4. Enter a server role name, project name, cluster name, or service name in the search box, and click **Search**. Fuzzy search is supported.
   You can view the information about the Docker containers that meet the filter conditions, including the server role name, type, hostname, host IP address, project name, cluster name, and service name.
5. (Optional) Click **Reset** to clear the filter conditions.

3.5.1.3. Manage scripts

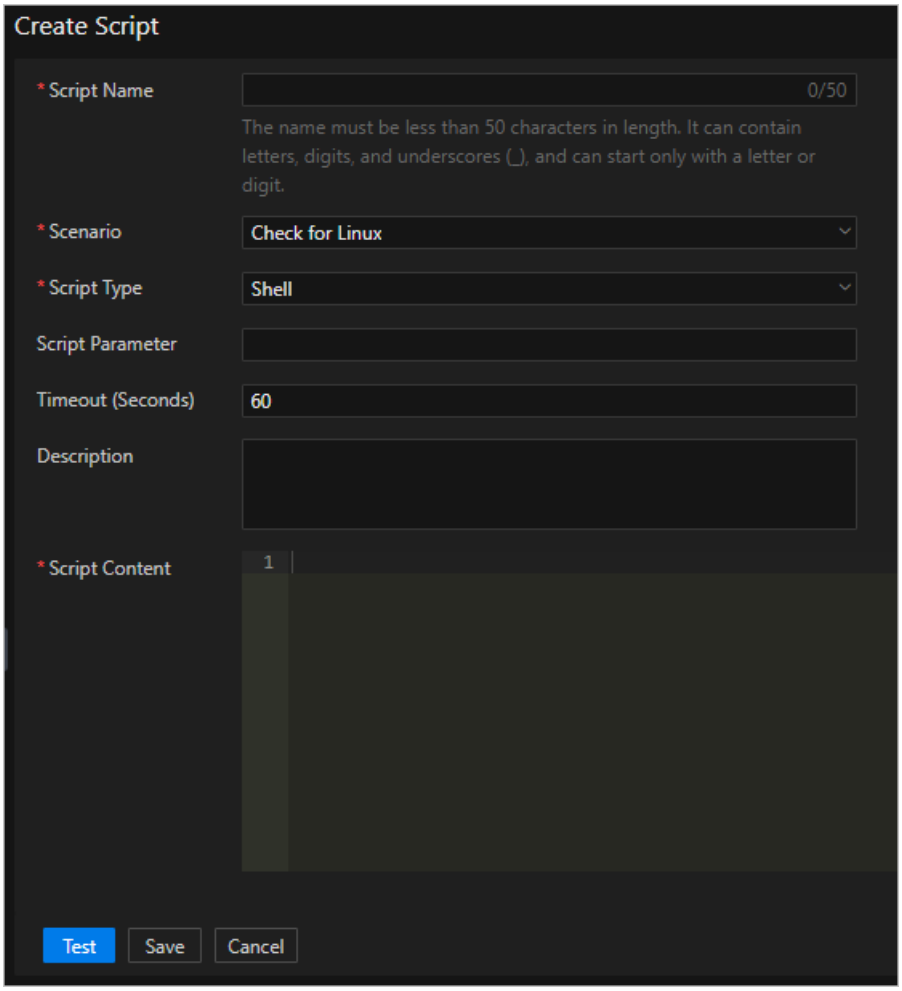
The script library is used to store scripts for implementing various features and is the basis for automated O&M. All O&M commands are run by using scripts. The system provides some common built-in default scripts, and supports custom scripting. You can create, import, view, modify, export, and delete scripts.

3.5.1.3.1. Create a script

You can create a script and test whether it can be executed properly.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.
4. Click **Create Script**.
5. Configure the parameters for the script.



The following table describes the parameters.

Parameter	Description
Script Name	The name of the script.
Scenario	The application scenario of the script. Valid values: **Check for Linux**, **Run Command**, and **Install Software**.
Script Type	The type of the script. Valid values: Shell and Python.
Script Parameter	The parameters passed in when the script is executed. Separate multiple parameters with spaces.
Timeout (Seconds)	The timeout period for script execution. After the specified number of seconds, the script stops executing and the execution timeout result is returned.
Description	The description of the script.

Script Content	The content of the script. When you write a script, you must add a script interpreter. For example, add `#!/bin/bash` for a Shell script or `#!/usr/bin/python` for a Python script. The path of the interpreter may vary with the execution resources and environments.

6. Click **Test** to test whether the script can be executed. If you confirm that the script can be executed, you can directly click **Save**.
   i. After you click **Save** or **Test**, the system checks the script content. If the **The script has high-risk commands. Do you want to continue?** message appears, check whether the script content is correct.
      - Correct: Click **OK**.
      - Incorrect: Modify the script and test again.
   ii. After you click **Test**, click **Host Resources** or **Docker Resources** in the **Script Test** dialog box, select one or more host resources or Docker resources, and then click **Execute**.

      > **Note** The SSH protocol is used to copy files to the host or Docker container. Therefore, the test execution process may be slow.

   iii. In the **Test Results** dialog box, view the test result of the script.
      - Click **OK** to exit the dialog box and click **Save** to save the script.
      - Click **Re-select Resources** to select other hosts or Docker containers to test the script.

3.5.1.3.2. Import a script

You can import an on-premises script to the script library.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.
4. Click **Import Script**.
5. In the **Upload Script File** dialog box, click **Click Here to Upload** to upload an on-premises script to the script library.

   > **Note** Only JSON files that are not larger than 500 KB in size can be uploaded.

3.5.1.3.3. View scripts

You can view scripts in the script library.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.

4. In the **Script Name** field, enter the name of the script that you want to view and click **Search**. Fuzzy search is supported.
   You can view the information about the scripts that meet the filter conditions, including the script name, script type, scenario, parameter, modification time, description, update user, and whether the script is a default script.
5. (Optional) Click **Reset** to clear the filter conditions.

3.5.1.3.4. Modify a script

After a script is created or imported, you can modify the script to suit your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.
4. Find the script that you want to modify and click **Modify** in the **Actions** column.
5. Modify the parameters and click **Test** to test whether the script can be executed. If you confirm that the script can be executed, you can directly click **Save**.
   i. After you click **Save** or **Test**, the system checks the script content. If the **The script has high-risk commands. Do you want to continue?** message appears, check whether the content of the script is correct.
      - Correct: Click **OK**.
      - Incorrect: Modify the script and test again.
   ii. After you click **Test**, click **Host Resources** or **Docker Resources** in the **Script Test** dialog box, select one or more host resources or Docker resources, and then click **Execute**.

      > **Note** The SSH protocol is used to copy files to the host or Docker container. Therefore, the test execution process may be slow.

   iii. In the **Test Results** dialog box, view the test result of the script.
      - Click **OK** to exit the dialog box and click **Save** to save the script.
      - Click **Re-select Resources** to select other hosts or Docker containers to test the script.

3.5.1.3.5. Export a script

You can export a script to your on-premises machine.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.
4. Select one or more scripts that you want to export and click **Export Script** to export the scripts to your on-premises machine.

   > **Note** If you export multiple scripts at a time, the content of the scripts is stored in a single JSON file.

3.5.1.3.6. Delete a script

You can delete a script that is no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Script Library**.
4. Select one or more scripts that you want to delete and click **Delete Script** in the lower part of the page, or click **Delete** in the **Actions** column.
5. In the dialog box that appears, click **OK**.

3.5.1.4. Manage software

The software repository is used for software management, including uploading, viewing, downloading, and deleting software. The term software used here is in its broad sense, including compressed packages, JAR packages, images, and files. Only software uploaded to the software repository can be used in subsequent jobs.

3.5.1.4.1. Upload software

You can upload software to the software repository.

Background information

When an O&M job is executed in an on-site environment, software is downloaded from the software repository and deployed on the host or Docker container. You must upload the software to the software repository before you can use it in subsequent jobs.

> **Note** Delete software that is no longer needed to free up storage space.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Software Repository**.
4. Click **Upload Software**.
5. In the **Upload Software** dialog box, enter a software name in the **Software Name** field and click **Click Here to Upload** to upload an on-premises file. If you do not enter a software name, the software name is the same as the file name.

   > **Note** The file that you want to upload cannot exceed 500 MB in size.

3.5.1.4.2. View software

You can view software in the software repository.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Software Repository**.
4. In the **Software Name** field, enter the name of the software that you want to view, and then click **Search**. Fuzzy search is supported.
   You can view information about software that meets the filter conditions, including the software name, file name, file size, upload time, and upload user.
5. (Optional) Click **Reset** to clear the filter conditions.

3.5.1.4.3. Download software

You can download software from the software repository to your on-premises machine.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Software Repository**.
4. Find the software that you want to download and click **Download** in the **Actions** column.

3.5.1.4.4. Delete software

To save storage space, you can delete software that is no longer needed after O&M jobs are executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Software Repository**.
4. Select one or more software programs that you want to delete and click **Delete Software** in the lower part of the page, or click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

3.5.1.5. Manage processes

Process orchestration is one of the core features of Operation Orchestration Service. It is used for process management, including creating, importing, viewing, exporting, modifying, running, and deleting processes. You can define a process to combine a series of logical actions into a task and automate O&M.

3.5.1.5.1. Create a process

You can create a process to visually orchestrate the O&M process and automate O&M.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.

3. In the left-side navigation pane, click **Process Orchestration**.
4. Click **Create Process**.
5. On the **Create Process** page, click **Process Settings**.
6. In the **Process Settings** dialog box, configure the following parameters:
   - **Process Name**: Enter a name for the process.
   - **Process Description**: Enter a description for the process.
   - **Trigger Method**: Select **Manual** or **Scheduled**.
     - **Manual**: The process must be manually triggered.
     - **Scheduled**: The process is triggered at the specified time.
   - **Timing Rule**: This parameter is available only when **Trigger Method** is set to **Scheduled**. Set the time to trigger the process.
     - **Once**: The process is triggered only once at the specified time. Select a date and time to trigger the process.
     - **Daily**: The process is triggered once at the specified time every day. Select a time to trigger the process every day.
     - **Monthly**: The process is triggered at the specified day and time every month. Select a day and time to trigger the process every month. For example, if you set **Days** to 10 and **Time** to 09:00:00, the process is triggered at 09:00:00 on the tenth day of every month.
7. Click **OK**.
8. Drag nodes on the left side to the right side and add lines between the nodes. The nodes that can be added to a process include the Start, Task, Judgement, Manual, Wait, and Notification nodes.
   -  : the Start node. Each process has only one Start node, which represents the start of the process. The Start node has no parameters and can have only one line to connect to another node.
   -  : the Task node. The Task node is the major node for process execution and can execute one script or job. Click the Task node and configure the following parameters in the **Node Properties** dialog box.

Tab	Parameter	Description
Specify Node	**Node Name**	The name of the node.
	Description	The description of the node.

Specify Parameters	**Input Parameters**	Input parameters are the output parameters of the previous node. If the previous node has no output parameters, the node has no input parameters. Input parameters follow a script in sequence when the script is executed. Example: `./test.sh params1 params2`. **Note** If you set Operation to **Execute Job** on the Select Operation tab, you do not need to specify the input parameters.
	Output Parameters	Output parameters take effect only if the node is used to execute a single script. Output parameters come from the execution result of the script. Therefore, the script must return a fixed result. For example, if the execution result is `echo "CPU=22,MEM=30"`, click **Add** to configure the output parameters. Specify **Output Parameter Name** and enter CPU and MEM in the **Parsed Key Value** field. **Note** If you set Operation to **Execute Job** on the Select Operation tab, you do not need to specify the output parameters.
Select Operation	**Operation**	Select **Script** or **Execute Job**, and then select a script from the Script drop-down list or select a job from the Execute Job drop-down list.

Select Execution Resources	**Resource Type**	Select **Host** or **Docker**. ▪ **Host**: Click **Select Host**. In the **Select Host** dialog box, select one or more hosts and click **OK**. You can also enter a hostname, project name, or cluster name in the **Host** field and press the Enter key to search for the hosts that you want to select. Fuzzy search is supported. ▪ **Docker**: Click **Select Docker**. In the **Select Docker** dialog box, select one or more Docker containers and click **OK**. You can also enter a server role name, project name, or cluster name in the **Docker** field and press the Enter key to search for the Docker containers that you want to select. Fuzzy search is supported. You can click the icon to delete the specified host or Docker container.

	Phased Execution Settings	Select **None**, **Automatically Executed**, or **Stop Waiting**. ▪ **None**: The scripts or jobs are executed on all the selected hosts or Docker containers in one batch. ▪ **Automatically Executed**: The scripts or jobs are executed on the selected hosts or Docker containers in two batches. One batch is executed at a time. After the first batch is executed, the second batch starts to be executed. If the first batch fails to be executed, the second batch is not executed. **Note** If you set Resource Type to Docker, the selected Docker containers are automatically divided into batches based on the server role name such that Docker containers with the same server role are in different batches. ▪ **Stop Waiting**: The scripts or jobs are executed on the selected hosts or Docker containers in two batches. The first batch is executed first. After the first batch is executed, a process approval is sent. The approver can click **Passed** or **Stop** in **Process Review**. When the approval is passed, the second batch starts to be executed. If the first batch fails to be executed, the execution stops and no process approval is sent. **Note** If you set Resource Type to Docker, the selected Docker containers are automatically divided into batches based on the server role name such that Docker containers with the same server role are in different batches.

-  : the Judgement node, which is used to judge the process routes of different directions.

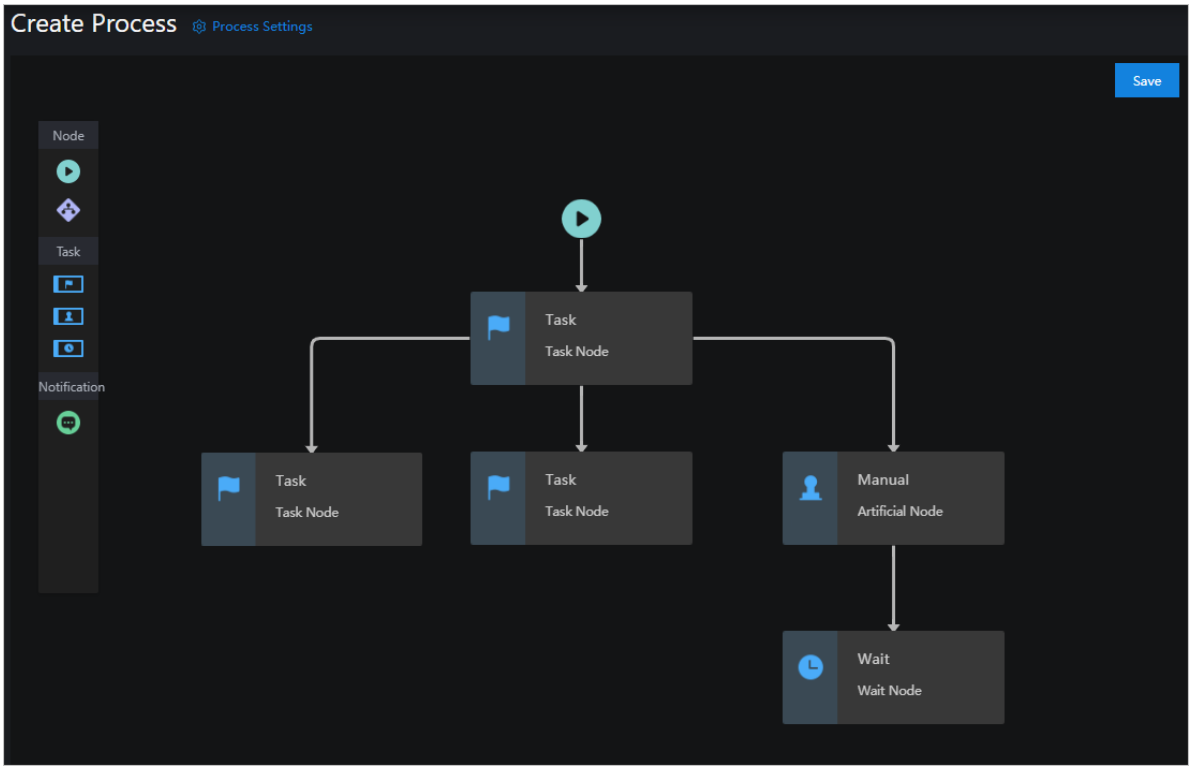
The previous node of the Judgement node must be a Task node that has output. Otherwise, the Judgement node is of no use. Click the Judgement node. In the **Node Properties** dialog box, configure the following parameters.

- **Node Name**: Enter a name for the node.
- **Description**: Enter a description for the node.
- **Judgement Condition**: Click **Add**. In the **Add** dialog box, set **Output Parameter Name** of the previous node and set the judgement condition by specifying **Judgement** and **Value**. Click **OK** to save the judgement condition.
- **Judgement Type**: If you set multiple judgement conditions, you must select **Or** or **And**.
  - **Or**: The judgement result is yes if one judgement condition is met. The judgement result is no if no judgement conditions are met.
  - **And**: The judgement result is no if one judgement condition is not met. The judgement result is yes if all the judgement conditions are met.

You must click the lines coming out from the Judgement node and set **Yes** or **No** to define the execution of the subsequent nodes in the process.

-  : the Manual node. When the process is executed to this node, the process is suspended for manual approval. If the approval is passed, the process continues execution. If the approval is not passed, the subsequent nodes in the process are not executed. If a timeout period is specified and manual approval is not performed after this period expires, the subsequent nodes in the process are automatically stopped.
-  : the Wait node. When the process is executed to this node, the process waits a specified period of time before the subsequent nodes in the process are executed. For example, the previous node executed the script for service startup, but usually the service startup takes some time. In this case, you can wait 1 minute and then check whether the service is normal in the next node.
-  : the Notification node. Notifications are sent by email. Select **Email** from the **Notification Type** drop-down list. Then, set Recipient, Notification Title, and Notification Content. Separate multiple email addresses with commas (,).

9. Click **Save** in the upper-right corner.



3.5.1.5.2. Import a process

You can import an existing process.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Process Orchestration**.
4. Click **Import Process**.
5. In the **Upload Process** dialog box, click **Click Here to Upload** to upload an existing process.

> **Note** Only JSON files that are not larger than 500 KB in size can be uploaded.

3.5.1.5.3. View processes

You can view existing processes.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Process Orchestration**.
4. In the **Name** search box, enter the name of the process that you want to view and click **Search**. Fuzzy search is supported.
   You can view the information of processes that meet the filter conditions, including the

process name, description, execution method, modification time, execution history, latest execution time, and latest execution status.

5. (Optional) Click **Reset** to clear the filter conditions.
6. Click the process name to go to the **Process Details** page.
   On the **Process Details** page, you can perform the following operations:
   - Click the **Process Details** tab to view the structure of the process.
   - Click the **Execution History** tab to view the execution history of the process. You can also click **View Details** to view the details of the execution history, including the node name, node type, start time, end time, task status, and execution information.
   - Click **Run** in the upper-right corner to manually run the process.
   - Click **Modify** in the upper-right corner to modify the process.
   - Click **Delete** in the upper-right corner to delete the process.

3.5.1.5.4. Export a process

You can export a process to your on-premises machine.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Process Orchestration**.
4. Select one or more processes that you want to export and click **Export Process** to export the processes to your on-premises machine.

> **Note** If you export multiple processes at a time, the content of the processes is stored in a single JSON file.

3.5.1.5.5. Modify a process

After a process is created or imported, you can modify the process to suit your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Process Orchestration**.
4. Find the process that you want to modify and click **Modify** in the **Actions** column.
5. Modify the process and click **Save** in the upper-right corner.

3.5.1.5.6. Run a process

You can manually trigger a process.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.

3. In the left-side navigation pane, click **Process Orchestration**.
4. Find the process that you want to run and click **Run** in the **Actions** column.
5. In the dialog box that appears, click **OK**.

3.5.1.5.7. Delete a process

You can delete a process that is no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Process Orchestration**.
4. Find the process that you want to delete and click **Delete** in the **Actions** column.
5. In the dialog box that appears, click **OK**.

3.5.1.6. Manage O&M jobs

O&M jobs are one of the core features of Operation Orchestration Service. An O&M job can be used to independently complete an O&M task such as software distribution, patch upgrade, and program update. You can create, import, view, export, modify, execute, and delete O&M jobs. A set of preset O&M tools are available in the platform. You can use them as needed.

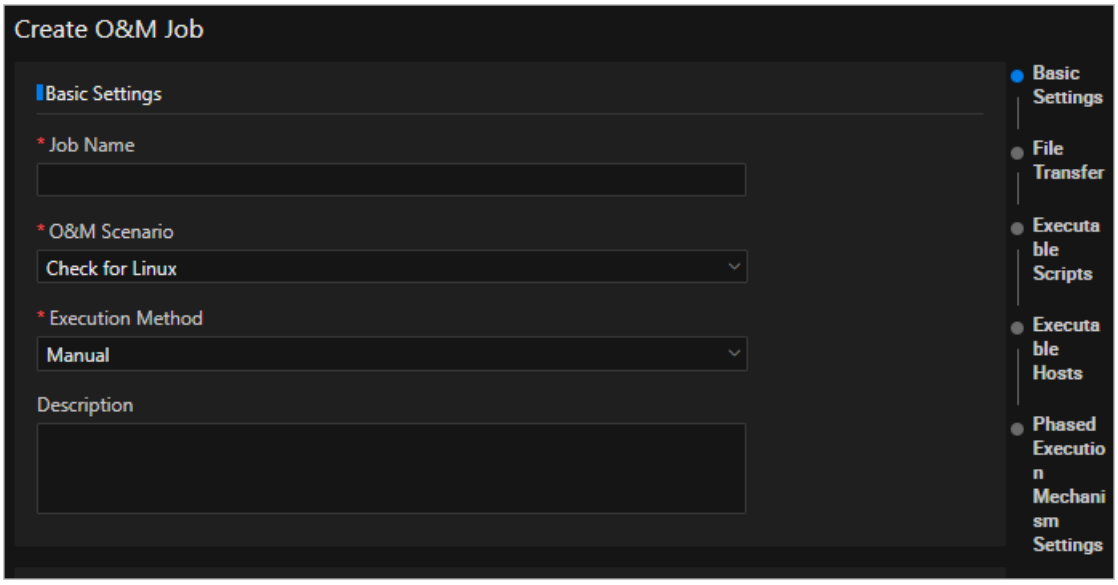
Each O&M job is a collection of features for O&M resources, software, and scripts. Scripts are used to implement features and are executed on different hosts or Docker containers in a specified order to reduce the workloads of O&M personnel.

3.5.1.6.1. Create an O&M job

You can create an O&M job to independently complete an O&M task. This way, automated O&M is implemented.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Click **Create O&M Job**.
5. On the **Create O&M Job** page, configure the parameters described in the following table.



Parameter	Description
Job Name	The name of the O&M job.
O&M Scenario	The scenario of the O&M job. You can select **Check for Linux**, **Run Command**, or **Install Software**.
Execution Method	Select **Manual** or **Scheduled**. ◦ **Manual**: The O&M job must be manually executed. ◦ **Scheduled**: The O&M job is executed at the specified time.
Timing Rule	This option is available only when **Execution Method** is set to **Scheduled**. Set the time to execute the O&M job. ◦ **Once**: The O&M job is executed only once at the specified time. Select a date and time to execute the O&M job. ◦ **Daily**: The O&M job is executed once at the specified time every day. Select a time to execute the O&M job every day. ◦ **Monthly**: The O&M job is executed at the specified day and time every month. Select a day and time to execute the O&M job every month. For example, if you set **Days** to 10 and **Time** to 09:00:00, the O&M job is executed at 09:00:00 on the tenth day of every month.
Description	The description of the O&M job.

File Transfer	Click **Add File**. In the **Add File** dialog box, select the file that you want to transmit to the host or Docker container, enter an absolute path in the Transmission Path field, and then click **OK**. You can add multiple files or click the icon to delete the files that are no longer needed. **Note** The files that you can select all come from the software repository.
Executable Scripts	Add one or more scripts that you want to execute on the host or Docker container, and the system executes them in sequence. Click **Add Executable Script** and select a script from the script library, or click **Add Script** to create a script. You can click the icon to modify the script. The modification does not change the original script content in the script library. You can click the or icon to change the order of execution of the script. You can also click the icon to delete the scripts that are no longer needed.
Executable Hosts	Set **Resource Type** to **Host** or **docker**. Click **Add Host Resources** or **Add Docker Resources** to add one or more hosts or Docker containers. These hosts or Docker containers are where all files are transmitted to and where the scripts are executed. **Note** You can specify only one resource type. You cannot add both host and Docker resources at the same time.
	You can select one of the following options to set the phased execution rules: ◦ **None (You do not need to specify this parameter, and all target hosts are executed directly.)**: The script is executed on all the selected hosts or Docker containers in a single batch. You can select this option if you are selecting only a few hosts or Docker containers, or if you have confirmed that you do not have problem with script execution. ◦ **Automatically Execute (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the second batch is automatically executed.)**: The script is executed in two batches on the selected hosts or Docker containers. One batch is executed at a time.

Phased Execution Rules	After the first batch is executed, the second batch starts to be executed. If the first batch fails to be executed, the second batch is not executed. **Note** If you set Resource Type to docker, the selected Docker containers are automatically divided into batches based on the server role name such that Docker containers with the same server role are in different batches. ◦ **Stop Waiting (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the process suspends. The second batch is executed after confirmation.)**: The script is executed in two batches on the selected hosts or Docker containers. The first batch is executed first. If the first batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job Review**. When the approval is passed, the second batch starts to be executed. If the first batch fails to be executed, the execution is stopped and no job approval is sent. **Note** If you set Resource Type to docker, the selected Docker containers are automatically divided into batches based on the server role name such that Docker containers with the same server role are in different batches. ◦ **Phased execution rules apply to physical servers by default but are not applicable to VMs or Docker containers. (The default phased execution rule is a cluster-based algorithm and is executed automatically on multiple hosts in parallel.)**: This option is applicable only to physical machines, but not to VMs or Docker containers. The script is executed in batches based on the phased execution rules provided in Apsara Infrastructure Management. After a batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job Review**. When the approval is passed, the next batch starts to be executed. If the batch fails to be executed, the execution is stopped and no job approval is sent. Jobs are executed by cluster based on the following rules on the machines in each cluster: ▪ For clusters in SLB, VPC, Apsara Infrastructure Management, ApsaraDB RDS, MiniRDS, OSS, and Blink, the job is executed machine by machine. ▪ For clusters other than the preceding ones and that contain 10 or fewer machines, the job is executed on the machines in the following order: 1 machine, 1 machine, 2 machines, 3 machines, and then the remaining machines.

- For clusters other than the preceding ones and that contain more than 10 machines, the job is executed on the machines in the following order: 1 machine, 3 machines, 5 machines, N/3-1 (rounded down) machines, and N/3-1 machines until the job is executed on all the machines. N is the number of machines in the cluster.

  > **Note** If a cluster contains both physical machines and VMs, the job is executed on all the VMs in the last batch.

- **Custom**: You can set the batches on your own to execute the job.

  In the **Batch Settings** drop-down list, select the hosts or Docker containers to add. You can click the icon to add batches or click the icon to delete batches. You can add up to three batches.

  Set **Phased Execution Condition** to **Automatic Execution per Batch** or **Waiting for Review and Confirmation**.

  - **Automatic Execution per Batch**: A batch is executed first. If the batch is executed, the next batch starts to be executed. If the batch fails to be executed, the next batch is not executed.
  - **Waiting for Review and Confirmation**: A batch is executed first. If the batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job Review**. When the approval is passed, the next batch starts to be executed. If the batch fails to be executed, the execution is stopped and no job approval is sent.

6. Click **Create**.

3.5.1.6.2. Import an O&M job

You can import existing O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Click **Import O&M Job**.
5. In the **Upload O&M Job** dialog box, click **Click Here to Upload** to upload an existing O&M Job.

> **Note**
> - Only JSON files that are not larger than 500 KB in size can be uploaded.
> - An imported O&M job cannot be directly executed. You must select a host before you can execute the job.

3.5.1.6.3. View O&M jobs

You can view existing O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. In the **O&M Job Name** field, enter the name of the O&M job that you want to view and click **Search**.

   > **Note** Fuzzy search is supported.

   You can view information of the O&M job that meets the filter conditions, including the job name, O&M scenario, description, execution method, modification time, execution history, latest execution time, latest execution status, update user, and whether the job is set to default.
5. **Optional:**In the upper-left corner of the page, click the icon to refresh the O&M job list.

3.5.1.6.4. Export an O&M job

You can export an existing O&M job to your on-premises machine.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Select one or more O&M jobs that you want to export and click **Export O&M Job** to export the O&M jobs to your on-premises machine.

   > **Note** If you export multiple O&M jobs at a time, the content of the jobs is stored in a single JSON file.

3.5.1.6.5. Modify an O&M job

After an O&M job is created or imported, you can modify the O&M job to suit your needs.

Procedure

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

2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Find the O&M job that you want to modify and click **Modify** in the **Actions** column.
5. On the Modify O&M Job page, modify the settings and click **Save**.

3.5.1.6.6. Execute an O&M job

You can manually execute an O&M job.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Find the O&M job that you want to execute and click **Execute** in the **Actions** column.
5. In the dialog box that appears, click **OK**. The **Execution Result Report** page appears.
6. On the **Execution Result Report** page, view the details of the O&M job.
   - Information including the **O&M Job Name**, **Start At**, **End At**, and **Result** is displayed.

     An execution has the following results:

     - Running: The O&M job is in progress. You can click **Refresh** in the upper-right corner to update the execution result.
     - Successful: The O&M job is successfully executed. You can view the details of the execution on this page.
     - Failed: The O&M job failed to be executed. On the **Execution History** page, you can view the cause of the failure.
   - Find the corresponding execution step, and click **View** in the **Result Record** column. In the **Result Record** dialog box that appears, view the results of the O&M job.

3.5.1.6.7. Delete an O&M job

You can delete O&M jobs that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **O&M Jobs**.
4. Select one or more O&M jobs that you want to delete and click **Delete Job** in the lower-left corner of the page, or click **Delete** in the **Actions** column.
5. In the dialog box that appears, click **OK**.

3.5.1.7. Manage execution history

You can view and delete execution history on the Execution History page. If an O&M job executed in batches fails to be executed, you can proceed with the execution. In addition, you can use the snapshot records feature to view the transferred files, executed scripts, and executed hosts of an O&M job.

3.5.1.7.1. View the execution history

You can query an O&M job to view the job name, start time, end time, execution method, execution result, and job information of the O&M job.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Execution History**. By default, all execution history information is displayed.
4. Enter a job name in the **O&M Job Name** field, select a start date and end date, and then click **Search**. The corresponding O&M jobs are displayed, and you can view the job name, start time, end time, execution method, execution result, and job information of these O&M jobs.

   > **Note**
   > - When you create an O&M job, you have two **execution methods** to choose from.
   >   - Manual: The O&M job must be manually executed.
   >   - Scheduled: The O&M job is executed at the specified time.
   > - **Job Information**: indicates the cause of an O&M job failure.

5. Find the destination O&M job and click **View** in the **Details** column. The **Execution History Report** page appears. You can view the execution history of the O&M job for different hosts.

3.5.1.7.2. Delete the execution history

You can permanently delete the execution history.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Execution History**.
4. Delete the execution history.
   - Delete a single execution: Find the destination execution and click **Delete** in the **Details** column.
   - Batch delete executions: Select multiple executions and click **Delete Execution History** in the upper-left corner of the page.
5. In the dialog box that appears, click **OK**.

3.5.1.7.3. View snapshot records

You can use the snapshot records feature to view the transferred files, executed scripts, and executed hosts of an O&M job.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Execution History**.
4. Find the destination O&M job and click **Snapshot Records** in the **Details** column.
5. In the **Job History Snapshot** panel, view the details of the transferred files, executed scripts, and executed hosts.

3.5.1.7.4. Proceed with execution

You can proceed with execution of an O&M job that is executed in batches.

Prerequisites

The following requirements must be met before you can proceed with execution of an O&M job on the **Execution History** page.

- The execution result of the O&M job is Failed.
- When you created the O&M job and set phased script execution, you selected the rule that implements batch execution.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, click **Execution History**.
4. Find the destination O&M job and click **Proceed** in the **Details** column.
5. In the dialog box that appears, click **OK**.

> **Note** If there are no subsequent batches to be executed, a prompt message is displayed.

3.5.1.8. Review jobs

If an O&M job is executed based on the phased execution rules, the system enables job review. After a batch is executed, the next batch does not start execution until the batch passes the review. You can pass or stop an O&M job.

Background information

During the execution of an O&M job, the system can only judge whether the O&M job is executed, but cannot know the execution result. If the O&M personnel want to confirm the execution result of one batch before they execute the next batch, they can set **Phased Execution Rules** to **Stop Waiting (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the process suspends. The second batch is executed after confirmation.)** to review the O&M job.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, choose **Audit Management > Job Review**.

4. Select the O&M job that you want to review and click **Pass** in the **Actions** column to execute the next batch, or click **Stop** to stop the execution of the next batch.
5. In the dialog box that appears, click **OK**.

3.5.1.9. Review processes

If a Manual node or a Task node for which **Phased Execution Settings** is set to **Stop Waiting** is available when a process is running, the system initiates process review. You can pass or stop the process.

Background information

When a process is running, the system can judge whether the task is complete but cannot determine whether the task is correctly executed. If a Manual node or a Task node for which **Phased Execution Settings** is set to **Stop Waiting** is available in a process, the O&M personnel can view the task execution result to determine whether to pass or stop the process.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, choose **Audit Management > Process Review**.
4. Select the process that you want to review and perform the following operations in the **Actions** column:
   - Click **Pass** to pass the process or execute the next batch.
   - Click **Stop** to stop the process or stop the execution of the next batch.
5. In the dialog box that appears, click **OK**.

3.5.1.10. View O&M logs

You can view the logs of various automated O&M operations.

Background information

You can view the type, time, user, and details of automated O&M operations to help you perform subsequent audits.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Operation Orchestration Service**.
3. In the left-side navigation pane, choose **Audit Management > Operation Logs**.
4. Select an O&M operation type from the **Type** drop-down list, select the start time and end time of the O&M operation, and then click **Search**.
   You can view the operation logs that meet the filter conditions, including the type, time, user, and details.
5. (Optional) Click **Reset** to clear the filter conditions.

3.5.2. Log Cleanup

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

3.5.2.1. Import container or physical server log cleanup rules

If configured log cleanup rules of containers or physical servers are available on your on-premises machine, you can batch import these cleanup rules.

Background information

Before you import a cleanup rule, take note of the following points:

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Container** or **Physical Machines** tab.
4. Click **Import**.
5. Select the XLS or XLSX files that you want to import and click **Open**. You can import multiple log cleanup rules.
   After you import the rules, corresponding execution plans are asynchronously generated.

3.5.2.2. Export container or physical server log cleanup rules

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. Perform the following operations to export the log cleanup rules of containers or physical

servers:

- Click **Export** to export all cleanup rules.
- In the upper part of the page, select a product, service, and server role, and click **Search**. In the search result, select the cleanup rules that you want to export and click **Export**.

> **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

3.5.2.3. Modify a log cleanup rule

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. **Optional:**In the upper part of the tab, select a product, service, and server role, and click **Search** to search for cleanup rules that meet the filter conditions.

   > **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

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

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

7. Click **OK**.

3.5.2.4. Delete a log cleanup rule

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. **Optional:**In the upper part of the tab, select a product, service, and server role, and click **Search** to search for cleanup rules that meet the filter conditions.

> **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

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

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

3.5.2.5. Obtain the usage information of containers or physical servers

You can query the disk usage information of containers or physical servers.

Method 1

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

     > **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

   - Select multiple containers or physical servers and click **Batch Query Usage** to obtain the disk usage information of these containers or physical servers.

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

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. **Optional:**In the upper part of the tab, select a product, service, and server role, and click

Search.

> **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

5. In the search results, select the cleanup rule of the container or physical server for which you want to obtain the disk usage information and click **Execution Plans** in the **Actions** column. The **Execution Plans** page appears.
6. Perform the following operations to obtain the disk usage information of a container or physical server:
   - Find the container or physical server for which you want to query disk usage information. Click **Query Usage** in the **Actions** column to obtain the disk usage information of the container or physical server.
   - Select multiple containers or physical servers and click **Batch Query Usage** to obtain the disk usage information of these containers or physical servers.

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

3.5.2.6. Clean up the logs of containers or physical servers

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

Method 1

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

     > **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

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

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

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. **Optional:**In the upper part of the tab, select a product, service, and server role, and click **Search**.

   > **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

5. Find the destination cleanup rule and click **Execution Plans** in the **Actions** column. The **Execution Plans** page appears.
6. Perform the following operations to clean up logs of containers or physical servers:
   - Find the destination container or physical server and click **Execute Clearance** in the **Actions** column to clean up the logs of the single container or physical server.
   - Select multiple containers or physical servers and click **Batch Clear** in the upper part of the tab to clean up the logs of these containers or physical servers at a time.

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

3.5.2.7. Configure automatic cleanups for container or physical server logs

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

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
   By default, the **Rules** page appears.
3. Click the **Containers** or **Physical Machines** tab.
4. Perform the following operations to configure automatic cleanups for container or physical server logs that meet the specified cleanup rules:
   - In the upper part of the tab, select a product, service, and server role, and click **Search**. In the search results, find the cleanup rule with which you want to set automatic log cleanups and turn on **Automatic Deletion**. The system cleans up the container or physical server logs that meet the cleanup rule.

> **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

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

- Select multiple cleanup rules and click **Enable Automatic Clearance** in the upper part of the tab. The system cleans up the container or physical server logs that meet the selected cleanup rules.

  If you want to disable the automatic log cleanup feature, click **Disable Automatic Clearance**.

3.5.2.8. View cleanup records

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

Background information

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

- Each time you perform a log cleanup operation, the numbers of cleanup executions, server roles, and machines are increased by one.
- Number of cleanup log files shows the number of log files that match all the available rules and that can be cleaned up, rather than the number of log files that have been cleaned up.
- Clean up space shows the accumulated available space after you clean up logs.

Method 1

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
3. In the left-side navigation pane, click **Records**.
4. **Optional:** In the upper part of the page, select a product, service, and server role, and click **Search**.

   > **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

5. Find the destination cleanup record and click **View Details** in the **Details** column to view the detailed cleanup information.

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Log Cleanup**.
3. In the left-side navigation pane, click **Plans**.
4. Click the **Containers** or **Physical Machines** tab.
5. **Optional:** In the upper part of the tab, select a product, service, and server role, and click **Search**.

> **Note** By default, the **product**, **service**, and **server role** fields on the page do not have options in their drop-down lists. When you specify these fields for the first time, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down lists.

6. Find the destination execution plan and click **Cleanup Records** in the **Actions** column. The **Records** page appears.
7. Find the destination cleanup record and click **View Details** in the **Details** column to view the detailed cleanup information.

3.5.3. Security O&M

The security O&M feature provides CLI logon and remote O&M, supports blocking and approval of high-risk operations, and allows you to audit all operations.

The security O&M feature provides a web terminal that can be used to:

- Log on to user machines such as virtual machines, hosts, and containers.
- View the environment metadata, OOB information, and cluster configurations of the current user.
- Upload and download files.
- Audit all operations.
- Enable blocking, secondary verification prompt, and execution after approval for high-risk operations.
- Implement security control configurations for projects to be connected to Apsara Stack Online.

3.5.3.1. Fast arrival

You can log on to machines in the Apsara Stack environment such as virtual machines, hosts, and containers and run Linux commands to perform operations. You can also view environment metadata, OOB information, and cluster configurations.

3.5.3.1.1. Log on to the machine where a server role is deployed

You can log on to the virtual machine, host, or container where a server role is deployed and upload or download files.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.

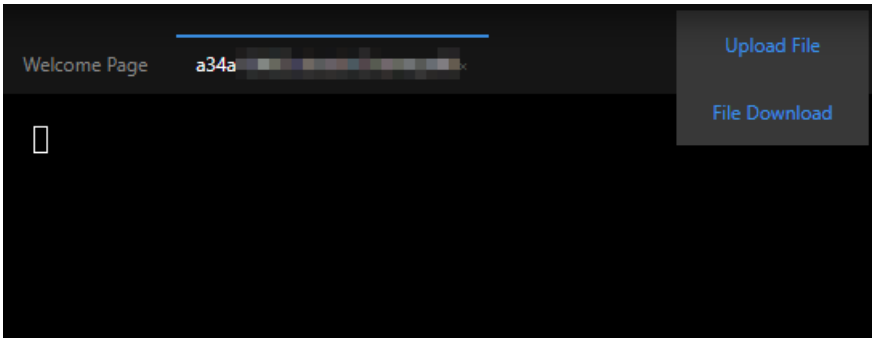
   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Select a server role from the **Server Role** drop-down list.

> **Note**
>
> The drop-down list also supports fuzzy search. You can move the pointer to and click the drop-down list, enter a keyword, and select a server role from the fuzzy search results.

4. In the **Host** column, find a host and click Log On to log on to the virtual machine or host where the server role is deployed.

   > **Note**
   >
   > If two links appear in the **Host** column, the first one is used to log on to the virtual machine and the second one is used to log on to the host of the virtual machine.

   i. After you log on to the virtual machine or host where a server role is deployed, enter Linux commands in the CLI window to perform related operations.

   ii. Click **Upload File** in the CLI window. The **Upload File** dialog box appears. You can upload a file in one of the following ways:

   - Click the dotted box. In the dialog box that appears, select the file that you want to upload and click **Open**. Click **Upload** in the **Upload File** dialog box.
   - Drag the file to the dotted box and then click **Upload**.

   iii. Click **Download File**. The **Download File** dialog box appears. Set **File Name** and **File Directory** and then click **Download** to download the file to the default download directory of your browser.

   > **Note**
   >
   > The file that you want to upload or download cannot exceed 200 MB in size.

5. In the **Docker** column, you can click the relevant links to log on to and restart the container, or view logs and inspection reports of the container.

3.5.3.1.2. Log on to the virtual machine where a server role group is deployed

You can log on to the virtual machine where a server role group is deployed and upload or download files.

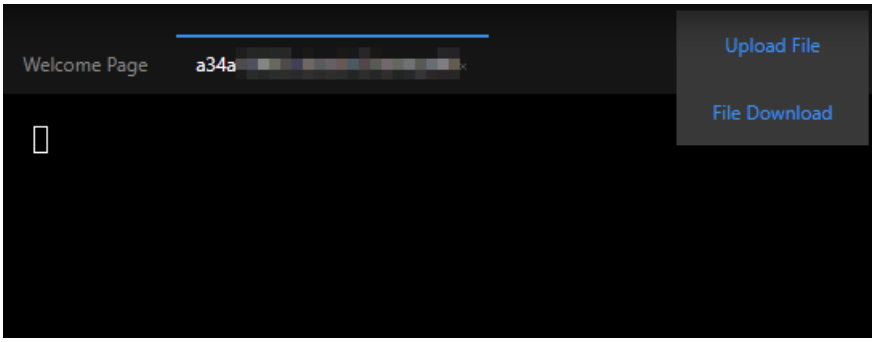
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.

   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Click the **Server Role Group Logon** tab.
4. Select a server role group of a product from the **Server Role Group** drop-down list. The server roles included in the group are displayed in the lower part of the page.

> **Note** The drop-down list also supports fuzzy search. You can move the pointer to and click the drop-down list, enter a keyword, and select a server role group from the fuzzy search results.

5. Find a server role and click **Log On** in the **Machine** column to log on to the virtual machine where the server role is deployed.
   i. After you log on to the virtual machine where a server role is deployed, enter Linux commands in the CLI window to perform related operations.



   ii. Click **Upload File** in the CLI window. The **Upload File** dialog box appears. You can upload a file in one of the following ways:
   - Click the dotted box. In the dialog box that appears, select the file that you want to upload and click **Open**. Click **Upload** in the **Upload File** dialog box.
   - Drag the file to the dotted box and then click **Upload**.

   iii. Click **Download File**. The **Download File** dialog box appears. Set **File Name** and **File Directory** and then click **Download** to download the file to the default download directory of your browser.

> **Note** The file that you want to upload or download cannot exceed 200 MB in size.

3.5.3.1.3. Query environment metadata

You can view the metadata of a service registered in Apsara Infrastructure Management.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.

   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Click the **Environment Metadata Query** tab.
4. Select a service from the **Service** drop-down list. The metadata of the service registered in Apsara Infrastructure Management is displayed in the lower part of the page.

> **Note**
> - The drop-down list also supports fuzzy search. You can move the pointer to and click the drop-down list, enter a keyword, and select a service from the fuzzy search results.
> - You can also enter a keyword in the box above the displayed metadata to filter metadata.

3.5.3.1.4. Query OOB information

You can query the OOB information by specifying an IP address or a serial number.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.

   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Click the **OOB Information Query** tab.
4. Enter an IP address or a serial number in the field. In the **Search** column, click **Search** to view the OOB information.

3.5.3.1.5. Query the configurations of a cluster

You can view the configuration files of all services deployed in a cluster.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.

   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Click the **Cluster Configuration Query** tab.
4. Select a cluster of a product from the **Cluster Name** drop-down list. The configuration files of all services deployed in the cluster are displayed in the lower part of the page.

   > **Note**
   >
   > The drop-down list also supports fuzzy search. You can move the pointer to and click the drop-down list, enter a keyword, and select a cluster from the fuzzy search results.
5. Click a configuration file on the left to view its details on the right.

3.5.3.1.6. Log on to a metadatabase

You can log on to a metadatabase used by a server role of a service and upload or download files.

Procedure

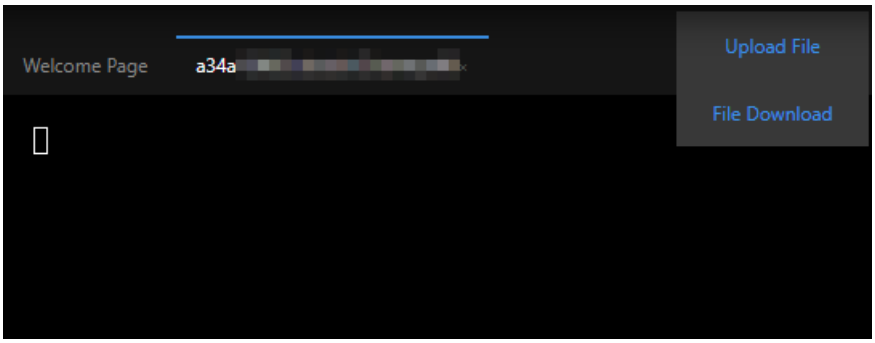
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.

   By default, the **Fast Arrival** > **Server Role Logon** page appears.
3. Click the **Metadatabase Logon** tab.
4. Select a service from the **Service** drop-down list.

   > **Note**
   >
   > The drop-down list also supports fuzzy search. You can move the pointer to and click the drop-down list, enter a keyword, and select a service from the fuzzy search results.
5. The metadatabases used by all server roles of the service are displayed in the lower part of

the page. Find a database and click **Writable Logon** in the **Actions** column.

i. After you log on to the metadatabase, enter SQL statements in the CLI window to perform related operations.



ii. Click **Upload File** in the CLI window. The **Upload File** dialog box appears. You can upload a file in one of the following ways:

- Click the dotted box. In the dialog box that appears, select the file that you want to upload and click **Open**. Click **Upload** in the **Upload File** dialog box.
- Drag the file to the dotted box and then click **Upload**.

iii. Click **Download File**. The **Download File** dialog box appears. Set **File Name** and **File Directory** and then click **Download** to download the file to the default download directory of your browser.

> **Note**
>
> The file that you want to upload or download cannot exceed 200 MB in size.

3.5.3.2. Audit

You can view command records and videos, file upload and download records, and authorization information related to the security O&M feature.

3.5.3.2.1. View command records

You can view the command records of the security O&M feature.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.
3. In the left-side navigation pane, click **Audit**.

   By default, the **Command Records** tab appears.
4. Enter a command in the **Command** field, select a time range, and then click **Search** to search for the command record.

> **Note**
>
> The system will audit the command that you enter and give one of the following audit results based on operational risks:
>
> - **pass**: The audit is successful.
> - **fail**: The audit fails.
> - **multiVerify**: A further verification is required.
> - **codeVerify**: Authorization is required for use.

5. (Optional)

   Click **Advanced** in the upper-right corner. The **Machine**, **Service**, **Server Role**, and **Operated By** fields appear. Enter values in the fields and click **Search** to further filter command records.

   > **Note**
   >
   > - Click **Reset** to clear the values that you enter.
   > - Click **Collapse** to hide the preceding fields.
   > - The preceding fields support fuzzy search.

3.5.3.2.2. View file upload and download records

You can view the information of file uploads and downloads performed in the Security O&M module.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.
3. In the left-side navigation pane, click **Audit**.
4. Click the **Upload and Download Audit** tab to view file upload and download records.

3.5.3.2.3. View authorization information

You can view command authorization information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.
3. In the left-side navigation pane, click **Audit**.
4. Click the **Authorize** tab to view command authorization information.

3.5.3.2.4. View command videos

You can view the videos of all commands executed on the machine.

Procedure

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

2. In the top navigation bar, choose **GeneralChangesSecurity O&M**.
3. In the left-side navigation pane, click **Audit**.
4. Click the **Playback** tab.
5. Select a time range, enter a value in the **Operated By** field, and then click **Search** to view the command records.
6. Find a command record and click **View** in the **Actions** column.
7. In the video playback window, click the icon to play the command video.
8. (Optional)

   Click **Advanced** in the upper-right corner. The **Machine**, **Service**, and **Server Role** fields appear. Enter values in the fields and click **Search** to further filter command records.

   > **Note**
   > - Click **Reset** to clear the values that you enter.
   > - Click **Collapse** to hide the preceding fields.
   > - The preceding fields support fuzzy search.

3.5.3.3. Rules

To control the risks of Linux commands, you can configure blocking rules for Linux commands.

3.5.3.3.1. View a rule

You can view the information of the command blocking rules that you create or import, such as their details, confirmation, and status.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. Enter a command in the **Command** field and then click **Search** to view the information of its blocking rules.
5. **Optional:**Click **Advanced** in the upper-right corner. The **Target Parameter**, **Service**, **Server Role**, **Verification Rule**, and **Status** fields appear. Enter values in the fields and click **Search** to further filter blocking rules.

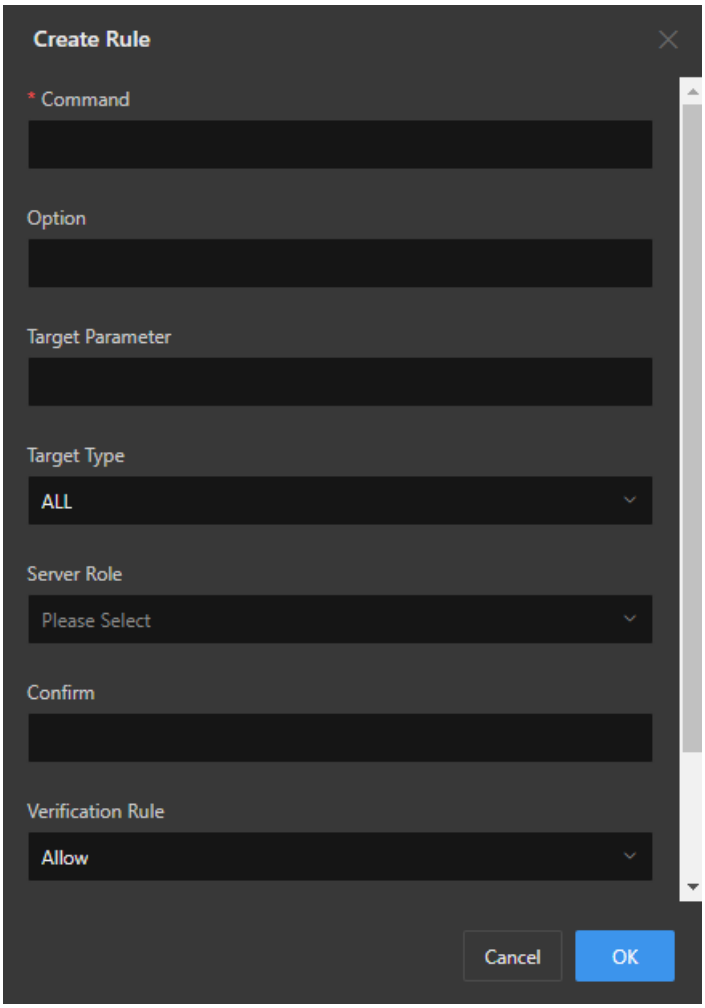
   > **Note**
   > - Click **Reset** to clear the values that you enter.
   > - Click **Collapse** to hide the preceding fields.

3.5.3.3.2. Create a rule

You can create a command blocking rule.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. In the upper-left corner, click **Create Rule**. In the dialog box that appears, configure the parameters and then click **OK**.



The following table describes the parameters.

Parameter	Description	Example
Command	The Linux command.	mv
Option	The option of the command. For example, the option of the `rm -rf` command is **rf**.	rf
Target Parameter	The parameter of the command option. For example, in the `find / -name test` command, **name** is the option and **test** is the parameter. If the option does not have a parameter, the value is empty.	test

Target Type	The type of the command option. Valid values: ◦ ALL ◦ FILE ◦ DIR ◦ OPTION	OPTION
Server Role	The server role of the machine where the command is implemented.	ram-ramService.RamPortalService#
Confirm	The prompt in the CLI window when the command is blocked.	Termination of the process is not allowed.
Verification Rule	The rule to block the command. Valid value: ◦ Allow: The command can be run. ◦ Block: The command is blocked. ◦ Confirm Again: You must confirm again whether the command can be run. ◦ Verification Code: The command can be run within a time range after the authorization is approved. If you select this value, a verification code is applied to the system. The verification code is required before the command can be run.	Pass
Status	The status of the command. You can click the **Status** button to modify the status.	The **Status** button is turned on.

3.5.3.3.3. Batch import rules

You can batch import command blocking rules.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. In the upper-left corner, click **Import Rules**. Select the command blocking rule file and then click **Open** to import the file.

> **Note** The file that you want to import must be in the .xlsx format. You can first export the template and then enter information in the template.

3.5.3.3.4. Batch export rules

You can batch export command blocking rules that you create.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. In the upper-left corner, click **Export Rules**. In the dialog box that appears, select the download directory (the Download directory by default), and click **Download** to download the command blocking rule file to your computer.

3.5.3.3.5. Modify a rule

You can modify a command blocking rule that you create.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. Find a rule and click **Modify** in the **Actions** column. In the dialog box that appears, modify the parameters and click **OK**.

3.5.3.3.6. Delete a rule

You can delete a command blocking rule that you create.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Rules**.
4. Find a rule and click **Delete** in the **Actions** column. In the dialog box that appears, click **OK** to delete the rule.

3.5.3.4. Settings

When a project is connected to Apsara Stack Online, you can configure the IP address and port number of the worker that the Apsara Uni-manager Operations Console can access, and the IP addresses in Apsara Stack Online that the Apsara Uni-manager Operations Console can access.

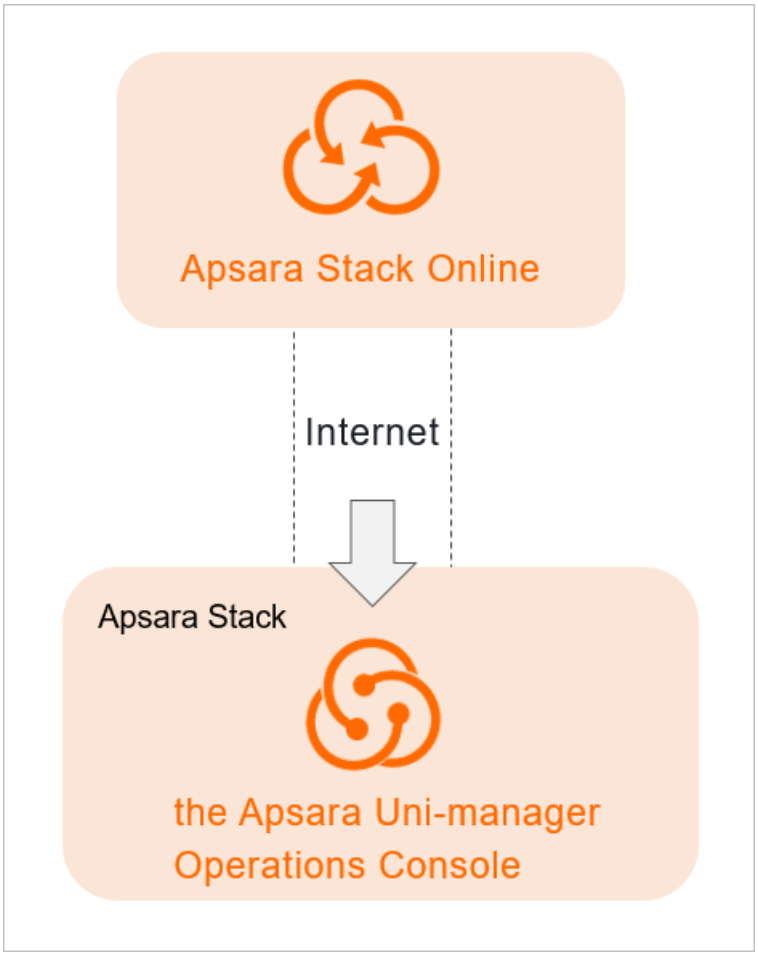
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Changes > Security O&M**.
3. In the left-side navigation pane, click **Settings**.
4. In the **Configure Worker** section, enter the IP address and port number of the worker, and then click **Save**.
5. In the **Configure Simplified O&M Whitelist** section, enter the allowed IP addresses in

Apsara Stack Online and click **Save**.

> **Note** Separate multiple IP addresses with commas (,).

The following figure shows the remote O&M process.



3.6. Archives

You can archive the key metadata of Apsara Stack. Only the metadata of Apsara Distributed File System and OPS DNS can be archived. The archived metadata information is used for quick recovery from Apsara Stack failures.

3.6.1. Add an archive product

You can add an archive product. Only the metadata of Apsara Distributed File System and OPS DNS can be archived.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralArchivesArchive Products**.
3. Click **Add Product**.
4. In the **Add Product** dialog box, add information of a product as described in the following table and click **OK**.

Parameter	Description	Example
Product	The name of the product. You can select a product from the drop-down list.	pangu
Archived Item	The product information to be archived.	ecs_pangu
Script	The name of the archive script.	metadata_backup.py
Retry Times	The number of retries after an error occurs. Typically, set this parameter to 3.	3

5. To add more archived items, repeatedly perform the preceding steps.

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

Result

You can view the added product on the **Archive Settings** page.

3.6.2. Configure archive settings

After an archived item of a product is added, you must configure archive settings for the item in the Apsara Uni-manager Operations Console.

Prerequisites

An archived item of a product is added. For information about how to add an archived item, see **Configure archive settings**.

Context

An archived item is the smallest unit for archiving. You can archive the metadata of Apsara Distributed File System for different services, such as ecs pangu, ots pangu, oss pangu, and ads pangu.

Procedure

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

   In the left side of the page, the current archived items that you can configure are displayed in a hierarchical tree-like structure. The root node is a product list and shows the products whose data can be archived in the system. Only the metadata of Apsara Distributed File System and OPS DNS can be archived.
3. Click an archived item of a product on the left and then configure the parameters on the right.

> **Note**
> If the #FTPMaster server is deployed in the cluster of the service, the system will automatically fill in the archive information of ecs pangu.

Parameter	Description
Product Cluster IP Address	The IP address of the actual transfer server.
Archive Folder	A folder on the transfer server. You are required only to enter a folder path in the field without manually creating a folder to store archive files. Examples: ◦ pangu: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bak ◦ opsdns: /apsarapangu/disk8/opsdns_bak/opsdns/bak
Script Execution Folder	A folder on the transfer server. You are required only to enter a folder path in the field without manually creating a folder to store script executions. Examples: ◦ pangu: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bin ◦ opsdns: /apsarapangu/disk8/opsdns_bak/opsdns/bak
Script Parameters	Required. The execution parameters for the script. You must enter the value in the `--ip=xxx.xxx.xxx.xxx` format. ◦ pangu: Enter any of the IP addresses of the pangu master. ◦ opsdns: We recommend that you enter `--ip=127.0.0.1`.
Archive Schedule	The execution period of recurring executions. In this example, a value of 1 is entered to specify that the archive is performed only once.
Archive Schedule Unit	The unit of the execution period. Valid values:**Day**, **Hour**, and **Minute**. In this example, **Hour** is selected to specify that the archive is performed by hour.
Timeout Period	The timeout period, in milliseconds. In this example, set the value to **3600**.

4. Click **Modify** to complete the configuration and trigger the archive.
5. Perform the preceding steps to configure all the archived items.

3.6.3. View archive details

During archiving, you can view the archive details of each archived item in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralArchivesArchive Details**.
3. On the **Archive Details** page, enter a product and archived item, select the start date and end date, and then click **Search**.
4. View the archive details of an archived item, including the product, archived item, the name of the file to be archived, start time, and status.

   The archive status includes **Not started**, **In transmission**, **Complete**, **Time-out**, and **Failed**.
5. (Optional)

   You can also click **Reset** to clear the filter conditions.

3.6.4. Configure the archive server

You can configure the archive server for the storage of archive files.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **GeneralArchivesArchiving Server Settings**.
3. Configure the archive server information.

   > **Note**
   >
   > If the #FTPMaster server is deployed in the cluster of the service, the system will automatically fill in the backup server information of ecs pangu.

   The following table describes the parameters.

Parameter	Description
Archive Server IP Address	The IP address of the archive server. The archive server must meet the following requirements: ◦ The archive server is an independent physical server. ◦ The archive server is controlled by the Apsara Infrastructure Management console. ◦ The network of the archive server is connected to other servers in Apsara Stack. ◦ Apsara Distributed File System cannot be deployed on the server or on the disk where archive metadata is stored.

Archive Server Monitoring Path	The storage path of archive files on the archive server. The archive service detects new archive files by monitoring the specified folder on the archive server and determines whether an archive is successful by comparing the MD5 value of the archive file with that of the original file.
Archive Retention Period	The actual period of time an archive file is saved. Overdue archive files are deleted.

4. Click **Save**.

3.6.5. Use cases

To ensure the availability of services, you must archive the data of different services stored on Apsara Distributed File System.

3.6.5.1. Prepare

This topic describes how to prepare for an archive.

Before an archive, take note of the following points:

- A buffer server is required as the archive server.

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

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

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

  No other requirements are needed for transfer servers.

- The network of the archive server must be connected with that of the Docker container where the offline archive service is located. This ensures that archive containers in the clusters of the Apsara Uni-manager Operations Console can log on to the transfer server and archive server by using SSH key pairs, without the need for you to provide the username and password.

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

You can collect the Apsara Distributed File System information of products to be archived, which helps add the archive product information to the Apsara Uni-manager Operations Console.

Background information

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

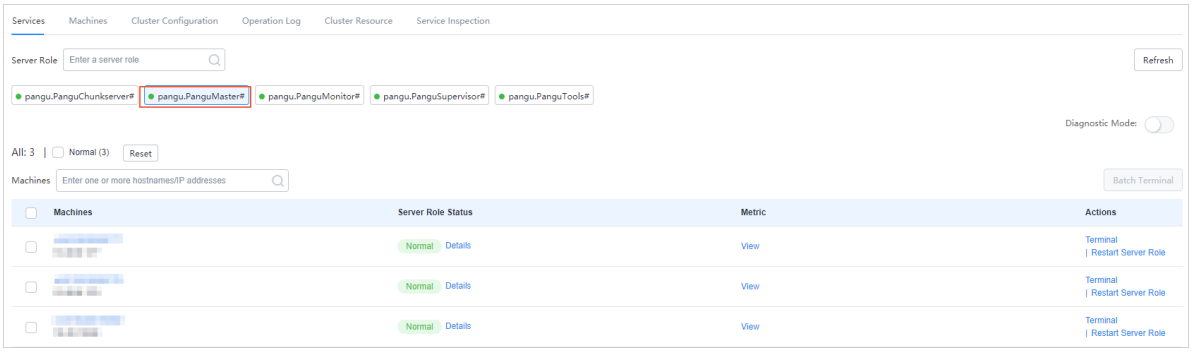
Procedure

1. Log on to the Apsara Infrastructure Management console.
   i. Log on to the Apsara Uni-manager Operations Console.
   ii. In the top navigation bar, choose **Products > Base/Platforms > Apsara Infrastructure Management**.

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

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

   Click the ECS-IO7-A-xx cluster in this example.
7. On the **Services** tab, click **pangu.PanguMaster#**.



8. View and record the IP addresses of Apsara Distributed File System master in the server list.
   Record one of the three IP addresses of **PanguMaster#**.
9. Repeat Steps 6 to 8 to view and record the Apsara Distributed File System information of each product. The recorded results are similar to those in the following table.

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

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

3.6.5.3. Configure the archive server

You can configure the archive server in the Apsara Uni-manager Operations console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Archives > Archiving Server Settings**.
3. Configure the archive server information.

   > **Note** If the #FTPMaster server is deployed in the cluster of the service, the system will automatically fill in the archive server information of ecs pangu.

   The following table describes the parameters.

Parameter	Description
Archive Server IP Address	The IP address of the archive server. The archive server must meet the following requirements: ◦ The archive server is an independent physical server. ◦ The archive server is controlled by the Apsara Infrastructure Management console. ◦ The network of the archive server is connected to other servers in Apsara Stack. ◦ Apsara Distributed File System cannot be deployed on the server or on the disk where archive metadata is stored.
Archive Server Monitoring Path	The storage path of archive files on the archive server. The archive service detects new archive files by monitoring the specified folder on the archive server and determines whether an archive is successful by comparing the MD5 value of the archive file with that of the original file.
Archive Retention Period	The actual period of time an archive file is saved. Overdue archive files are deleted.

4. Click **Save**.

3.6.5.4. Add an archive product

You can add an archive product in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Archives > Archive Products**.

3. Click **Add Product**.
4. In the **Add Product** dialog box, add information of a product as described in the following table and click **OK**.

Parameter	Description	Example
Product	The name of the product. You can select a product from the drop-down list.	pangu
Archived Item	The product information to be archived. Set this parameter based on the product information described in the Collect the Apsara Distributed File System information of each product topic.	ecs_pangu
Script	The name of the archive script.	metadata_backup.py
Retry Times	The number of retries after an error occurs. Typically, set this parameter to 3.	3

5. Repeat the preceding steps to add all the archived items.

Result

Example

You can view the added product on the **Archive Settings** page.

3.6.5.5. Configure archive settings

After an archived item is added, you can configure archive settings for the item in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Archives > Archive Settings**.
3. Click an archived item of a product on the left and then configure the parameters on the right.

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

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

4. Click **Modify** to complete the configuration and trigger the archive.
5. Perform the preceding steps to configure all the archived items.

3.6.5.6. View archive details

After you configure an archived item, you can check whether the archived item functions normally in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General > Archives > Archive Details**.
3. On the **Archive Details** page, enter a product and archived item, select the start date and end date, and then click **Search**.

   If the status of an archived item is **Complete**, the archived item functions normally.

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

4.Product operations

4.1. Elastic computing operations

4.1.1. Compute Operations Console

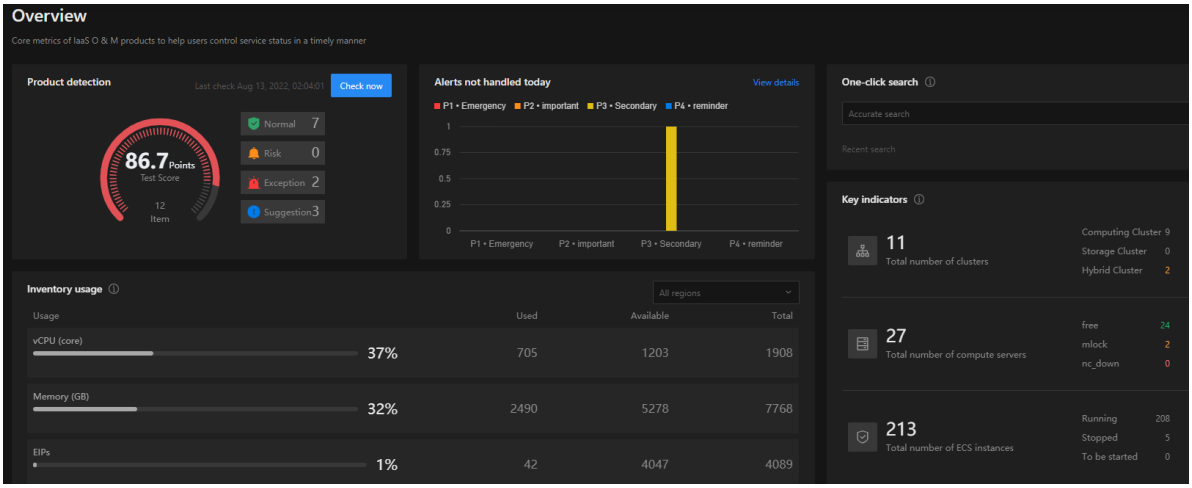
You can manage ECS instances and monitor the performance, alerts, and service status of ECS instances in the Compute Operations Console. The Compute Operations Console allows you to manage compute clusters, physical servers, ECS instances, and logs. You can also configure monitoring and alerts and perform inventory analysis in the console.

4.1.1.1. Overview

You can query the core metrics of products in IaaS O&M, obtain up-to-date information about services, and view information such as diagnostics, alerts, and key metrics of products, and health status and services.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
   By default, the **Computing Overview** page is displayed.



3. In the product diagnostics section, view the test score displayed on the dashboard. The score is calculated based on 12 check items. You can also view the number of items that are in the Normal, Risk, and Abnormal states.

   > **Note** If the score is 100, the dashboard is displayed in green. If the score is lower than 100, the dashboard is displayed in red.

   In the upper-right corner of the section, click **Check Now**. In the **Service Check** dialog box that appears, view the test score, the status of each check item, and error details.
4. In the **Unhandled Alerts Today** section, view the statistics of alerts at all risk levels. In the upper-right corner of the section, click **View Details**. You are redirected to the **Alerts**page. **>**
5. In the **One-click Search** section, enter an instance ID, a disk ID, an image ID, an ENI ID, a security group ID, the private or public IP address of an ECS instance, or the IP address of a physical server to search for relevant information and click the displayed information to go

the corresponding page.

6. In the **Inventory usage** section, view the inventory usage of vCPUs, memory, and EIPs. You can also view the number of used resources, available resources, and total resources.

   > **Note** By default, the metric statistics of all clusters are displayed. You can select a cluster from the drop down list in the upper-right corner of this section to display only the statistics of the selected cluster.

   The following table describes the metrics.

Metric	Description
vCPU (Cores)	The virtual CPU of a virtual machine.
Memory (GB)	The size of the memory for sale.
EIPs	The number of EIPs.

7. In the **Core Metrics** section, view the total number of clusters and the numbers of compute clusters, storage clusters, and hybrid clusters. You can also view the total number of compute servers in the free, mlock, and nc_down states and the total number of ECS instances in the running, stopped, and pending states.
   Perform the following operations to view the cluster details:
   - Click the total number of clusters to view the cluster details on the **Cluster O&M** page.
   - Click the total number of servers to view the server details on the **ECS O&M** page.
   - Click the total number of ECS instances to view the instance details on the **Instances** page.
8. In the **Health Status of Services** section, view the health status of each service.

   Click a service name. In the **Deploy Servers** dialog box that appears, view the status, server role, IP address of the physical machine on which the service is deployed, hostname, cluster, description, and the service to which the service belongs.

4.1.1.2. Cluster O&M

4.1.1.2.1. View the cluster list

You can query and view the information about all computing clusters. You can also view the total number of clusters, the number of clusters that have not reached the final state, and the number of clusters that have reached the final state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
   By default, details of all clusters are displayed.
4. In the upper-right corner of the page, view the total number of clusters, the number of clusters that have not reached the final state, and the number of clusters that have reached the final state.
   The number of clusters that have not reached the final state is displayed in red.
5. **Optional:** In the upper-left corner of the page, enter the name of a cluster and click the

icon to query the cluster.

6. **Optional:**Select items to display in the cluster list and customize the columns.
   i. In the upper-right corner of the cluster list, click the icon.
   ii. Select items that you want to display in the cluster list.
   iii. Move the pointer over an item and click the icon to adjust the position where the item is displayed.
7. View the following information about the cluster: region, type, status, zone, the number of servers, instance type, and sales form.

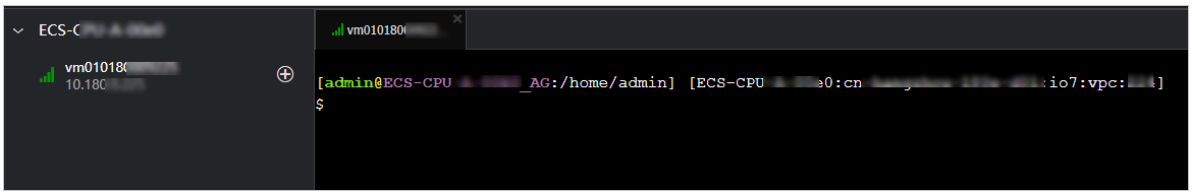
> **Note** Sales forms:
> - exclusive: exclusive instance
> - share: shared instance
> - bare_metal: ECS bare metal instance
> - cpu_credit: T5 instance

4.1.1.2.2. Connect to cluster AG

You can log on to Admin Gateway and access the TerminalService page to perform O&M operations on virtual machines by using the CLI. You can enter the TerminalService page from the Cluster O&M or Compute Cluster Details page. This topic describes how to connect to the cluster AG from the Cluster O&M page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. On the page that appears, find the cluster that you want to manage and click **Log on to Cluster AG** in the **Operation** column.
5. Go to the TerminalService page.
6. In the left-side navigation pane, click the dockervm name. Then, specify the O&M operation that you want to perform in the CLI on the right side.



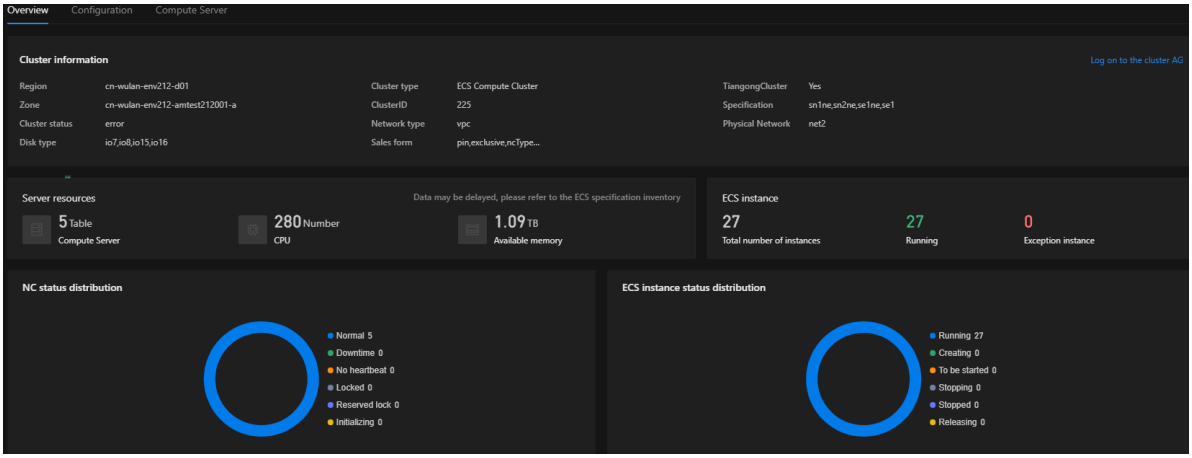
4.1.1.2.3. O&M details

4.1.1.2.3.1. Cluster overview

You can view the following information about clusters: servers, ECS instances, state distribution of physical servers and ECS instances, inventory utilization, and inventory details of the cluster specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to view and click the cluster name in the **Cluster Name** column.
   By default, the **Overview** tab of the **Computing Cluster Details** page is displayed.



5. View the details of physical machines and ECS instances in the cluster.
   - In the **Cluster Information** section, view the following information about the cluster: the region in which the cluster is deployed, cluster type, whether the cluster uses only ECS resources, zone, cluster ID, cluster specification, cluster status, network type, physical network, disk type, and sales form.

     In the upper-right corner of this section, click **Connect to Cluster AG** to log on to the Admin Gateway and perform O&M operations on the cluster. For more information, see Connect to cluster AG.
   - In the **Server Resources** section, view the number of compute servers, the number of CPUs, and the available memory.
   - In the **ECS Instances** section, view the total number of instances, the number of running instances, and the number of abnormal instances.
   - In the **NC State Distribution** section, view the distribution of physical servers in different states.

     > **Note** Move the pointer over the figure. The number of servers in each state is displayed.

     The following table describes the server states.

State	Description
Failover	The physical server is down.
Normal	The physical server is running normally. You can schedule instances to the physical server.
No Heartbeat	The physical server has no heartbeats.
MIock	The physical server is manually locked.

RIock	The physical server is forcibly reserved for server downtime.
Initializing	The physical server is being initialized. All the VPC configurations of the physical server are being reissued by the RegionMaster.

- In the **ECS Instance State Distribution** section, view the distribution of ECS instances in different states.
  The following table describes the instance states.

State	Description
Running	The instance is running normally.
Stopped	After an instance is stopped or after an instance is created but not started, it is in the Stopped state. Instances in the Stopped state cannot provide external services.
Pending	After an instance is created, it is in the Pending state before it enters the Running state. If the instance remains in this state for an extended period of time, an exception occurs.
Creating	After you start or restart an instance in the ECS console or by calling an API operation, the instance enters the Creating state before it enters the Running state. If the instance remains in this state for an extended period of time, an exception occurs.
Stopping	After you stop an instance in the ECS console or by calling an API operation, the instance enters the Stopping state before it enters the Stopped state. If the instance remains in this state for an extended period of time, an exception occurs.
Releasing	After you release an instance, it enters the Releasing state before it enters the Released state.

- In the **Inventory Utilization** section, view the total amount of resources, the amount of used resources, and the percentage of the used resources to the total resources.
- In the **Inventory** section, view the inventory details of the cluster specifications.

4.1.1.2.3.2. Cluster configuration management

View configuration information of a cluster

You can view the configuration information of clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to view and click the cluster name in the **Cluster Name** column.
   By default, the **Overview** tab of the **Computing Cluster O & M details** page is displayed.
5. In the upper-left corner of the page, click the **Configurations** tab.
   The **Cluster Configurations** tab appears.
6. View the configuration information of the cluster and the last time when the configurations

are modified.

Modify cluster configurations

You can modify the configurations of clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to manage and click the cluster name in the **Cluster Name** column.
   By default, the **Overview** tab of the **Computing Cluster Details** page is displayed.
5. In the upper-left corner of the page, click the **Configurations** tab.
   The **Cluster Configurations** tab appears.
6. Find the configuration that you want to modify and click **Edit** in the **Operation** column.
7. In the dialog box that appears, enter the value and a reason for the modification.
8. Click **OK**.

View configuration change records

You can query and view the change records of cluster configurations.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to view and click the cluster name in the **Cluster Name** column.
   By default, the **Overview** tab of the **Computing Cluster Details** page is displayed.
5. In the upper-left corner of the page, click the **Configurations** tab.
   The **Configuration Management** tab appears.
6. In the upper-left corner of the page, click the **Change Records** tab. All the change records of the cluster configurations are displayed.
7. In the upper-left corner of the page, enter a ticket ID in the search box and click the  icon.
8. View the following information about the change record: configuration name, source value, destination value, operator, change status, and the time when the configuration was modified.

4.1.1.2.3.3. Computing server management

View the server information

You can view the following information about computing servers: basic information, O&M details, and ECS instances deployed on the servers.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations**

Console.

3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to view and click the cluster name displayed in blue in the **Cluster Name** column.
   By default, the **Overview** tab of the **Computing Cluster Details** page is displayed.
5. In the upper-left corner of the page, click the **Computing Servers** tab.
6. View the physical servers deployed on the cluster.
   i. **Optional:**Change the items displayed on the physical server list.
      a. In the upper-right corner of the page, click the icon.
      b. In the **Custom list item display** dialog box, select the items that you want to display in the server list.
      c. Click **OK**.
   ii. View the following information about the servers: hostname, IP address, server ID, server type, vCPU (cores), memory, server state, instances, data center, rack, and serial number.

      > **Note** For more information about the server states, see Cluster overview.

7. **Optional:**View O&M details of a computing server.
   i. Find the server that you want to view and click the server name in the **Hostname** column.
   ii. View the information about the server on the **Computing Server O&M** page that appears. For more information, see Server O&M details.

Manage the server status

You can lock, unlock, and activate the computing servers in a computing cluster to manage the status of the servers. For more information, see Server O&M > Machines.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Computing Cluster O&M**.
4. Find the cluster that you want to manage and click the cluster name in the**Cluster Name** column.
   By default, the **Overview** tab is displayed on the **Computing Cluster O & M details** page that appears.
5. In the upper-left corner of the page, click the **Computing Servers** tab.
6. Manage the business status of servers. The following table describes the operations that you can perform on servers.

Operation	Description	Procedure

Lock NC	◦ You can lock abnormal servers to prevent instances from being scheduled to these servers. ◦ You can also lock servers for which you want to reserve resources.	i. In the Compute Servers tab, find the server that you want to lock and click **Lock NC** in the **Operation** column. ii. In the **Lock NC** dialog box that appears, select a state from the drop-down list and enter a ticket title and a reason for locking the sever. iii. Click **OK**.
Unlock NC	You can unlock servers in the No Heartbeat, Mlock, and Rlock states. After you unlock a server, the server is automatically activated and you can schedule instances to the server.	i. In the Compute Servers tab, find the server that you want to unlock and click **Unlock NC** in the **Operation** column. ii. In the **Unlock NC** dialog box that appears, enter a reason for unlocking the server. iii. Click **OK**.
Business Launch	You can activate servers in the No Heartbeat, Mlock, Rlock, Failover, and Initializing states.	i. In the Compute Servers tab, find the server that you want to activate and click **Business Launch** in the **Operation** column. ii. In the dialog box that appears, enter a reason for activating the server, the user who performed the operation, and a ticket title in the **Reason** field. iii. Click **OK**.

4.1.1.3. Server O&M

4.1.1.3.1. Machines

4.1.1.3.1.1. View physical servers

You can view the following information about physical servers: IP address, model, vCPU (cores), memory, architecture, status, and the cluster in which the server is deployed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. In the upper-right corner of the page, view the total number of computing servers and the number of computing servers in the free, mlock, and nc_down states.
5. **Optional:**In the upper-left corner of the page, enter an IP address, hostname, or serial number and click the  icon to query the target server.

Alternatively, you can click **Advanced Search** and specify the model, data center, or rack.

6. **Optional:**Select items that you want to display in the server list.
   i. In the upper-right corner of the instance list, click the icon.
   ii. In the **Custom list item display** dialog box, select the items that you want to display in the server list.
   iii. Click **OK**.
7. In the server list, view the following information about servers: hostname, IP address, model, vCPU (cores), memory, architecture, status, cluster, data center, rack, serial number, and region.

   > **Note** For more information about the server states, see Cluster overview.

8. **Optional:**View O&M details of a physical server.
   i. Find the server you want to view and click the name in the **Hostname** column.
   ii. On the **Computing Server O&M** page, view the server information. For more information, see Server O&M details.

4.1.1.3.1.2. Server O&M details

You can view the business information, hardware information, resource information, ECS instances, performance monitoring information, alert information, control service status, machine migration tasks, and operation audit information about physical servers. You can also perform operations in different tabs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   In the **Machines** tab, view details of all physical servers.
4. Find the server you want to view and click the name in the **Hostname** column.
5. View the O&M details of the target physical server.
   The following table describes the information you can view about a physical server and the operations that you can perform.

Section or tab	Description
Business Information	View the following information about the server: business ID, IP address, hostname, status, management heartbeat, selling mode, cluster name, instance type, and operating system. Procedure: In the **Machines** tab, find the server that you want to view and click the name in the Hostname column. Then, view the server O&M details on the **Computing Server O&M** page. For more information, see **O&M details**.
Hardware Information	View the following information about the server: serial number, model, rack, CPU model, GPU, vCPU (cores), and memory.

Resource Information	View the usage of vCPU and memory of the server.
ECS Instances	◦ View the following information about the instances that are deployed on the server: occupied vCPU and memory, status, private or public IP address, bandwidth, user information, images, creation time, and whether the instance uses only ECS resources. ◦ Perform the following operations on an instance: diagnose the instance, migrate the instance, view the migration history, view audit logs, change the instance status, connect to the Virtual Network Computing (VNC) platform, and manage ISO files. For more information, see **ECS instances**.
Performance Monitoring	Specify a start time and an end time in the Date Range field and view the trend charts of the following performance metrics: CPU (%), memory (%), system load, network retransmission (%), and network traffic (MB).
Alert Information	View the following information about alerts: name, cause, details, the first and last time when the alert was reported, and the number of times that the alert was reported.
Control Service	◦ Query and view the status of the server roles. ◦ Perform the following operations to view the information about Apsara infrastructure O&M: Find the server role that you want to view and click **Apsara Infrastructure Management** in the **Operation** column. Then, view the information displayed on the page that appears.
Machine Migration Task	◦ View the following information about migration tasks: the number of migrated instances, destination physical machine, task status, migration progress, start time, update time, and the task creator. ◦ Perform the following operations to view the information about migration tasks: Find the migration task that you want to view and click the task ID in the Task ID column. Then, view the migration status, destination physical machine, migration type, and number of retries displayed on the **Migrated Instance Details** panel. **Note** ▪ Cold Migration: The instance is in the Pending state when the migration starts. ▪ Hot Migration: The instance is in the Running state when the migration starts. ◦ Perform the following operations to restart a task: If a migration task fails, click **Restart** in the **Operation** column. In the dialog box that appears, click**OK**. If you want to cancel the task, click **Cancel** in the **Operation** column. In the dialog box that appears, enter a reason for canceling the task and click **OK**.
Operation Audit	O&M operations that may introduce risks are audited. View the historical operations in the Apsara Uni-manager Operations Console, historical POP API calls, and historical server controller API calls. For information, see Audit logs.

4.1.1.3.1.3. Diagnose servers

You can view the server diagnostics on the **End-to-end diagnostics & demarcation** page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   In the **Machines** tab, view details of all physical servers.
4. Find the server that you want to diagnose and click **Diagnose** in the **Operation** column.

   > **Note** In the upper-left corner of the page, you can enter the IP address, hostname, or serial number to query the target server. Alternatively, you can click **Advanced Search** to query the target server.

5. On the **End-to-end diagnostics & demarcation** page, view the server diagnostics.

4.1.1.3.1.4. View audit logs

Server O&M operations that may introduce risks are audited. You can view the historical operations in the Apsara Uni-manager Operations Console, historical POP API calls, and historical server controller API calls.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   In the **Machines** tab, view details of all physical servers.
4. Find the server for which you want to view the audit logs and click **Audit Operations** in the **Operation** column.
5. View the information displayed on the **Audit Operations** panel that appears. For more information, see Audit logs.

4.1.1.3.1.5. Lock a server

You can lock servers based on your business requirements. You cannot create instances on locked servers.

Background information

- You can lock abnormal servers to prevent instances from being assigned to these servers.
- You can also lock servers for which you want to reserve resources.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. Find the target server and click **Lock** in the **Operation** column.
5. In the **Lock NC** dialog box, select a lock status from the drop-down list, enter a ticket title and the lock reason.

6. Click **OK**.

4.1.1.3.1.6. Unlock a server

After you unlock a server, the server is automatically activated and you can schedule instances to the server.

Background information

Only servers in the No Heartbeat, Mlock, and Rlock states can be unlocked.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. Find the target server, move the pointer over the ... icon in the **Operation** column, and click **Unlock**.
5. In the **Unlock NC** dialog box that appears, view the IP address of the server and enter the operation reason in the **Reason** field.
6. Click **OK**.

4.1.1.3.1.7. Activate a server

You can manually activate the computing server.

Background information

Only servers in the No Heartbeat, Mlock, Rlock, Failover, and Initializing states can be activated.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. Find the target server, move the pointer over the ... icon in the **Operation** column, and click **Activate**.
5. In the dialog box that appears, view the host name and enter the operation reason in the **Reason** field.
6. Click **OK**.

4.1.1.3.1.8. Migrate all instances from a server

You can migrate all the ECS instances deployed on a physical server to another server on which available resources are sufficient. After you submit a migration task, the source physical server is locked. You can manually unlock the server after the task is complete.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. Find the target server, move the pointer over the  icon in the **Operation** column, and click **Migrate All Instances**.
5. In the **Machine Migration** dialog box that appears, view the information about the source server, specify the operator, ticket title, and migration reason.
6. Click **OK**.

4.1.1.3.2. View migration tasks

After a migration task is triggered in the Apsara Uni-manager Operations Console, you can view the status and result of the migration task. You can also view details about all the instances and O&M details on the computing servers that are associated with the migration task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **ECS O&M**.
   On the **Machines** tab, view details of all physical servers.
4. Click the **Machine Migration Task** tab to view details of migration tasks.
5. View the following information about migration tasks: task ID, source physical machine, the number of instances, destination physical machine, task status, migration progress, start time, and initiator.

   > **Note** If a migration task fails, we recommend that you click **Machine Migration** again. If a migration task fails multiple times, we recommend that you perform the migration based on the KB solution or contact the Alibaba Cloud team TAM or L2.

6. **Optional:** View the migration details of all instances in a migration task.
   i. On the Machine Migration Task tab, find the target migration task and click the task ID in the **Task ID** column. Alternatively, click the number displayed in the **Instances** column to view the migration details of all instances in the migration task.
   ii. In the **Migrated Instance Details** panel, view the migration status, destination physical machine, migration type, and number of retries of all instances.
7. **Optional:** View the O&M details of the source physical machine.
   i. On the Machine Migration Task tab, find the source physical machine and click the IP address in the **Source Physical Machine** column.
   ii. On the **Computing Server O&M** page that appears, view the O&M details. For more information, see Server O&M details.

4.1.1.4. ECS O&M

4.1.1.4.1. ECS instances

An Elastic Compute Service (ECS) instance is a virtual computing environment that consists of the most basic server components, such as the CPU and memory. Users perform operations on ECS instances. This topic describes how to perform the following O&M operations on ECS instances: view instance details, diagnose instances, migrate instances, view instance migration history, change instance status, connect to VNC, and manage ISO files.

4.1.1.4.1.1. View ECS instances

You can view the list of ECS instances and the physical server and cluster to which each instance belongs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**. In the upper-right corner of the ECS instance page that appears, view the number of ECS instances that are running, stopped, being created, or being released.

   > **Note** The number of ECS instances displayed in the upper-right corner of the page may be different from that displayed in the ECS instance list due to workflow errors. The number displayed in the upper-right corner of the page prevails.

4. **Optional:**Enter the instance ID, private IP address, or public IP address in the search box to query a specific instance.
   Alternatively, click **Advanced Search**, specify Status, AliUid, or VPC to query a specific instance. You can also select **All in ECS Project** in the upper-right corner of the instance list to filter instances.
5. **Optional:**Change the columns that are displayed on the instance list.
   i. In the upper-right corner of the instance list, click the  icon.
   ii. In the **Custom list item display** dialog box, select the items that you want to display in the instance list.
   iii. Click **OK**.
6. View the values of Host, Cluster, CPU/memory, Status, Private IP/public IP address, and Bandwidth of the ECS instances.
7. View the details of an instance.
   i. On the **Instances** page, click the ID of the instance that you want to view in the **Instance ID/Name** column.
   ii. On the **Instance Details** page that appears, view the instance details. For more information, see View instance details.
8. View O&M details of a computing server.
   i. On the **Instances** page, find the server that you want to view and click the NC IP in the **Host** column.
   ii. On the **Computing Server O&M** page that appears, view the server details. For more information, see Server O&M details.
9. View O&M details of a cluster.
   i. On the **Instances** page, find the cluster that you want to view and click the cluster name

in the **Cluster** column.

ii. On the **Computing Cluster Details** page that appears, view the cluster details. For more information, see **O&M details**.

4.1.1.4.1.2. View instance details

You can view details of an ECS instance and perform operations on the instance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the Instances page, click the name of the instance that you want to view in the **Instance ID/Name** column.
5. **Optional:**In the upper-right corner of the page that appears, manage the instance. The following table describes the operations that you can perform on the instance.

Operation	Step
Migration	In the upper-right corner of the page, click**Migration**. For more information, see Migrate instances.
Log on to the cluster AG	In the upper-right corner of the page, click**Connect to AG**. For more information, see Connect to cluster AG.
Log on to VNC.	In the upper-right corner of the page, choose**More actions > Connect to VNC**. For more information, see Connect to VNC.
Change the instance status	In the upper-right corner of the page, select Start, Stop, or Restart from the **More actions** drop-down list based on your needs. For more information, see **Change the instance status**. You can also select multiple instances and change the instance status at a time in the lower part of the page.
Manage ISOs	In the upper-right corner of the page, choose**More actions > Manage ISO**. For more information, see ISO management.

6. View the instance details and perform operations based on your needs.
The following table describes the information you can view about an instance.

Section or tab	Description
Basic Information	View the following information about the instance: instance ID, instance name, specification, region, zone, creation time, AliUid, state in business, state in server controller, cluster, host ID, host name, and rack.
Configuration information	View the following information about the instance configuration: I/O optimization status, system image, OS, system disk, network type, internal bandwidth, private IP address, VPC ID, vSwitch, and NAT IP address.

Disks	◦ Displayed information: such as the cloud disk ID, disk type, status, cluster, and features. ◦ Supported operations:operation audit, snapshot creation, and snapshot viewing. For more information, see **Cloud disk**.
ENIs	◦ Displayed information: such as the ENI ID, MAC address, ENI status, ENI type, vSwitch, and IP address. ◦ Supported operation: operation audit. For more information, see .
Security Groups	◦ Displayed information: such as the security group ID, security group name, network type, VPC ID, and creation time. ◦ Supported operation: operation audit. For more information, see **Security group**.
Snapshots	◦ Displayed information: such as the snapshot ID, snapshot name, snapshot ID in server controller, snapshot type, disk ID, disk type, progress, and creation time. ◦ Supported operations: snapshot deletion and operation audit. For more information, see **Snapshot**.
Performance monitoring	View the charts that describe the instance performance during a specific period of time in the following aspects: CPU utilization, disk read/write (byte/s), disk IOPS, public bandwidth (bit/s), and internal bandwidth (bit/s).
ASO Migration Tasks	After a migration task is triggered in the Apsara Uni-manager Operations Console, view the status and result of the migration task on this tab. Displayed information: such as the source NC ID and IP address, destination NC ID and IP address, migration type (cold migration or hot migration), retry count (including the number of executed retries and the maximum number of retries allowed), migration status, start time, update time, migration reason, creator, and migration result.
Migration History	View the historical migration tasks created within the lifecycle of the ECS instance. Both cold migration and hot migration tasks are displayed. Displayed information: such as the source NC, target NC, status, migration time, end time, and migration reason.
Audit Operations	View the historical operations performed in the Apsara Uni-manager Operations Console, historical POP API calls, and historical server controller API calls for the instance. For more information, see Audit logs.
Associate Resources	View the association/topology between ECS instance resources including the VPCs, ECS virtual machine, computing servers, clusters, images, system disks, data disks, NICs, and security groups. Move the pointer over an orange icon and click **Go to Diagnostics**. View the diagnosis result on the page that appears.

4.1.1.4.1.3. Diagnose ECS instances

You can diagnose the health status of ECS instances, view the error messages of virtual machines and physical machines, and view change events about the racks, IDCs, and vSwtiches of instances.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. Find the instance that you want to diagnose and click **Diagnose** in the **Operation** column.
5. On the **End-to-end diagnostics & demarcation** page, view the server diagnostics.

4.1.1.4.1.4. Migrate instances

You can migrate instances and configure the migration parameters. Cold migration and hot migration are supported for instance migration.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. Find the instance that you want to migrate and choose **Migrate > Migrate Instance** in the **Operation** column.
5. In the **Migrate Instance** dialog box that appears, set the parameters.

> **Note** The system automatically selects a migration type based on the instance status. You can configure the parameters for the cold migration or hot migration. Cold migration indicates that the instance is in the Pending, Shutted, or StartFailure states when the migration task is created, and hot migration indicates that the instance is in the Running state when the migration task is created.

The following table describes the parameters.

Parameter	Description
Migration Rate	The migration rate. Unit: Mbit/s.
Enhanced Hot Migration Compatibility	If you enable this feature, both physical servers that support hot and cross-generation migration and those that support only basic migration are displayed.
Destination NC	◦ Random Selection: The instance is migrated to a random server in which resources are sufficient. ◦ Manually Specify: Manually specify a server to which the instance is migrated. In the Destination NC section, enter a host name, a server IP, or a server ID in the search box to query and select the target server.

Operator	The owner of the instance migration task.
Change Ticket Title	The ticket title of the instance migration task.
Reason	The reason for migrating the instance. The reason is used to facilitate troubleshooting.

6. Select **I have read the preceding notes and confirm this operation.** and click **OK**. Then, a message indicating that the operation is successful appears.

4.1.1.4.1.5. View instance migration history

You can view the historical migration tasks created within the lifecycle of an ECS instance. Both cold migration and hot migration tasks are displayed. You can view the following information about historical migration tasks: source server, destination server, instance status, the time when the migration task was created, the time when the task was complete, and migration reason.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. Find the instance for which you want to view the migration history and choose **Migrate > View Migration History** in the **Operation** column.
5. In the **Migration History** panel, view the historical migration tasks displayed on the Cold Migration and Hot Migration tabs.
   - View the following information about the cold migration tasks: source server, destination server, instance status, the time when the migration task was created, the time when the task was complete, and migration reason.
   - View the following information about the hot migration tasks: source server, destination server, instance status, the time when the migration task was created, the time when the task was updated, migration rate, and migration reason.

4.1.1.4.1.6. View audit logs

When you perform O&M operations on instances, all the operations that may introduce risks are audited. You can view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls about instances.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. Find the instance for which you want to view audit logs and click **Audit Operations** in the **Operation** column.
5. In the **Audit Operations** panel that appears, view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls. For more information, see Audit logs.

4.1.1.4.1.7. Change the instance status

Start instances

You can start instances that are in the Pending, Shutted, and StartFailure states.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the page that appears, find the instance that you want to manage and move the pointer over the icon in the **Operation** column. Then, select **Start** from the drop-down list.

   You can also select multiple instances and click **Start** in the lower part of the page. This way, multiple instances are started at a time.
5. In the dialog box that appears, enter a reason for the start operation in the **Reason** field.
6. Click **OK**.

Stop instances

You can stop instances that are in the Running state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the page that appears, find the instance that you want to manage and move the pointer over the icon in the **Operation** column. Then, select **Stop** from the drop-down list.

   You can also select multiple instances and click **Stop** in the lower part of the page. This way, multiple instances are stopped at a time.
5. In the dialog box that appears, enter a reason for the stop operation in the **Reason** field.
6. Click **OK**.

Restart instances

You can restart instances that are in the Running state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the page that appears, find the instance that you want to manage and move the pointer over the icon in the **Operation** column. Then, select **Restart** from the drop-down list.

   You can also select multiple instances and click **Restart** in the lower part of the page. This way, multiple instances are restarted at a time.
5. In the dialog box that appears, select a restart mode and enter a reason for the restart operation.

6. Click **OK**.

4.1.1.4.1.8. Connect to VNC

You can connect to the VNC platform to remotely log on to your instance and perform operations.

Prerequisites

The instance for which you want to connect to VNC is in the Running state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the page that appears, find the instance to which you want to log on and move the pointer over the  icon in the **Operation** column. Then, select **Connect to VNC** from the drop-down list.
5. In the dialog box that appears, enter a reason for connecting to the VNC platform and click **OK**. Then, you are redirected to another page.
6. On the page that appears, specify the operation that you want to perform in the CLI.

4.1.1.4.1.9. ISO management

You can mount an ISO to or unmount an ISO from an instance. After you mount an ISO to an instance, the system enters the rescue mode and performs operations on the instance. ISOs can be mounted to or uninstall from instances that are in the Stopped state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ECS Instances**.
4. On the page that appears, find the instance that you want to manage and move the pointer over the  icon in the **Operation** column. Then, select **Manage ISO** from the drop-down list.
5. Manage ISOs in the **Manage ISO** dialog box that appears.
   - Mount ISO:
     a. In the **Available ISOs** list, find the ISO that you want to mount and click **Mount** in the **Operation** column.
     b. In the dialog box that appears, enter the operator name, ticket title, and reason for the operation.
     c. Click **OK**. The system displays the mounted ISO in the **Mounted ISOs** list.
   - Uninstall ISO
     a. In the **Mounted ISOs** list, find the ISO that you want to uninstall and click **Uninstall** in the **Operation** column.

b. In the dialog box that appears, enter the operator name, ticket title, and reason for the operation.
c. Click **OK**. The uninstalled ISO is displayed in the **Available ISOs** list.

4.1.1.4.2. Cloud disk

You can attach disks to ECS instances to increase the storage space of instances. This topic describes how to query and view disk details, detach disks from instances, view operation audit logs, and create and view snapshots.

4.1.1.4.2.1. View disks

You can view the following information about disks: basic information, ECS instances attached to the disk, O&M details of computing clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Disk**.
4. In the upper part of the page, specify the disk information and click **Search** to query the target disk.
   In the upper-right corner of the page, select **Tiangong Resources Only** to filter disks.
5. View the following information about the disk: disk ID and name, disk type, capacity, ECS instances attached to the disk, mount point, the cluster on which the disk is deployed, disk status, storage type, Houyi disk ID, AliUID, and the time when the disk was created.

   > **Note**
   > - Supported disk types: system disk and data disk
   > - Supported storage types: local disk, local SSD, basic disk, standard SSD, preconfigured SSD, ultra disk, enhanced SSD, premium performance disk, and standard performance disk

6. Find the disk that you want to view and click the disk ID in the **Disk ID/Name** column to view the disk information on the **Details** page that appears. For more information, see View disk details.
7. Find the instance that you want to view and click the instance ID in the **ECS Instance** column to view the instance details on the **Instance Details** page that appears. For more information, see View instance details.
8. Find the cluster that you want to view and click the cluster name in the **Cluster** column to view the cluster information on the **Computing Cluster Details** page that appears. For more information, see **O&M details**.

4.1.1.4.2.2. View disk details

You can view the basic information and snapshot information of disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.

3. In the left-side navigation pane, choose **ECS O&M > Disk**.
4. Find the disk that you want to view and click the disk ID in the **Disk ID/Name** column.
5. View the basic information and snapshot information about the disk.
   - View the following basic information about the disk: disk ID, disk ID in server controller, disk name, disk type, storage type, capacity, mount point, the time when the disk was created, attached, detached, and modified, the region in which the disk is deployed, zone, cluster, and AliUID.
   - Snapshot Information: the ID of the automatic snapshot policy.

4.1.1.4.2.3. View audit logs

You can query and view the historical operations performed on disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Disk**.
4. Find the disk that you want to view and click **Audit Operations** in the **Operation** column.
5. In the **Audit Operations** panel that appears, view the historical operations in the Apsara Uni-manager Operations Console, historical POP API calls, and historical server controller API calls. For more information, see Audit logs.

4.1.1.4.2.4. Create snapshots

You can manually create snapshots to back up data.

Prerequisites

- You can create snapshots only for disks that are attached to instances in the Stopped or Running states. You cannot create snapshots for disks attached to instances that have not been started.
- If you create a snapshot for a new system disk or a new data disk created from another snapshot, an error returns because the disk has not finished loading data. In most cases, you can create snapshots for a system disk one hour after the disk is created. After a data disk is added, you must wait for a period of time before you can create snapshots for the disk. The amount of waiting time varies based on the amount of disk data.
- Snapshots cannot be created for a newly added disk if the instance to which the disk is attached has not been started.
- If the creation progress has not reached 100%, the snapshot is being created. You cannot create another snapshot when a snapshot is being created for the disk.
- The maximum number of snapshots you can create varies based on the total number of disks owned by your account. The maximum number of snapshots you can create = The number of disks × 6 + 6.
- Snapshots can be created for a disk only after the instance to which the disk is attached has been started.
- An error returns if you create a snapshot for an independent basic disk that has never been attached to an instance.

Background information

You can use snapshots to back up data, restore ECS instances that were accidentally released, and create custom images. You can create snapshots of disks to improve fault tolerance before you roll back a disk, modify key system files, or change the operating system of an instance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Disk**.
4. Find the disk for which you want to create snapshots and click **Create Snapshot** in the **Operation** column.
5. In the **Create Snapshot** dialog box, enter the snapshot name, snapshot description, and the reason for creating a snapshot.

   The following table describes the parameters.

Parameter	Description
Snapshot Name	The snapshot name must meet the following requirements: ◦ The name must be 2 to 128 characters in length. ◦ The name must start with a letter but cannot start with http:// or https://. ◦ The name can contain letters, digits, colons (:), underscores (_), and hyphens (-). ◦ The name cannot start with auto because snapshots whose names start with auto are recognized as automatic snapshots.
Snapshot Description	The snapshot description must meet the following requirements: ◦ The description can be up to 256 characters in length. You can leave this field empty. This field is empty by default. ◦ The description cannot start with http:// or https://.
Reason	The reason for creating the snapshot. This reason is used when audit logs are generated to facilitate troubleshooting.

6. Click **OK**.

4.1.1.4.2.5. View snapshots

You can view the snapshots of disks, manage snapshots, and view automatic snapshot policies. For more information, see **ECS O&M > Snapshots**.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Disk**.
4. Find the disk that you want to view and click **View Snapshots** in the **Operation** column. For more information, see **Snapshots**.

4.1.1.4.3. Image

An image is a template for running environments within ECS instances. An image includes an operating system and pre-installed applications.

An image works as a copy that stores data from one or more disks. An image may store data from a system disk or from both system and data disks. You can use an image to create an ECS instance or replace the system disk of an ECS instance.

4.1.1.4.3.1. Manage images

You can view the following information about images: operating system, capacity, status, type, and the region in which the image is deployed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Image**.
   By default, the **Image Management** tab appears.
4. In the upper part of the page, enter an image ID, select an AliUID from the AliUid drop-down list, and click **Search**.
5. View the following information about images: operating system, capacity, status, type, and the region in which the image is deployed.

4.1.1.4.3.2. View ISO details

You can view the operating system types of ISO files and whether the files can be mounted.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Images**.
   By default, the **Image Management** tab appears.
4. Click the **ISO Management** tab.
5. In the upper-left corner of the ISO Management tab, enter the name of the ISO file and click the  icon to query the file.
6. View the operating system type of the ISO file.

4.1.1.4.4. Snapshots

You can use snapshots to back up data, restore ECS instances that were accidentally released, and create custom images. You can create snapshots of disks to improve fault tolerance before you roll back a disk, modify key system files, or change the operating system of an instance.

4.1.1.4.4.1. Manage snapshots

You can view and delete snapshots, view operation audit logs, and create images.

View snapshots

You can query and view information about snapshots.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Snapshots**.
   By default, the **Snapshots** tab is displayed.
4. Select an AliUID from the **AliUid** drop down list, specify the **Snapshot ID**, **Disk ID**, and **Instance ID** fields based on your needs, and click **Search**.

   > **Note** Only AliUid is required.

5. View the following information about the snapshots: snapshot ID and name, snapshot ID in server controller, snapshot type, disk ID and type, snapshot creation progress, region, creation time, and modification time.

   > **Note** The supported snapshot types include system snapshot, user snapshot, scheduled snapshot, and snapshot copy.

6. Find the disk you want to view and click the disk ID in the **Disk ID/Type** column. Then, view the information displayed on the **Details** page. For more information, see View disk details.

Delete snapshots

You can delete snapshots that are no longer used.

Prerequisites

If a snapshot has been used to create custom images, you must delete those custom images before the snapshot can be deleted.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Snapshots**.
   By default, the **Snapshots** tab is displayed.
4. Select an AliUID from the **AliUid** drop-down list, specify the **Snapshot ID**, **Disk ID**, and **Instance ID** fields based on your needs, and click **Search**.

   > **Note** Only AliUid is required.

5. Find the snapshot that you want to delete and click **Delete** in the **Operation** column.
6. In the dialog box that appears, enter a reason and click **OK**.

View audit logs

You can view audit logs of snapshots in the Compute Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations**

Console.

3. In the left-side navigation pane, choose **ECS O&M > Snapshots**.
   By default, the **Snapshots** tab is displayed.
4. Select an AliUID from the **AliUid** drop-down list, specify the **Snapshot ID**, **Disk ID**, and **Instance ID** fields based on your needs, and click **Search**.

   > **Note** Only AliUid is required.

5. Find the snapshot for which you want to view the audit logs and click **Audit Operations** in the **Operation** column.
6. In the **Audit Operations** panel that appears, view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls. For more information, see Audit logs.

Create an image

You can create a custom image and use it to create identical instances or replace the system disks of existing instances. This way, you can configure many instances that have identical operating systems and data environments.

Prerequisites

- The progress of the snapshot is 100%.
- The disk of the snapshot is a system disk.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Snapshots**.
   By default, the **Snapshots** tab is displayed.
4. Select an AliUID from the **AliUid** drop-down list, specify the **Snapshot ID**, **Disk ID**, and **Instance ID** fields based on your needs, and click **Search**.

   > **Note** Only AliUid is required.

5. Find the snapshot for which you want to create an image and click **Create Image** in the **Operation** column.
6. In the **Create Image** dialog box, configure the parameters.
   The following table describes the parameters.

Parameter	Description
Image Name	The image name must meet the following requirements: ◦ The name must be 2 to 128 characters in length. ◦ It must start with a letter but cannot start with http:// or https://.
Public Image	If you select Yes, the image you create can be used by other users. Default value: No.

Image Description	The description must meet the following requirements: ◦ The description can be up to 256 characters in length. You can leave this field empty. This field is empty by default. ◦ The description cannot start with http:// or https://.
Reason	The reason for creating the image. This reason is used when audit logs are generated to facilitate troubleshooting.

7. Click **OK**.

4.1.1.4.4.2. Automatic snapshot policy

Automatic snapshot policies can be applied to system disks and data disks to create periodical snapshots of the disks. You can view the IDs and names of automatic snapshot policies and the number of associated disks.

Background information

Automatic snapshot policies can effectively avoid following risks associated with manual snapshots:

- When applications such as personal websites or databases deployed on an ECS instance encounter attacks or system vulnerabilities, you may be unable to manually create snapshots. In this case, you can use the latest automatic snapshots to roll back the affected disks to restore your data and reduce loss.
- You can also specify an automatic snapshot policy to create snapshots before regular system maintenance tasks are performed. This frees you from manually creating snapshots and ensures that snapshots are always created before maintenance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Snapshots**.
   By default, the **Snapshots** tab is displayed.
4. In the upper part of the page, click the **Automatic Snapshot Policies** tab.
5. In the **Automatic Snapshot Policies** list, view the IDs and names of automatic snapshot policies and the number of associated disks.

4.1.1.4.5. ENIs

You can unbind and release elastic network interfaces (ENIs), and view the audit logs of the preceding operations.

An ENI is a virtual network interface controller (NIC) that can be bound to an ECS instance of the Virtual Private Cloud (VPC) type. You can use ENIs to deploy high availability clusters and perform low-cost failover and fine-grained network management.

4.1.1.4.5.1. View ENIs

You can view the basic information about ENIs in the Compute Operations Console.

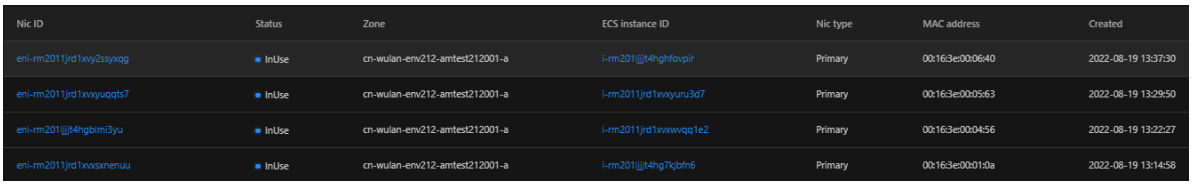
Procedure

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

2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ENIs**.
4. In the upper part of the page, select an AliUID from the **AliUid** drop down list, fill in the **ENI ID**, **VPC**, **Instance ID**, and **Private IP Address** fields, and then click **Search**.

   > **Note** Only AliUid is required.

5. View the information about the ENIs.



6. **Optional:**Find the ENI you want to view and click the ENI ID in the **ENI ID** column to view the ENI information on the **ENI Details** page that appears. For more information, see View ENI details.
7. **Optional:**Find the instance you want to view and click the instance ID in the **Instance ID** column to view the instance details on the **Instance Details** page that appears. For more information, see View instance details.

4.1.1.4.5.2. View ENI details

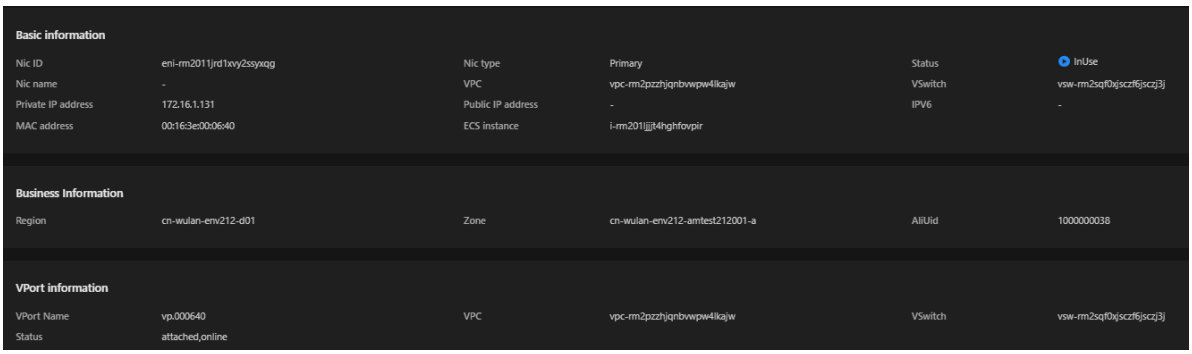
You can view the basic information, business information, and VPort information of ENIs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ENIs**.
4. In the upper part of the page, select an AliUID from the **AliUid** drop down list, fill in the **ENI ID**, **VPC**, **Instance ID**, and **Private IP Address** fields, and then click **Search**.

   > **Note** Only AliUid is required.

5. Find the ENI you want to view and click the ENI ID in the **ENI ID** column.
6. On the **ENI Details** page, view the basic information, business information, and VPort information of ENIs.



7. **Optional:**View the information displayed in the **Security Group** section. For more information, see **Security Groups**.

4.1.1.4.5.3. View audit logs

You can view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls about ENIs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > ENIs**.
4. In the upper part of the page, select an AliUID from the **AliUid** drop down list, fill in the **ENI ID**, **VPC**, **Instance ID**, and **Private IP Address** fields, and then click **Search**.

   > **Note** Only AliUid is required.

5. Find the ENI for which you want to view the audit logs and click **Audit Operations** in the **Operation** column.
6. In the **Audit Operations** panel that appears, view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls. For more information, see Audit logs.

4.1.1.4.6. Security group

You can view security groups, query security group information, rules, and instances, and view the audit logs of the preceding operations.

A security group acts as a virtual firewall to control the inbound and outbound traffic of ECS instances to improve security. Security groups provide Stateful Packet Inspection (SPI) and packet filtering capabilities. You can use security groups and security group rules to define security domains in the cloud.

4.1.1.4.6.1. View security groups

In the Compute Operations Console, you can view information about security groups, including the region, network type, VPC ID, associated instance, and creation time.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Security Groups**.
4. **Optional:**On the page that appears, select an UID from the AliUid drop-down list, specify the security group ID and the ECS instance ID, and then click **Search**.
5. View the basic information about the security group.
6. **Optional:**Find the security group that you want to view and click the group name in the **Security group ID/Name** column. Then, view the security group details on the page that appears. For more information, see View security group details.

4.1.1.4.6.2. View security group details

You can view the basic information about security groups, the inbound and outbound access rules of security groups, and the details of the ECS instances associated with the security groups.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Security Groups**.
4. **Optional:**On the page that appears, select an UID from the AliUid drop-down list, specify the security group ID and the ECS instance ID, and then click **Search**.
5. On the Security Groups page, find the security group you want to view and click the ID of the security group in the **Security Group ID/Name** column.
6. On the **Security Group Details** page, view the following information:
   - In the **Basic Information** section, view the basic information about the security group including the security group ID, VPC, description, creation time, and modification time.
   - In the **Rules** tab, view the **Inbound** and **Outbound** access rules of the security group.

     The following table describes the parameters.

Parameter	Description
Direction	▪ **Outbound**: access from the ECS instances in the current security group to other ECS instances on the internal network or to resources on the Internet. ▪ **Inbound**: access from other ECS instances on the internal network or from resources on the Internet to the ECS instances in the current security group.
Action	▪ **Allow**: allows access requests that are sent to specified ports. ▪ **Deny** :denies access requests and drops data packets without returning a response. If two security group rules use the same settings except for the action, the **Deny** action takes precedence over the **Allow** action.
NIC Type	Valid value: intranet. No public NICs are available for ECS instances that are deployed in VPCs. You can only add internal security group rules. However, the added security group rules apply to both the Internet and the internal network.

Protocol Type	The protocol type of the security group rule. Valid values: ▪ **All**: This value can be used in scenarios in which requests are sent from trusted sources. ▪ **TCP**: This value can be used to allow or deny traffic on one or more consecutive ports. ▪ **UDP**: This value can be used to allow or deny traffic on one or more consecutive ports. ▪ **ICMP**: This value can be used when the `ping` command is used to test the status of network connection between instances. ▪ **ICMPv6**: This value can be used when the `ping6` command is used to test the status of network connection between instances. ▪ **GRE**: This value can be used for VPN.
Authorized Object	Authorization objects vary based on the authorization type.
Port Range	The port range varies based on the protocol type. ▪ If you set Protocol Type to **All**, the value **-1/-1** is displayed, which indicates all ports. ▪ If you set Protocol Type to **TCP**, you can specify a port range in the <start port>/<end port> format. Valid values: 1 to 65535. For example, 80/80 indicates port 80, and 1/22 indicates ports 1 to 22. ▪ If you set Protocol Type to **UDP**, you can specify a port range in the <start port>/<end port> format. Valid values: 1 to 65535. For example, 80/80 indicates port 80, and 1/22 indicates ports 1 to 22. ▪ If you set Protocol Type to **ICMP**, the value **-1/-1** is displayed, which indicates all ports. ▪ If you set Protocol Type to **ICMPv6**, the value **-1/-1** is displayed, which indicates all ports. ▪ If you set Protocol Type to **GRE**, the value **-1/-1** is displayed, which indicates all ports.
Priority	Valid values: 1 to 100. The default value is 1, which indicates the highest priority.
Description	The description of the security group rule. To simplify future management operations, we recommend that you provide a specific description. The description must be 1 to 512 characters in length.

- On the **Instances** tab, view the list of ECS instances associated with the security group. For more information, see View ECS instances.

4.1.1.4.6.3. View audit logs

You can view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls about ENIs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Security Groups**.

4. **Optional:**On the page that appears, select an UID from the AliUid drop-down list, specify the security group ID and the ECS instance ID, and then click **Search**.
5. Find the security group for which you want to view the audit logs and click **Audit Operations** in the **Operation** column.
6. In the **Audit Operations** panel that appears, view the operations in the Apsara Uni-manager Operations Console, POP API calls, and server controller API calls. For more information, see Audit logs.

4.1.1.4.7. Manage instance specifications

You can add, modify, and delete instance specifications and view audit logs of the preceding operations.

ECS instance specifications define the basic attributes of instances, such as the number of vCPUs, memory size, network capabilities, and storage capabilities. Network capabilities include the network bandwidth, packet forwarding rate, maximum number of elastic network interfaces (ENIs) per instance, and maximum number of IP addresses per ENI. Storage capabilities include the maximum disk bandwidth, maximum disk IOPS, and maximum number of attached disks per instance. The network and storage performance of instances within the same instance family depend on their computing capacities. The larger computing capacity the instances have, the higher network and storage performance the instances can deliver.

4.1.1.4.7.1. View instance specifications

You can view all custom instance specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Custom Specifications**.
4. **Optional:**In the upper-left corner of the page that appears, enter an instance type name in the search box and click the  icon to query the instance specifications.
5. View the following information about the instances: instance family, instance type, vCPU (cores), memory (GB), baseline bandwidth, packet forwarding rate (Kpps), and the number of ENIs bound to the instance.

4.1.1.4.7.2. Add an instance specification

If the existing ECS instance specifications cannot meet your business requirements, you can add custom instance specifications. Then, you can create instances of the custom specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Custom Specifications**.
4. In the upper-left corner of the page, click **Add**.
5. In the **Add Custom Instance Type** dialog box, set the parameters.

The following table describes the parameters.

Parameter	Description
Instance Family	**ecs.anyshare** indicates the custom instance specification.
Instance Type Name	Required. The instance type name consists of the instance family and a custom value. The custom value cannot contain Chinese characters.
vCPU(C)	Required. The number of vCPUs. You can specify this value in the vCPU(C) field.
mem(GB)	Required. After you specify the number of vCPUs, the minimum memory allowed is displayed in the mem(GB) field. You can enter a value or click the arrows to specify a value greater than the minimum value.
Baseline Bandwidth	This value is automatically calculated and generated by the system.
Packet Forwarding Rate (× 10,000 PPS)	This value is automatically calculated and generated by the system.
NIC Multi-queue	This value is automatically calculated and generated by the system.
ENIs	This value is automatically calculated and generated by the system.
Instance Type	Default value: ecs-4.
Exclusive or Shared	Required. Valid value: Shared.

The following table describes how the parameters are calculated for a custom instance specification.

Instance family	vCPU (cores)	Memory (GB)	Baseline bandwidth (Gbit/s)	Packet forwarding rate (bidirectional, Kpps)	NIC queues	ENIs (including a primary ENI)
Custom instance specification **ecs.anyshare**	0<x<=2	1~16	0.5	10	1	2
	2<x<=4	2~32	0.8	10+(x-2)/0.2	1	2
	4<x<=8	4~64	0.8+(x-5)/4	20+(x-4)/0.2	1	3
	8<x<=12	8~96	1.5+(x-8)/8	40+(x-8)/0.8	2	3
	12<x<=16	12~128	2+(x-12)/4	45+(x-12)/0.8	3	4
	16<x<=24	16~196	3+(x-16)/8	50+(x-16)/0.8	3	5

	24<x<=32	24~256	4+(x-24)/8	60+(x-24)/0.4	4	6
	32<x<=64	32~352	min(5+(x-32)/8, 10)	min(80+(x-32)/0.8, 120)	4	8

6. Enter the operation reason and click **OK**.

> **Note** The creation does not take effect immediately. You need to wait until the system synchronizes the operation.

4.1.1.4.7.3. Modify instance specifications

You can modify only the custom instance specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Custom Specifications**.
4. Find the custom instance specification that you want to modify and click **Modify** in the **Operation** column.
5. In the **Modify Custom Instance Type** dialog box, set the parameters. For more information, see Add an instance specification.
6. Enter the operation reason and click **OK**.

> **Note** The modifications on the custom instance specification does not take effect immediately. You need to wait until the system synchronizes the operation.

4.1.1.4.7.4. Delete an instance specification

You can delete custom instance specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Custom Specifications**.
4. Find the custom instance specification that you want to delete and click **Delete** in the **Operation** column.
5. In the dialog box that appears, enter the reason and click **Delete**.

> **Note** The deletion does not take effect immediately. You need to wait until the system synchronizes the operation.

4.1.1.4.7.5. View audit logs

You can view the historical operations performed in the Apsara Uni-manager Operations Console and historical POP API calls for the custom instance specification.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **ECS O&M > Custom Specifications**.
4. Find the custom instance specification that you want to view and click **Operations** in the **Operation** column.
5. In the **View Operations** panel, view the historical operations performed in the Apsara Uni-manager Operations Console and historical POP API calls. For more information, see Audit logs.

4.1.1.5. Log management

4.1.1.5.1. Audit logs

In the Compute Operations Console, you can view the historical operations performed on resources, historical POP API calls, and historical API calls in server controller. This way, operations in the console are traceable and you can view the high-risk operations.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **Logs > Audit Logs**.
   Then, the **ASO Operation History** tab is displayed.
4. View the information displayed on each tab. The following table describes the information that you can view on each tab.

Tab name	Description
ASO Operation History	In the upper part of the tab, you can perform the following operations to search for specific resources: enter the resource information in the **Resource** field or specify a time range in the Time Range field, and click **Search**. View the following operation information: operation, start time, request result, error message, request ID, request parameters, and operator.
POP API Call History	In the upper part of the tab, you can perform the following operations to search for specific calls: enter keywords in the **Keywords** field or specify a time range in the Time Range field, and click **Search**. View the following information about calls: operation, start time, request ID, HTTP status code, error message, product name, request parameters, and caller.

API Call History in Server Controller	In the upper part of the tab, you can perform the following operations to search for specific calls: enter the operation name, request ID, or request IP address in the **Keyword** field or specify a time range in the Time Range field, and click **Search**. View the following information about calls: operation name, request ID, start time, response code, request IP address, request duration, and request parameters.

4.1.1.5.2. Query logs

You can query logs of all the ECS-related applications to quickly locate errors.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, choose **Logs > Log Query**.
4. On the page that appears, enter the request ID in the **Search Condition** field, specify a time range in the Time field, and click **Search**.
5. In the left-side navigation pane, click the name of the operation for which you want to view logs. Then, view the logs displayed on the right side.

4.1.1.6. Control and monitoring

You can view the server management information including database status, execution status of scheduled tasks, abnormal workflows, and the workflow queue in the Compute Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Control and Monitoring**.
4. View the information displayed in each section or on each tab.
   - In the **RDS Instances** section, view the following information about the managed databases: CPU utilization, connections (the percentage of real-time connections to the maximum number of connections allowed), and disk usage. Find the database that you want to view and click the database name in the **Database Instance** column. Then, you are redirected to the **ApsaraDB Operations and Maintenance System**.
   - In the **Scheduled Tasks** section, view the execution status of the scheduled tasks.

     View the execution status of scheduled tasks including the task name, task status, the last time when the task is triggered, and task description.
   - In the **Abnormal Workflow** section, view the abnormal workflows and perform retry operations.
     - View the workflow ID, workflow name, request ID, AliUid, instance ID, workflow start time and end time, and the node on which the workflow is executed.

- View the details of an exceptional workflow.
  a. Find the workflow that you want to view and click **Details** in the **Operation** column. Alternatively, you can click the ID of the workflow that you want to view in the **Workflow ID** column.
  b. In the **Activity Details** panel, view the ID, name, status, start time, and end time of the workflow activities.
  c. Find the ID of the activity that you want to view and click **Add Input** in the **Operation** column. In the **Workflow Input** dialog box, view the input information.
  d. Find the ID of the activity that you want to view and click **Add Output** in the **Operation** column. In the **Workflow Output** dialog box, view the output information.
  e. Find the ID of the activity that you want to view and click **Add Error** in the **Operation** column. In the **Workflow Error** dialog box, view the error message.
- Retry an abnormal workflow
  a. On the Abnormal Workflow tab, find the workflow that you want to retry and click **Retry** in the **Operation** column.
  b. In the dialog box that appears, click **OK**.

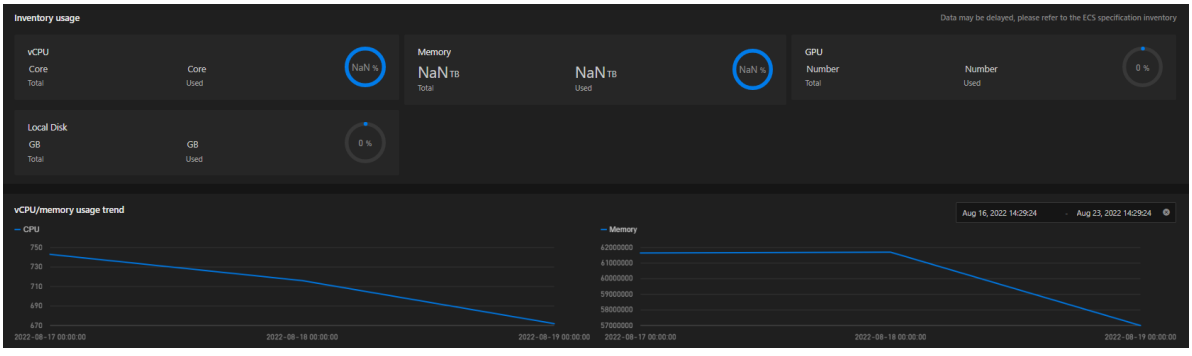
- On the **Workflows** tab, view the workflow name, request ID, AliUid, status, creation time, update time, and the node on which the workflow is executed.

4.1.1.7. Inventory analysis

You can query the ECS instance inventory in the Compute Operations Console. This way, you can view the usage of ECS instances in different specifications.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Computing > Compute Operations Console**.
3. In the left-side navigation pane, click **Compute Capacity Analytics**.
4. On the page that appears, view the information displayed in each section. The following image provides an example.



- In the **Usage** section, view the total and used resources including vCPU, memory, GPU, and local disk usage.
- In the **vCPU/Memory Usage Trend** section, specify a time range in the upper right corner to view the usage trends of vCPU and memory in the specified period of time.

> **Note** Move the pointer over a data point on a line chart to view the resource usage details on a specific day.

- In the **Inventory** section, select a cluster from the drop-down list in the upper left corner, enter an instance family in the search box, and click the icon to view the inventory information.

4.2. Network operations

4.2.1. Network service diagnosis

The network service diagnosis feature allows you to analyze the running status of network instances with a few clicks. The diagnosis feature of forwarding paths is provided to facilitate fault analysis.

4.2.1.1. Network instance diagnosis

The network instance diagnosis feature allows you to analyze the running status of network instances with a few clicks.

This feature helps you analyze DNS or SLB instances to determine whether they have unexpected running states. Visualized and automated diagnosis capabilities are provided. This feature can improve the O&M efficiency of network O&M engineers, reduce O&M risks, and improve the quality of Apsara Stack network O&M.

4.2.1.1.1. View the diagnostic information of an instance

You can view the diagnostic information of historical instances.

Background information

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
   The **Network instance diagnosis** page appears. The list of diagnostic tasks is displayed on this page.
3. **Optional:**You can select a time range and view the diagnostic task information in the specified time range.
4. Find the desired diagnostic task and click **Details** in the **Operation** column to view the diagnostic result (only for SLB instance diagnosis), including the instance details, topology, and diagnostic details.

4.2.1.1.2. Diagnose an SLB instance

You can diagnose Server Load Balancer (SLB) instances based on your business requirements.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

- When you diagnose an SLB instance, you can enter the SLB instance ID or virtual IP address (VIP). Only VIPs in classic networks are supported.
- After a diagnostic task is started, it does not stop until the diagnosis is complete. You cannot pause or terminate the task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
   The **Network instance diagnosis** page appears.
3. Select **SLB** as the diagnosis type from the drop-down list, enter the SLB instance ID or VIP, and click **Diagnose now**. The diagnosis result page appears.

   > **Note** In the field at the top of the diagnosis result page, the ID of the diagnosed instance is displayed. You can also enter the ID of another instance and click **Diagnose** to perform another diagnosis.

4. On the diagnosis result page, view the instance details, instance topology, and diagnostic details:
   - Instance topology

   > **Note**
   > - In the topology example shown in the preceding figure, the first column displays the SLB instance, the second column displays the listener instances that correspond to the SLB instance, and the third column displays the backend servers that correspond to the listener instances.
   > - If the backend servers are of the ECS type or the machine type of Apsara Infrastructure Management, click **realServer** in the topology. A panel appears to show the server details.
   > - After you select the topology, you can drag the topology and change the position of the topology.

- The diagnosis details include the name and description of each diagnostic item, diagnosis results, and detailed diagnosis information returned by the system.

4.2.1.1.3. Diagnose DNS instances

You can diagnose DNS instances based on your business requirements.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

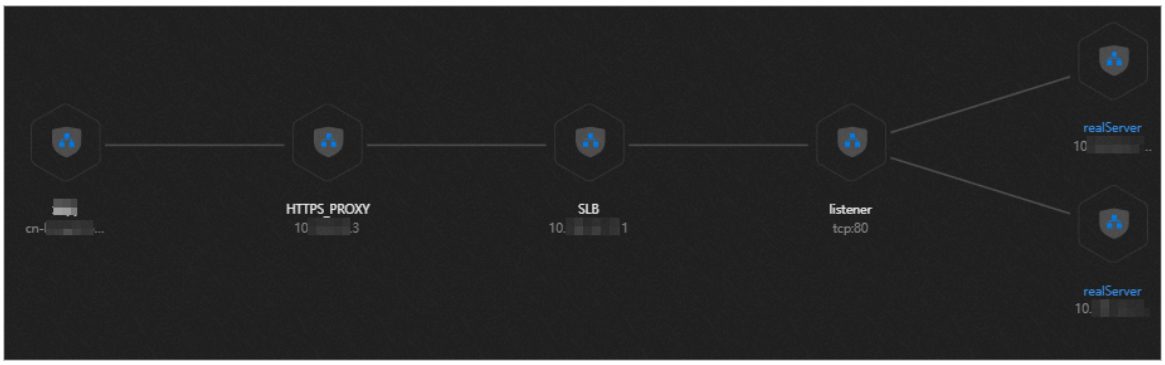
- DNS instance diagnostics are valid only for domain names.
- After a diagnostic task is started, it does not stop until the diagnosis is complete. You cannot pause or terminate the task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
   By default, the **Network instance diagnosis** page appears.
3. Select **DNS** as the diagnosis type from the drop-down list, enter the DNS domain name, and click **Diagnose now**. The diagnosis result page appears.

   > **Note** In the field at the top of the Diagnostic Results page, the ID of the currently diagnosed instance is displayed. You can also enter the ID of another instance and click **Diagnose** to perform another diagnosis.

4. On the diagnosis result page, view the instance topology, and diagnostic details:
   - Instance topology



> **Note**
>
> - In the topology shown in the preceding figure, the first column displays the domain name of the DNS instance, the second column displays the HTTPS proxy that corresponds to the DNS instance domain name resolution, the third column displays the SLB instance, the fourth column displays the listener instance that corresponds to the SLB instance, and the fifth column displays the backend servers that corresponds to the listener instance.
> - If the backend server is of the ECS type or the machine type of Apsara Infrastructure Management, click **realServer** in the topology. A panel appears to show the server details.
> - After you select the topology, you can drag the topology and change the position of the entire topology.

- The diagnosis details include the name and description of each diagnostic item, diagnosis results, and detailed diagnosis information returned by the system.

4.2.1.2. Intelligent path analysis

The intelligent path analysis and forwarding feature provides path diagnosis capabilities. This feature allows you to establish IP paths and start end-to-end path analysis in an efficient manner, and facilitates fault analysis

4.2.1.2.1. View analysis details

You can view the details of a completed intelligent path analysis.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. Click **Intelligent Path Analysis**.
4. **Optional:**You can select a time range to view the information about the intelligent path analysis task within the specified time range.
5. Find the desired analysis task and click **Details** in the **Operation** column to view the analysis results, including the results of path analysis, diagnosis details, and analysis results of each item.

4.2.1.2.2. Create an analysis task

You can create an intelligent path analysis task based on your business requirements.

Prerequisites

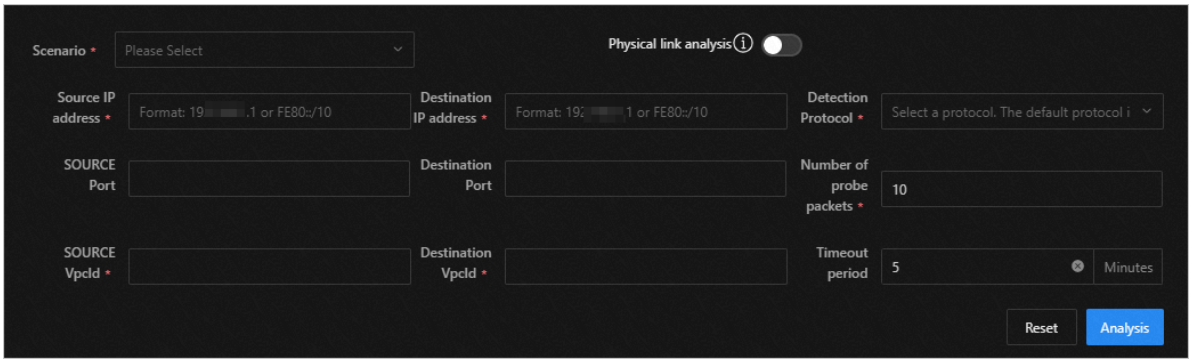
The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

- Intelligent path analysis supports the following scenarios: Mutual access between ECS instances, ECS access server load balancer, ECS access AnyTunnel, and ECS access SingleTunnel.
- The states of a path analysis task include: **Waiting**, **Configuring**, **Running**, **Analyzing**, **Completed**, **Canceling**, and **Canceled**. The following states indicate that the task is normal: **Waiting**, **Configuring**, **Running**, **Analyzing**, and **Completed**.
- The packets in the path can be captured only when the task is in the **Running** state. In other states, the packets in the path do not affect the task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. Click **Intelligent Path Analysis**.
4. Click **Create Path Analysis**. In the upper part of the page, configure the parameters and click **Analysis**.



Parameter	Description	Example
Scenario	Required. The scenario of path analysis.	Mutual access between ECS instances
Source IP address	Required. The IP address of the source node.	172.X.X.1
Destination IP address	Required. The IP address of the destination node.	172.X.X.2
Detection Protocol	Required. The protocol type of the detection packets for the path analysis.	TCP
Source Port	Optional. The port of the source node. If you leave this parameter empty, all ports are used.	80
Destination Port	Optional. The port of the destination node. If you leave this parameter empty, all ports are used.	8080
Number of probe packets	Required. The total number of detection packets for path analysis.	5

Source VpcId	Required. The ID of the VPC in which the source node resides.	vpc-**fczvaczv
Destination VpcId	Required. The ID of the VPC in which the destination node resides.	vpc-**fczvaczv
Timeout period	Optional. When the total time of packet capture in the analysis task exceeds this period, the packet capture stops. Unit: minutes.	5

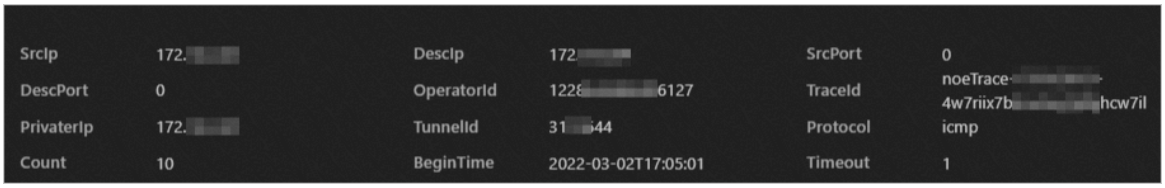
> **Note** If you turn off **Physical link analysis**, the analysis time is shortened. However, the packet capture data of the physical devices is not contained.

- In the **Path Analysis** section, the status timeline of the analysis task is displayed, and the estimated time required for each phase is displayed. The topology of the path is displayed at the bottom of the timeline.

  After the analysis is complete, the analysis result is displayed.

> **Note**
> - For path nodes of the ECS type or NC type, you can click the blue link in the topology to open the details page.
> - After you select the topology, you can drag the topology and change the location of the topology.

- In the **Diagnostic Details** section, the details of the task are displayed.



- In the **Analysis of Each Packet** section, if the analysis task is successfully executed, the analysis details of the packets captured by the task are displayed. You can view the analysis details of packets one by one.

4.2.1.2.3. Terminate an analysis task

You can terminate an analysis task that is in the **Waiting**, **Configuring**, **Running**, **Analyzing**, or **Canceling** state. After the task is terminated, the status of the task changes to **Canceled**.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. Click **Intelligent Path Analysis**.
4. Find the task that you want to terminate and click **Terminate** in the **Operation** column.

4.2.1.3. Monitoring rule management

You can associate the monitoring metrics of a monitored instance with an alert template. When the monitoring metrics meet the conditions set in the alert template, an alert event is triggered.

4.2.1.3.1. View monitoring rules

You can view the created monitoring rules.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
   By default, the created monitoring rules are displayed on the page.
4. Click the name of a monitoring rule. On the details page, you can view the details of the monitoring rule, including the configuration information and associated alert template.

> **Note** To modify a monitoring rule, click **Modify Rule** in the upper-right corner.

4.2.1.3.2. Create a monitoring rule

You can create monitoring rules based on your business requirements. The monitoring rules apply alert templates to the corresponding monitoring instances.

Prerequisites

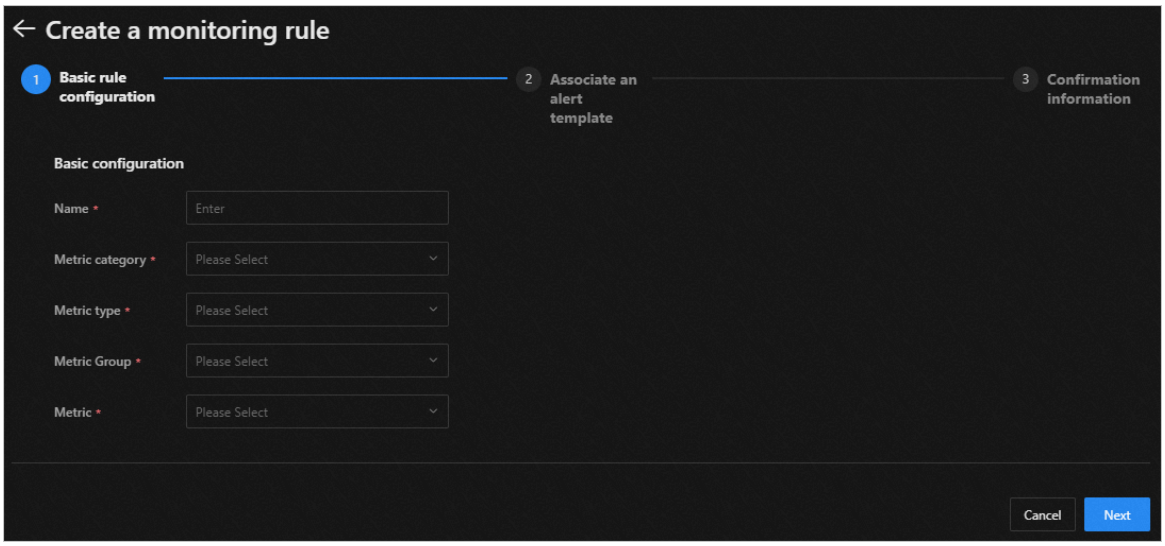
The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

In this version, you can only configure monitoring rules for port monitoring items of physical network devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
4. Click **Create a monitoring rule** to go to the rule creation page. Follow the procedure to complete all configurations.
   i. Configure basic information.
   Configure the basic information of the monitoring rule as prompted. After you select a metric category, the supplementary fields appear. After you specify all the parameters, click **Next**.



   ii. Associate an alert template.
   On the page, select the alert template to associate with the metric and click **Next**.
   iii. Confirm the settings.
   On the page, check whether the parameters are configured as expected:
   - If the parameters are not configured as expected, click **Previous**.
   - If the parameters are configured as expected, click **Create** to create the monitoring rule.

> **Note** After you create the monitoring rule, the rule is in the Enabled state by default.

4.2.1.3.3. Edit a monitoring rule

You can edit a created monitoring rule.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
4. Find the monitoring rule that you want to edit and click **Edit** in the **Operation** column.

4.2.1.3.4. Enable a monitoring rule

You can enable a disabled monitoring rule.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
4. Find the desired monitoring rule and click **Enable** in the **Operation** column. In the message that appears, click **OK**.

4.2.1.3.5. Disable a monitoring rule

You can disable an enabled monitoring rule.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
4. Find the desired monitoring rule and click **Disable** in the **Operation** column. In the message that appears, click **OK**.

4.2.1.3.6. Delete a monitoring rule

You can delete a configured monitoring rule.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Monitoring Rules**.
4. Find the desired monitoring rule and click **Delete** in the **Operation** column. In the message that appears, click **Delete**.

4.2.1.4. Alert template management

The alert conditions for monitoring metrics are configured in alert templates. When the monitoring metrics meet the specified alert conditions, alert notifications or message suppression actions are performed based on the configured alert rule or the suppression rule.

4.2.1.4.1. View alert templates

You can view the details of a created alert template.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.
   The created alert templates are displayed.
4. Click the name of an alert template to view the details of the template in the displayed panel.

4.2.1.4.2. Create an alert template

You can create an alert template for the monitoring metrics of a monitored instance and define configuration items such as alert thresholds, alert determination logic, and alert suppression settings.

Prerequisites

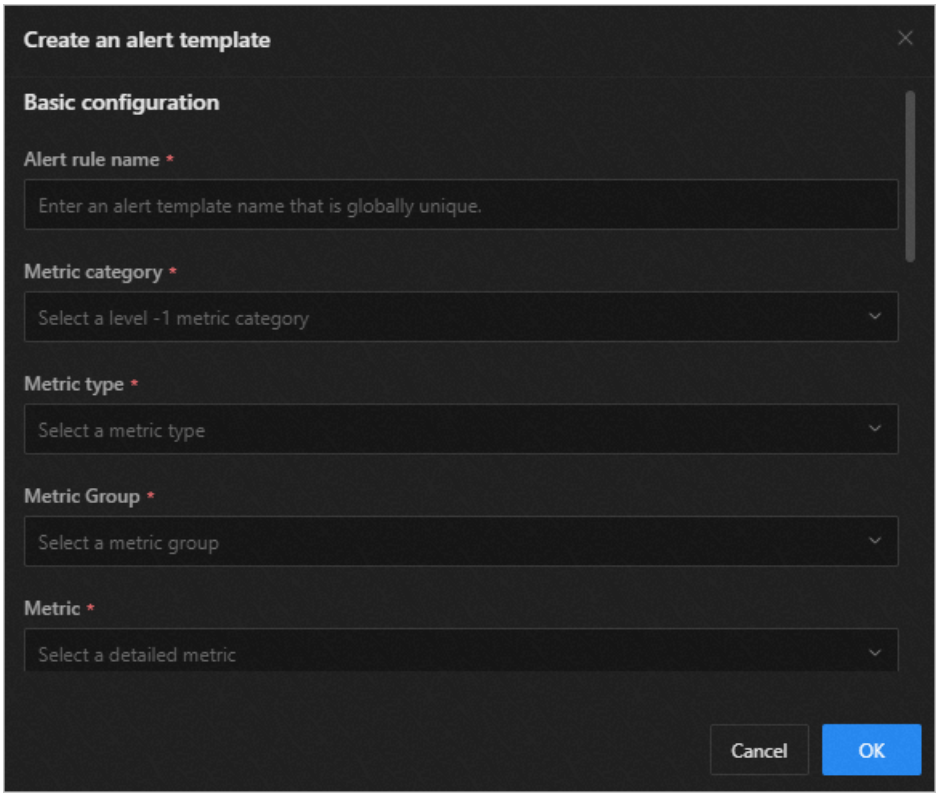
The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

The current version only supports the creation of the alert templates for the monitoring metrics of physical network device interfaces.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.
4. Click **Create alert template**. In the dialog box that appears, configure the parameters and click **OK**.



> **Note**
> - For some parameters, you can click the explanation icon on the right side of the parameter to view the detailed explanation of the parameter.
> - By default, the newly created alert template is enabled.

4.2.1.4.3. Edit an alert template

You can edit a created alert template.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.

4. Find the desired template and click **Edit** in the **Operation** column. In the dialog box that appears, edit the parameters and click **OK**.

4.2.1.4.4. Enable an alert template

You can enable an disabled alert template.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.
4. Find the desired template and click **Enable** in the **Operation** column. In the message that appears, click **OK**.

4.2.1.4.5. Disable an alert template

You can disable an enabled alert template.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.
4. Find the desired template and click **Disabled** in the **Operation** column. In the message that appears, click **OK**.

4.2.1.4.6. Delete an alert template

You can delete the alert templates that are no longer used.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Service Diagnosis**.
3. In the left-side navigation pane, choose **Network Alert Management > Alert Templates**.
4. Find the desired template and click **Delete** in the **Operation** column. In the message that appears, click **Delete**.

4.2.2. Network operations console

Network Operations Console is a comprehensive operations platform that covers the entire network, including the virtual network and the physical network.

The Network Operations Console module provides operations capabilities such as the visualization of end-to-end monitoring, automated implementation, automated fault locating, and network traffic analysis to enhance the efficiency of network operations engineers, reduce the operations risk, and improves the quality of Apsara Stack services.

4.2.2.1. Dashboard

4.2.2.1.1. View the dashboard

You can view the status of the current devices, network, and traffic on the Dashboard tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
   The **Dashboard** page appears.
3. On the **Dashboard** tab, view the dashboard information.

Item		Description
Device Management	**Device Overview**	The model distribution of the network devices in use.
	Port Occupation	◦ **Ports Utilization**: the proportion of the number of ports in use to the total number of ports in the network devices. ◦ **Error Packets by Port**: the total number of error packets generated by the device ports within a specified time range, of which the top five are displayed.
	Settings	◦ **System Backup**: shows the proportions of **Backup Completed**, **Connection Failed**, and **Out-of-Scope** data sources. Move the pointer over the corresponding section and the details are displayed. ◦ **Configuration Sync**: shows the proportions of **Config Desynchronized**, **Connection Failed**, and **Out-of-Scope** data sources. Move the pointer over the corresponding section and the details are displayed.
Network Monitoring	**Alerts**	The total number of alerts generated by network devices.
	Alert Device	The number of network devices that generate alerts and the total number of network devices.

	Alarm Information	The details of the alert.
Traffic Dashboard	**SLB Overview**	The bandwidth usage of SLB clusters.
	XGW Overview	The bandwidth usage of XGW clusters.

4.2.2.1.2. View the network topology

You can view the physical network topology on the **Network Topology** tab.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
   The **Dashboard** page appears.
3. Click the **Network Topology** tab.
4. On the **Network Topology** tab, view the physical network topology of a physical data center.

   You can select **Standard Topology** or **Dynamic Topology** from the **Current Topology** drop-down list.

   If an offset exists between the dynamic topology and the standard topology, a message appears when you go to the **Network Topology** tab in the upper-right corner of the tab and disappears after a few seconds. You can click **Update Topology** to update the standard topology.

   > **Note**
   > The colors of connections between network devices indicate the connectivity between the network devices:
   > - Green: The connection works normally.
   > - Red: The connection has an error.
   > - Grey: The connection is inactive.

   If you select **Standard Topology** from the **Current Topology** drop-down list, the **Alerts Refreshed** switch is turned on. You can turn off **Alerts Refreshed** to stop receiving new alerts that are triggered for the devices or the connection statuses within the topology.

   If you select **Dynamic Topology** from the **Current Topology** drop-down list, **Alerts Refreshed** is turned off.
5. In the topology, double-click a connection between two devices to view the connection and the alerts between the two devices.
6. In the topology, double-click a physical network device to view the basic information and node alerts of the device on the right.

4.2.2.1.3. Manage custom views

You can create a custom view to configure how to show the independent monitoring data set. You can configure the content and rules to summarize and demonstrate the monitoring data and graph information you are interested in.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Go to the Dashboard page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
   The **Dashboard** page appears.

Create a view

1. Click the **Customize View** tab.
2. Create a view.
   i. In the upper part of the tab, click **Create View**.
   ii. In the dialog box that appears, configure View Name and View Description and click **OK**.

   The view name cannot be the same as the name of an existing view. If the **A view with the same name already exists** message appears, you must change the view name to a unique one and then click **OK**.
3. Add a subview.
   By default, no subviews exist in a view after you create the view.
   i. Select the created view from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.
   ii. Click the  icon.
   iii. In the panel that appears, configure the parameters.

Parameter	Description
Device	Required. Select the device to be monitored from the drop-down list.
Monitoring Type	Required. Select the monitoring type from the drop-down list. ▪ **interface**: the switch interface, including the water level, packet error, and packet loss of the interface. ▪ **hardware**: the switch hardware, including the memory usage and CPU usage. ▪ **capacity**: others, which is not supported.
Metric	Required. Select the monitoring metric from the drop-down list.
Submetric	Optional. Select the monitoring submetric from the drop-down list.

   iv. Click **OK**.

   After the subview is added, the system automatically shows the subview on the view to which the subview belongs.
   v. You can add other subviews.

Delete a subview

1. Click the **Customize View** tab.
2. Select the view to which the subview that you want to delete belongs from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.
3. Click the close icon in the upper-right corner of the subview.
4. In the message that appears, click **OK**.

Delete a view

> **Important** If you delete a view, all subviews of the view are also deleted. Proceed with caution.

1. Click the **Customize View** tab.
2. Select the view that you want to delete from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.
3. Click **Delete View** in the upper part of the tab.
4. In the message that appears, click **OK**.

4.2.2.2. Network element management

Network elements are network devices such as vSwitches and routers. The Network Element Management module shows the basic information and running status of physical network devices. The module also provides configuration management operations for physical network devices, including device management, password management, and configuration comparison.

4.2.2.2.1. Device management

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

4.2.2.2.1.1. View network monitoring information

The Network Monitoring tab allows you to view the basic information, running status, and traffic monitoring information of Apsara Stack physical network devices and check the health status of network devices in a timely manner.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **Network Monitoring** tab.
5. In the upper part of the tab, select an IDC and perform the following operations:
   - View the basic information, ping status, and SNMP status of Apsara Stack physical

- View the basic information, ping status, and SNMP status of Apsara Stack physical network devices.

  > **Note** You can also click **Export** to export network device information to your computer.

  If a device has a business connectivity or gateway connectivity problem, the value in the Ping Status or SNMP Status column turns from green to red. The O&M personnel must troubleshoot the problem.

- In the upper-right corner of the tab, enter the device name or IP address in the search box to search for the monitoring information of a specific device.
- View the port information, CPU utilization, memory usage, aggregation port information, and alert information of a device.
  a. Click a device name, or click **Details** in the **Details** column corresponding to a device.
  b. On the **Port** tab, view the ports, port operation status, and link information of the device.
     a. On the **Ports** tab, select the port that you want to view and click **See** in the **Details** column.
     b. Select a time range on the right and click to view the traffic in the selected time range.

        You can select a time range in the **Quick query** section to view the traffic in the specified time range.
  c. On the **CPU usage** tab, view all the CPU utilization information of the device.
  d. On the **Memory usage** tab, view all the memory usage information of the device.
  e. On the **Aggregation Port Management** tab, view the information of all aggregation ports of the device. You can click **View** in the **Operation** column corresponding to a port to view the usage of the aggregation port.
  f. On the **Alert information** tab, view the alert information of the device.

     During routine O&M, you must closely monitor the alert list of the device. If no data is displayed on the **Alert information** tab, the device is operating normally.

     If alert events occur, unrecovered alert events are displayed in the list. You must handle these exceptions in a timely manner. When exceptions are handled, their corresponding alerts are cleared from the list.

4.2.2.2.1.2. View logs

The SYSLOG management tab allows you to view logs of physical network element devices and provides necessary data for fault location and diagnosis information collection.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **SYSLOG management** tab.
5. In the upper-right corner of the tab, select a device name from the drop-down list, select a time range, and then click to check the system logs generated by the device within the specified time range.

   If the device has a configuration exception or does not have any generated logs for the specified time range, no search results are returned.
6. **Optional:**You can filter the search results based on log keywords.
7. **Optional:**Click **Export** in the upper-right corner to export the search results to your computer.

4.2.2.2.1.3. Collection settings

The Collection Settings tab allows you to set the collection interval of physical network element devices and manage out-of-band (OOB) network segments.

Configure the collection interval

Before you collect network device information, you must configure a collection interval.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **Collection settings** tab.
5. In the **Collection cycle settings** section, configure the auto scan interval, device scan interval, port scan interval, and link scan interval.

   If you have no special requirements, we recommend that you use the initial default value.
6. Click **Submit**.
   Then, the system collects the device information based on your configurations.

Modify the collection interval

This topic describes how to modify the interval at which network device information is collected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **Collection settings** tab.
5. In the **Collection cycle settings** section, modify the parameter values.
6. Click **Submit**.
   The modified collection interval of the network device information takes effect after 1 minute.

Add an OOB network segment

If this is the first time you are using the Network Elements feature of Network Operations Center, you must add the device loopback network segment planned by the current Apsara Stack network device, which is typically the network segment of the netdev.loopback field in the IP address planning list.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

The OOB Network Segments section is used to configure the management scope of a physical network element device. Typically, operations engineers must add the loopback network segment in which the network device to be managed resides.

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **Collection Settings** tab.
5. In the lower part of the **OOB CIDR block management** section, click **Add CIDR block**.
6. In the Add Network Segment dialog box, enter the network segment that contains the mask information and a subnet mask and select an IDC.
7. Click **OK**.
   The initial data entry is complete.

   To modify or delete an OOB network segment, find it in the list and click **Edit** or **Delete** in the **Operation** column.

View the OOB CIDR block information

You can search for and view the information about the out-of-band (OOB) CIDR block of your managed devices.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. On the **Device Management** tab, click the **Collection settings** tab.
5. In the **OOB CIDR block management** section, click **Refresh** on the right.
6. In the list, view the CIDR block information of your managed devices.

> **Note** You can search for the information of a specific CIDR block by entering keywords in the search box.

4.2.2.2.2. Modify the device password

You can modify the passwords of physical network devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. Click the **Password management** tab.
5. **Optional:**Enter the name of the device for which you want to modify the password in the search box of the **Current network equipment** section and click **Query**.
   To search for another device, you can click **Reset** to reset the previous search conditions.
6. Select one or more devices and click **Add to implementation**.
   The selected devices are displayed in the **Implementation equipment** section on the right.

   > **Note** To remove a device from the **Implementation equipment** section, choose **Management > Delete** in the **Operation** column corresponding to the device. You can also click **Empty** in the upper-right corner to remove all the devices from the Implementation equipment section.
7. The system verifies the old password before you can modify the passwords. Enter **User name** and **Old password** in the lower-right corner and click **Verification**.
   You must verify the old passwords for all the devices in the **Implementation equipment** section.
8. After the verification is passed, you can modify the passwords for one or more devices.
   - Modify the password of a device
     a. Add a device to the Implementation equipment section at a time. You can also choose **Management** > **Delete** in the **Operation** column corresponding to the devices for which you do not want to modify the passwords to remove the devices.
     b. In the lower part of the **Implementation equipment** section, click **Modify**.
     c. In the dialog box that appears, enter and confirm the new password, and click **OK**.
   - Modify the passwords of all devices
     a. In the lower part of the **Implementation equipment** section, click **Modify**.
     b. In the dialog box that appears, enter and confirm the new password, and then click **OK**. The passwords of all the devices that are added to the **Implementation equipment** section and that are in the **Accessible** and **Verified** states are modified.

4.2.2.2.3. Compare device configurations

You can compare the current configurations of a device with its configurations on startup and check whether the configurations are consistent.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. Click the **Configuration consistency comparison** tab.
5. **Optional:**Enter the name of the device whose configurations you want to compare in the **Device Name** search box and click **Query**.
6. Select the devices and click **Consistency comparison**.
   After you compare the configurations, click **Refresh status** and click **Export result**.

4.2.2.3. SLB cluster management

After you add SLB cluster tags, you can easily select clusters in the tenant console. This improves the usability of SLB clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **SLB Cluster Management**.
4. Select a cluster and click **Search** to view the cluster information.
5. Find the cluster and click **Edit Tag** in the **Actions** column. In the dialog box that appears, modify the tag name and click **OK**.

> **Note** The default cluster tag **default** cannot be modified.

4.2.2.4. SLB management

The SLB Management module contains the Cluster Monitoring and Instance Monitoring tabs and shows the basic information, running status, and usage of SLB network products.

4.2.2.4.1. View cluster monitoring information

The Cluster Monitoring tab allows you to view the basic information, inbound limit (bit/s), outbound limit (bit/s), inbound limit (PPS), outbound limit (PPS), active connection limit, inactive connection limit, and usage of a single device node in a cluster.

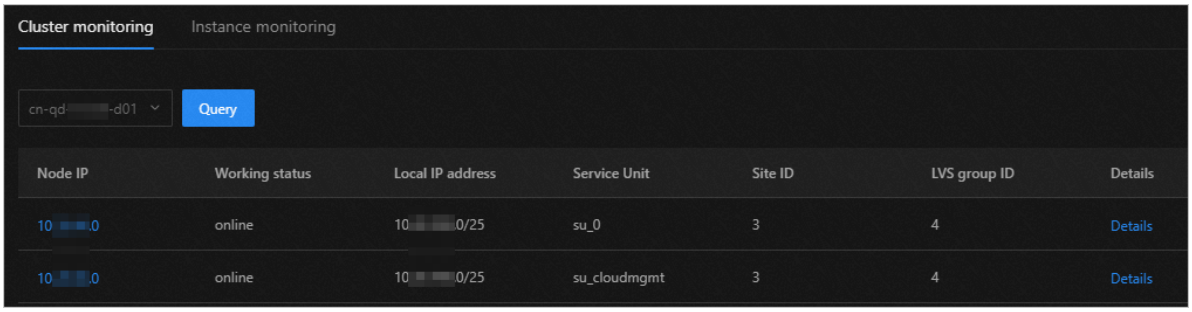
Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

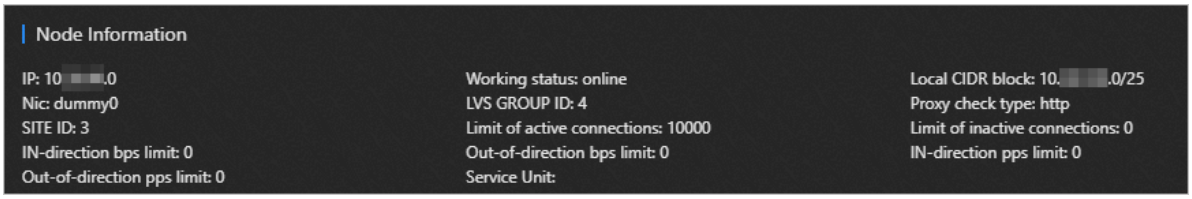
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, click **SLB Management**.
   The **Cluster monitoring** page appears.
4. Select the cluster that you want to view from the drop-down list and click **Query**.
   Information of all the device nodes in the cluster is displayed.

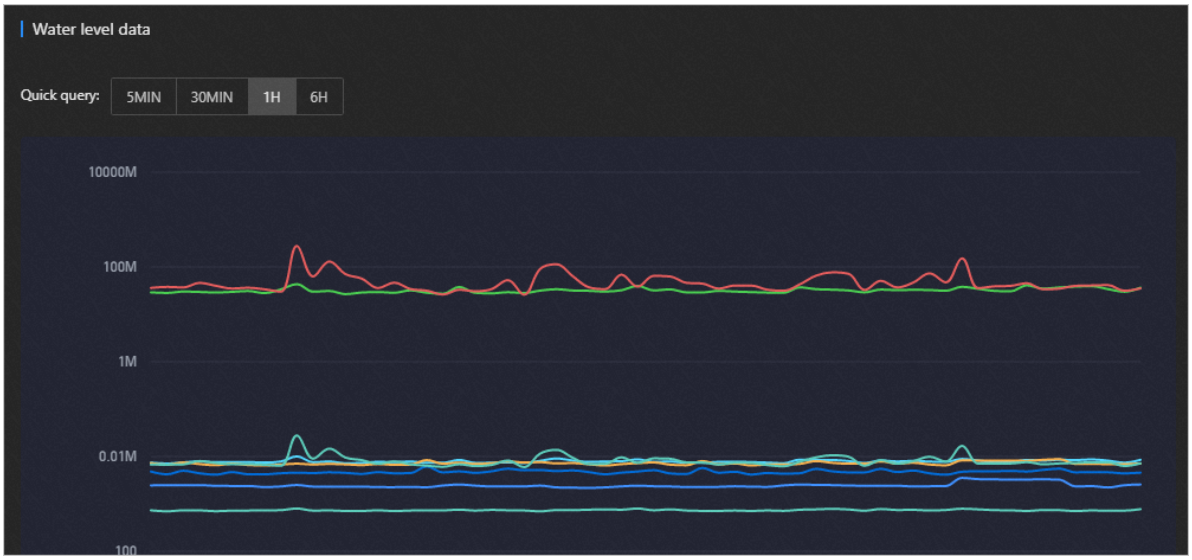


5. Find the desired device node and click **Details** in the **Details** column.
6. In the **Node Information** section, view the basic information of the node.



7. In the **Water level data** section, view the water level chart of the cluster. Select the start time, month, day, hour, minute, and second, and click **Query** to view the water level chart of the instance over a period of time.

> **Note**
> - The range between the start time and end time must not exceed 12 hours.
> - You can also click **5MIN**, **30MIN**, **1H**, or **6H** in the upper-left corner to query the usage data within the corresponding time range.
> - Move the pointer over a point in time to display the values of all metrics for that point in time.



Metric	Description	Example

ActConnsPS	Number of active connections	0
ConnsPS	Number of new connections	1
DropConnsPS	Dropped connections per second	0
FailConnPS	Failed connections per second	0
InActConnPS	Inactive connections	1
InBitsPS	Amount of inbound data per second (bits)	248
InDBitesPS	Amount of dropped inbound data per second (bits)	0
InDPktsPS	Number of dropped inbound packets per second	0
InPktsPS	Number of inbound packets per second	1
MaxConnsPs	Concurrent connections per second	1
OutBitsPS	Amount of outbound data per second (bits)	208
OutDBitesPS	Amount of dropped outbound data per second (bits)	0
OutDPktsPS	Number of dropped outbound packets per second	0
OutPktsPS	Number of outbound packets per second	1

4.2.2.4.2. View the monitoring information of an instance

The Instance Monitoring tab allows you to view the basic information and usage of an instance, including the BPS and PPS.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **SLB Management**.
4. On the **SLB management** page, click the **Instance Monitoring** tab.

5. Select the cluster where the instance that you want to view is located from the Cluster drop-down list. Enter the ID or VIP address of the instance that you want to query in the field and click **Query**.
6. In the **Node Information** section, you can view the basic information of the SLB instance, which can be used by O&M engineers to troubleshoot faults and confirm the ownership of the device.

   > **Note** Move the pointer over **View** to view the throttling rules of the SLB instance.

7. In the **Water level data** section, view the running water level chart of the cluster. Select the start time, month, day, hour, minute, and second, and click **Query** to view the running water level chart of the instance over a period of time.

   > **Note**
   > - The range between the start time and end time must not exceed 12 hours.
   > - You can also click **5MIN**, **30MIN**, **1H**, or **6H** in the upper-left corner to query the usage data within the corresponding time range.
   > - Move the pointer over a point in time to display the values of all metrics for that point in time.

Metric	Description	Required value
ActConnsPS	Number of active connections	0
ConnsPS	Number of new connections	1
DropConnsPS	Dropped connections per second	0
FailConnPS	Failed connections per second	0
InActConnPS	Inactive connections	1
InBitsPS	Amount of inbound data per second (bits)	248
InDBitesPS	Amount of dropped inbound data per second (bits)	0
InDPktsPS	Number of dropped inbound packets per second	0
InPktsPS	Inbound packets per second	1
MaxConnsPs	Concurrent connections per second	1
OutBitsPS	Amount of outbound data per second (bits)	208
OutDBitesPS	Amount of dropped outbound data per second (bits)	0
OutDPktsPS	Number of dropped outbound packets per second	0

OutPktsPS	Number of outbound packets per second	1

4.2.2.5. SLB proxy management

4.2.2.5.1. SLB proxy cluster monitoring

You can view the node status, water level data, and cluster aggregation monitoring metrics of an SLB proxy cluster.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **SLB Proxy**.
   The **Cluster monitoring** page appears.
4. Select the cluster that you want to view and click **Query** to view the cluster node information.
5. Find the desired node and click **Details** in the **Actions** column to view the metrics of the node.

   > **Note** You can select a time range in the **Quick query** section to view the water level during the specified time range. You can also select the start time and end time, and click **Query** to view the water level data in the specified time range.

   The following table describes the metrics.

   slb_proxy_cpu

Metric	Description
sys	System CPU utilization
msTimestamp	Timestamp (milliseconds)
util	Percentage of CPU usage time to total time
sirq	Percentage of time the system handles soft interrupts to the total time
user	Percentage of time that the CPU executes user processes to the total time
hirq	Percentage of time the system handles hard interrupts to the total time
wait	Percentage of time the CPU waits for I/O operations to the total time

slb_proxy_diskio

Metric	Description
rsecs	Number of sectors read from the device per second
rqsize	Average size of requests made to the device by sector
wrqms	Number of combined write requests to the device per second
rs	Number of read requests to the device per second
await	Average time to make I/O requests to the devices (milliseconds)
msTimestamp	Timestamp (milliseconds)
util	Percentage of the time that is taken by CPU to make I/O requests to the device to the total CPU time (bandwidth utilization of the device)
svctm	Average service time to make I/O requests to the device (milliseconds)
wsecs	Number of sectors written to the device per second
rrqms	Number of sectors read from the device per second
ws	Number of write requests to the device per second
qusize	Average queue length of requests to the device

slb_proxy_load

Metric	Description
runq	Number of tasks in the queue during the sampling time
load15	Average system load in 15 minutes (%)
plit	Number of active tasks in the system during the sampling time (excluding the completed tasks)
msTimestamp	Timestamp (milliseconds)
load1	Average system load within 1 minute (%)
load5	Average system load with 5 minutes (%)

slb_proxy_mem

Metric	Description
Writeback	Size of data being written back (KB)
used	Size of memory used (KB)
SReclaimable	Size of recoverable slab memory (KB)
buff	Size of memory used by buff (KB)
free	Idle physical memory size (KB)
msTimestamp	Timestamp (milliseconds)
util	Memory usage
Shmem	Size of shared memory that has been allocated (KB)
total	Total system memory size (KB)
Slab	Cache size of kernel data structure (KB)
cach	Size of memory allocated by the operating system to the file buffer (KB)
Dirty	Size of data waiting to be written back to the disk (KB)

slb_proxy_qps

Metric	Description
rt	Average response time (milliseconds)
spdyps	Number of SPDY requests processed per second
handle	Total number of processed TCP connections
msTimestamp	Timestamp (milliseconds)
read	Number of TCP connections that read request data
sslhst	Average SSL handshake time (milliseconds)
accept	Total number of new TCP connections received
reqs	Total number of generated requests
write	Number of TCP connections that write response data to users
qps	Number of requests processed per second
active	Number of active TCP connections, including the read, write, and waiting requests
sslqps	Number of SSL requests processed per second

cps	Average number of TCP connections received per second
wait	Number of waiting persistent TCP connections

slb_proxy_tcp

Metric	Description
pasive	Number of passively generated TCP connections per second
EstRes	Number of times that TCP connections are reset per second
lisove	Number of TCP requests dropped because the listenaccept queue is full
msTimestamp	Timestamp (milliseconds)
outseg	Number of outbound TCP segments per second
retran	Retransmission rate of segments. The value is calculated based on the retransmitted segments and the total segments.
iseg	Number of inbound TCP segments per second
active	Number of TCP connections that are actively initiated per second
CurrEs	Number of current TCP connections
AtmpFa	Number of failed TCP connections per second

6. View the aggregated monitoring data of a cluster.
   In the **Cluster aggregation monitoring** section, select the start time and end time, and click **Query**. You can view the cluster aggregation metrics on the **Core Metrics** and **All metrics** tabs.

   The following table describes the metrics.

Metric	Description
rt	Average response time (milliseconds)
spdyps	Number of SPDY requests processed per second
handle	Total number of processed TCP connections
msTimestamp	Timestamp (milliseconds)
read	Number of TCP connections that read request data
sslhst	Average SSL handshake time (milliseconds)
accept	Total number of received TCP connections

reqs	Total number of generated requests
write	Number of TCP connections that write response data to users
qps	Number of requests processed per second
active	Number of active TCP connections, including the read, write, and waiting requests
sslqps	Number of SSL requests processed per second
cps	Average number of TCP connections received per second
wait	Number of waiting persistent TCP connections

4.2.2.5.2. SLB proxy instance monitoring

You can view the monitoring metrics and water level charts of SLB proxy instances.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **SLB Proxy**.
4. Click the **Instance monitoring** tab.
5. Select a cluster, enter the instance ID or VIP address, and then click **Query**.
6. Select a listener instance and click the metrics (request, link, traffic, latency, and status code) below to view the water level chart of the corresponding metrics.
   The following table describes the metrics.

Metric	Description
qps	Average number of TCP connections received per second
req_concurrent	Number of concurrent requests
conn_concurrent	Number of concurrent connections
cps	Average number of TCP connections received per second
outBitsPS	Outbound traffic (bits/second)
inBitsPS	Inbound traffic (bits/second)
upstream_rt	Average processing latency of backend ECS instances (milliseconds)

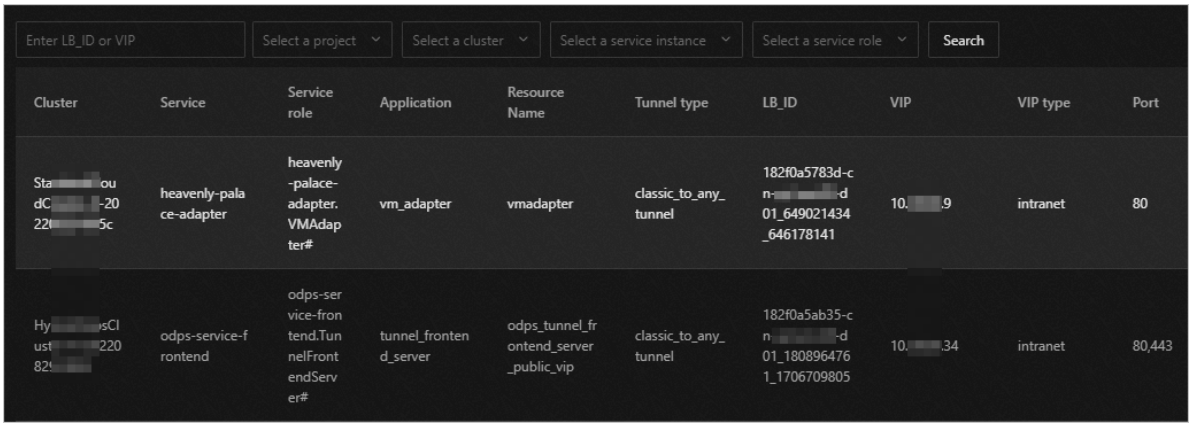
status_code_2xx	Number of requests for which 2xx response codes are returned
status_code_3xx	Number of requests for which 3xx response codes are returned
status_code_4xx	Number of requests for which 4xx response codes are returned
status_code_5xx	Number of requests for which a 5xx response code is returned
status_code_other	Number of requests for which response codes other than 2xx, 3xx, 4xx, and 5xx are returned
upstream_code_4xx	Number of requests with 4xx response codes returned by the backend ECS

4.2.2.6. Query AnyTunnel information

You can view the AnyTunnel information to see the AnyTunnel resources registered by projects within the current environment or whether a project has AnyTunnel registered. The system allows you to query the registration information of AnyTunnel resources by the LB_ID, VIP, project, cluster, service instance, and server role. You can use the global query feature to query the usage of all the AnyTunnel resources in the current environment.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **AnyTunnel Management**. The registration information of all AnyTunnel resources is displayed.
4. In the upper part of the page, enter an LB_ID or VIP, select the desired project, cluster, service instance, or service role from the drop-down list, and click **Search** to view the registration information of AnyTunnel resources in the current environment.



4.2.2.7. XGW management

The XGW Management module allows you to manage VPC gateways and view the water level information of device nodes and service instances.

4.2.2.7.1. View the information of nodes

The XGW Management module allows you to view the basic information, running status, aggregated traffic, and usage of each device node of XGW network products.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **XGW Management**.
4. Select the cluster that you want to view from the drop-down list and click **Query**.
   The system shows the basic information and usage information of aggregated traffic of all device nodes within the selected cluster. By default, the usage information of the last 1 hour is displayed. You can select 1 hour, 3 hours, 6 hours, or 1 day as the time range, or customize the time range to search for the usage information.
5. Find a device node and click **See** in the **Details** column.
6. On the page that appears, view the traffic usage information of the device node.
   The following table describes the metrics.

Metric	Description
InByteRate	The inbound data transmission rate. Unit: bit/s.
OutByteRate	The outbound data transmission rate. Unit: bit/s.
PacketLossRateIn	The inbound packet loss rate. Unit: PPS.
PacketLossRateOut	The outbound packet loss rate. Unit: PPS.
PacketRateIn	The inbound packet rate. Unit: PPS.
PacketRateOut	The outbound packet rate. Unit: PPS.

4.2.2.7.2. View the monitoring information about an instance

The Instance monitoring tab allows you to view information such as bps, pps, drop_speed, fin_speed, ratelimit_drop_speed, rst_speed, and syn_ack_speed.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations**

Console.

3. In the left-side navigation pane, click **XGW Management**.
4. Click the **Instance monitoring** tab.
5. Select the cluster where the instance you want to view is located from the drop-down list, enter the instance ID (elastic IP address) in the search box, and then click **Query**.
   By default, the data information within the last one hour is displayed. You can select a time range such as 5 minutes, 30 minutes, 1 hour, or 6 hours.

   The following table describes the metrics.

Metric	Description
InBps	The inbound data transmission rate. Unit: bit/s.
InDropSpeed	The inbound packet loss rate. Unit: PPS.
InFinSpeed	The inbound Fin packet forwarding rate. Unit: PPS.
InPps	The inbound packet forwarding rate. Unit: PPS.
InRateLimitDropSpeed	The inbound throttling packet loss rate. Unit: PPS.
InRstSpeed	The inbound RST packet forwarding rate. Unit: PPS.
InSynAckSpeed	The inbound SYN/ACK packet forwarding rate. Unit: PPS.
OutBps	The outbound data transmission rate. Unit: bit/s.
OutDropSpeed	The outbound packet loss rate. Unit: PPS.
OutFinSpeed	The outbound FIN packet forwarding rate. Unit: PPS.
OutPps	The outbound packet forwarding rate. Unit: PPS.
OutRateLimitDropSpeed	The outbound throttling packet loss rate. Unit: PPS.
OutRstSpeed	The outbound RST packet forwarding rate. Unit: PPS.
OutSynAckSpeed	The outbound SYN/ACK packet forwarding rate. Unit: PPS.

4.2.2.8. CGW management

4.2.2.8.1. View node information

The CGW Management module allows you to view the basic information, running status, aggregated traffic, and usage of each device node of CGW network products.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

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

2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **CGW Management**.
4. Select the cluster that you want to view from the drop-down list and click **Query**.

> **Note** The system shows the basic information and usage information of aggregated traffic of all device nodes within the selected cluster. By default, the usage information of the last one hour is displayed. You can also select **3 Hours**, **6 Hours**, or **1 Day** as the time range, or customize the time range to search for the usage information.

5. Find a device node and click **View** in the **Details** column. On the page that appears, view the traffic usage information of the device node.
   The following table describes the parameters.

Parameter	Description
InByteRate	The inbound data transmission rate. Unit: bit/s.
OutByteRate	The outbound data transmission rate. Unit: bit/s.
PacketLossRateIn	The inbound packet loss rate. Unit: PPS.
PacketLossRateOut	The outbound packet loss rate. Unit: PPS.
PacketRateIn	The inbound packet rate. Unit: PPS.
PacketRateOut	The outbound packet rate. Unit: PPS.

4.2.2.8.2. View the monitoring information of an instance

You can view the water level information of instance metrics.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **CGW Management**.
4. Click the **Instance monitoring** tab. Select a cluster from the drop-down list, enter the instance ID (tunnel ID), and click **Query**. You can view the usage charts of the instance.

> **Note** By default, the usage information of the last one hour is displayed. You can also select **5MIN** (5 minutes), **30MIN** (30 minutes), **1H** (1 hour), and **6H** (6 hours) as the time range to search for the usage information.

   The following table describes the metrics.

Metric	Description
InBps	The inbound data transmission rate. Unit: bit/s.
InDropSpeed	The inbound packet loss rate. Unit: PPS.
InFinSpeed	The inbound Fin packet forwarding rate. Unit: PPS.
InPps	The inbound packet forwarding rate. Unit: PPS.
InRateLimitDropSpeed	The inbound throttling packet loss rate. Unit: PPS.
InRstSpeed	The inbound RST packet forwarding rate. Unit: PPS.
InSynAckSpeed	The inbound SYN/ACK packet forwarding rate. Unit: PPS.
OutBps	The outbound data transmission rate. Unit: bit/s.
OutDropSpeed	The outbound packet loss rate. Unit: PPS.
OutFinSpeed	The outbound FIN packet forwarding rate. Unit: PPS.
OutPps	The outbound packet forwarding rate. Unit: PPS.
OutRateLimitDropSpeed	The outbound throttling packet loss rate. Unit: PPS.
OutRstSpeed	The outbound RST packet forwarding rate. Unit: PPS.
OutSynAckSpeed	The outbound SYN/ACK packet forwarding rate. Unit: PPS.

4.2.2.9. Cloud firewall management

If the cloud firewall is deployed in your environment, you can use the firewall feature to isolate or restore the firewall.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

> **Important** Confirm with the administrator that the cloud firewall is deployed in your environment. Otherwise, you cannot use this feature to perform bypass isolation and restoration.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, click **Cloud Firewall Management**.
4. Select the operation type, firewall type, and data center from the corresponding drop-down list and click **Confirmation**.

   Supported operations:

   - **Firewall bypass isolation**: physically isolates the firewall from the network structure. If an exception occurs on the cloud firewall service, the system removes the firewall device from the network forwarding path to ensure that the forwarding of business traffic is not affected.
   - **Firewall isolation and recovery**: restores the firewall from the network isolated state to the normal state. After the exception on the cloud firewall is resolved, the system restores the firewall device back to the network forwarding path to ensure that the firewall is restored to the initial online status.
5. In the **Select operating device** step, select devices and click **Next**.
6. In the **Configuration review** step, check the selected devices and template information. If the information is correct, click **Confirm delivery**.
7. In the message that appears, click **OK**.

   Then, the system automatically isolates or restores the firewall in the selected devices based on the configuration template.

   The results are automatically displayed in the **Result verification** step.
8. In the **Result verification** step, click **Details** in the **Release details** column corresponding to each device to view the corresponding result.
9. Click **Complete**.

4.2.2.10. Alert dashboard

4.2.2.10.1. View and process current alerts

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Alert Dashboard**.
4. Click the **Current alert** tab.
5. In the upper-right corner, enter a keyword in the search box and click **Search**.
   Alerts that meet the search conditions are displayed.
6. **Optional:**Filter the search results by device name, device IP address, or alert name.
7. Find an alert and move the pointer over **Details** in the **Details** column to view the detailed alert information.
8. Find the reason why the alert is triggered and then process the alert.
   - If the alert does not affect the operation of the system, you can click **Ignore** in the **Actions** column. In the **Confirm Operation** message that appears, click **OK** to ignore the alert.
   - If the alert is meaningless, you can click **Delete** in the **Actions** column. In the **Confirm Operation** message that appears, click **OK** to delete the alert.

   After the alert is deleted, you can query it on the **History alerts** tab.

9. **Optional:**Click **Export tables** to export the alert information to an on-premises machine.

4.2.2.10.2. View historical alerts

You can view historical alerts on the History Alerts tab.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Alert Dashboard**.
4. Click the **History alerts** tab.
5. In the upper-left corner, select a filter condition, enter the query fields, select the start time and end time, and click **Search**. Alert events that meet the conditions are displayed.
6. Click **Details** in the **Alert details** column of an alert to view detailed information about the alert.
7. **Optional:**Click **Export tables** to export the alert information to your computer.

4.2.2.11. Network alert settings

4.2.2.11.1. Add a trap

If the initially configured trap subscription does not meet the monitoring requirements, you can add a trap for monitoring match.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

Simple Network Management Protocol (SNMP) traps are used in this topic. SNMP trap is a part of SNMP and is a mechanism that enables the managed network devices, such as switches and routers, to send SNMP messages to NOC monitoring servers. If an exception occurs on the device being monitored or the switch monitoring metrics have an exception, the SNMP agent running in the switch sends an alert event to the NOC monitoring server.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Alert Settings**.
4. On the **Alert Settings** page, click **Add Trap**.
5. In the **Add Trap** dialog box that appears, configure the parameters.
   The following table describes the parameters.

Parameter	Description	Example
Trap Name	The name of the alert event.	linkdown or BGPneighbor down. You can customize the value.
Trap OID	The OID of the alert event.	.1.3.6.1.4.1.25506.8.35.12.1.12 The value must be configured based on the device document and cannot be customized.
Trap Type	The type of the alert event.	None
Trap Index	The index ID of the alert item. The KV information in trap messages, which is used to identify alert objects. Typically, the value of this parameter can be an API name, protocol ID, or index ID. You can configure multiple values for this parameter. The value must be configured based on the device document and cannot be customized.	None
Trap Msg	The message of the alert item. The KV information in trap messages, which is used to identify the alert data. Typically, the value of this parameter can be the additional information of the alert item, such as a system message or a message indicating the location of the state machine or the current status. You can configure multiple values for this parameter. The value must be configured based on the device document and cannot be customized.	None
Alert type	Select Fault or the Recovery as the alert type.	None
Alert Association	Select Recovery alert or No recovery alert. **Note** If **Recovery alert** is selected, you must configure the settings of the associated alert trap.	None

6. Click **OK**.

After the configuration is submitted, the system checks whether the values of Trap OID and Trap Name are the same as the existing ones. If not, the trap is added.

After the trap is added, the alert events of the configured Trap OID are monitored and are displayed on the **Current Alerts** and **Alert History** tabs of the **Alert Dashboard** module.

4.2.2.11.2. View traps

You can view traps configured in the current system.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Alert Settings**.
4. In the upper-right corner, enter a keyword in the search box and click .

   > **Note** You can click **Export tables** in the upper-right corner of the list to export the trap information to your computer.

5. **Optional:**Filter the search results by trap name, trap type, or OID.
6. Move the pointer over **Details** in the **Operation** column of a trap to view detailed information about the trap.

   > **Note** If a trap is no longer needed, you can click **Delete** in the **Operation** column.

4.2.2.12. Check IP address conflicts

The IP Address Conflicts module allows you to check whether the current Apsara Stack environment contains conflicting IP addresses.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **IP Address Conflicts**.
   After the **IP address conflict detection** page appears, the system checks whether the current Apsara Stack environment contains conflicting IP addresses. If it does, the conflicting IP addresses are displayed in the list. You can also view the port information, device name, and corresponding logon IP address of each conflicting IP address.

4.2.2.13. Leased line detection

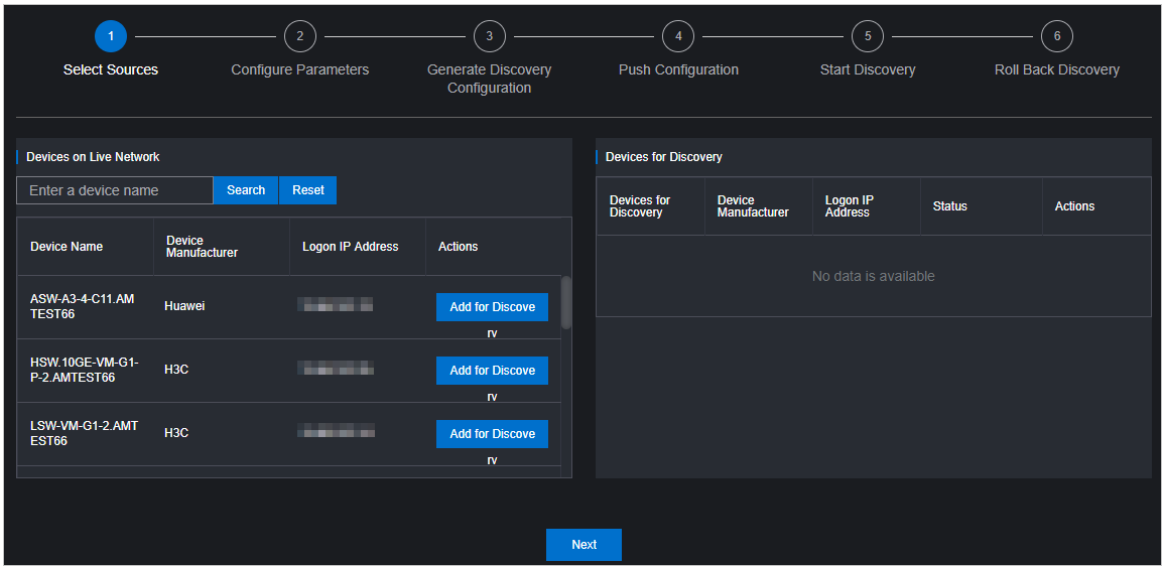
You can automate the leased line detection for devices by using graphical user interfaces. After the O&M engineers configure the detection parameters, Network Operations Center (NOC) automatically generates the detection configurations, pushes the configurations to a specific device, and then performs the detection test.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Leased Line Discovery**.
4. Select a detection source.
   i. In the **Select a probe source** step, enter a device name in the search box of the **Current network equipment** section and click **Query**.
   After you add a device, you can click **Reset** to clear the search condition and search for other devices to add to the list.



   ii. Click **Add Probe** in the Actions column corresponding to a device to add the device on the live network to the Implementation equipment section on the right.
   To remove a device from the Implementation equipment section, choose **Management > Delete** in the Operation column corresponding to the device. You can also choose **Management > Set account password** in the Operation column to modify the logon username and password of the device.
   iii. Click **Next**.
5. Configure the detection parameters.
   i. In the **Set probe parameters** step, click **Editing**. The **Set probe parameters** section is displayed.
   ii. Set **Link name**, **Destination IP address**, **Source IP address**, **Probe interval (seconds)** , **Number of probes**, and **Probe timeout (seconds)**, and then click **Add** to add the information to the list.
   You can choose **Management > Edit** or **Management > Delete** in the Actions column to modify or delete the detection parameters.
   iii. Click **Next**.
6. In the **Generate probe configurations** step, click **Generate configurations** to generate the detection configurations and roll back commands of all devices that have detection parameters configured.

i. Click **View** in the **Operation** column. The corresponding commands are displayed on the left.

ii. You can also select one or more devices and click **Export configuration** to export the files that contain the configurations and rollback commands of detection devices to your computer.

iii. Click **Next**.

7. In the **Send configuration** step, click **Next**.
   i. In the message that appears, click **Continue** to send the detection configuration commands to the corresponding device.
   ii. After the configuration is sent, you can click **View Logs** to view detailed sent logs.
   iii. Click **Next**.
8. In the **Enable leased line detection** step, click **Start** in the Actions column corresponding to a device to perform the test of leased line detection.

   After the test is complete, click **Next**.
9. In the **Rollback leased line detection** step, click **Roll Back** in the Actions column corresponding to the device on which you have performed the leased line test to roll back the corresponding NQA configurations in the device.
   i. If the rollback fails, you can click **View Logs** to view the detailed rollback logs.
   ii. Click **Complete**.

4.2.2.14. Baseline configuration audit

The Baseline Configuration Audit module allows you to compare the baseline and the current running configurations of devices.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Baseline Configuration Audit**.
4. Select one or more devices in the device list and click **Start audit**. The system begins to audit the baseline configurations of the selected devices.

   The following table describes the audit states.

State	Description
Pending audit	The initial state.
Auditing	The baseline configurations of the device are being audited in the background.
Pass	The current configurations are consistent with the baseline configurations.
Fail	The current configuration is not consistent with the baseline configuration.

Disconnected	The system cannot connect to the device.
No Data	The system cannot obtain the baseline configurations of the device.

5. After the audit is complete, click **Refresh** to update the audit results.
6. Click **Detection** in the **Detection** column of the device. The audit result is displayed on the right.

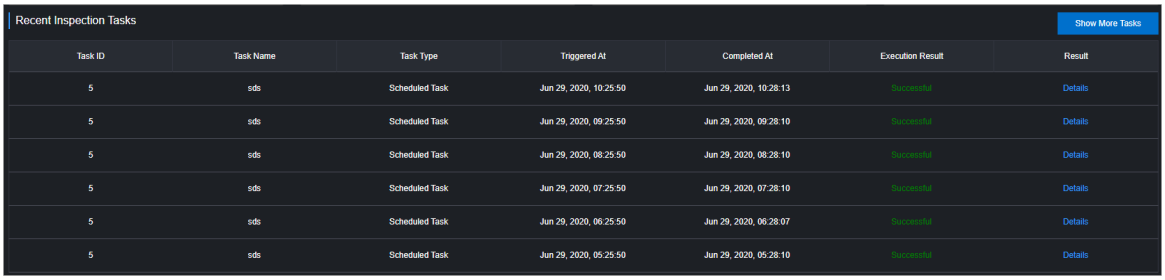
4.2.2.15. Inspection Dashboard

The Inspection Dashboard module allows you to view the inspection data and the last 10 inspection records.

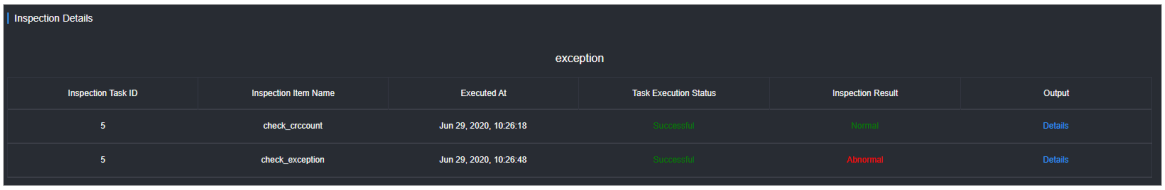
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Dashborad**.
4. Perform the following operations:
   - View the inspection statistics of the current day and the last 10 inspection records. The inspection statistics include the number of successful tasks, failed tasks, and scheduled tasks for the current day, as well as the progress.
   - View inspection records

     In the **Recent Inspection Tasks** section, click **Details** in the **Result** column corresponding to a task. The following information about the task is displayed: inspection time, inspection template, execution progress, inspection health status, task type, task status, task name, and inspection details of each subtask.

     In the **Inspection Details** section, move the pointer over **Details** in the **Rollback** column corresponding to a subtask. The inspection result of the inspection subtask is displayed.

   - Click **Show More Tasks** to go to the **Inspection History** page to view the inspection history.

4.2.2.16. Inspection history

You can query the inspection history and view detailed inspection records by task type and time range.

Background information

Inspection tasks can be divided into one-time tasks and scheduled tasks. A one-time task can be executed only once. You can set an execution interval for a scheduled task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection History**.
   By default, all inspection records in the last 24 hours are displayed.
4. Select the inspection type (**All**, **One-time Task**, or **Scheduled Task**), specify the time range, and then click **Search**.
5. View inspection records that meet the query conditions.
6. Click **Details** in the **Results** column corresponding to an inspection record. The following information is displayed: inspection time, inspection template, execution progress, inspection health status, task type, task status, task name, and inspection details of each subtask.
7. In the **Inspection Details** section, move the pointer over **Details** in the **Rollback** column corresponding to a subtask. The inspection result of the inspection subtask is displayed.

4.2.2.17. Inspection management

The Inspection Management module allows you to create, view, modify, start, suspend, and delete inspection tasks.

4.2.2.17.1. Create a one-time task

This topic describes how to create a one-time task.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Background information

By default, a one-time task can be executed only once after it is created. After a one-time task is executed once, the task automatically enters the **Suspended** state. The task can be manually started and then executed again.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Management**.
4. Click the **One-time Task** icon.
   The configuration wizard for the inspection task appears.
5. In the Specify Inspection Task Name step, enter the inspection task name and click **Next**.
6. In the **Add Inspection Device** step, select one or more devices from the drop-down list

and click **Next**.

7. In the **Select Inspection Template** step, select an existing template from the drop-down list or click **Create Temporary Inspection Template**.
   To create a temporary inspection template, click **Create Temporary Inspection Template**. In the dialog box that appears, select the inspection items that you want to associate with the temporary inspection template and click **OK**.

   > **Note** Some inspection items are provisioned by manufacturers. You must select proper inspection templates or inspection items based on devices.

8. Click **Next**.
9. In the **Inspection Task Preview** step, confirm the inspection task information and click **Next**.
0. Click **Processed**.

   The message **Created** is displayed. You can choose **Network Operations Console > Inspection Management** to view the created one-time inspection task on the **Scheduled Inspection Management** tab.

4.2.2.17.2. Create a scheduled task

This topic describes how to create a scheduled task based on routine inspection requirements. You can set an execution interval for the scheduled task.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Management**.
4. Click the **Scheduled** icon.
   The configuration wizard for the inspection task appears.
5. In the Inspection Task Name step, enter the inspection task name and click **Next**.
6. In the **Add Inspection Device** step, select one or more devices from the drop-down list and click **Next**.
7. In the **Select Inspection Template** step, select an existing template from the drop-down list or click **Create Temporary Inspection Template**.
   To create a temporary inspection template, click **Create Temporary Inspection Template**. In the dialog box that appears, select the inspection items that you want to associate with the temporary inspection template and click **OK**.
8. Click **Next**.
9. Specify the inspection cycle and the time point when the task is triggered and click **Next**.
0. In the **Inspection Task Preview** step, confirm the inspection task information and click **Next**.
1. Click **Proceed**.

   The message **Created** is displayed. You can choose **Network Operations Console > Inspection Management** to view the newly created scheduled task on the **Scheduled Inspection Management** tab.

4.2.2.17.3. Manage scheduled inspection tasks

After an inspection task is created, you can view, modify, start, suspend, or delete the task.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Go to the scheduled inspection task management page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Management**.
4. Click the **Scheduled Inspection Management** tab.

View a task

View the information of all the created inspection tasks in the system, including the task ID, task name, task type, associated template, creation time, and running status.

Modify task parameters

1. In the task list, find the task that you want to modify and click **Modify** in the **Actions** column.
2. In the dialog box that appears, modify the task parameters.
   - For a one-time task, you can modify the inspection name, inspection type, inspection template, and inspection device.
   - If the current task is a scheduled task, you cannot modify the task parameters.
3. Click **OK**.

Start or suspend a task

You can start a suspended task or suspend a running task based on your business requirements.

1. In the task list, find a task and click **Start** or **Suspend** in the **Actions** column.

   > **Note** After a one-time task is executed, it automatically enters the **Suspended** state. You can click **Start** to execute it again.

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

Delete a task

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

4.2.2.18. Network inspection templates

The Inspection Templates module allows you to manage, create, view, modify, and delete inspection templates.

4.2.2.18.1. Create a template

You can create a common inspection template to facilitate the creation of routine inspection tasks.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Templates**.
4. Click **Create Template**.
5. In the dialog box that appears, enter the template name and template tag, and select a manufacturer and a template inspection item collection for the device.

Parameter	Description
Template Name	The name of the inspection template. The name must be unique.
Associated Vendor	The manufacturer of the device.
Template Tag	The tag added to the template to make it easier to differentiate.
Inspection Item Collection	The collection of inspection items associated with the template.

6. Click **OK**.
   After the template is created, you can view the new template in the template list.

4.2.2.18.2. View template details

Before you use an inspection template, you can view its details to determine whether it meets your requirements.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Templates**.
4. In the template list, find the template that you want to view and click **Details** in the **Actions** column.
5. View the basic information about the template and the inspection items related to the template.

6. **Optional:**To manage an inspection item in the template, click **Go to** in the **Actions** column to go to the management page of the inspection item.
   For other operations that can be performed on inspection items, see **Network operations > Network management and operations > Network automation > Configure templates** in **Apsara Stack Enterprise Operations and Maintenance Guide** .

   > **Note** Generally, no other operations are required for inspection items.

4.2.2.18.3. Modify a template

After you create a template, you can modify its information based on your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Templates**.
4. In the template list, find the template that you want to modify and click **Modify** in the **Actions** column.
5. In the dialog box that appears, modify the template name, associated manufacturer, template tag, and template inspection item collection.
6. Click **OK**.

4.2.2.18.4. Delete a template

You can delete inspection templates that are no longer needed for routine O&M.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Templates**.
4. In the template list, find the template that you want to delete and click **Delete** in the **Actions** column.

   > **Important** When you delete a template, its associated inspection tasks and records are also deleted. Exercise caution when you delete templates.

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

4.2.2.18.5. View inspection items

You can view the details of all inspection items in the system, including the item IDs, categories, names, tags, and description.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Inspection Templates**.

4. Click the **Inspection Template Management** tab.
5. View the information of all inspection items in the system.
6. To perform other operations on an inspection item, click **Go to** in the **Actions** column to go to the management page of the inspection item.
   For other operations that can be performed on inspection items, see **Network operations > Network management and operations > Network automation > Configure templates** in **Apsara Stack Enterprise Operations and Maintenance Guide**.

   > **Note** Generally, no other operations are required for inspection items.

4.2.2.19. Hybrid cloud networks

4.2.2.19.1. Cloud service interconnection

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

4.2.2.19.1.1. Dynamic VIP

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

Background information

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

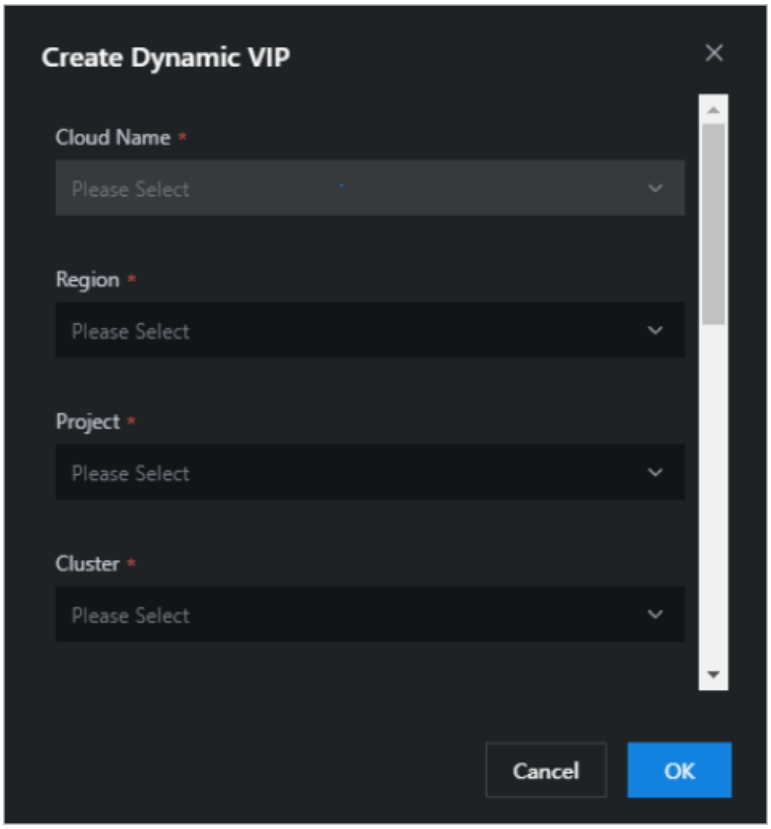
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Hybrid Cloud Network > Cloud Service Interaction > Dynamic VIPs**.
4. On the **Dynamic VIP** page, view the dynamic VIPs.
   - Enter a VIP name in the **VIP Address** search box, enter a template VIP name in the **Template VIP Name** search box, and then select a type from the **SLB Instance Type** drop-down list. Then, click **Search** to view the dynamic VIP. Click **Details** in the Actions column to view the details of the dynamic VIP.
   - Use more filter conditions to view more about the dynamic VIP.
     a. Click **Advanced**, select one or more types from the **Tunnel Type** drop-down list, and enter a region name in the **Region** search box. Then, click **Search**.

b. (Optional) Click **Reset** to clear the search conditions.

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

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



The following table describes the parameters.

Parameter	Description
Cloud Name	The name of the cloud instance.
Region	The ID of the region.
Project	The name of the project.
Cluster	The name of the cluster.
Service	The name of the service.
ServiceRole	The name of the server role.
Application	The name of the application.
Template VIP Name	The name of the template VIP.
type	The type of the SLB instance.
tunnel_ type	The type of the tunnel.
Ipprotocol	The type of the VIP.

- Update a dynamic VIP.

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

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

  - If the abnormal dynamic VIP status is caused by resource changes during product upgrades or scaling, click **Update** in the Actions column. The system queries the template VIP parameters by calling Apsara Infrastructure Management API operations and combines these parameters with the variable properties of the dynamic VIP to update the dynamic VIP.
  - If the abnormal dynamic VIP status is not caused by resource changes during product upgrades or scaling, submit a ticket to contact Apsara Stack technical support.
- Find the dynamic VIP that you want to delete and click **Delete** in the Actions column. In the message that appears, click **OK**.

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

4.2.2.19.1.2. Dynamic DNS

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

Background information

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

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

> **Warning** Before you resolve DNS domain names in the Apsara Infrastructure Management console, make sure that the parameters of the dynamic VIPs and the static VIP are exactly the same, and VIP listening on access is normal. Otherwise, network exceptions may occur.

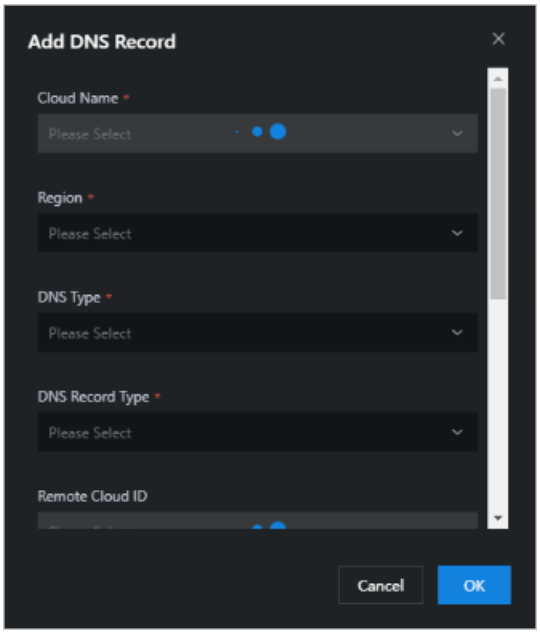
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Hybrid Cloud Network > Cloud Service Interaction > Dynamic DNS**.
4. On the **Dynamic DNS** page, view the dynamic DNS records.
   - Select a type from the **DNS Type** drop-down list, select a cloud ID from the **Remote**

Cloud ID drop-down list, and then enter a domain name in the **ZoneName** search box. Then, click **Search** to view the dynamic DNS records.

- Use more filter conditions to search for the dynamic DNS records.
  a. Click **Advanced**, enter a domain name in the **DnsDomain** search box, and then enter a DNS record in the **DNS Record** search box. Then, click **Search** to view the dynamic DNS records.
  b. (Optional) Click **Reset** to clear the search conditions.
  c. (Optional) Click **Collapse** to hide the **DnsDomain** and **DNS Record** options.

5. Create, update, or delete a dynamic DNS record.
   - Click **Add DNS Record** above the dynamic DNS record list. In the Add DNS Record dialog box, configure the parameters. Then, click **OK** to create a dynamic DNS record.



The following table describes the parameters.

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

DnsRecord	The IP address recorded by the DNS.

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

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

4.2.2.19.2. Cross-cloud access

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

Prerequisites

You have configured IP network routing based on the access matrix data and granted the network access permissions.

Background information

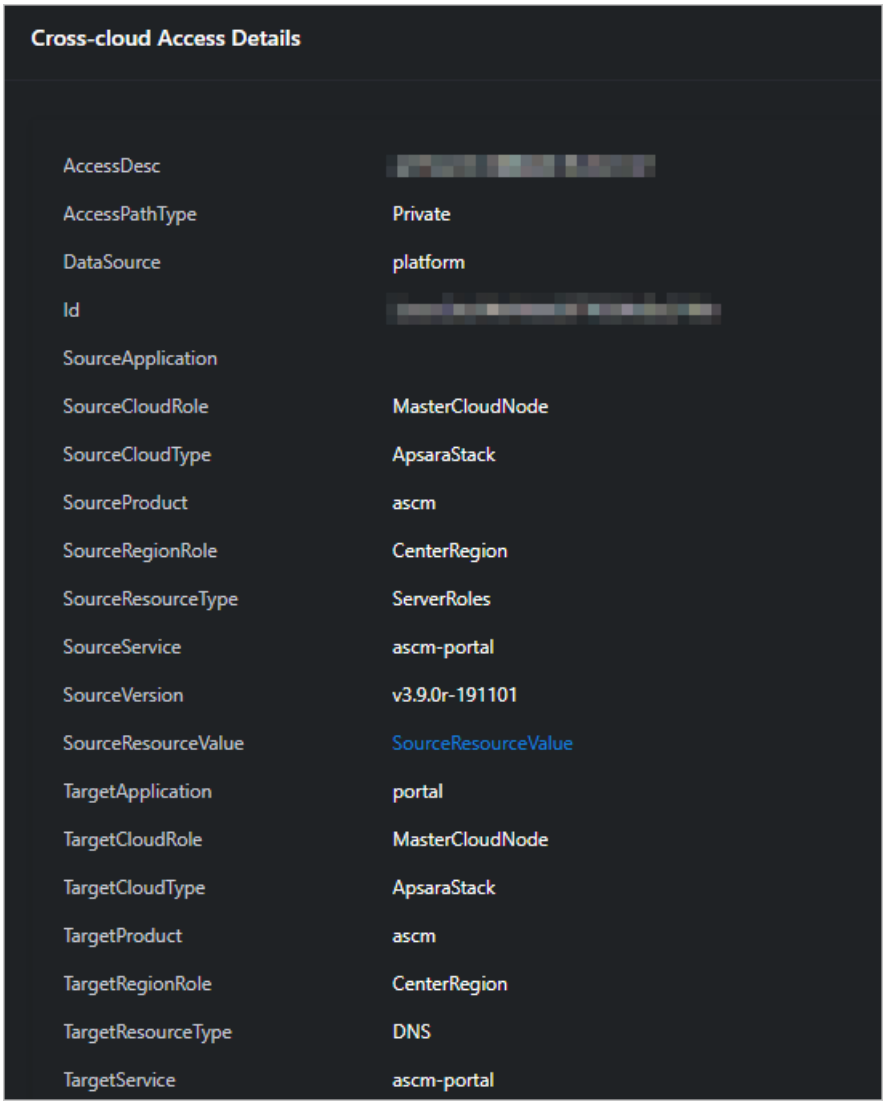
Cross-cloud access is applicable to the following scenarios:

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Hybrid Cloud Network > Cross-cloud Access**.
4. In the left-side navigation pane, click **Cross-cloud Access**. On the **Cross-cloud Access** page, view the information about access matrix.
   i. Enter a product name in the **Product Name** search box and click **Search**. The access matrix is displayed in the lower part of the page.

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



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

iii. **Optional:**Click **Reset** to clear the search conditions.

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

4.2.2.20. Network service provider

4.2.2.20.1. View access gateway instances

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

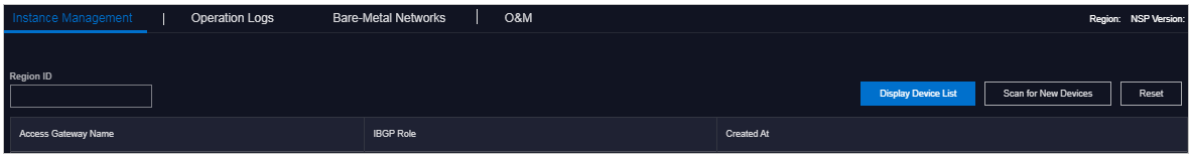
Procedure

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

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

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

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



Parameter	Description
The name of the CCN instance.	The access gateway name in the current system.
IBGP role	The role of the access gateway in the environment. Valid values: ◦ **RR-Active**: indicates that the role of the current gateway device is RR active device. ◦ **Client**: indicates that the role of the current gateway is not RR active device.
Management IP addresses	The management IP address of the current HSW vSwitch.
Created	The time when the current vSwitch began to act as an access gateway instance.
Authorization Status	Indicates whether the access gateway instance is authorized.

4.2.2.20.2. View the operation history

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.

4. Click the **Operation History** tab.
5. Set filter conditions such as vSwitch ID, bare metal instance name, access gateway name, and time range, and click Search to search for the operation logs that meet the filter conditions.

   The following table describes some of the filter conditions.

Filter condition	Description
Vswitch ID	The ID of the vSwitch when the bare metal instance is applied for or released in the VPC.
Bare Metal name	The name of the bare metal instance that was applied for or released in the VPC. The serial number is used to identify the bare metal instance as a unique one in the region.
The name of the CCN instance.	The name of the access gateway to query.
Created	The time range of the API operation to query.

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

The following table describes the fields in the query result.

Parameter	Description
ID	The index of the operation log.
Created	The time when the operation was performed.
API operations	The category of the API operation, such as applying for or releasing a bare metal instance in the VPC. Valid values: ◦ **add** indicates that a bare metal instance is applied for in the VPC. ◦ **del** indicates that a bare metal instance is released in the VPC. ◦ **del_pc** indicates that a physical connection is deleted. ◦ **del_vbr** indicates that a Virtual Border Router (VBR) is deleted. ◦ **del_router_intf** indicates that a router interface is deleted. ◦ **del_route_entry** indicates that a route table entry is deleted.
Vswitch ID	The ID of the vSwitch when the bare metal instance is applied for or released in the VPC.
The name of the CCN instance.	The name of the access gateway involved with the current operation.
Port	The port to which the bare metal instance belongs.
Bare Metal name	The name of the bare metal instance that is applied for or released in the VPC. To identify the bare metal instance as a unique one in the region, the serial number of the bare metal instance is displayed.

State	The status of the API operation. **success** indicates that the operation was successful. If the API operation is in progress, the value indicates the real-time status of the API operation. If the API operation is complete but the value is not **success**, you can view the failure information in this column.

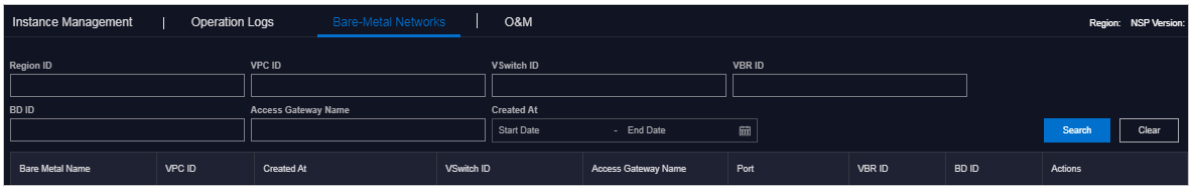
6. Find an operation log in the search results and click **View Details** in the **Details** column to view the details of the API operation.

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

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **Bare Metal network management** tab.
   By default, the network information of bare metal instances in the current system is displayed by page.
5. Configure the filters such as bare metal instance name, VPC ID, vSwitch ID, VBR ID, BD ID, access gateway name, and time range, and click Search to search for the bare metal instance that meets the filter conditions.



Filter condition	Description
Bare Metal name	The name of the bare metal instance that was applied for or released in the VPC. The serial number is used to identify the bare metal instance as a unique one in the region.
VPC ID	The ID of the VPC to which the bare metal instance belongs.
Vswitch ID	The ID of the vSwitch to which the bare metal instance belongs.
VBR ID	The VBR ID of the physical connection created on HSW by the VPC to which the bare metal instance belongs.
BD ID	The value of the hardware bridge-domain (BD) to which the bare metal instance is added.
The name of the CCN instance.	The name of the access gateway to which the bare metal instance belongs.

Created	The time range within which the bare metal instance is allocated to the VPC.

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

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

4.2.2.20.4. O&M configurations

4.2.2.20.4.1. Check the initialization configuration

In O&M emergency scenarios, you can use this feature to check whether the initialization configuration of the HSW vSwitch is successful.

Prerequisites

The correct HSW device name and the ID of the region where the device is located are obtained.

Background information

This feature only checks the initialization status of the HSW vSwitch and whether the initialization configuration is successful. No operation is performed on the bare metal instance.

> ⚠ **Warning** This operation is only used for emergency situations. Therefore, perform this operation under the guidance of Alibaba Cloud technical personnel. Otherwise, normal business operations will be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**. The **Instance management** tab appears.
4. Click the **O & M configuration** tab.
5. Select **Check the initialization configuration** from the drop-down list in the upper-left corner.
6. Configure the parameters described in the following table.

Parameter	Description
The region ID.	The ID of the region in the current environment.
HSW name	The name of the vSwitch to be checked in instance management.

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

7. After you specify the parameters, click **Next** and click **Check** to check the initial configuration of the vSwitch.

4.2.2.20.4.2. Check the route configuration

In O&M emergency scenarios, you can use this feature to locate abnormal operations and check whether the route configuration of the bare metal instance is correct.

Prerequisites

The correct bare metal instance name and the ID of the region where the instance is deployed are obtained.

Background information

You can use this operation to locate the exception and scan the HSW device after a bare metal instance fails to be added. This feature only checks whether the route configuration of the bare metal instance is correct. No operation is performed on the bare metal instance.

Procedure

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

Parameter	Description
The region ID.	The ID of the region in the current environment.
Bare Metal name	The name of the bare metal instance that was applied for or released in a VPC. It uniquely identifies the bare metal instance within a region.

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

7. After you specify the parameters, click **Next** and click **Check**.

4.2.2.20.4.3. Display information about bare metal network gateways

In O&M emergency scenarios, you can use this feature to check the gateway of the vSwitch.

Prerequisites

The vSwitch gateway information, region ID, AccessKey ID, and AccessKey secret have been obtained.

Background information

This operation is used only in emergency situations where the bare metal network is inaccessible. This operation is used to check the vSwitch gateway information and has no impact on the bare metal instance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. In the left-side drop-down list, select **Display bare metal Gateway Information**.
6. Configure the parameters described in the following table.

Parameter	Description
The region ID.	The name of the region in the current environment.
Vswitch ID	The ID of the vSwitch. You can obtain the vSwitch ID from the VPC console.
AK	The AccessKey ID of the organization to which the VPC belongs, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console.
SK	The AccessKey secret of the organization to which the VPC belongs, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console.

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

7. After you configure the parameters, click **Next** and click **Check** to check the bare metal gateway information.

4.2.2.20.4.4. Apply for a bare metal instance in a VPC

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

Prerequisites

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

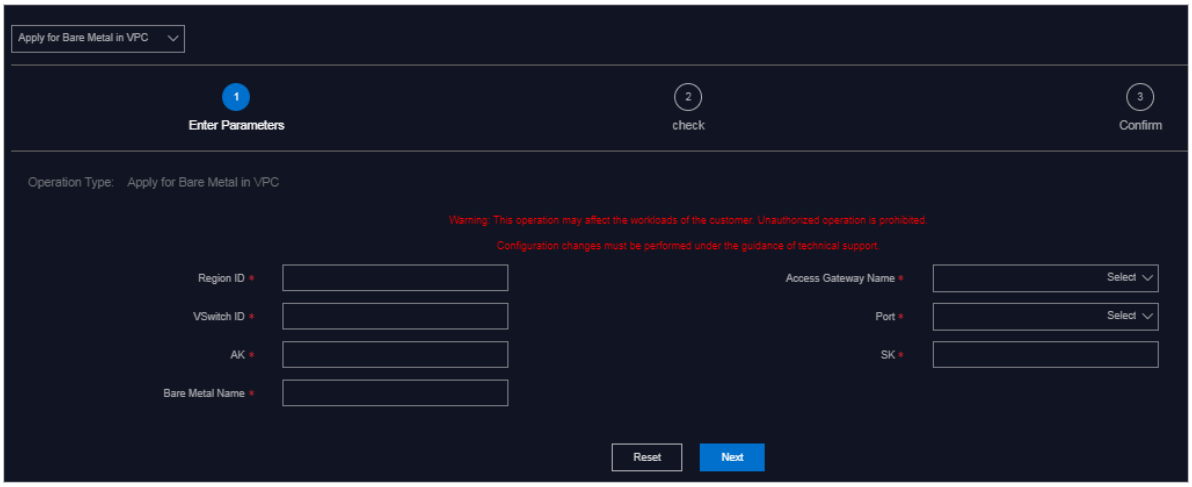
Before you use this feature, take note of the following items:

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

corresponding product team for guidance.

Procedure

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



6. Configure the parameters described in the following table.

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

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

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

Result: Successful message appears.

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

4.2.2.20.4.5. Release a bare metal instance in a VPC

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

Prerequisites

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

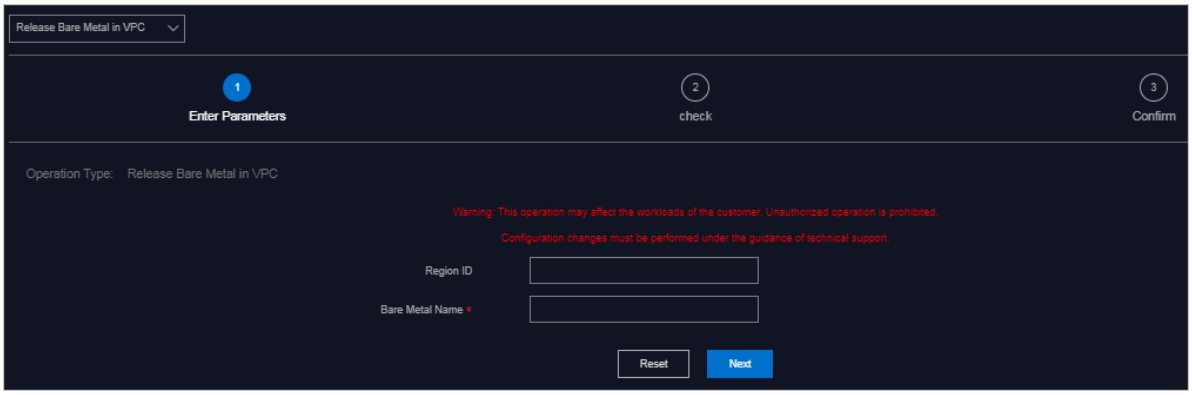
- Typically, you cannot use this feature to release a bare metal in the VPC. You can use the bare metal controller to call an API operation to delete the bare metal network.
- This feature can only be used to connect the bare metal instance to the access gateway port but cannot be used to perform operations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

Background information

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

Procedure

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



6. Configure the parameters described in the following table.

Parameter	Description

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

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

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

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

4.2.2.20.4.6. Delete a VPC route table entry

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

Prerequisites

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

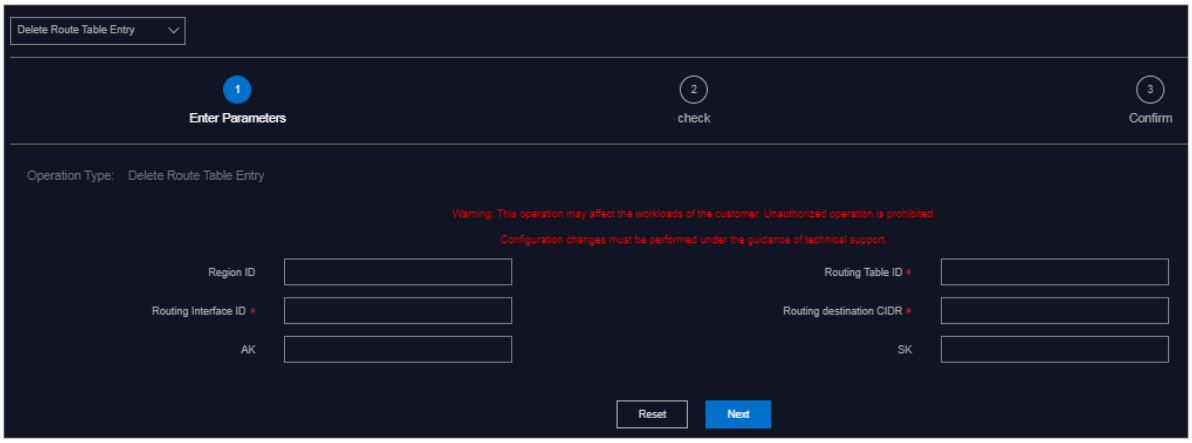
- Typically, you cannot use this feature to delete a VPC route table entry. This operation is only used for emergency situations.
- You can perform this operation to delete only a single route table entry at a time. To delete multiple route table entries, you must perform this operation multiple times.

Background information

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

Procedure

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



6. Configure the parameters described in the following table.

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

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

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

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

4.2.2.20.4.7. Delete a VBR route table entry

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

Background information

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

Procedure

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

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

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

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

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

4.2.2.20.4.8. Delete a VPC router interface

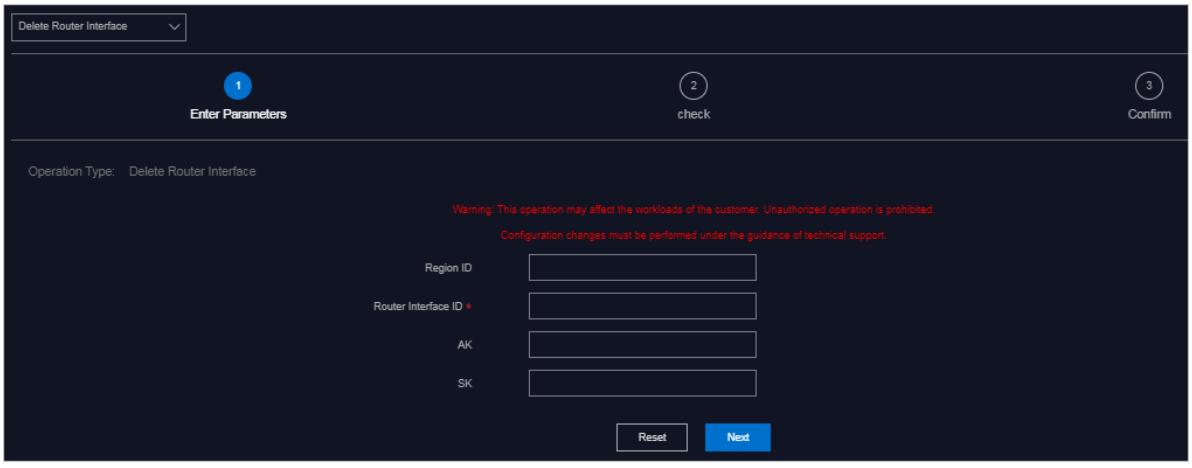
In O&M emergency scenarios, you can use this feature to delete a VPC router interface.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. In the left-side drop-down list, select **Delete a router interface**.



6. Configure the parameters described in the following table.

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

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

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

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

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

4.2.2.20.4.9. Delete a VBR router interface

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

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. In the left-side drop-down list, select **Delete a router interface**.
6. Configure the parameters described in the following table.

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

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

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

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

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

4.2.2.20.4.10. Delete a VBR

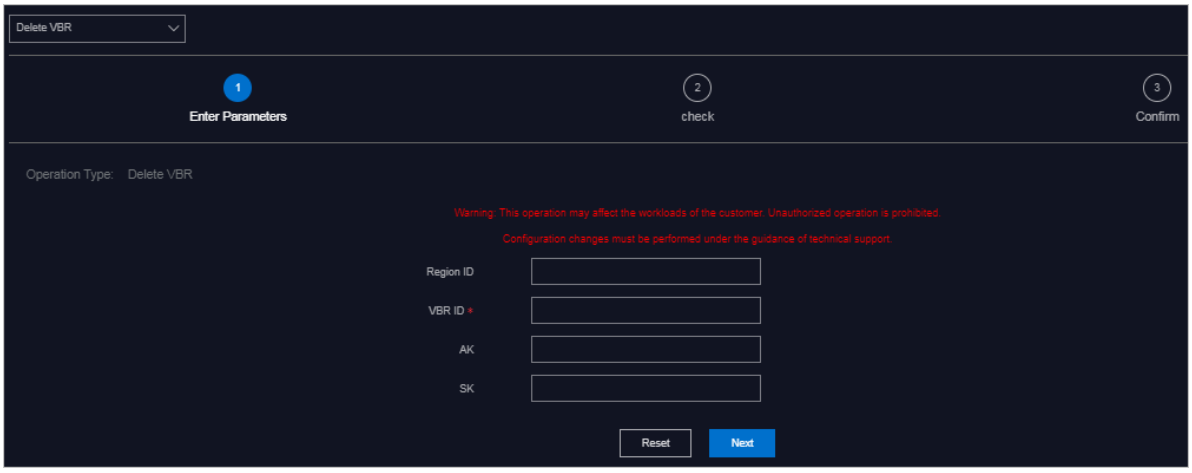
In O&M emergency scenarios, you can use this feature to delete a VBR.

Background information

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

Procedure

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



6. Configure the parameters described in the following table.

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

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

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

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

4.2.2.20.4.11. Delete a physical connection

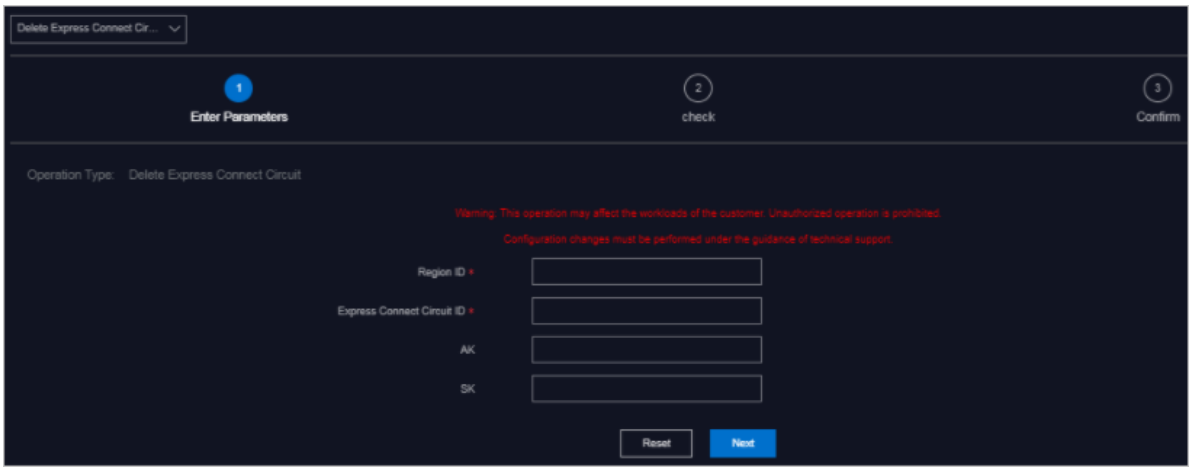
In O&M emergency scenarios, you can use this feature to delete a physical connection.

Background information

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

Procedure

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



6. Configure the parameters described in the following table.

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

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

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

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

4.2.2.20.4.12. Delete all resources

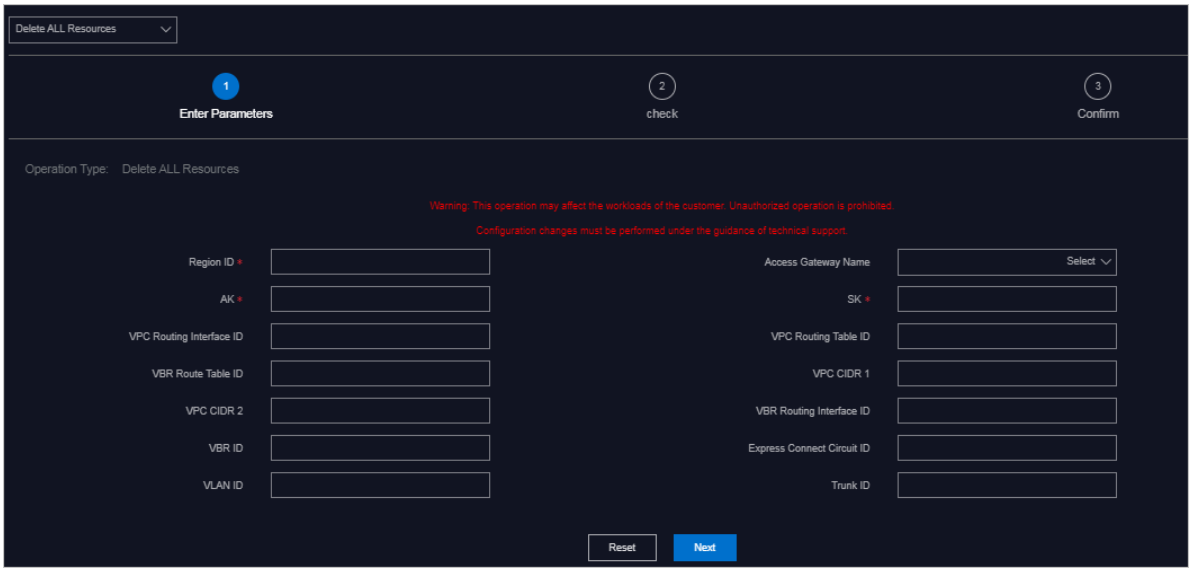
In O&M emergency scenarios, you can use this feature to delete all resources, including the VPC route table entries, VBR route table entries, VPC router interfaces, VBR router interfaces, VBRs, and physical connections.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. In the left-side drop-down list, select **Clear resources with one click**.



6. Configure the parameters described in the following table.

Parameter	Description
The region ID.	The ID of the region in the current environment.
The name of the CCN instance.	The name of the access gateway to which the bare metal instance is connected.
AK and **SK**	The AccessKey ID and AccessKey secret of the organization to which the VBR belongs, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console.
The ID of the VPC routing interface.	The VPC router interface ID, which can be obtained from the VPC console. For more information about how to obtain the router interface ID, see **VPC User Guide**.

VPC Routing Table ID	The VPC route table ID, which can be obtained from the VPC console. For more information about how to obtain the route table ID, see **VPC User Guide**.
VBR Routing Table ID	The VBR route table ID. If the bare metal instance involved with the VBR is added to the VPC, you can search for the bare metal instance on the **Bare Metal network management** tab based on the bare metal instance name, and click Details. The **VBR Route table ID** in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to the VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API operations** is **Add** on the **Operation History** tab. Click Details.The **VBR Route table ID** in the details is the value of this parameter.
CPC CIDR1	The destination CIDR block 1 to which the VPC points, which can be obtained from the VPC console. For more information about how to obtain the VPC CIDR block 1, see **VPC User Guide**.
VPC CIDR2	The destination CIDR block 2 to which the VPC points, which can be obtained from the VPC console. For more information about how to obtain the VPC CIDR block 2, see **VPC User Guide**.
The ID of the VBR route interface.	The VBR router interface ID. If the bare metal instance involved with the VBR is added to the VPC, you can search for the bare metal instance on the **Bare Metal network management** tab based on the bare metal instance name, and then click Details. The **VBR ID** in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API operations** is **Add** on the **Operation History** tab. Click Details. The **VBR ID** in the details is the value of this parameter.
VBR ID	The ID of the VBR to be deleted. On the**Operation History** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API operations** is **Add**. Click Details. The**VBR ID** in the details is the value of this parameter.
Physical line ID	The ID of the physical connection to be deleted. On the **Operation History** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API operations** is **Add**. Click Details. The **Physical line ID** in the details is the value of this parameter.
Trunk ID	You do not need to configure this parameter.

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

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

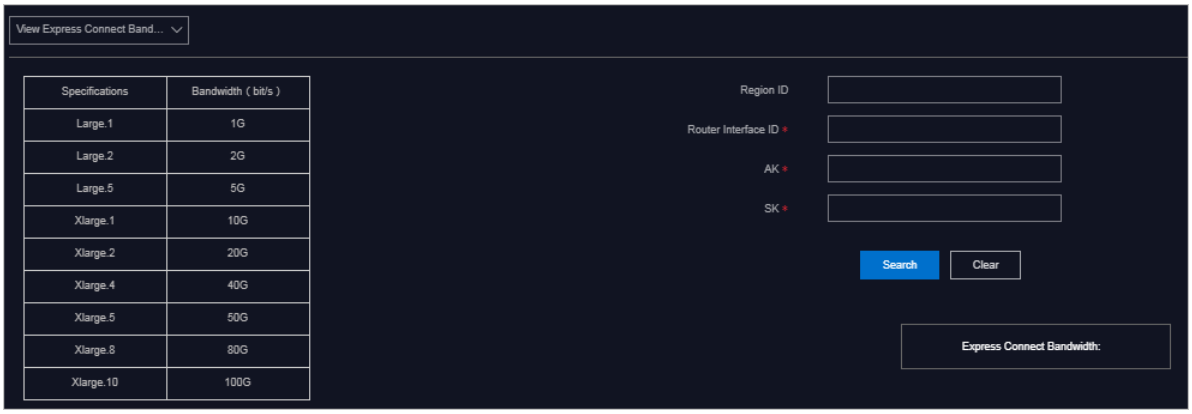
After the configurations are pushed, use the methods provided in Delete a VPC route table entry, Delete a VBR route table entry, Delete a VPC router interface, Delete a VBR router interface, Delete a VBR, and Delete a physical connection to check whether the VPC route table entries, VBR route table entries,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

4.2.2.20.4.13. View the leased line bandwidth

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

Procedure

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



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

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

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

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

4.2.2.20.4.14. Modify the physical connection bandwidth

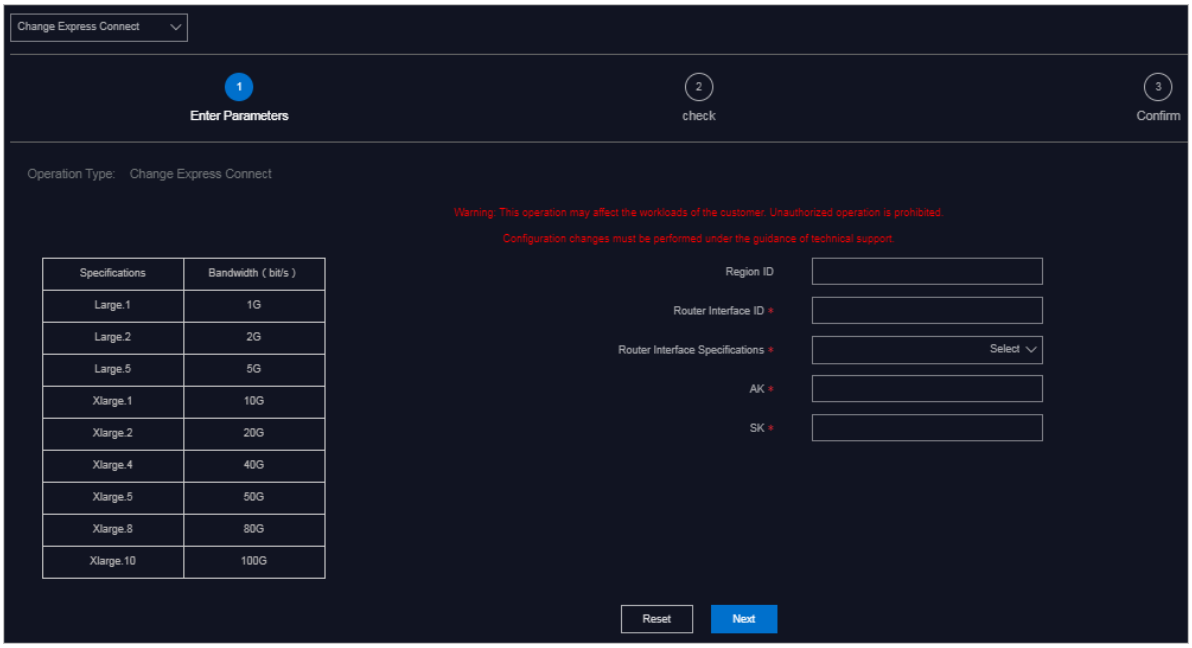
In O&M emergency scenarios, you can use this feature to modify the physical connection bandwidth.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. In the left-side drop-down list, select **Modify leased line broadband**.



6. Configure the parameters described in the following table.

Parameter	Description
The region ID.	The name of the region in the current environment.
Router interface ID	The ID of the router interface to which the physical connection bandwidth to be modified corresponds. On the **Bare Metal network management** tab, specify the VPC ID and access gateway name to search for the bare metal instance. Click Details. The **VBR ID** in the details is the value of this parameter.

Router interface specifications	The specification of the physical connection bandwidth.
AK and **SK**	The AccessKey ID and AccessKey secret of the organization to which the VPC belongs, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console.

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

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

   After the configurations are pushed, check whether the physical connection bandwidth is modified. For more information, see View the leased line bandwidth.

4.2.2.20.4.15. View BD usage

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

Procedure

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

4.2.2.20.4.16. View BM VPN usage

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

Procedure

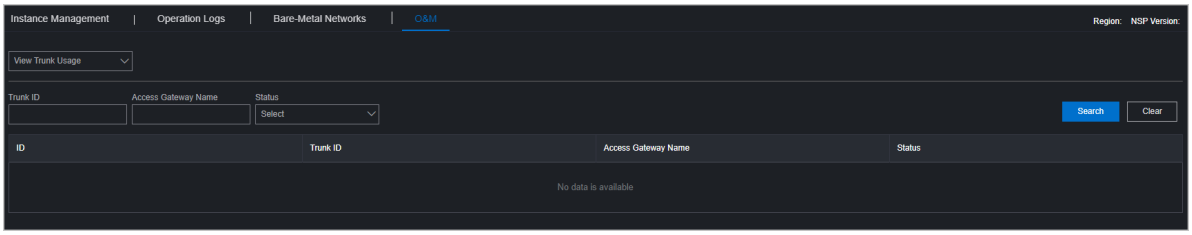
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O & M configuration** tab.
5. Select **View BMVPN usage** from the drop-down list in the upper-left corner.
6. Specify **Gateway name**, **vxlan id**, and **BM VPN name**, select a state from the **Select a status** drop-down list, and then click **Search** to view the BM VPNs assigned to all the HSW vSwitches.

4.2.2.20.4.17. View trunk usage

You can view trunk usage to obtain up-to-date information about the usage of hardware ports in a timely manner.

Procedure

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



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

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

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

4.2.2.21. Network security and protection

4.2.2.21.1. Border protection policies

The border protection policies are used to manage and maintain the matrix of interactions between the hybrid cloud platform and customers outside the cloud. The feature covers the matrix of services exposed by the cloud platform to outside the cloud and the matrix of services that are actively accessed by the cloud platform.

As the operations portal of the border security policies of the cloud platform, the border protection policy feature provides the following capabilities:

- Unified display and management of border interaction policies between the cloud platform and outside the cloud, including policies for services exposed by the cloud platform to outside the cloud and policies for outside resources that are actively accessed by the cloud platform. The displayed information includes related products, services, IP addresses, and ports. The information is used as input to policies when security protection is imposed on the border.
- Combined with the displayed border interaction policies and the cloud firewall product developed by Alibaba Cloud, the automatic issuance of border security policies for the cloud platform and the integrated management of cloud border security are realized.

The implementation location of border protection policies varies depending on the location where the cloud platform is connected to the customer network outside the cloud. Currently, the standard location where the cloud platform is connected to the customer network outside the cloud is CSW or ISW.

4.2.2.21.1.1. Inbound border protection policies for CSW

View inbound border protection policies on CSW

You can view inbound boundary protection policies on CSW, namely, the exposure matrix of the cloud platform to services outside the cloud.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > CSW**.
   The **Inbound** tab appears.
4. You can view all border protection policies for CSW. You can also filter border protection policies by using the following methods:
   - On the left side of the page, enter the destination protocol, select a status, and click **Search**.
   - On the right side of the page, click **Advanced**, enter more filter conditions, and then click **Search**.
5. In the **Actions** column of the border protection policy, click **Details**. In the panel that appears, view Basic Information, Destination Information, and Source Information of the policy.
   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Actions	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.
Status	The status of the protection policy on the firewall. Valid values: ◦ Issued ◦ NoIssued
Destination Cloud	The destination cloud that is defined in the policy. Valid value: ApsaraStack.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.

Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.
Destination IP Address	The destination IP address that is defined in the policy.
Destination Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Destination Port	The destination port that is defined in the policy.
Destination Name	The destination resource name that is defined in the policy.
Destination Type	The destination network type that is defined in the policy. Valid values: ◦ internet ◦ intranet
Destination BID	The destination network domain that is defined in the policy. Valid values: ◦ cloudops: operation domain. ◦ cloudbiz: business domain. ◦ cloudmgmt: management domain.
Source Cloud	The source cloud that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
SourceProduct	The source product that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Service	The source service that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Server Role	The source server role that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Application	The source application that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source IP Address	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.

6. Click **Refresh Policy** to refresh all policies.

Modify the inbound border protection policies on CSW

You can modify inbound boundary protection policies on CSW, namely, the exposure matrix of the cloud platform to services outside the cloud.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > CSW**.
   The **Inbound** tab appears.
4. In the **Actions** column of the border protection policy, click **Modify**. On the page that appears, modify parameters in Source Information and Operation Information, and click **Submit**.

   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Direction	Access direction between the cloud platform and outside. Valid values: ◦ Inbound: Access to the cloud platform from outside. ◦ Outbound: Active access from the cloud platform to outside. By default, the direction of inbound boundary protection policies on CSW is inbound and cannot be modified.
Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Source IP Address	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.
Destination Cloud	The destination cloud that is defined in the policy.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.
Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.

Destination Name	The destination resource name that is defined in the policy.
Destination Type	The destination network type that is defined in the policy. Valid values: ◦ internet ◦ intranet
Destination BID	The destination network domain that is defined in the policy. Valid values: ◦ cloudops: operation domain. ◦ cloudbiz: business domain. ◦ cloudmgmt: management domain.
Destination IP Address	The destination IP address that is defined in the policy.
Destination Port	The destination port that is defined in the policy.
Actions	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.

4.2.2.21.1.2. Outbound border protection policies for CSW

View outbound border protection policies on CSW

You can view the outbound boundary protection policies on CSW, namely, the service matrix for active outbound access by the cloud platform.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > CSW**.
4. Click the **Outbound** tab.
5. You can view all border protection policies for CSW. You can also filter border protection policies by using the following methods:
   - On the left side of the page, enter the destination protocol, select a status, and click **Search**.
   - On the right side of the page, click **Advanced**, enter more filter conditions, and then click **Search**.
6. In the **Actions** column of the border protection policy, click **Details**. In the panel that appears, view Basic Information, Source Information, and Source Destination of the policy.

The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Actions	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.
Status	The status of the protection policy on the firewall. Valid values: ◦ Issued ◦ NoIssued
Source IP Address	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.
Destination Cloud	The destination cloud that is defined in the policy. Valid value: ApsaraStack.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.
Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.
Destination IP Address	The destination IP address that is defined in the policy.
Destination Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Destination Port	The destination port that is defined in the policy.

7. Click **Refresh Policy** to refresh all policies.

Modify the outbound border protection policies on CSW

You can modify the outbound boundary protection policies on CSW, namely, the service matrix for active outbound access by the cloud platform.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > CSW**.
4. Click the **Outbound** tab.
5. In the **Actions** column of the border protection policy, click **Modify**. On the page that appears, modify parameters in Destination Information and Operation Information, and click **Submit**.

   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Direction	Access direction between the cloud platform and outside. Valid values: ◦ Inbound: Access to the cloud platform from outside. ◦ Outbound: Active access from the cloud platform to outside. By default, the direction of outbound boundary protection policies on CSW is outbound and cannot be modified.
Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Destination IP Address	The destination IP address that is defined in the policy.
Destination Port	The destination port that is defined in the policy.
Source Cloud	The source cloud that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
SourceProduct	The source product that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Service	The source service that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Server Role	The source server role that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Application	The source application that is defined in the policy. This parameter is not involved when the access source is outside the cloud.

Source IP Address	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.
Actions	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.

4.2.2.21.1.3. Inbound border protection policies for ISW

View outbound border protection policies on CSW

You can view inbound boundary protection policies on ISW, namely, the exposure matrix of the cloud platform to services outside the cloud.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > ISW**.
4. You can view all border protection policies for ISW. You can also filter border protection policies by using the following methods:
   - On the left side of the page, enter the destination protocol, select a status, and click **Search**.
   - On the right side of the page, click **Advanced**, enter more filter conditions, and then click **Search**.
5. In the **Actions** column of the border protection policy, click **Details**. In the panel that appears, view Basic Information, Destination Information, and Source Information of the policy.
   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Actions	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.

Status	The status of the protection policy on the firewall. Valid values: ◦ Issued ◦ NoIssued
Destination Cloud	The destination cloud that is defined in the policy. Valid value: ApsaraStack.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.
Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.
Destination IP Address	The destination IP address that is defined in the policy.
Destination Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Destination Port	The destination port that is defined in the policy.
Destination Name	The destination resource name that is defined in the policy.
Destination Type	The destination network type that is defined in the policy. Valid values: ◦ internet ◦ intranet
Destination BID	The destination network domain that is defined in the policy. Valid values: ◦ cloudops: operation domain. ◦ cloudbiz: business domain. ◦ cloudmgmt: management domain.
Source Cloud	The source cloud that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
SourceProduct	The source product that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Service	The source service that is defined in the policy. This parameter is not involved when the access source is outside the cloud.

Source Server Role	The source server role that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source Application	The source application that is defined in the policy. This parameter is not involved when the access source is outside the cloud.
Source IP Address	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.

6. Click **Refresh Policy** to refresh all policies.

Modify inbound border protection policies for ISW

You can modify inbound boundary protection policies on ISW, namely, the exposure matrix of the cloud platform to services outside the cloud.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > ISW**.
4. In the **Actions** column of the border protection policy, click **Edit**. In the panel that appears, modify the source information and operation, click **OK**.

   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Direction	The access direction between the cloud platform and outside. Valid values: ◦ Inbound: Access to the cloud platform from outside. ◦ Outbound: Active access from the cloud platform to outside. By default, the direction of inbound boundary protection policies on ISW is inbound and cannot be modified.
Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Source IP	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.

Destination Cloud	The destination cloud that is defined in the policy.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.
Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.
Destination Name	The destination resource name that is defined in the policy.
Destination Type	The destination network type that is defined in the policy. Valid values: ◦ internet ◦ intranet
Destination BID	The destination network domain that is defined in the policy. Valid values: ◦ cloudops: operation domain. ◦ cloudbiz: business domain. ◦ cloudmgmt: management domain.
Destination IP	The destination IP address that is defined in the policy.
Destination Port	The destination port that is defined in the policy.
Protection Action	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.

4.2.2.21.1.4. Outbound border protection policies for ISW

View outbound border protection policies on ISW

You can view outbound boundary protection policies on ISW, namely, the matrix of outside services accessed by the cloud platform.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations**

Console.

3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > ISW**.
4. Click the **Outbound** tab.
5. View all outbound border protection policies for ISW. You can also filter border protection policies by using the following methods:
   - On the left side of the page, enter the destination protocol, select a status, and click **Search**.
   - On the right side of the page, click **Advanced**, enter more filter conditions, and then click **Search**.
6. In the **Actions** column of the border protection policy, click **Details**. In the panel that appears, view Basic Information, Source Information, and Destination Information of the policy.
   The following table describes the parameters in the panel.

Parameter	Description
Location	The location of the protection policy.
Protection Action	The action that is defined in the protection policy. Valid values: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: checks the network status. After this option is selected, if any traffic matches the policy, the traffic exists in the network.
Status	The status of the protection policy on the firewall. Valid values: ◦ Issued ◦ NoIssued
Source IP	The source IP address that is defined in the policy.
Source Port	The source port that is defined in the policy.
Destination Cloud	The destination cloud that is defined in the policy. Valid value: ApsaraStack.
Destination Product	The destination product that is defined in the policy.
Destination Service	The destination service that is defined in the policy.
Destination Server Role	The destination server role that is defined in the policy.
Destination Application	The destination application that is defined in the policy.
Destination IP	The destination IP address that is defined in the policy.

Destination Protocol	The destination protocol that is defined in the policy. ◦ TCP ◦ UDP
Destination Port	The destination port that is defined in the policy.

7. Click **Refresh Policy** to refresh all policies.

Modify the outbound border protection policies on ISW

You can modify the outbound boundary protection policies on ISW, namely, the service matrix for active outbound access by the cloud platform.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Border Protection Policies > ISW**.
4. Click the **Outbound** tab.
5. In the **Actions** column of the border protection policy, click **Modify**. On the page that appears, modify parameters in Destination Information and Operation Information, and click **Submit**.

   The following table describes the parameters on the page.

Parameter	Description
Location	The location of the protection policy.
Direction	Access direction between the cloud platform and outside. Valid values: ◦ Inbound: Access to the cloud platform from outside. ◦ Outbound: Active access from the cloud platform to outside. By default, the direction of outbound boundary protection policies on ISW is outbound and cannot be modified.
Protocol	The protocol of the policy destination: ◦ TCP ◦ UDP
Destination IP Address	The IP address of the policy destination:
Destination Port	The port opened the policy destination
Source Cloud	The policy source type (not available when the access source is outside the cloud)
SourceProduct	The product of the policy source (not available when the access source is outside the cloud)

Source Service	The service of the policy source (not available when the access source is outside the cloud)
Source Server Role	The service role of the policy source (not available when the access source is outside the cloud)
Source Application	The application of the policy source (not available when the access source is outside the cloud)
Source IP Address	The IP address of the policy source
Source Port	The port opened for the policy source
Actions	The action defined in the protection policy: ◦ Allow: allows the traffic. ◦ Deny: denies the traffic. ◦ Check: check the network status. After this option is selected, if traffic matches this policy, the traffic exists in the network.

4.2.2.21.2. SRS

Security Reinforce Service (SRS) is a security hardening component for internal access of cloud services that are deployed on Apsara Infrastructure Management. The Apsara Uni-manager Operations Console provides an entry point for SRS.

SRS provides security isolation. SRS allows you to configure the SRS security isolation status, service persistence upon network disconnections, SRS IP address whitelist, SRS IP address blacklist, isolation-free products, SRS bypass baseline, SRS VIPS information, dynamic allow settings, and baseline allow settings, and view the IP address whitelist in the cloud, audit logs, client status, and packet loss dashboard.

4.2.2.21.2.1. SRS management

SRS provides security isolation capabilities for the hybrid cloud platform instead of for tenants. The capabilities are invisible to users. Therefore, contact Alibaba Cloud engineers to perform SRS-related operations, especially the operation to enable SRS security isolation. Otherwise, service interruptions may occur. SRS security isolation can be disabled at any time. Each time SRS security isolation is enabled, the impact is the same. Each time SRS security isolation is disabled, the impact is the same.

You can configure the SRS security isolation status, service persistence upon network disconnections, SRS IP address whitelist, SRS IP address blacklist, isolation-free products, SRS bypass baseline, SRS VIPs, and view the IP address whitelist in the cloud and audit logs.

Configuration management

Enable SRS security isolation

In DEBUG mode, you can enable SRS security isolation when the clients no longer generate unexpected packet loss.

Prerequisites

> ⚠ **Warning** Before you enable SRS security isolation, check the following requirements are met. If one of the requirements is not met, your business may be impacted after you enable SRS security isolation. We recommend that you enable the DEBUG mode before you enable SRS security isolation.

- SRS has reached the desired state.
- All products have reached the desired state.
- The upstream products have been deployed and have reached the desired state.
  - Skyline (baseServiceAll): centralized deployment in multiple regions.
  - Networkbase (baseServiceAll): unitized deployment in multiple regions.
  - Metadatasync (baseServiceAll): centralized deployment in multiple regions.
- SRS runs dependencies stably. Otherwise, stability risks may occur.
  - Version requirements:
    - The version of Apsara Stack Enterprise Edition for all products must be the same as that of the Apsara Infrastructure Management console.
    - In multi-region scenarios, the version of all regions must be the same as that of the Apsara Infrastructure Management console.
    - In the zone-disaster recovery scenario, Apsara Stack Enterprise Edition and the SRS version must be consistent in the primary and secondary data centers.
  - Networkbase cannot collect IP addresses of some network devices (ISW, DSW, or LSW) of V3.13.0 or earlier versions. Make sure that Networkbase can collect IP addresses of your network devices (ISW, DSW, or LSW).
- SRS runs dependencies normally. Otherwise, SRS features may be partially or completely unavailable, but no stability risks will occur.
  - The upstream products and services, including Apsara Uni-manager Operations console, Apsara Infrastructure Management console, Networkbase, Metadatasync, Skyline, and Hostservice, run as expected.
  - The OSs of the master and client run normally.
  - The version of AliOS7U is 4.19 and the version of the Linux kernel is 3.10.
  - The kernel module slb-kernel-modules or kernel-modules-ctk is installed.
- For scenarios where existing sites are upgraded to the current version, you must enable SRS security isolation after the evaluation by an architect of Apsara Uni-manager Management console, because the networks of existing sites may involve various non-standard scenarios.
- You must disable SRS security isolation before you perform any O&M operations that involve changes of IP addresses or service deployment patterns, including but not limited to upgrade, scale-out, and migration. After the changes are complete, you need to confirm that SRS has obtained the latest isolation configuration data of products from Apsara Infrastructure Management.

Background information

SRS sets security rules for the service ports on the cloud platform, and manages the internal VIPs. After SRS security isolation is enabled, if traffic exceptions occur, disable SRS security isolation at the earliest opportunity. Traffic exceptions include but are not limited to:

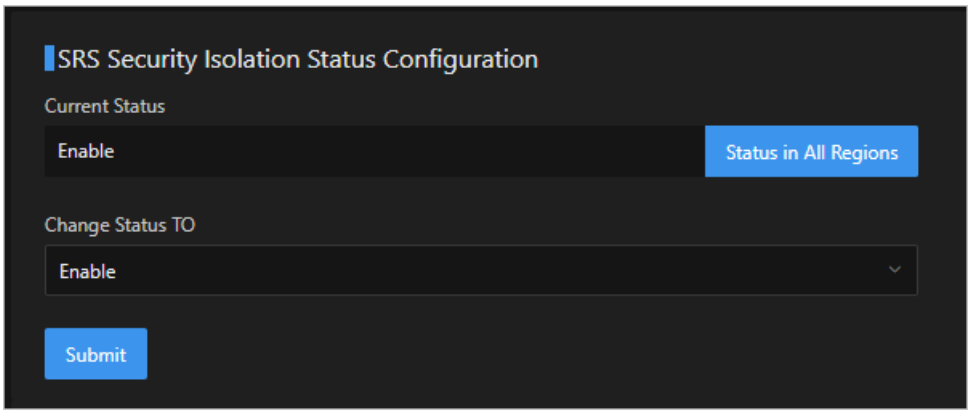
- A service port or management domain VIP on the cloud platform cannot be accessed but can be pinged. Disable SRS security isolation and troubleshoot issues.
- The **Packet Loss Dashboard** tab of SRS displays a large number of lost packets with valid IP addresses in the cloud. Disable SRS security isolation and troubleshoot issues.

> **Note** The issues of tenant-side access to cloud products, for example, through public VIPs, business domain VIPs, and operation domain VIPs, are not related to SRS.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS Security Isolation Status Configuration** section, view the SRS security isolation status.

   The **Current Status** field shows the current SRS security isolation status. Click **Status in All Regions** to view the SRS security isolation status of all nodes in the dialog box that appears.



5. Set **Change Status TO** to **Enable**, and click **Submit**. In the dialog box that appears, click **OK**.

> **Warning** Strict conditions are required for enabling SRS security isolation. For more information, see **Prerequisites**. Contact Alibaba Cloud O&M engineers for evaluation before you enable SRS security isolation. Otherwise, the business traffic may be interrupted.

Disable SRS security isolation

You must disable SRS security isolation before you perform any operations that involve changes of IP addresses and service deployment forms.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Background information

The following list describes scenarios where SRS security isolation must be disabled:

- SRS security isolation must be disabled before you perform any operations that involve changes of IP address and service deployment forms, including but not limited to upgrade, scale-out, and migration. After a change is complete, make sure that SRS has obtained the latest IP address and service deployment form.
- You must disable SRS security isolation and troubleshoot issues when a service port or

management domain VIP on the cloud platform cannot be accessed but echo reply messages are returned.

- You must disable SRS security isolation and troubleshoot issues when the **Packet Loss Dashboard** tab of SRS displays a large number of lost packets with valid IP addresses in the cloud.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS Security Isolation Status Configuration** section, select **Close** from the **Change Status TO** drop-down list and click **Submit**. In the message that appears, click **OK**.

> ⚠ **Warning**
> - After SRS security isolation is disabled, the cloud service ports that are originally protected by SRS may be detected and scanned by devices outside the cloud.
> - By default, SRS security isolation is disabled. You can change it to Enable or DEBUG Mode. We recommend that you do not frequently change SRS isolation status. You can change SRS security isolation status 10 minutes after you change it.
> - SRS uses the unit deployment method. To disable SRS for the entire cloud instance, you must disable SRS for each region.
> - You can disable SRS in the following ways:
>   - General scenarios: Disable SRS for the current region.
>   - Multi-region scenarios: Disable SRS for the current region, SRS for the central region, and SRS for the associated regions. Then, wait for a maximum of 10 minutes for the disabling operation to complete. Then, start O&M tasks.

Enable the DEBUG mode

DEBUG mode is equivalent to the half-enabled state. The involved traffic is recorded, but not actually isolated. If you want to test the isolated traffic, you can enable the DEBUG mode.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS Security Isolation Status Configuration** section, select **DEBUG Mode** from the **Change Status TO** drop-down list and click **Submit**. In the message that appears,

click **OK**.

> ⚠ **Warning** You can change the status from DEBUG Mode to close. You can change the status from DEBUG Mode to Enable only if no packet loss occurs or the packet loss is within the expected range. We recommend that you do not frequently change the SRS security isolation status. You can change the SRS security isolation status again 10 minutes after you change it.

Configure disconnection hold

In the scenario where the network of the general region and the central region is disconnected, SRS cannot obtain the latest rules from the central region and will delete security rules. If you want SRS to continue to provide security protection, you can enable the disconnection hold feature to distribute rules from each region to SRS.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Background information

When the network of the general region and the central region is disconnected, the rules of the general region is old after you enable the disconnection hold feature. If other general regions or central regions are expanded with IP addresses, the new IP addresses cannot access the general region. Therefore, you must fully evaluate the possible impact of the disconnection hold feature. Otherwise, the service traffic may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **Whether Enable SRS Disconnection Hold** section, turn on or off the **Status** switch.

> ⓘ **Important** By default, the disconnection hold feature is disabled. In this case, if the network of the general region and the central region is disconnected, the rules cannot be synchronized to SRS. As a result, the timestamp expires and all rules are cleared.

Configure an SRS IP whitelist

SRS only trusts internal IP addresses. After SRS is enabled, public IP addresses cannot access the services on the cloud that are connected to SRS over the classic network of the base for security isolation. You can add the public IP addresses allowed to access the services to an SRS IP whitelist.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

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

2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS IP Address Whitelist Configuration** section, add or delete an SRS IP whitelist.
   - Add an SRS IP whitelist: Click **Add**. In the dialog box that appears, enter one or more IP addresses. Separate multiple IP addresses with commas (,). Click **OK**.
   - Delete an SRS IP whitelist: Click Expand. In the Actions column, click **Delete**. In the message that appears, click **OK**.

Configure an SRS IP blacklist

You can add IP addresses that have been identified as illegal to the IP blacklist. The IP addresses cannot access any products or services in the cloud after being added to the blacklist.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Background information

- SRS does not further detect IP addresses in the blacklist to prevent the occupation of platform resources.
- IP addresses in the blacklist are not recorded in the packet loss logs or displayed in the alert dashboard.

> ⓘ **Important** If an IP address exists in both the blacklist and the whitelist, the blacklist rule take effect, and the whitelist rule is ignored.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS IP Address Blacklist Configuration** section, add or delete an SRS IP blacklist.

   > ⚠ **Warning** IP addresses added to the IP blacklist cannot access any products or services in the cloud. Proceed with caution.

   - Add an SRS IP blacklist: Click **Add**. In the dialog box that appears, enter one or more IP addresses. Separate multiple IP addresses with commas (,). Click **OK**.
   - Delete an SRS IP blacklist: Click **Expand**. In the **Actions** column, click **Delete**. In the message that appears, click **OK**.

Add isolation-free products

If you do not want a product that is connected to SRS for security isolation to be protected by SRS, you can add an isolation-free product.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS Isolation-free Product Configuration** section, add or delete an isolation-free product.
   - Add an isolation-free product: Click **Add**. In the dialog box that appears, enter one or more product names. Separate multiple product names with commas (,). Click **OK**.
   - Delete an isolation-free product: Click **Expand**. In the **Actions** column, click **Delete**. In the message that appears, click **OK**.

Configure the SRS bypass baseline

The products in the baseline allow list are not isolated. If you want to isolate products that are in the list, you can configure the SRS bypass baseline.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. In the **SRS Bypass Baseline Settings** section, add a product for isolation or delete an isolated product.
   - Add an isolation-free product: Click **Add**. In the dialog box that appears, enter one or more product names. Separate multiple product names with commas (,). Click **OK**.
   - Delete an isolation-free product: Click **Expand**. In the **Actions** column, click **Delete**. In the message that appears, click **OK**.

Data management

View the IP address whitelist in the cloud

After SRS isolation is enabled, external IP addresses cannot access the services in the cloud that are connected to SRS over the classic network of the base for security isolation. Only IP addresses in the whitelist can access the services. You can view the initial whitelist configured by SRS that the product applied for from the Apsara Infrastructure Operations console.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Background information

The IP addresses in the initial whitelist configured by SRS that the product applied for from the Apsara Infrastructure Operations console can be modified only in the Apsara Infrastructure Management console, and cannot be modified in SRS.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. Click the **Data Management** tab.
5. In the **IP Address Whitelist** section, click the domain name to view related IP addresses in the whitelist.

Configure SRS VIPs

You can view SRS VIPs and modify the VIP forwarding mode.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. Click the **Data Management** tab.
5. In the **SRS VIPS Information** section, view all managed VIP information. You can also enter the SR information and click **Search** to view the VIP information of a specified SR.

   > **Note** Do not include the number sign (#) in the SR information.

6. Find the VIP information that you want to modify and click **Modify** in the **Actions** column. In the dialog box that appears, select the desired forwarding mode and click **OK**.

   After the forwarding mode is modified, wait for about 5 minutes, and click the icon in the upper-right corner to view the refreshed VIP information in the list. If there are a great number of VIPs to be refreshed, it takes a longer period of time.

> **Note** Currently, the VIP forwarding mode supports only NAT, including FNAT and DNAT. The VIP forwarding mode that you set is used as the default forwarding mode. The NAT mode is forcibly switched to FNAT instead of the specified mode in the following scenarios:
>
> - The SRS isolation is disabled or in the debug mode.
> - The physical machine that corresponds to the VIP does not have a CTK module or the CTK module version is incorrect.
> - An internal problem occurs in SRS, causing the timestamp to expire.
>
> If the NAT mode of all VIPs are switched to FNAT and SRS isolation is enabled, contact Alibaba Cloud technical support.

Refresh SRS isolation settings

If SRS isolation settings are not distributed because the server cache is not updated, you can use this feature to refresh the cache.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. Click the **Data Management** tab.
5. **Required:**Click **Refresh SRS Isolation Settings**to refresh existing SRS isolation settings in the server cache.

View audit logs

You can view records of historical SRS operations for auditing after misoperations.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > SRS Management**.
   The **Configuration Management** tab appears.
4. Click the **Audit Logs** tab.
5. View historical SRS operation information in the list, including the API operation, operator, request method, data, and operation time.
   You can also enter an API operation name and operator name, and click **Search** to query the audit logs.

4.2.2.21.2.2. Isolation configuration management

SRS allows products that do not need to be isolated. The allow rules include baseline allow rules and dynamic allow rules. You can view baseline allow rules and dynamic allow rules, and configure dynamic allow rules.

The following list describes baseline allow rules and dynamic allow rules.

- Baseline allow rules: allow rules initially defined for products that SRS obtains from Apsara Infrastructure Management. The rules cannot be configured on SRS.
- Dynamic allow rules: allow rules of products that can be configured on SRS.

View dynamic allow settings

You can view dynamic allow rules that are configured for products in SRS.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > Isolation Configuration Management**.
   The **Dynamic Allow Settings** tab appears.
4. View the configured dynamic allow rules in the list. You can also enter SR information and click **Search** to view the dynamic allow rules of a specified SR.

Add dynamic allow settings

You can add dynamic allow rules for products in SRS.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

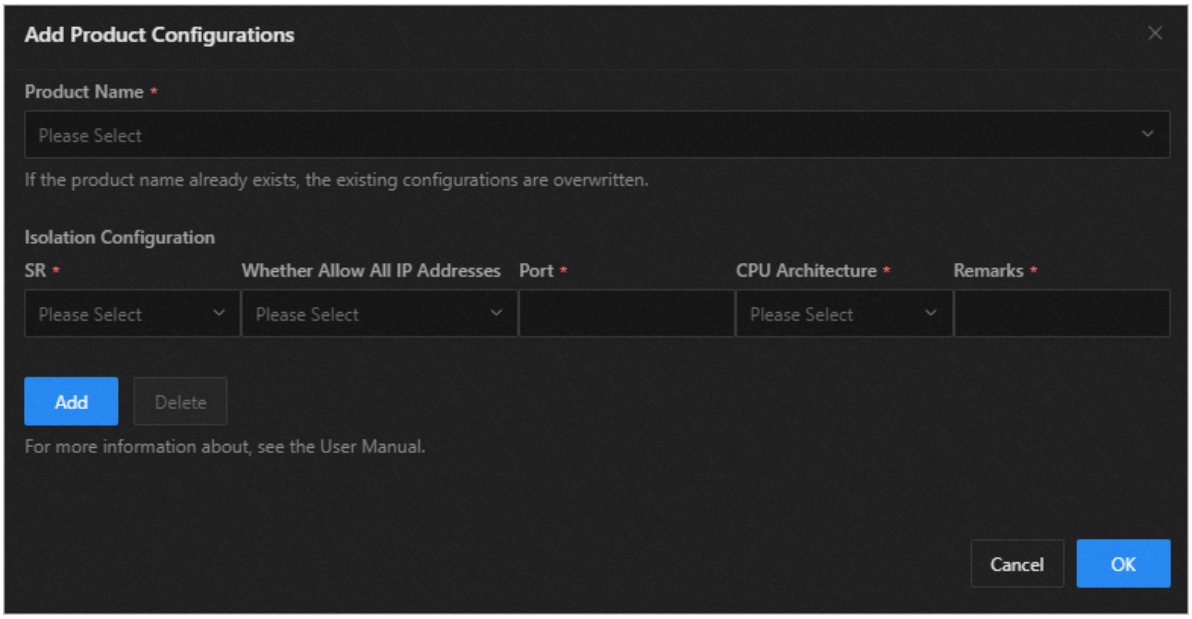
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > Isolation Configuration Management**.

   The **Dynamic Allow Settings** tab appears.

   > ⚠ **Warning** Adding dynamic allow settings is a high-risk operation. You must carefully evaluate the impacts. Do not perform the operation unless necessary.

4. Click **Add Dynamic Allow Settings**. In the dialog box that appears, set the parameters and click **OK**.

   To add multiple SR configurations, click **Add**, set the parameters, and click **OK**.



> **Note**
> - You can click **Delete** to delete a dynamic allow configuration for the product.
> - If the new product name and SR are the same as those in an existing configuration, the existing configuration is overwritten.
> - If the product name and SR are the same as those in the configuration where the Remarks is "ASRDR Rule, DO NOT delete!", the configuration is not overwritten. The configuration applies to products required by Apsara Stack Resilience for Disaster Recovery.

The following table describes the parameters.

Parameter	Description
Product Name	The name of the cloud product to which the dynamic allow configuration applies.
SR	The server role to which the dynamic allow configuration applies.
Whether Allow All IP Addresses	Valid values: ◦ Yes: allowes all IP addresses of physical machines that belong to the SR. ◦ No: does not allow all IP addresses of physical machines that belong to the SR.

Parameter	Description
Port	The value consists of two parts, the protocol and the port number, which are separated by a colon (:). The two parts conform to the following requirements: ◦ Protocol: ▪ Valid values are TCP and UDP in uppercase. ▪ If both protocols are used, separate them with a semicolon (;).The order of the protocols makes no difference. ◦ Port number: ▪ The port number cannot be empty. ▪ A single number indicates that one port is open. For example, 80 indicates that port 80 is open. ▪ Number-number (port range) indicates that ports with a closed interval are open. For example, 10-8000 indicates that ports 10 to 8000 are open. The preceding number must be smaller than or equal to the following number. If the two numbers are equal, they are considered one port. ▪ Separate multiple port ranges with commas (,). ▪ Valid values: 0 to 65535. ▪ Port ranges can be repeated or overlapped. **Important** Other characters are invalid. The following examples show valid values of Port. ◦ TCP:10 ◦ UDP:40-90 ◦ TCP:10,20-30 ◦ UDP:20,20,20-20;TCP:0-65535 ◦ TCP:10-10,20-40,30-50;UDP:30-50,20-40,30-30,10-60
CPU architecture	The CPU architecture. Valid values: ◦ x86_64 ◦ aarch64
Remarks	The remarks for the configuration.

Delete dynamic allow settings

You can delete dynamic allow rules for products from SRS.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Management & Protection > SRS Management > Isolation Configuration Management**.
   The **Dynamic Allow Settings** tab appears.

   > ⚠ **Warning**
   > - Deleting dynamic allow settings is a high-risk operation. You must carefully evaluate the impacts. Do not perform the operation unless necessary.
   > - Do not delete the rules where the Remarks is "ASRDR Rule, DO NOT delete!", which apply to products required by Apsara Stack Resilience for Disaster Recovery. If the rules are deleted, some features of Apsara Stack Resilience for Disaster Recovery may be unavailable.

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

View the baseline allow rules

You can view the baseline allow rules of each product in SRS, namely, the allow rules initially defined for each product that SRS obtained from Apsara Infrastructure Management.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > Isolation Configuration Management**.
   The **Dynamic Allow Settings** tab appears.
4. Click the **Baseline Allow List** tab.
5. You can view the baseline allow rules of a product in the list, including the product name, service, SR, port, CPU architecture, and operation time.

4.2.2.21.2.3. Client status

View client status

You can view the status of SRS clients.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > Client Status**.
   The **Clients** tab appears.
4. View the status of SRS clients.

   > **Note** You can enter Hostname, and select **Only Packet Loss Host** to filter client information.

   The following table describes the parameters.

Parameter	Description
Hostname	The name of the cloud host where the SRS client is deployed.
cpu_arch	The CPU architecture of the physical machine where the client resides.
version	The version of the client.
RPM Version	The version of the RPM package that is installed on the client.
CTK Loading Status	The CTK module loading status of the client.
Logs	The latest log that is reported by the client.
Packet Loss Logs	The packet loss log of the client, which contains information about packets intercepted by SRS.
Operation At	The time when the latest log was reported by the client.

5. In the **Packet Loss Logs** column of the target client, click the icon. In the dialog box that appears, view the information about packets that are intercepted by SRS, including Source IP Address, Access Method, Destination IP Address, Port, SR, Drop Interval, and Packet Loss Events.

View the packet loss dashboard

If isolation rules are configured for SRS, unexpected connections generate packet loss. You can view the packet loss host, project, service, and SR.

Prerequisites

- SRS has reached the desired state.
- All products have reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, choose **Network Security & Protection > SRS Management > Client Status**.
   By default, the **Clients** tab appears.
4. Click the **Packet Loss Dashboard** tab.
5. View information about the packet loss host, project, service, and SR.
   You can also enter the SR information in the search box and click **Search** to view the packet loss information of the SR.

> **Note** Do not include the number sign (#) in the SR information.

4.2.2.21.3. Donghuangzhong

Donghuangzhong is a security hardening tool for cloud products based on PaaS. It isolates cloud products from networks outside the cloud platform and protects the cloud platform together with SRS on Apsara Infrastructure Management.

The networks protected by Donghuangzhong include the Kubernetes cluster host networks and container networks managed by the PaaS platform, and the management domain VIPs applied by the PaaS platform. By default, the protection for Kubernetes cluster container networks is enabled and cannot be disabled.

4.2.2.21.3.1. Donghuangzhong configuration

Host network isolation

You can enable or disable the host network isolation feature to control whether the Kubernetes cluster host network managed by the PaaS in the cloud platform can be accessed from outside the cloud platform.

Background information

- By default, the host network isolation feature is disabled, and the Kubernetes cluster host network managed by the PaaS in the cloud platform can be accessed from outside the cloud platform.
- Host network isolation takes effect only for Kubernetes nodes managed by the PaaS. Non-Kubernetes node networks managed by Apsara Infrastructure Management of the cloud platform are protected by SRS.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > Donghuangzhong Settings**.

> ⚠ **Warning** Enabling host network isolation is a high-risk operation. After the feature is enabled, the host network of Kubernetes nodes managed by the PaaS is isolated from outside the cloud platform and only port 22 is open for outside the cloud platform. Therefore, ports opened by some hosts may be inaccessible from outside the cloud platform.
>
> You can use the debugging log feature of the node to analyze the network traffic of accesses to the host from outside the cloud platform, and determine whether to enable the host network isolation feature.

4. Turn on or off **Host Network isolation** in the upper-left corner. In the dialog box that appears, click **OK** to enable or disable the host network isolation feature.

Whitelist CIDR block configuration

By default, the network in the cloud platform is isolated from outside the cloud platform. If you want to allow CIDR blocks outside the cloud platform, you can add the CIDR blocks to the whitelist.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > Donghuangzhong Settings**.
4. In the **Whitelist CIDR block configuration** section, view CIDR blocks, add CIDR blocks to the whitelist, or delete CIDR blocks from the whitelist.
   - View CIDR blocks: View the configured CIDR blocks in the whitelist.
   - Add CIDR blocks to the whitelist: Click **Add**. In the dialog box that appears, enter a CIDR block and click **OK**.
   - Delete CIDR blocks from the whitelist: In the **Operation** column, click **Delete**. In the message that appears, click **OK**.

Host allow port configuration

By default, the host network only allows port 22 for networks outside the cloud platform. To allow other ports, perform the following steps.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > Donghuangzhong Settings**.
4. In the **Host allow port configuration** section, view, add, modify, or delete host allow ports.
   - View host allow ports: view the information about the ports that are allowed for the host.
   - Add host allow ports: Click **Add**. In the dialog box that appears, specify the start port number, end port number, protocol, and nodes, and then click **OK**.
   - Modify host allow ports: In the **Operation** column, click **Modify**. In the dialog box that appears, modify the parameters and click **OK**.
   - Delete host allow ports: In the **Operation** column, click **Delete**. In the message that appears, click **OK**.

4.2.2.21.3.2. Node debugging logs

You can view the requests of hosts outside the cloud platform accessing to the host network in the cloud platform to determine whether to enable host network isolation. If host network isolation is enabled, the network traffic that is viewed is denied.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations**

Console.

3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > Node Debugging Logs**.
4. Turn on or off**Observation mode**.
   - Enable: Turn on **Observation mode** in the upper-left corner. In the dialog box that appears, click **OK**. You can view the previous and subsequent requests of hosts outside the cloud platform accessing to the host network in the cloud platform.
   - Disable: Turn off **Observation mode** in the upper-left corner. In the dialog box that appears, click **OK**. You cannot view subsequent requests of hosts outside the cloud platform accessing to the host network in the cloud platform.
5. Use one of the following methods to view requests of hosts outside the cloud platform accessing to the host network in the cloud platform:
   - Specify a start time and an end time, and click **Search**.
   - Click **Advanced**, enter more filter conditions, and then click **Search**.

   > **Note** The list displays aggregated requests of hosts outside the cloud platform accessing to the host network in the cloud platform. If you want to view the unaggregated data, see **Unaggregated Details**.
6. Find the request and click **Unaggregated Details** in the **Operation** column. In the dialog box that appears, view the unaggregated requests of hosts outside the cloud platform accessing to the host network in the cloud platform.

4.2.2.21.3.3. VIP list

Virtual IP addresses (VIPs) of the management domain are used for mutual access within cloud products and are not used for accessing outside the cloud platform. Donghuangzhong protects VIPs of the management domain. The protection takes effect only when the VIP mode of the management domain is dnat. You can view the VIPs of all management domains that you applied in the PaaS.

Background information

By default, the VIP mode of a management domain is auto. You do not need to configure it. If the VIP mode is auto:

- If all the CTK modules on the host of the cloud platform are loaded, the system forcibly sets the VIP of the management domain to dnat.
- If some of the CTK modules on the host of the cloud platform fail to be loaded, the system forcibly sets the VIP mode of the management domain to fullnat.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > VIPs**.
4. You can view the VIPs of all management domains. You can also select the VIPs of the management domain and click **OK**.
   The following table describes the parameters.

Parameter	Description

Product	The name of the cloud service.
ClusterInstance	An application model of the PaaS, which corresponds to the cluster of the Apsara Infrastructure Management console.
AppInstance	An application model of the PaaS, which corresponds to the chart instance.
namespace	Kubernetes namespace
service name	The name of the service in Kubernetes.
vip address	The VIP of the management domain applied for by the cloud products deployed on the PaaS.
bid	The attribute for isolating VIPs from the classic network, VPCs, and the Internet. Valid values: cloudbiz (business domain), cloudops (operation domain), and cloudmgmt (management domain).
Forwarding mode	The forwarding model of VIPs. Valid values for the management domain: ◦ fullnat: corresponds to fullnat of the VIP mode. ◦ dnat: corresponds to dnat of the VIP mode. ◦ auto: automatically sets the VIP mode based on the current environment. In normal cases, the value is dnat. In abnormal cases, the value is fullnat.

4.2.2.21.3.4. CIDR block whitelist

You can view the whitelist of all CIDR blocks in the cloud platform to check whether a specific IP address is in the whitelist.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, choose **Network Security & Protection > Donghuangzhong > CIDR Block Whitelist**.
4. View the whitelist.
5. In the upper-left corner, enter an IP address in the search bar and click **Check**.
   - If the message **The IP address is not in the cloud platform whitelist** appears, the IP address is not in the cloud platform whitelist.
   - If the message **The IP address is not included in the cloud platform whitelist** does not appear, the IP address is in the cloud platform whitelist.

4.2.2.22. Hybrid cloud resources

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

4.2.2.22.1. Physical topology

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

Background information

You can view the following types of physical network topologies:

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

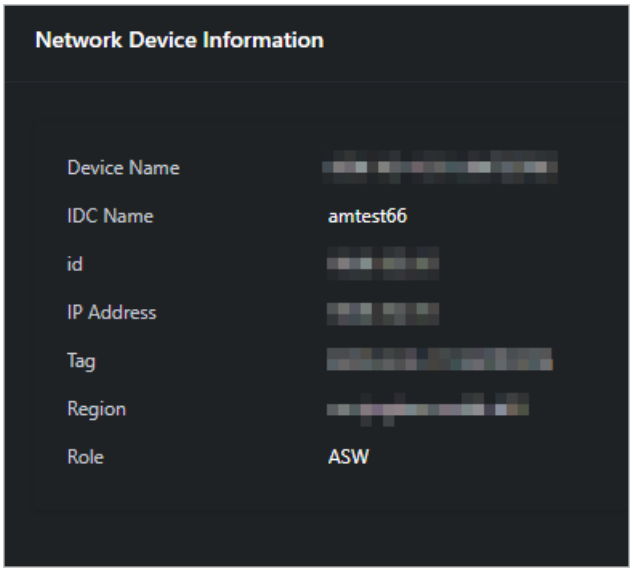
Procedure

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

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

> **Note** Action icons:
>
> - : proceeds with the next step.
> - : goes back to the previous step.
> - : zooms in.
> - : zooms out.
> - : scales in proportion to the original aspect ratio.
> - : scales to fit canvas.

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



iii. **Optional:**Click **Reset** to clear the search conditions.

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

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

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

The following table describes the parameters.

Parameter	Description
in_discard	The inbound packet loss rate.
out_discard	The outbound packet loss rate.
in_pps	The inbound packet forwarding rate.
out_pps	The outbound packet forwarding rate.
in_bps	The inbound byte rate.
out_bps	The outbound byte rate.
in_error	The inbound packet error rate.
out_error	The outbound packet error rate.

ii. **Optional:**Click **Reset** to clear the search conditions.

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

4.2.2.22.2. Network element management

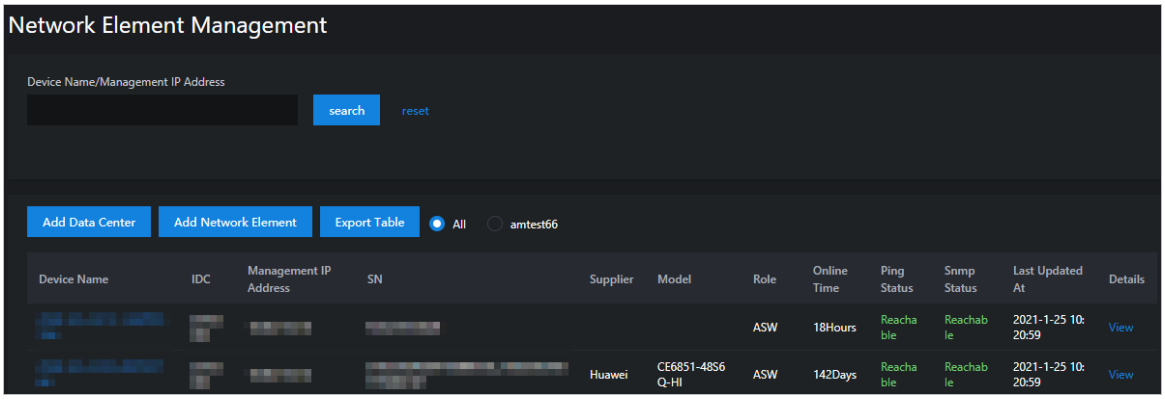
You can manage Apsara Stack data centers and user-managed data centers as well as their network element devices on the Network Element Management page.

Procedure

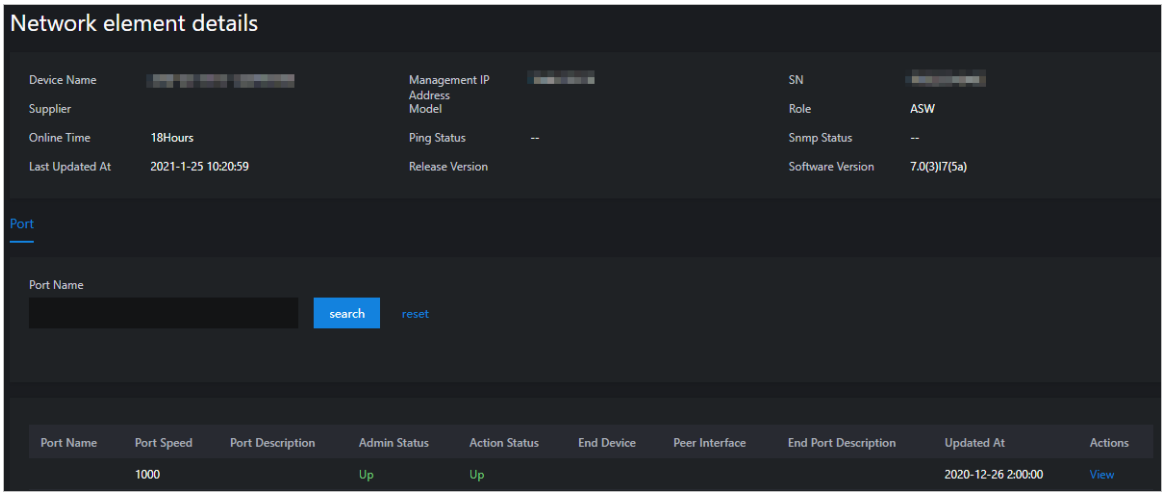
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, choose **Hybrid Cloud Resources > Network Element Management**. On the **Network Element Management** page, view the details of the network element devices.
   i. Enter a keyword in the **Device Name/Management IP Address** search box and click **Search** to view the information about the network element device.

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



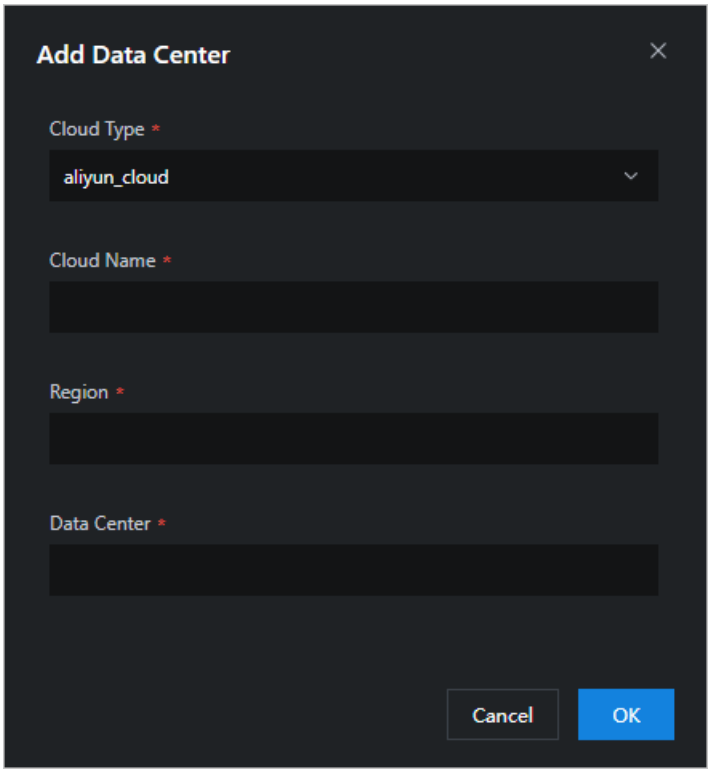
   ii. Find the desired device and click **View** in the **Details** column.
   iii. On the **Network element details** page, enter a port name in the **Port Name** search box and click **Search** to view the port information.



   iv. Find the port that you want to view and click **View** in the **Actions** column.

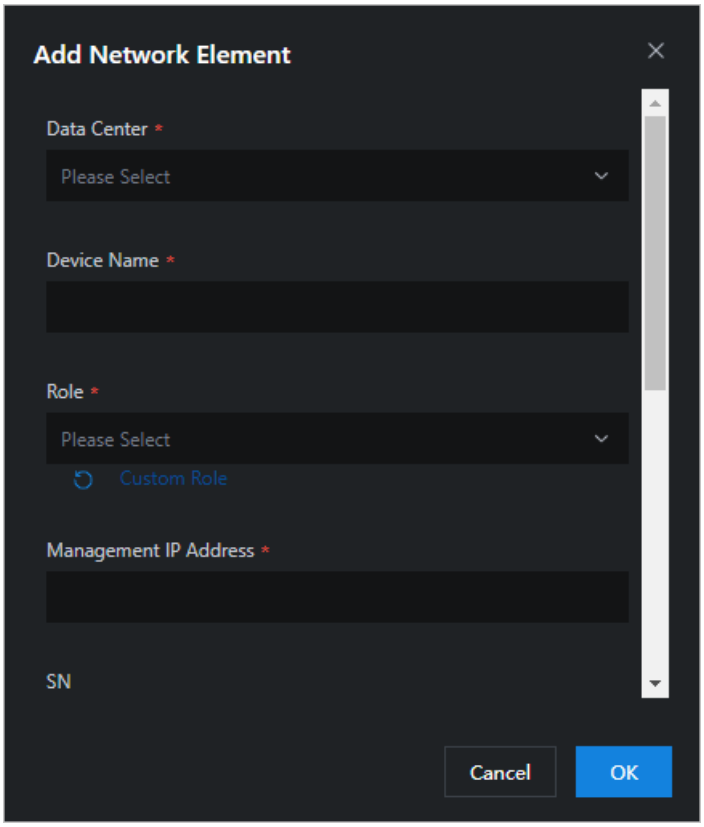
   > **Note** The current Apsara Stack version supports management and monitoring only for network element ports in the Apsara Stack data center.

   v. **Optional:**Go back to the **Network Element Management** page and click **Reset** to clear the filter conditions.
4. Click **Add Data Center**. In the Add Data Center dialog box, configure the parameters and click **OK** to add a data center.



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

5. Add a network element.
   i. Click **Add Network Element**. In the Add Network Element dialog box, configure the parameters.



Parameter	Description	Example
Data Center	The name of the data center where the network element device is located.	amtest11
Device Name	The name of the network element device.	DSW-VM-G1-P-1.xxxx
Role	The role of the network element device.	ASW
Management IP Address	The management IP address of the network element device.	10.66.1.1
SN	The serial number (SN) of the device.	FDO23511111
Version	The version number of the software run by the network element device.	7.1.070
Distribution	The release version of the network element device.	V200R002C50SPC800
Supplier	The supplier of the network element device.	Ruijie
Model	Device Model	S6510-48VS8CQ

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

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

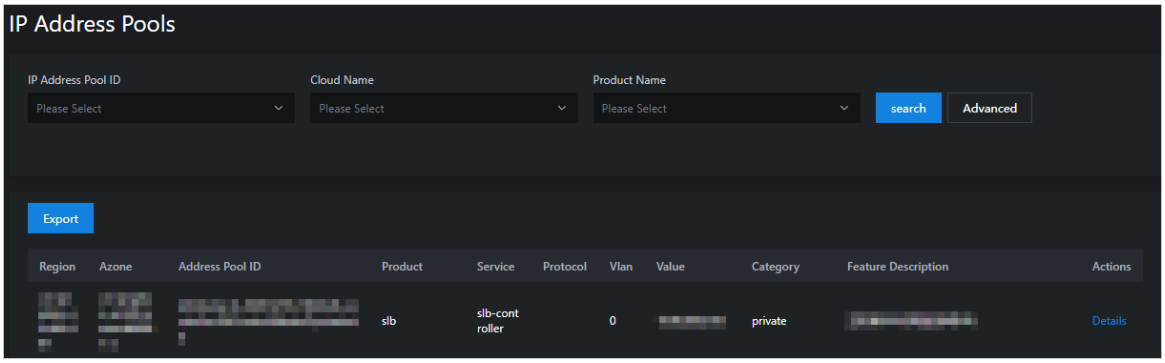
6. Click **Export Table** to download the information about the network element device to your computer.

4.2.2.22.3. IP address pools

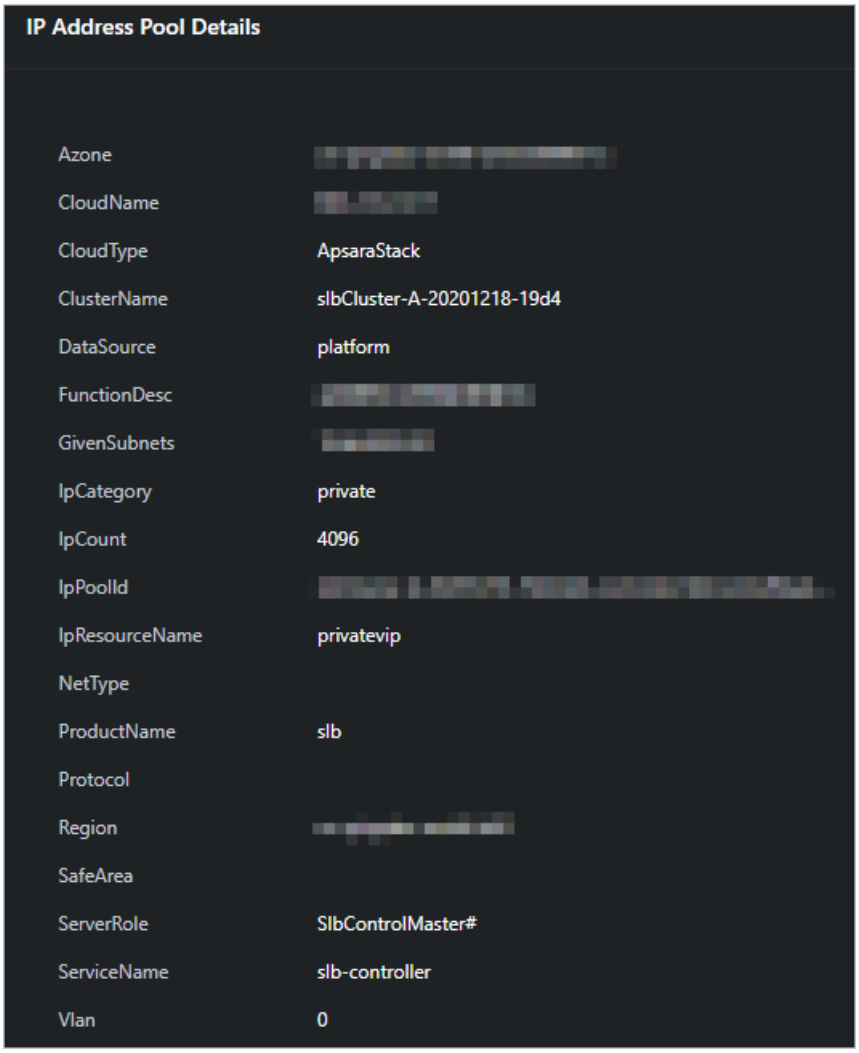
Multiple cloud services may be deployed on a single cloud instance and you may need to view the IP addresses of the cloud services in scenarios such as network changes and security audits. You can view the IP address pool of each cloud service on a cloud instance on the IP Address Pools page.

Procedure

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



   - Use more filter conditions to view the information about the IP address pool.
     a. Click **Advanced**. Select the required options from the additional **IP Resource Name**, **IP Address Type**, **CIDR Block of the IP Address Pool**, **Protocol**, and **Data Source** drop-down lists, and click **search** to view the information about the IP address pool.
     b. (Optional) Click **Reset** to clear the search conditions.
     c. (Optional) Click **Collapse** to hide the advanced filter options.
4. Click **Details** in the **Actions** column to view the details of the IP address pool.



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

4.2.2.23. Use cases

4.2.2.23.1. Troubleshoot network failures

This topic uses a typical case to describe how to use the Network Operations Network module to troubleshoot network failures.

Scenarios

If the visit latency and retransmission time of a cloud service increase, you must determine whether this is caused by network failures.

Prerequisites

The NetworkBaseServiceCluster cluster for BaseServiceAll has been deployed and has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.

3. In the left-side navigation pane, click **Dashboard**.
4. Click the **Network Topology** tab.
5. In the **Current Topology** drop-down list, select **Standard Topology**.

   Wait five seconds. After the page loads, the system shows the network-wide topology and device connections of the AZ in the current environment.

   If device alerts are not triggered in the network, device icons are blue, links between devices are green, and device names are white in the topology. If device alerts are triggered in the network, the topology updates the alert information in the current network every five seconds and shows the updated alert information.
6. If a device name or link in the topology becomes red, alerts are detected in the network device or link port. Double-click the icon of a red device name. In the panel that appears, you can view the basic information of the device and the network alert information related to the device.

   In the preceding figure, the port that is connected to the DSW has a **linkDown** alert and a bgp peer alert. An ASW is identified based on the IP address of the BGP peer. This allows you to determine that a problem in a link between DSW and ASW exists, which caused the port to go down and triggered the alerts.
7. Click the red link in the topology. In the panel that appears, you can view one or more physical links contained in the logical link and the alert information of the link between devices.

   In the preceding figure, the logical link that connects the two devices contains four physical end-to-end links. The port 0/0/2:2 has a port **linkDown** alert. Then, you can proceed to log on to the device and check whether this is caused by the low optical power or damaged modules.
8. When the problem corresponding to the previous alerts is solved, the system updates the alert information. When the fault is repaired, the alerts automatically disappear, the topology is restored to the normal state, and no device names or links remain red.

Use the Alert Management module as a supplement to troubleshoot problems

If a device name or link in the topology becomes red, alerts are detected in the network device or link. You can choose **Network Operations Center > Alert Dashboard** and view the current alerts that are not recovered in the network on the **Current alerts** tab.

The Current Alerts tab shows more detailed alert information.

If an alert is for test or generated because of a cutover, you can click **Ignore** or **Delete** in the **Actions** column corresponding to the alert to ignore or delete the alert.

Use the syslog log query tool as a supplement to troubleshoot problems

If a device name or link in the topology becomes red and you have confirmed that the device alert is not caused by expected changes or because of a cutover by using the alert management feature, you must view the detailed exception logs. You can use the syslog log query tool of vSwitches to search for logs.

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Networking > Network Operations Console**.
3. In the left-side navigation pane, click **Network Element Management**.
4. Click the **SYSLOG management** tab.
5. In the upper-right corner, select the device that you want to query, specify the time range, and then click **Search**. Logs generated within the specified time range are displayed.

By default, you can query a maximum of 1,000 logs.

6. In the upper-left corner, enter a keyword in the search box and click **Search**.
7. After the query is complete, if you want to export logs to submit a ticket or submit logs to device vendors for troubleshooting, click **Export** in the upper-right corner. Logs are stored in your computer as a .csv file.

4.3. Storage operations

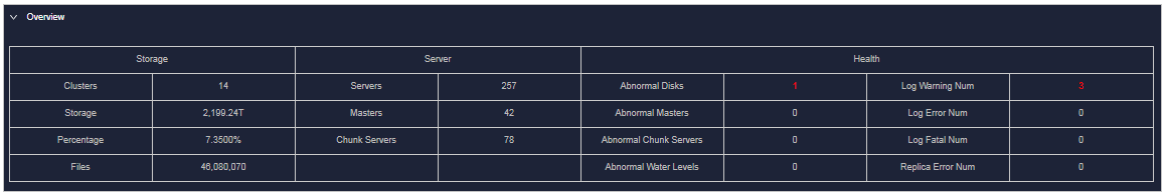
4.3.1. Dashboard

The Dashboard module allows you to view the overview information, health heatmap, and data of the top five clusters of a product.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > Apsara Distributed File System**.
3. In the left-side navigation pane, click **Dashboard**.
4. Select the product that you want to view from the **Service** drop-down list.
   The Apsara Distributed File System module shows the overview information, health heatmap, and data of top five clusters of a product for the current date.
   - **Overview**

     The Overview section shows the storage space, server information, and health information of the specified product. In the **Health** column, values that are greater than 0 are displayed in red.

     
     Overview

Storage		Server		Health			
Clusters	14	Servers	257	Abnormal Disks	1	Log Warning Num	3
Storage	2,199.24T	Masters	42	Abnormal Masters	0	Log Error Num	0
Percentage	7.3500%	Chunk Servers	78	Abnormal Chunk Servers	0	Log Fatal Num	0
Files	46,080,070			Abnormal Water Levels	0	Replica Error Num	0

   - **Heatmap of Health**

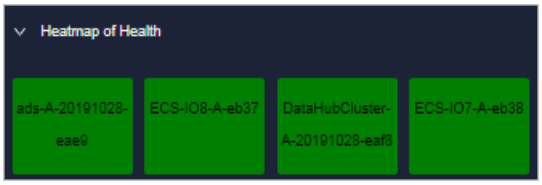
     The Heatmap of Health section shows the health information of all clusters in the specified product. Clusters in different health states are displayed in different colors,

     where:

     - Green indicates that the cluster is working as expected.
     - Yellow indicates that the cluster has an alert.
     - Red indicates that the cluster has an exception.
     - Dark red indicates that the cluster has a fatal error.
     - Grey indicates that the cluster is disabled.

     Click the name of an enabled cluster to go to the Alarm Log page.

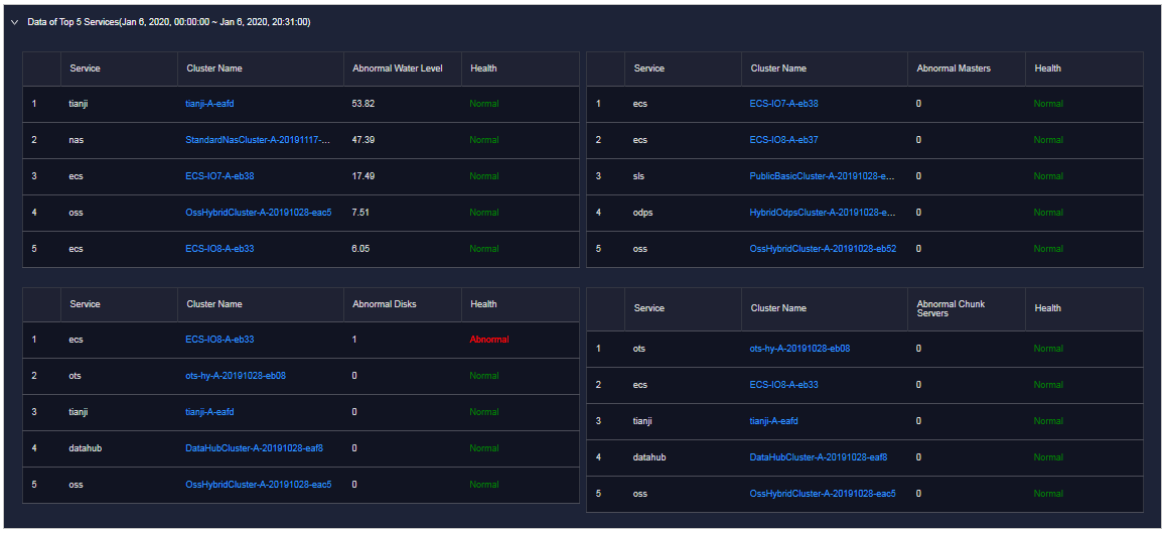
     Move the pointer over the color block of each cluster to view the corresponding product name, server name, and IP address.



- **Data of Top 5 Services**

  The Data of Top 5 Services section shows the data of the top five healthy clusters of the specified product for the current date over the time range from 00:00 to the current time.

  The data in this section includes the abnormal disk usage, abnormal masters, abnormal disks, and abnormal chunk servers of the top five healthy clusters. Click the name of a cluster to go to the Alarm Log page.



4.3.2. Clusters

The Clusters module allows you to view the overview information, alert monitoring information, replica information, trend charts, and rack information of a cluster.

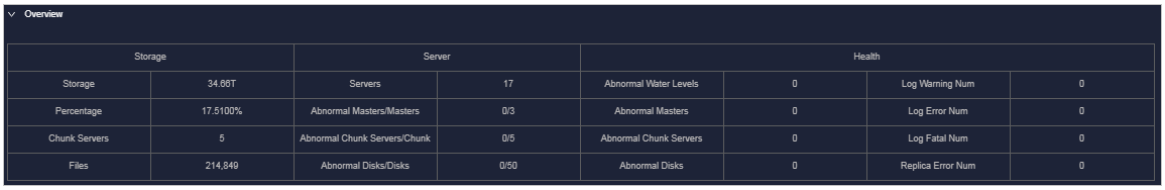
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > Apsara Distributed File System**.
3. In the left-side navigation pane, click **Clusters**.
4. Select the cluster that you want to view from the **Cluster Name** drop-down list. The following information is displayed:

   > **Note** All the enabled clusters in the current environment are displayed in the **Cluster Name** drop-down list.

   - **Overview**

     This section shows the storage space, device information, and health information of the specified cluster. In the **Health** column, values that are greater than 0 are displayed in red.



- **Alarm Monitor**

  This section shows the alert information of the specified cluster, such as the level, server, and server role. You can query data by keywords.

- **Replica**

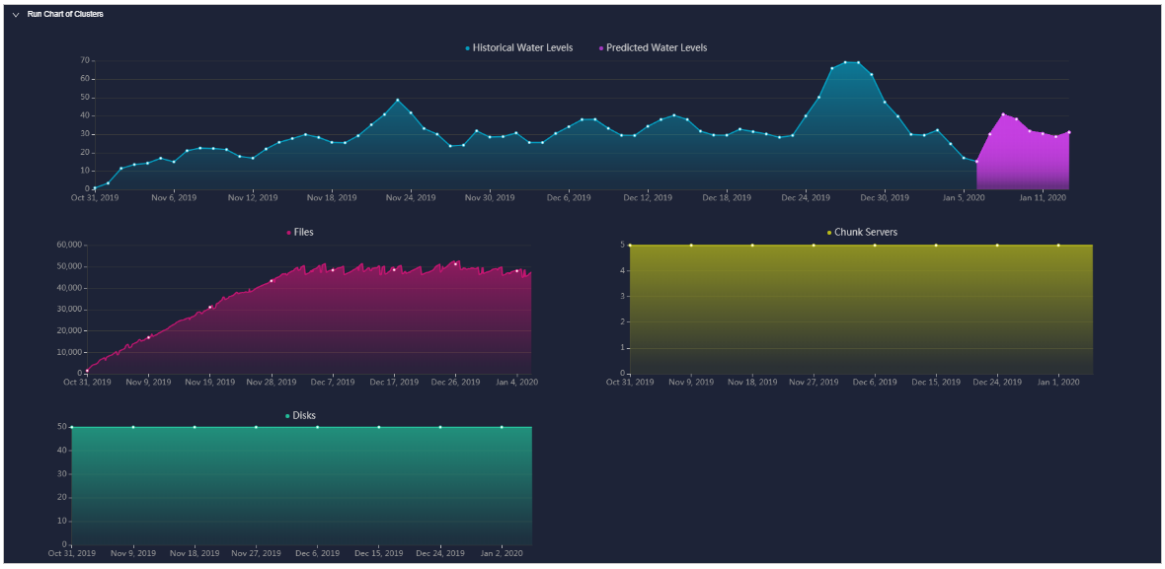
  This section shows the replica information of the specified cluster.

- **Run Chart of Clusters**

  This section shows the charts of historical usage, predicted usage, file number, chunk server number, and disk number for the specified cluster.

  Predicted disk usage shows the run chart for the next seven days.

  > **Note** The disk usage can be predicted only when the data of historical disk usage exist. Therefore, some clusters may not have the data of predicted disk usage.



- **Rack Information**

  This section contains Servers in Rack and Storage.

  - **Servers in Rack** shows the number of servers in each rack in the specified cluster.

- **Storage** shows the total and used storage of each rack in the specified cluster.

4.3.3. Apsara Distributed File System nodes

The Nodes module allows you to view the information about master and chunk servers in a cluster.

Procedure

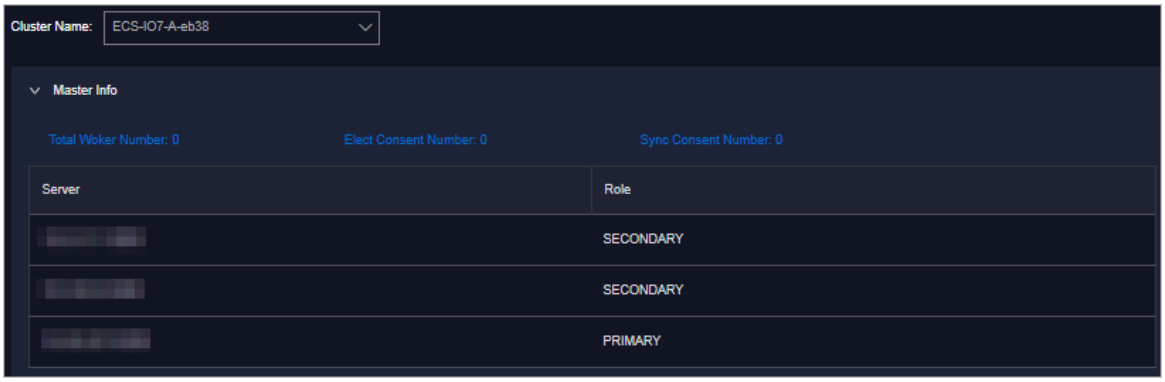
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > Aspara Distributed File System**.
3. In the left-side navigation pane, click **Nodes**.

   On the page that appears, the data of the first cluster in the **Cluster Name** drop-down list is displayed, including the information about master and chunk servers.
4. Select the name of the cluster that you want to view from the **Cluster Name** drop-down list. The following information is displayed:

   > **Note** All the enabled clusters in the current environment are displayed in the **Cluster Name** drop-down list.

   - **Master Info**

     This section shows the information about the master node in the specified cluster. You can click **Refresh** in the upper-right corner of the section to refresh the information.



   - **Chunk Server Info**

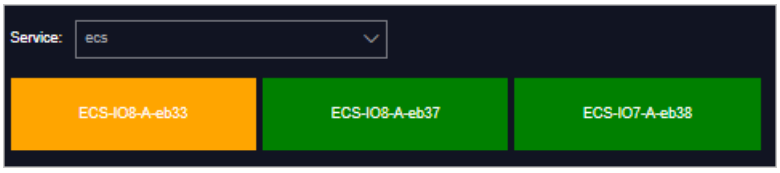
     This section shows the information about the chunk server in the specified cluster. You can click **Refresh** in the upper-right corner of the section to refresh the information. You can click the + icon on the left of a server to view the information about the disk and SSD cache of the server. Fuzzy search is supported in this section.

4.3.4. Operations and maintenance

The O&M module allows you to view the status of each cluster.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > Apsara Distributed File System**.
3. In the left-side navigation pane, click **O&M**.
4. Select a service from the **Service** drop-down list to view the cluster status of the service. Clusters are displayed in different colors based on their health status.
   - Green indicates that the cluster is running as expected.
   - Yellow indicates that the cluster has a warning.
   - Red indicates that the cluster has an exception.
   - Dark red indicates that the cluster has a fatal error.
   - Grey indicates that the cluster is disabled.



5. Move the pointer over a cluster name to view the service name, server name, and IP address of the cluster.

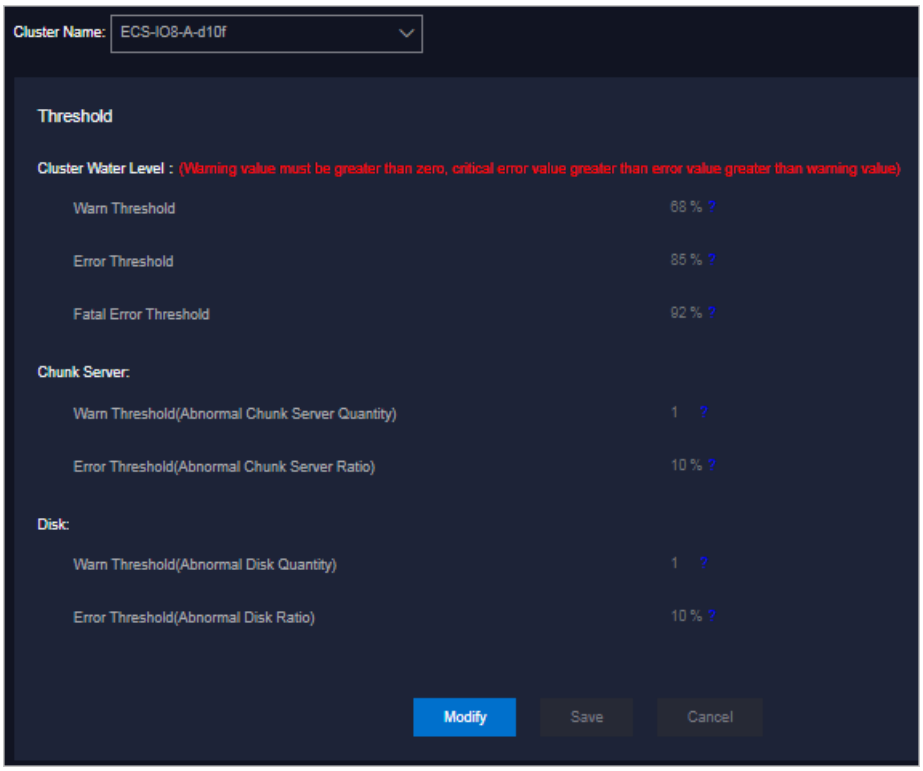
4.3.5. Modify cluster thresholds

By default, the thresholds for all clusters are configured by the system. You can modify these thresholds for storage usage, chunk server, and disk of each cluster based on your business requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > Apsara Distributed File System**.
3. In the left-side navigation pane, click **Settings**.
4. In the **Cluster Name** drop-down list, select a cluster for which you want to modify the thresholds.

5. In the lower part of the page, click **Modify** and configure the parameters.



The following table describes the parameters.

Parameter		Description
Cluster Water Level	**Warn Threshold**	When the storage usage of the cluster is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. Value range: (0,100]. The default threshold for the cluster storage usage is 65%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warning threshold value.
	Error Threshold	When the storage usage of the cluster is greater than or equal to this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. Value range: (0,100]. The default threshold for the cluster storage usage is 85%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warning threshold value.

	Fatal Error Threshold	When the storage usage of the cluster is greater than or equal to this value, a fatal-error alert is triggered and the health heatmap of the cluster is displayed in dark red. Value range: (0,100]. The default threshold for the cluster storage usage is 92%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warning threshold value.
Chunk Server	**Warn Threshold (Abnormal Chunk Server Quantity)**	When the number of abnormal chunk servers is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. The default threshold for the number of abnormal chunk servers is 1.
	Error Threshold (Abnormal Chunk Server Ratio)	If the ratio of abnormal chunk servers to all chunk servers is greater than this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. The default threshold for the ratio of abnormal chunk servers to all chunk servers is 10%.
Disk	**Warn Threshold (Abnormal Disk Quantity)**	When the number of abnormal disks is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. The default threshold for the number of abnormal disks is 1.
	Error Threshold (Abnormal Disk Ratio)	When the ratio of abnormal disks to all disks is greater than this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. The default threshold for the ratio of abnormal disks to all disks is 10%.

Note To reset the configurations, you can click **Cancel** to cancel the current configurations.

6. Click **Save**.

4.3.6. Load information

The Load Information module allows you to view the NC information, VM information, and block device information.

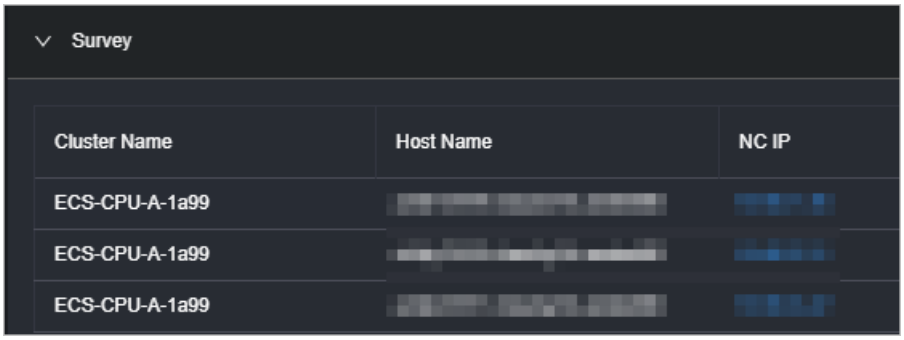
4.3.6.1. View NC information

The Load Information module allows you to view the detailed data of each NC and real-time data such as the load, CPU utilization, memory information, SDA utilization, traffic, TCP information, network exception metrics, read and write rate, BPS, kernel status, IOPS, and latency.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
   By default, the **NC Infor** tab on the **Load Information** page appears.
3. Select a cluster from the **Cluster Name** drop-down list and specify **Time Frame**. You can select **One Hour**, **Three Hours**, or **Six Hours**, or you can customize a time range. Click **Search** and view the following information:
   - Data overview

     The **Survey** section shows all NCs in the current cluster. You can click the IP address of an NC to view the trend charts of real-time data of the NC in the current cluster.

   - Real-time load

     In the **Survey** section, click the IP address of an NC. In the **Real Time Load** section, the load trend chart of the NC within the specified time range is displayed. By default, the real-time load trend chart corresponding to the NC in the first row of the **Survey** section is displayed.

     The following information is displayed in the real-time load trend chart:

     - **load_1**: the average load of the NC within the last minute.
     - **load_5**: the average load of the NC within the last 5 minutes.
     - **load_15**: the average load of the NC within the last 15 minutes.

     You can drag the slider below the chart to zoom in or out the chart.

   - Real-time CPU utilization

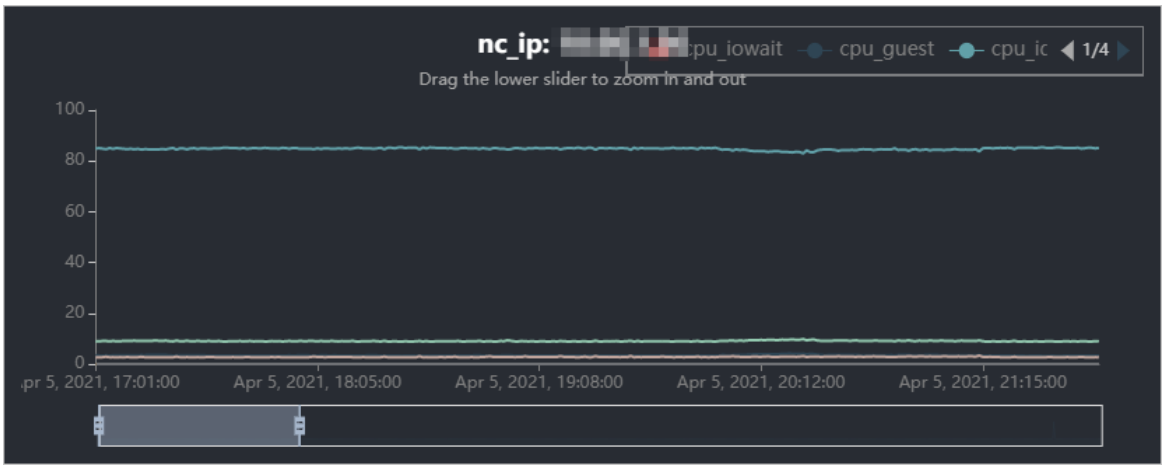
     In the **Survey** section, click the IP address of an NC. In the **Real-time CPU utilization** section, the CPU utilization trend chart of the NC within the specified time range is displayed.

     The following information is displayed in the real-time CPU utilization trend chart:

     - **cpu_iowait**: the time spent waiting for an I/O response.
     - **cpu_guest**: the running time of a vCPU in a guest OS.
     - **cpu_idle**: the time that a CPU spent idling.
     - **cpu_hardirp**: the time spent servicing hardware interrupts.
     - **cpu_user**: the CPU time in user mode.
     - **cpu_softirp**: the time spent servicing software interrupts.

- **cpu_steal**: the percentage of time that a vCPU waits for a real CPU while the hypervisor is servicing another virtual processor.
- **cpu_sys**: the CPU time in system mode.
- **cpu_nice**: the CPU time occupied by low-priority programs in user mode.

You can drag the slider below the chart to zoom in or out the chart.



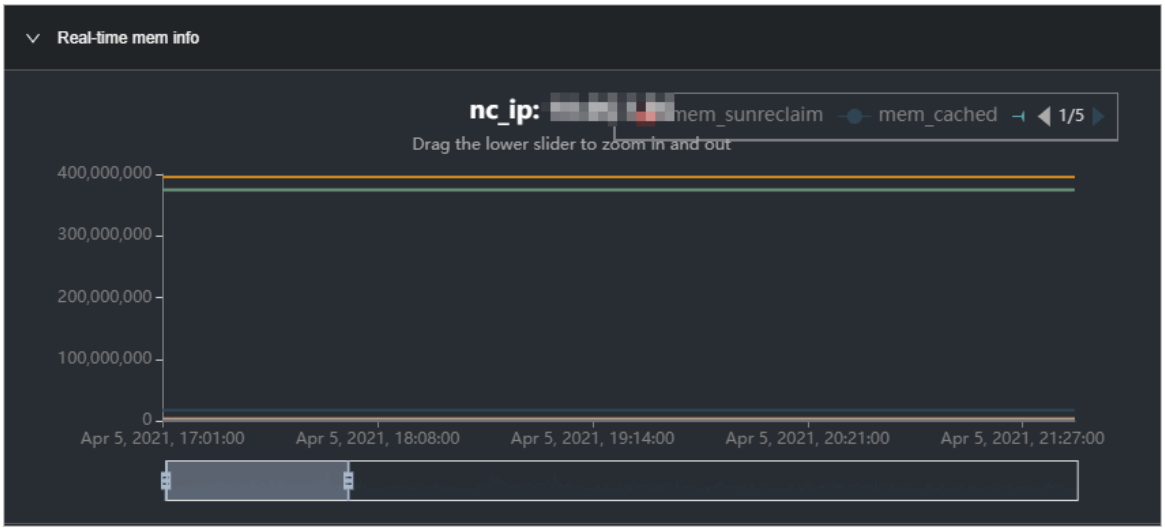
- Real-time memory information

  In the **Survey** section, click the IP address of an NC. In the **Real-time mem info** section, the memory utilization trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time memory utilization trend chart:

  - **mem_sunreclaim**: the slab capacity that cannot be reclaimed when the object is active.
  - **mem_cached**: the physical memory that has been cached.
  - **mem_slab**: the total amount of the memory allocated by the slab allocator.
  - **mem_free**: the available physical memory and swap space.
  - **mem_shmem**: the memory utilization.
  - **mem_used**: the physical memory and swap space that are occupied.
  - **mem_total**: the total amount of the physical memory and swap space of the system.
  - **mem_buffer**: the physical memory that has been buffered.
  - **mem_dirty**: the dirty data, which is the data that is stored in the buffer zone but has not been written to physical disks.

  You can drag the slider below the chart to zoom in or out the chart.

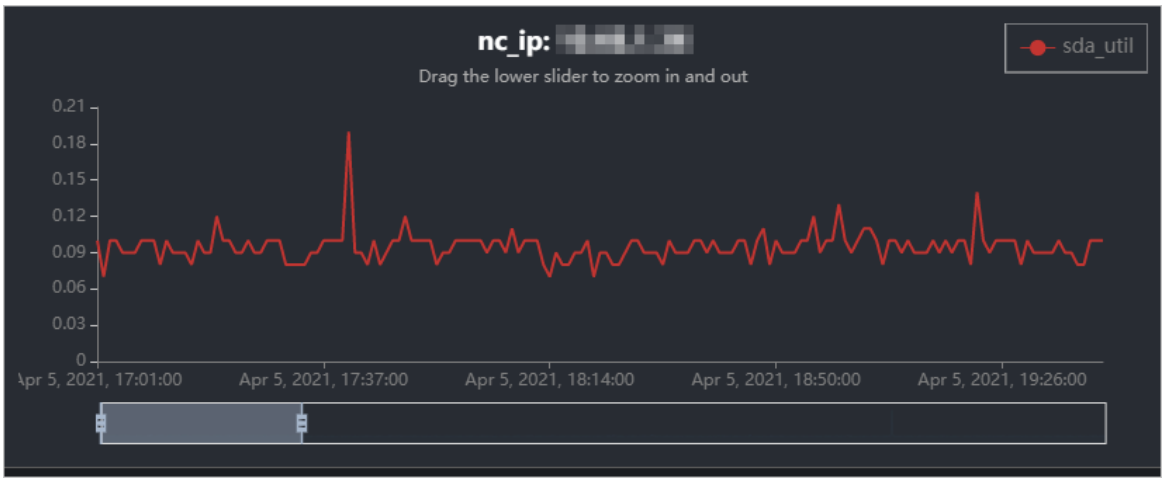


- Real-time SDA utilization

  In the **Survey** section, click the IP address of an NC. In the **Real-time SDA utilization** section, the disk utilization trend chart of the NC within the specified time range is displayed.

  In the real-time SDA utilization trend chart, **sda_until** indicates the SDA utilization.

  You can drag the slider below the chart to zoom in or out the chart.



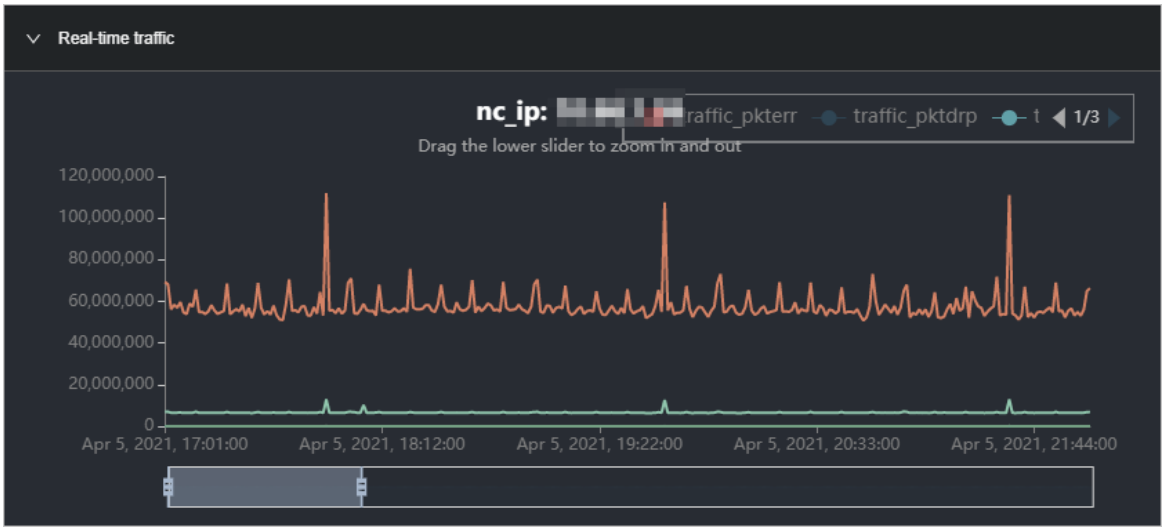
- Real-time traffic

  In the **Survey** section, click the IP address of an NC. In the **Real-time traffic** section, the traffic trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time traffic trend chart:

  - **traffic_pkterr**: the number of errors for transmission packets.
  - **traffic_pktdrp**: the number of lost transmission packets.
  - **traffic_pktin**: the number of input bytes during the traffic peak.
  - **traffic_bytesout**: the number of output bytes.
  - **traffic_bytesin**: the number of input bytes.
  - **traffic_pktout**: the number of output bytes during the traffic peak.

  You can drag the slider below the chart to zoom in or out the chart.



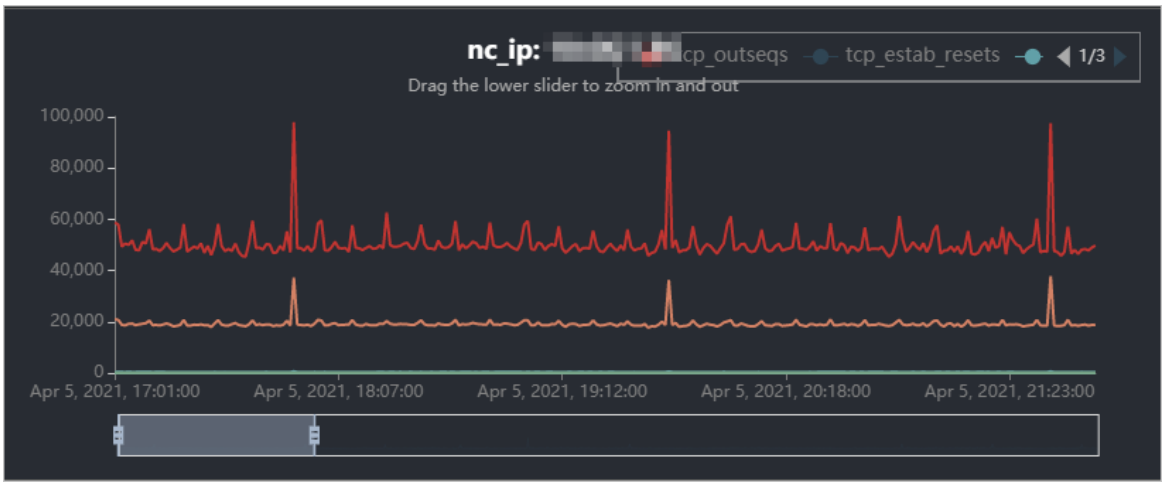
- Real-time TCP information

  In the **Survey** section, click the IP address of an NC. In the **Real-time tcp Info** section, the TCP connection trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time TCP connection trend chart:

  - **tcp_outseqs**: the number of TCP packets that have been sent.
  - **tcp_estab_resets**: the number of retry attempts of TCP connections that are in the ESTABLISHED state.
  - **tcp_opens**: the number of open TCP connections.
  - **tcp_inseqs**: the number of received TCP packets.
  - **tcp_attempt_fails**: the number of failed connection attempts.
  - **tcp_curr_estab**: the number of TCP connections that are in the ESTABLISHED state.

  You can drag the slider below the chart to zoom in or out the chart.



- Real-time network exception index

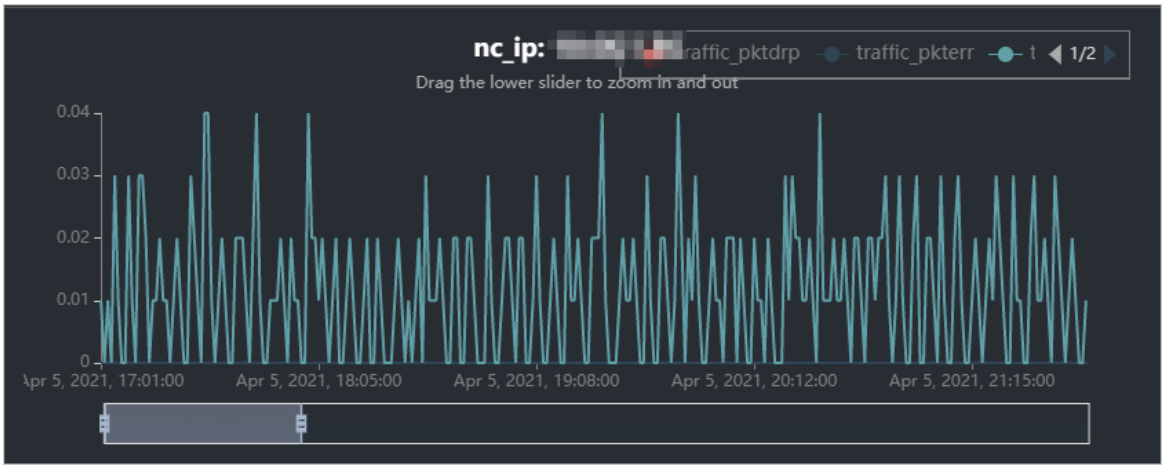
  In the **Survey** section, click the IP address of an NC. In the **Real-time network anomaly index** section, the trend chart of the network exception index of the NC within the specified time range is displayed.

  The following information is displayed in the trend chart of the real-time network exception index:

  - **traffic_pktdrp**: the number of transmission packets that are lost.

- **traffic_pkterr**: the number of errors for transmission packets.
- **traffic_retrans_ratio**: the number of retry attempts of transmission packets.

You can drag the slider below the chart to zoom in or out the chart.



- Read and write B/s

  In the **Survey** section, click the IP address of an NC. In the **Reading and Writing B/S** section, the trend chart of the read and write rate of the NC within the specified time range is displayed.

  The following information is displayed in the trend chart of the read and write rate :

  - **bs_w**: the write rate in byte/s.
  - **bs_r**: the read rate in byte/s.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time BPS

  In the **Survey** section, click the IP address of an NC. In the **Real-time BPS** section, the BPS trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time BPS trend chart:

  - **bps_w**: the write rate in bit/s.
  - **bps_r**: the read rate in bit/s.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time kernel status

  In the **Survey** section, click the IP address of an NC. In the **Real-time Kernel State** section, the kernel status trend chart of the NC within the specified time range is displayed.

  In the real-time kernel status trend chart, **kernel_status** indicates the real-time kernel status.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time IOPS

  In the **Survey** section, click the IP address of an NC. In the **Real-time iops** section, the IOPS trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time IOPS trend chart:

  - **iops_w**: the number of I/O writes per second.
  - **iops_r**: the number of I/O reads per second.

You can drag the slider below the chart to zoom in or out the chart.

- Real-time latency

  In the **Survey** section, click the IP address of an NC. In the **Real-time latency** section, the latency trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time latency trend chart:

  - **latency_w**: the real-time latency of data writes
  - **latency_r**: the real-time latency of data reads
  - **latency_w_qos**: the QoS intelligent adjustment for real-time latency of data writes
  - **latency_r_qos**: the QoS intelligent adjustment for real-time latency of data reads

  You can drag the slider below the chart to zoom in or out the chart.

4.3.6.2. View virtual machine information

The Load Information module allows you to view the detailed information about data and trend charts of read and write rate, real-time BPS, real-time IOPS, and real-time latency of all virtual machines (VMs).

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
   By default, the **Load Information** page appears.
3. Click the **Virtual Machine Information** tab.
4. Select a cluster from the **Cluster Name** drop-down list, select an NC IP address from the **nc_Ip** drop-down list, and then set **Time Frame** to **One Hour**, **Three Hours**, **Six Hours**, or a custom time range. Click **Search** and view the following information:

   - Data overview

     The **Survey** section shows a list of all VMs under an NC of the selected cluster. Click a VM name to view the trend charts of the real-time data of the VM.

   - Read and write B/s

     Click a VM name in the **Survey** section. In the **Reading and Writing B/S** section, the trend chart of the read and write rate of the current VM within the specified time range is displayed.

     You can drag the slider below the chart to zoom in or out the chart.

     - bs_w: the write rate of the instance
     - bs_r: the read rate of the instance

   - Real-time BPS

     Click a VM name in the **Survey** section. In the **Real-time BPS** section, the BPS trend of the current VM within the specified time range is displayed.

     You can drag the slider below the chart to zoom in or out the chart.

     - bps_w: the amount of data written per unit time
     - bps_r: the amount of data read per unit time

   - Real-time IOPS

     Click a VM name in the **Survey** section. In the **Real-time iops** section, the IOPS trend chart of the current VM within the specified time range is displayed.

     You can drag the slider below the chart to zoom in or out the chart.

- iops_w: the number of disk writes per second
- iops_r: the number of disk reads per second

- Real-time latency

  Click a VM name in the **Survey** section. In the **Real-time latency** section, the latency trend of the current VM within the specified time range is displayed.

  You can drag the slider below the chart to zoom in or out the chart.

  - latency_w: the real-time latency of data writes
  - latency_r: the real-time latency of data reads
  - latency_w_qos: the QoS adjustment for real-time latency of data writes
  - latency_r_qos: the QoS adjustment for real-time latency of data reads

4.3.6.3. View block device information

The Load Information module allows you to view the overview information and the trend charts of the data read and write rate, real-time BPS, real-time IOPS, and real-time latency for each device.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
   By default, the **Load Information** page appears.
3. Click the **Block Device Information** tab.
4. Select a cluster from the **Cluster Name** drop-down list, select an NC IP from the **nc_Ip** drop-down list, select an instance name from the **vmName** drop-down list, and then specify **Time Frame** (**One Hour**, **Three Hours**, **Six Hours**, or a custom time range). Click **Search** to view the following information:

   - Data overview

     The **Survey** section shows the information about all block devices in each VM of an NC in the current cluster. You can click a disk ID to view the data trend charts for the block device in real time.

   - Read and write B/s

     In the **Survey** section, click a disk ID. In the **Reading and Writing B/S** section, the read and write rate trend chart of the current block device within the specified time range appears.

     You can drag the slider below the chart to zoom in or out the chart.

     - bs_w: the write rate of the instance
     - bs_r: the read rate of the instance

   - Real-time BPS

     In the **Survey** section, click a disk ID. In the **Real-time BPS** section, the BPS trend chart of the current block device within the specified time range appears.

     You can drag the slider below the chart to zoom in or out the chart.

     - bps_w: data written per unit time
     - bps_r: data read per unit time

   - Real-time IOPS

In the **Survey** section, click a disk ID. In the **Real-time iops** section, the IOPS trend chart of the current block device within the specified time range appears.

You can drag the slider below the chart to zoom in or out the chart.

- iops_w: disk writes per second
- iops_r: disk reads per second

- Real-time latency

  In the **Survey** section, click a disk ID. In the **Real-time latency** section, the latency trend chart of the current block device within the specified time range appears.

  You can drag the slider below the chart to zoom in or out the chart.

  - latency_w: the real-time latency of data writes
  - latency_r: the real-time latency of data reads
  - latency_w_qos: the QoS adjustment for the real-time latency of data writes
  - latency_r_qos: the QoS adjustment for the real-time latency of data reads

4.3.7. EBS dashboard

The EBS Dashboard module allows you to view data details and usage trend charts of EBS clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **EBS Dashboard**.
   On the page that appears, data details and usage trend charts of all EBS clusters are displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. View the following information:
   - **Overview**: shows the data details of the selected cluster, including the storage space, server information, and health information.

     In the **Health** section, when the value of **Abnormal Cloud Disks**, **Abnormal Masters**, **deleting state**, **Abnormal Block GcWorkers**, or **Abnormal Block Servers** is greater than 0, the corresponding value is displayed in red.
   - The **Trend Chart of Cluster Usage** section shows the storage usage curve of the cluster for the last 30 days.

4.3.8. Block master operations

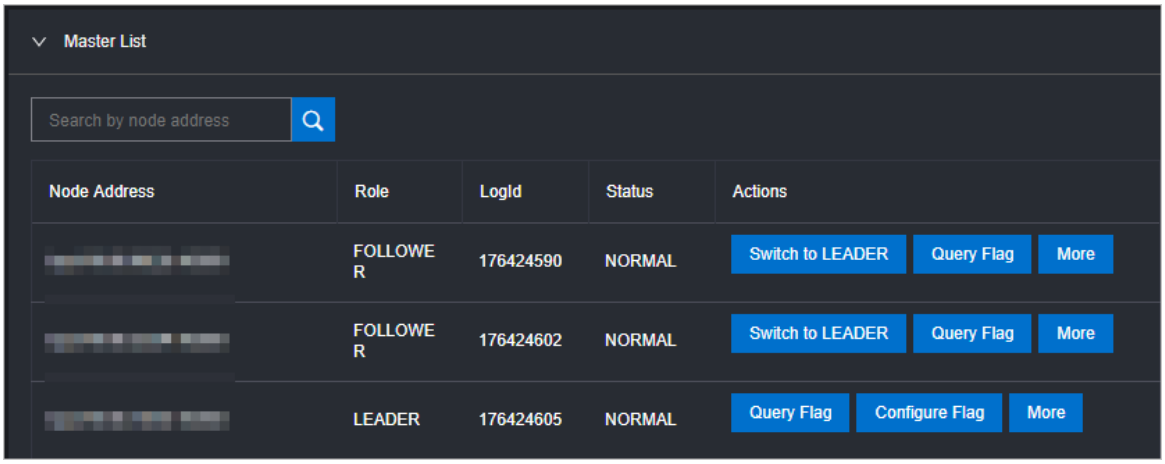
The Block Master O&M module shows the information about the block master nodes of Elastic Block Storage (EBS) clusters, including the IP addresses and roles. The module also allows you to switch the role of a node to leader as well as query and configure flags.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Block Master O&M**.
   On the page that appears, the list of block master nodes of and the information about the first cluster in the **Cluster Name** drop-down list are displayed by default.

4. Select the cluster that you want to manage from the **Cluster Name** drop-down list.
5. In the **Master List** section, perform the following operations:
   - View block master nodes

     You can view the information about the block master nodes of the selected cluster, including the IP address, role, log ID, and status.



   - Switch to leader

     A leader role for a block master node assumes the same responsibilities as a follower role, including controlling and scheduling resources, as well as controlling deployment and service configurations.

     If a node in the list of block master nodes assumes a follower role, you must switch its role to leader. To switch the role to leader, click **Switch to LEADER** in the **Actions** column. In the message that appears, click **OK**.

   - Query a flag

     In the list of block master nodes, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block master node are displayed.

     To query the flag_key value, perform the following steps:

     a. In the left-side navigation pane of the Apsara Infrastructure Management console, choose **Operations > Cluster Operations**.
     b. Enter EBS in the **Cluster** search box.
     c. Find the EBS cluster and click the cluster name.
     d. Click the **Cluster Configure** tab.
     e. Find the pangu_blockmaster_flag.json file in /services/EbsBlockMaster/user/pangu_blockmaster.

        The flag_key values of all block master nodes are stored in the pangu_blockmaster_flag.json file.

   - Configure a flag

     If you want to modify the deployment and service configurations of a block master node, you can configure a flag and assign it to the node.

     In the list of block master nodes, find a node that assumes the leader role and click **Configure Flag** in the **Actions** column. In the dialog box that appears, configure the parameters and click **OK**.

     The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the pangu_blockmaster_flag.json file.
flag_value	The custom flag value.
flag_type	The flag type. Valid values: ▪ **int** ▪ **bool** ▪ **string** ▪ **double**

- Check the maser node status

  In the list of block master nodes, find a node and choose **More > Check Master Status** in the **Actions** column.

- Query version information

  In the list of block master nodes, find a node and choose **More > Query Version Information** in the **Actions** column.

6. In the **Cluster Overview** section, you can query the disk size, number of segments, total capacity, and storage usage of the cluster.

4.3.9. Block server operations

The Block Server O&M module shows the information about the block server nodes of Elastic Block Storage (EBS) clusters, including the IP address, status, and real-time server load. The module also allows you to query and modify flags, configure the server node status, as well as add nodes to and delete nodes from the blacklist.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Block Server O&M**.
   On the page that appears, the information about the first cluster in the **Cluster Name** drop-down list is displayed by default.
4. Select the cluster that you want to manage from the **Cluster Name** drop-down list.
5. In the **Server List** section, perform the following operations:
   - View block server nodes

     You can view the information about the server nodes of the cluster, including the IP addresses, status, number of segments, and real-time load (read IOPS, write IOPS, read bandwidth, write bandwidth, read latency, and write latency).

   - Query a flag

     In the list of block server nodes, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block server node are displayed.

     To query the flag_key value, perform the following steps:

a. In the left-side navigation pane of the Apsara Infrastructure Management console, choose **Operations > Cluster Operations**.
b. Enter EBS in the **Cluster** search box.
c. Find the EBS cluster and click the cluster name.
d. Click the **Cluster Configure** tab.
e. Find the pangu_blockserver_flag.json file in /services/EbsBlockServer/user/pangu_blockserver.

   The flag_key values of all block server nodes are stored in the pangu_blockserver_flag.json file.

- Configure a flag

  In the list of block server nodes, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key and flag_value, select flag_type, and then click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the pangu_blockserver_flag.json file.
flag_value	The custom flag value.
flag_type	The flag type. Valid values: ▪ **int** ▪ **bool** ▪ **string** ▪ **double**

- Configure the server node status

  In the list of block server nodes, find a node and choose **More > Set Server Status** in the **Actions** column. In the dialog box that appears, specify the server node status and click **OK**.

  The following table describes the server node status.

Status	Description
NORMAL	The node is running as expected.
DISCONNECTED	The node is disconnected.
OFFLOADING	The node is being disabled.
OFFLOADED	The node is disabled.
UPGRADE	The node is upgraded.
RECOVERY	The node is restored.

- Query version information

In the list of block server nodes, find a node and choose **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block server node.

6. In the **Block Server Blacklist** section, perform the following operations:
   - Add a block server node to the blacklist

     In the upper-right corner of the **Block Server Blacklist** section, click **Add**. In the dialog box that appears, select the IP address of the block server node that you want to add to the blacklist and click **OK**.

     The block server node that is added to the blacklist is disabled and no longer provides services.
   - View the block server blacklist

     In the **Block Server Blacklist** section, you can view all block server nodes that are added to the blacklist.
   - Remove a block server node from the blacklist

     In the **Block Server Blacklist** section, find the block server node that you want to remove from the blacklist and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

     The block server node that is removed from the blacklist can continue to provide services.

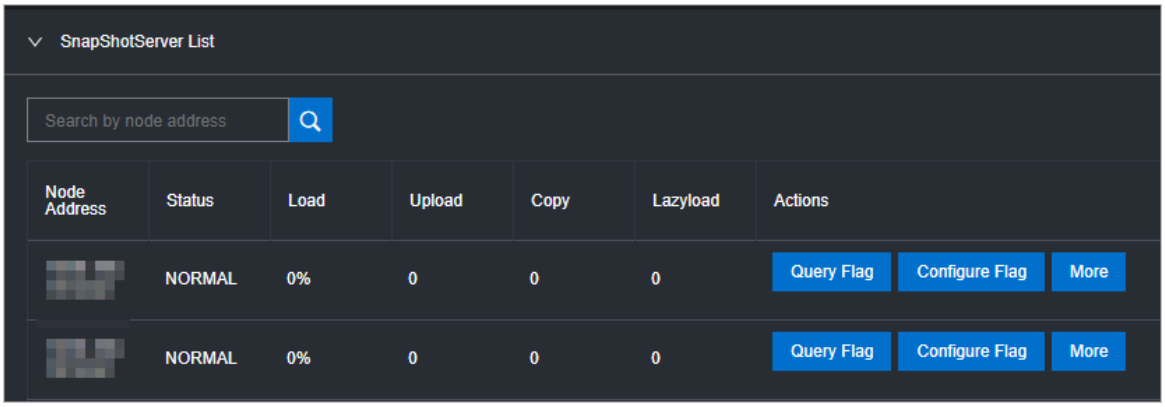
4.3.10. SnapShot Server

The SnapShotServer module shows the information about the snapshot server nodes of Elastic Block Storage (EBS) clusters, including the IP address, status, and performance parameters. The module also allows you to query and modify flags and configure the status of a snapshot server node.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **SnapShot Server**.
   On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed by default.
4. Select the cluster that you want to manage from the **Cluster Name** drop-down list.
5. You can perform the following operations:
   - View snapshot server nodes

     You can view the information about the snapshot server nodes of the cluster, including the IP address, status, loading rate, the number of uploads, replicas, and delayed loadings.



- Query a flag

  In the snapshot server list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the snapshot server node are displayed.

  To query the flag_key value, perform the following steps:

  a. In the left-side navigation pane of the Apsara Infrastructure Management console, choose **Operations > Cluster Operations**.
  b. Enter EBS in the **Cluster** search box.
  c. Find the EBS cluster and click the cluster name.
  d. Click the **Cluster Configure** tab.
  e. Find the pangu_snapshotserver_flag.json file in /services/EbsSnapshotServer/user/pangu_snapshotserver.

     The flag_key values of all snapshot server nodes are stored in the pangu_snapshotserver_flag.json file.

- Configure a flag

  In the list of snapshot server nodes, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key and flag_value, select flag_type, and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the pangu_snapshotserver_flag.json file.
flag_value	The custom flag value.
flag_type	The flag type. Valid values: ▪ **int** ▪ **bool** ▪ **string** ▪ **double**

- Configure the snapshot server node status

In the list of snapshot server nodes, find a node and choose **More > Set snapshotserver Status** in the **Actions** column. In the dialog box that appears, select the snapshot server node status and click **OK**.

The following table describes the snapshot server node status.

Status	Description
NORMAL	The node is running as expected.
DISCONNECTED	The node is disconnected.
OFFLOADING	The node is being disabled.
OFFLOADED	The node is disabled.

- Query version information

  In the list of snapshot server nodes, find a node and choose **More > Version** in the **Actions** column. In the dialog box that appears, view the version information of the node.

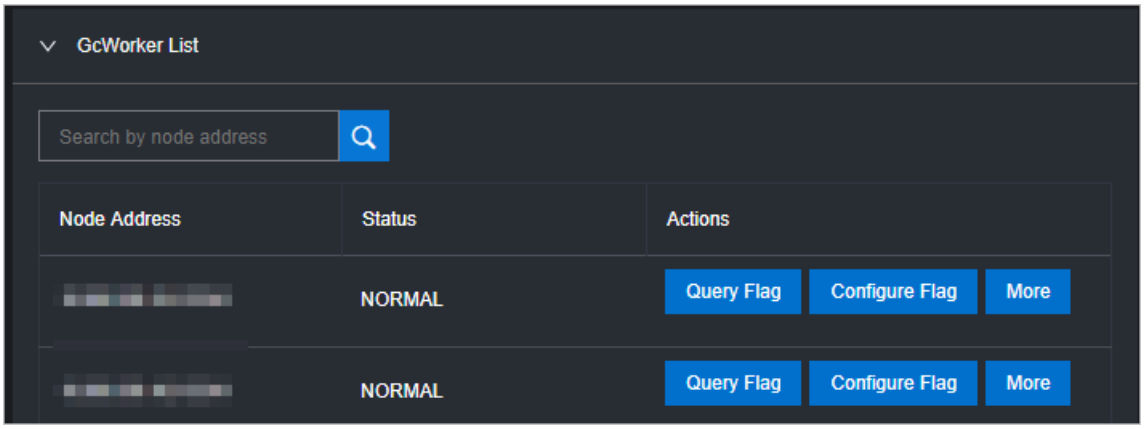
4.3.11. Block gcworker operations

The Block Gcworker O&M module allows you to view the IP addresses and status of block gcworker nodes in Elastic Block Storage (EBS) clusters. You can also query and modify flags, configure the gcworker node status, and query version information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Block Gcworker O&M**.
   On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. You can perform the following operations:
   - View the gcworker node list

     You can view the IP addresses and status of the block gcworker nodes in the selected cluster.

   - Query a flag

In the gcworker node list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block gcworker node are displayed.

Perform the following steps to query the flag_key value:

a. In the left-side navigation pane of the Apsara Infrastructure Management console, choose **Operations > Cluster Operations**.
b. Enter EBS in the **Cluster** field.
c. Find the EBS cluster and click the cluster name.
d. Click the **Cluster Configuration** tab.
e. Find the pangu_blockgcworker_flag.json file in /services/EbsBlockGCWorker/user/pangu_blockgcworker.

   The flag_key values of all block server nodes are stored in the pangu_blockgcworker_flag.json file.

- Configure a flag

  In the gcworker node list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key, flag_value, and flag_type, and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the pangu_blockgcworker_flag.json file.
flag_value	The custom flag value.
flag_type	The flag type. Valid values: ▪ **int** ▪ **bool** ▪ **string** ▪ **double**

- Configure the gcworker node status

  In the gcworker node list, find a node and click **More > Set GcWorker Status** in the **Actions** column. In the dialog box that appears, specify the gcworket node status and click **OK**.

  The following table describes the gcworker status.

State	Description
NORMAL	The node is running as expected.
DISCONNECTED	The node is disconnected.
OFFLOADING	The node is being disabled.
OFFLOADED	The node is disabled.

- Query the version information

In the gcworker node list, find a node and click **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block gcworker node.

4.3.12. Device operations

The Device Operations module allows you to view disk information in Elastic Block Storage (EBS) clusters such as the disk ID, status, capacity, and type. You can also perform flush operations, modify disk configurations, query segment information, and enable, disable, delete, and restore devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Device Operations**.
   On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. You can perform the following operations:
   - View the device list
     You can view the total number of devices, the total logical space of devices, and information about each device in the cluster, including the device ID, status, logical capacity, number of segments, mode, and flags.

     > **Note** You can filter device information by device ID and status.
   - Check global segments

     In the upper-right corner of the **Device List** section, click **Global Check Segment**. You can view all the segments in the selected cluster and their indexes and status.
   - Check disk status

     In the upper-right corner of the **Device List** section, click **Check Cloud Disk Status**. You can view the number of invalid disks in the selected cluster.
   - Query device information

     In the device list, find the device whose information you want to query and click **Query Device Information** in the **Actions** column. In the dialog box that appears, view the disk information such as the disk ID, status, and capacity.
   - Delete a device

     In the device list, find the device that you want to delete and click **Delete** in the **Actions** column.

     After you delete the device, its status becomes **DELETING**, and the device is unavailable. You are not allowed to perform operations such as enabling the device or modifying the configurations.
   - Restore a device

     In the device list, find a deleted device that is in the **DELETING** state and click **Restore** in the **Actions** column. In the message that appears, click **OK** to restore the deleted device to its normal state.

     After you restore the device, it becomes available. You can perform operations such as enabling the device and modifying the configurations.
   - Enable a device

In the device list, find the device that you want to enable and choose **More > Turn On** in the **Actions** column. In the dialog box that appears, configure the required parameters and click **Submit**.

> **Note** You can perform read and write operations on a disk only after the disk is enabled.

The following table describes the parameters for enabling a device.

Parameter	Description
client_ip	Optional. Specifies the client on which the disk is enabled. The client IP address is the IP address of the block server. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies a string as a token to be used to disable the device.
mode	Specifies the disk mode. Valid values: ▪ **ro**: read-only ▪ **rw**: read and write Default value: **rw**.

- Disable a device

> **Important** After a disk is disabled, data can no longer be read from or written to the disk. Proceed with caution.

In the device list, find the device that you want to disable and choose **More > Turn Off** in the **Actions** column. In the dialog box that appears, configure the parameters and click **Submit**.

The following table describes the parameters for disabling a device.

Parameter	Description
client_ip	Specifies the client IP address of the disk to be disabled. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies the token used to disable the device. The token is configured when the device is enabled. You can query the token by running the **dev -query** command on a server in the EBS cluster.

open_ver	Specifies the current OpenVersion of the device if the client IP address is not specified. If a client IP address is specified, you do not need to specify the OpenVersion. You can query the OpenVersion by running the **dev -query** command on a server in the EBS cluster.

- Flush a device

  In the device list, find the device that you want to flush and choose **More > Flush** in the **Actions** column. In the dialog box that appears, configure the parameters and click **Submit**.

  The following table describes the parameters for flushing a device.

Parameter	Description
segment	Select the segment to be flushed. If you do not specify this parameter, all segments are flushed.
ifnsw	Specifies whether to flush the index file. Valid values: ▪ **0**: specifies to flush the index file. ▪ **1**: specifies not to flush the index file.
dfnsw	Specifies whether to flush the data file. Valid values: ▪ **0**: specifies to flush the data files. ▪ **1**: specifies not to flush the data files.

- Flush globally

  You can perform the flush operation to clear the transaction logs of disks or segments.

  On the right of the **Device List** section, click **Global Flush**. In the dialog box that appears, select ifnsw and dfnsw, and click **OK**. Then, the transaction logs of all the disks or segments in the current cluster are flushed.

- Query the configuration status

  In the device list, find the device whose configuration status you want to query and choose **More > Query Configuration Status** in the **Actions** column. In the dialog box that appears, enter config_ver and click **OK**. You can determine whether the disk is configurable based on the check result.

  config_ver is the config_version parameter in the information about the queried device.

- Modify device configurations

  You can modify the configurations of a disk, such as the compression algorithms, storage modes, and whether to enable data compression.

  In the device list, find the device whose configurations you want to modify and choose **More > Modify Device Configurations** in the **Actions** column. In the dialog box that appears, modify the parameters and click **OK**.

The following table describes the parameters.

Parameter	Description
compress	Specifies whether to enable data compression. Valid values: ▪ **enable** ▪ **disable**
algorithm	Specifies a data compression algorithm. Valid values: ▪ **0**: specifies not to use data compression algorithms. ▪ **1**: specifies to use the snappy data compression algorithm. ▪ **2**: specifies to use the lz4 data compression algorithm.
ec	Specifies whether to enable the EC storage mode. Default value: disable. Valid values: ▪ **enable** ▪ **disable**
data_chunks	Specifies the number of data chunks. Default value: 8.
parity_chunks	Specifies the number of parity chunks. Default value: 3.
packet_bits	Specifies the size of a single data block in EC mode. Default value: 15.
copy	Specifies the number of data replicas. Default value: 3.
storage_mode	Specifies the storage mode of the disk.
cache	Specifies whether to enable the cache mode. Default value: 0. Valid values: ▪ **0**: disables the cache mode. ▪ **1**: enables the cache mode.
storage_app_name	Specifies the data storage name.
simsuppress	Specifies whether to enable the delay simulation feature. Default value: disable. Valid values: ▪ **enable** ▪ **disable**
baselatency	Specifies the basic latency. Default value: 300.
consumespeed	Specifies the processing speed. Default value: 256 bit/μs.
lat80th	Specifies the quantile jitter control of the latency as 80%.
lat90th	Specifies the quantile jitter control of the latency as 90%.
lat99th	Specifies the quantile jitter control of the latency as 99%.

- Query segment information

  In the device list, find the device whose segment information you want to query and choose **More > Segment Information** in the **Actions** column. In the dialog box that appears, view the information about the segments, such as the index and status.

- Check a segment

  In the device list, find the device whose segment you want to check and choose **More > Check Segment** in the **Actions** column. In the dialog box that appears, select the segment to be checked and click **Submit**.

4.3.13. Enable or disable rebalance

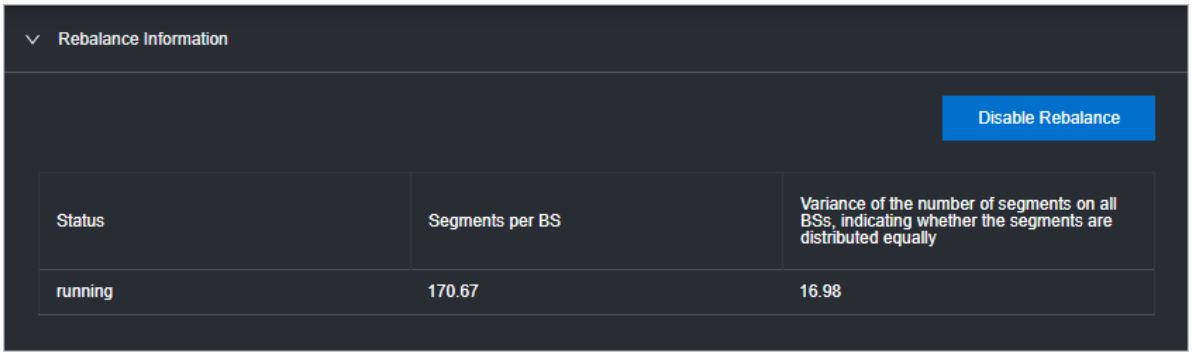
When segments are unevenly distributed in a block server, you can enable the rebalance feature to redistribute the segments. After you redistribute the segments, you can disable rebalance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Rebalance**.
4. Click **Enable Rebalance** or **Disable Rebalance**.

   After you click **Enable Rebalance**, the status of rebalance changes to **running**.

   After you click **Disable Rebalance**, the status of rebalance changes to **stopped**.



4.3.14. I/O hang analysis

The IO HANG module allows you to view the list of affected virtual machines (VMs), VM cluster statistics, and device cluster statistics.

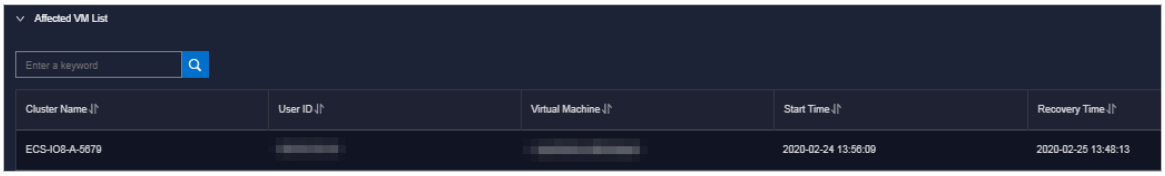
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **IO HANG**.
   By default, the system shows the list of affected VMs, VM cluster statistics, and device cluster statistics for the last 24 hours.
4. Select a time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or a custom time range) and click **Search**. View the following information:

   - **Affected VM List**

     The **Affected VM List** section shows the I/O hang start time and recovery time of all the VMs, as well as the cluster name and user ID of the cluster to which these VMs belong.

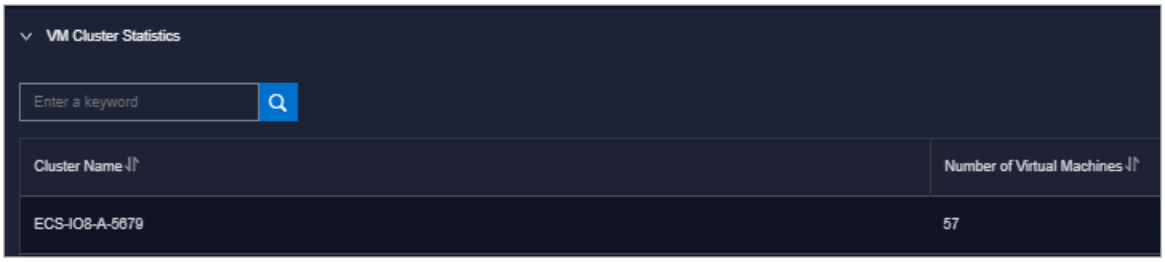
To view the information of a cluster, a user, or a VM, enter the cluster name, user ID, or VM name in the search box to perform a fuzzy search.



- **VM Cluster Statistics**

  The **VM Cluster Statistics** section shows the number of affected VMs in a cluster.

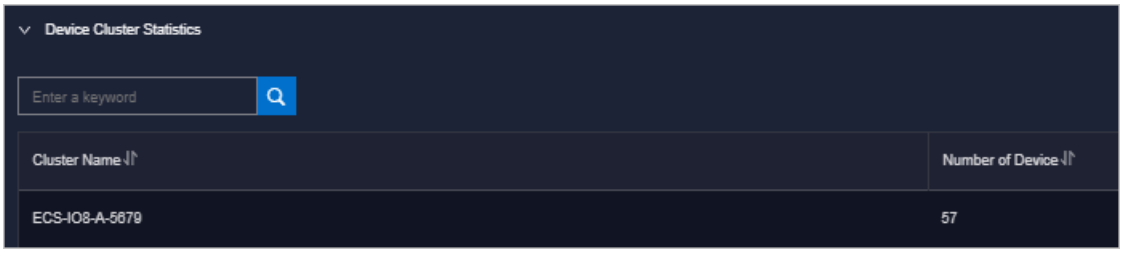
  To view the VM statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.



- **Device Cluster Statistics**

  The **Device Cluster Statistics** section shows the number of affected devices in a cluster.

  To view the device statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.



4.3.15. Slow I/O analysis

The Slow IO Analysis page allows you to view the list of slow I/Os, top ten NCs, cluster statistics, statistics of top 5 clusters, and reasons.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **SLOW IO**.
   By default, the system shows the slow I/O list, top ten NCs, cluster statistics, top 5 cluster statistics, and reasons in the last 24 hours.
4. Select a time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or a customized time range) and click **Search**. View the following information:

   - **Slow IO List**

     The **Slow IO List** section shows the following information related to slow I/Os: the cluster name, NC IP address, virtual machine, device ID, storage type, start time, recovery time, number of slow I/Os, and reasons.

To view the information of a cluster, an NC, or a block device, you can enter the cluster name, NC IP address, or device ID in the search box to perform a fuzzy search.

You can also sort data by Cluster Name, NC IP, Virtual Machine, Device ID, Storage Type, Start Time, Recovery Time, Number of Slow IO, or Reason.

- **Top Ten NC**

  The system shows the information of the top ten NCs by using a graph and a table,

  where:

  - The **Graphical Analysis** section shows the proportion of slow I/Os for each cluster of the top ten NCs by using a pie chart.
  - The **Top Ten NC** section shows the NC IP address, cluster name, as well as number, percentage, and major cause of slow I/Os for each of the top ten NCs.

    To view the information of a cluster or an NC, enter the NC IP address or cluster name in the search box to perform a fuzzy search.

    You can also sort data by NC IP, Cluster Name, Slow IO, and Major Reason.

- **Cluster Statistics**

  The **Cluster Statistics** section shows the cluster name, number of devices, as well as number, percentage, and major reason of slow I/Os for each cluster.

  To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

  You can also sort data by Cluster Name, Number of Device, Number of Slow IO, and Major Reason.

- **Top Five Cluster Statistics**

  The system shows the statistics of top 5 clusters by using a graph and a table,

  where:

  - The **Graphical Analysis** section shows the proportion of slow I/Os for each of the top 5 clusters by using a pie chart.
  - The **Top Five Cluster Statistics** section shows the cluster name, number of devices, as well as number, percentage, and major reason of slow I/Os for each of the top 5 clusters by using a table.

    To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

    You can also sort data by Top Five Cluster, Number of Device, Number of Slow IO, and Major Problem.

- **Reason**

  The system shows reasons on a graph and a table,

  where:

  - The **Graphical Analysis** section shows the proportion of each reason by using a pie chart.
  - The **Reason** section shows the number of slow I/Os from the dimension of reasons.

    To query a specific reason, enter a keyword in the search box to perform a fuzzy search.

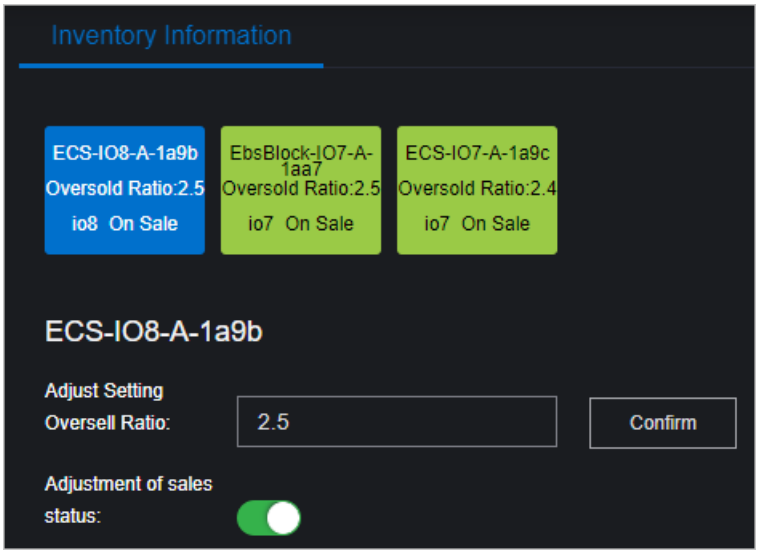
    You can also sort data by Reason and Number of Slow IO.

4.3.16. Product settings

The Product Settings module allows you to view the sales status of a cluster, configure the oversold ratio of a cluster, and specify whether a cluster is available for sale.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **Product Settings**.
   By default, the system shows the data of each cluster in the current environment, including the cluster name, oversold ratio, and sales status.



> **Note** An oversold ratio is the ratio of the marketable capacity of a storage device to the physical capacity. For example, if the physical storage capacity of a storage device is 1 TB and marketabe capacity is 2.5 TB, then the oversold ratio is 2.5.

4. Perform the following operations:
   - Select a cluster, enter a number in the **Adjust Setting Oversell Ratio** field, and then click **Confirm** to set the oversold ratio of the cluster.
   - Select a cluster and turn on or off **Adjustment of sales status** to enable or disable the cluster for sale.

4.3.17. View the disk size rankings of an ECS cluster

The ECS Disk Size Ranking module allows you to view the amount of space occupied by each disk within the elastic block storage attached to an ECS cluster in Apsara Distributed File System.

Background information

When an ECS cluster occupies a large amount of space in Apsara Distributed File System, the on-site O&M personnel must check the space occupied by each disk in the elastic block storage attached to the ECS cluster. Then, they must contact the business side to migrate data and release disk space. The disk size ranking feature helps O&M personnel easily identify which disks occupy a large space in Apsara Distributed File System so that they can perform targeted cleaning and quickly lower the space usage.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Products > Storage > EBS**.
3. In the left-side navigation pane, click **ECS Disk Size Ranking**.
4. Select the ECS cluster that you want to query from the cluster drop-down list and click **Search**.
   All disks attached to the elastic block storage of the selected ECS cluster are listed from large to small based on the actual size of the space they occupy in Apsara Distributed File System. You can view the cluster name, cluster ID, and zone of the selected cluster. You can also view the storage type, size, and identifier of each disk.

4.4. Bases and cloud platforms

4.4.1. Apsara Infrastructure Management

4.4.1.1. Apsara Infrastructure Management 2.0

4.4.1.1.1. Apsara Infrastructure Management overview

This topic describes the overview, features, and terms of Apsara Infrastructure Management.

4.4.1.1.1.1. Apsara Infrastructure Management

Apsara Infrastructure Management is a distributed data center management system. It can manage applications within clusters that contain multiple machines and provide basic features such as deployment, upgrade, scale-in, scale-out, and configuration change.

Apsara Infrastructure Management also provides data monitoring and report analysis features to facilitate end-to-end operations and maintenance (O&M) and management. In large-scale distributed scenarios, Apsara Infrastructure Management offers automatic O&M to improve O&M efficiency and system availability.

Apsara Infrastructure Management is composed of TianjiMaster and TianjiClient. TianjiClient is installed as an agent on a machine. TianjiMaster delivers the received commands to TianjiClient. Apsara Infrastructure Management uses components to implement different features and provides users with the APIServer and console.

4.4.1.1.1.2. Features

This topic describes the core features of Apsara Infrastructure Management.

Apsara Infrastructure Management provides the following core features:

- Initializes networks within a data center.
- Manages server installation and maintenance processes.
- Deploys, scales, and upgrades cloud services.
- Manages cloud service configurations.
- Applies for cloud service resources.
- Repairs software and hardware faults.

- Monitors software and hardware infrastructure and business processes.

4.4.1.1.1.3. Terms

This topic describes the terms that are used in Apsara Infrastructure Management.

project

A group of clusters. A project provides services for users.

cluster

A group of physical machines. A cluster provides services logically and is used to deploy software of a project.

A cluster can only belong to a single project. Multiple services can be deployed within a cluster.

service

A group of software programs used to provide an independent set of features. A service is composed of one or more server roles. A service can be deployed within multiple clusters to provide service capabilities. For example, 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 within a cluster.

server role

One or more indivisible feature units of a service. A server role is composed of one or more applications. If a service is deployed within a cluster, all server roles of the service must be deployed on machines within the same cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same machine.

server role instance

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

application

A process component contained in a server role. Each application works independently. Applications are the minimum units that can be deployed and upgraded in Apsara Infrastructure Management, and can be deployed on each machine. Typically, an application is an executable software program or Docker container.

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

rolling

A process in which Apsara Infrastructure Management upgrades services and modifies cluster configurations based on the configurations updated by users. This process is called rolling.

service configuration template

A template that contains the same service configurations. A service configuration template can make it easy to write the same configurations to different clusters, and applies to large-scale deployment and upgrade scenarios.

associated service template

A file named template.conf in service configurations. The file declares that a specific version of a service configuration template is used by a service instance.

service deployment

An action that deploys a service from scratch within a cluster.

desired state

A state in which all hardware and software on each machine of a cluster work normally and all software programs are in the desired versions.

dependency

A dependency relationship between server roles in a service. Tasks are executed or configurations are upgraded based on the dependency relationship. For example, assume that A depends on B. In this case, A is downloaded after B is downloaded and upgraded after B is upgraded. By default, the dependency of configuration upgrade does not take effect.

upgrade

A way to change the current state of a service to the desired state. After a user submits a version change request, Apsara Infrastructure Management can upgrade the service version to the desired version. An upgrade is performed on each server role, and aims to upgrade all machines to the desired version.

Before an upgrade starts, the current and desired states of a cluster are the same. When a user submits a version change request, the current state remains unchanged, but the desired state changes. A rolling task is generated to gradually approximate the current state to the desired state. When the upgrade ends, the current state is exactly the same as the desired state.

4.4.1.1.2. Log on to Apsara Infrastructure Management

This topic describes how to log on to the Apsara Infrastructure Management console as a role such as an O&M engineer.

Prerequisites

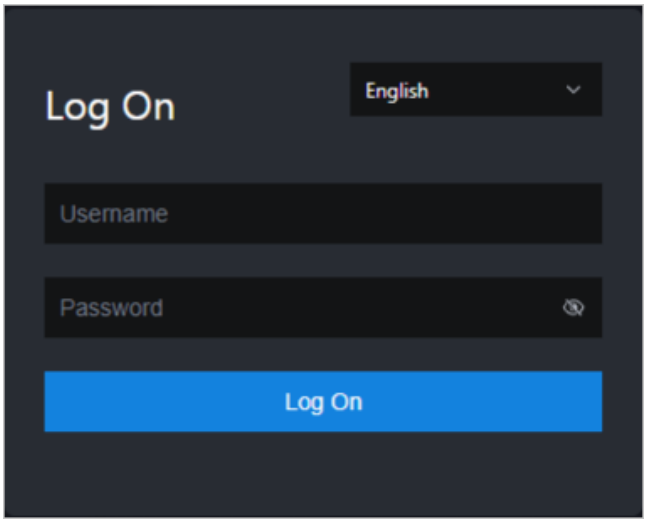
- The URL of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from a deployment engineer or an administrator.

The endpoint of the Apsara Uni-manager Operations Console is in the following format: *region-id.*ops.asconsole.*intranet-domain-id*.

- A supported browser. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the endpoint of the Apsara Uni-manager Operations Console. Press the Enter key.



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

3. Enter your username and password.

   > **Note**
   >
   > Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   The first time you log on to the Apsara Uni-manager Operations Console, follow the prompt to change the password of your username.

   To enhance security, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains at least one of the following special characters: ! @ # $ %
   - The password is 10 to 20 characters in length.

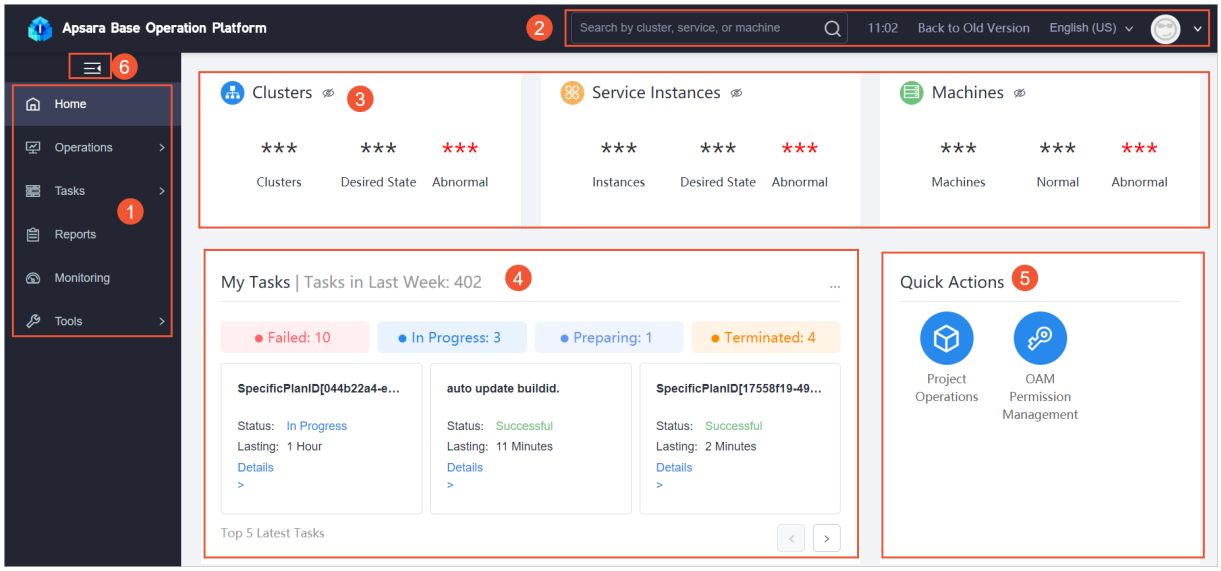
4. Click **Log On**.
5. In the top navigation bar, choose **Products** > **Base/Platforms** > **Apsara Infrastructure Management**.

4.4.1.1.3. Instructions for the homepage

After you log on to the Apsara Infrastructure Management console, the homepage appears. This topic describes the basic operations and functions on the homepage.

Log on to the Apsara Infrastructure Management console. The homepage appears, as shown in the following figure.

Figure 1. Apsara Infrastructure Management homepage



The following table describes the functional sections on the homepage.

Table 1. Sections on Apsara Infrastructure Management homepage

Section	Item	Description
①	Left-side navigation pane	• **Operations**: the quick entrance to operations & maintenance (O&M) operations, which allows you to find operations and their objects. This menu consists of the following submenus: ◦ **Project Operations**: allows you to manage projects based on your project permissions. ◦ **Cluster Operations**: allows you to perform O&M and management operations on clusters based on your project permissions. For example, you can view the status of clusters. ◦ **Service Operations**: allows you to manage services based on your service permissions. For example, you can view the service list. ◦ **Machine Operations**: allows you to perform O&M and management operations on all machines. For example, you can view the status of machines. • **Tasks**: Rolling tasks are generated after you modify configurations in the system. This menu allows you to view the running tasks, task history, and deployment of clusters, services, and server roles in all projects. • **Reports**: allows you to view monitoring data in tables and find specific reports by using fuzzy search. • **Monitoring**: monitors metrics during system operations and sends alert notifications for abnormal situations. This menu allows you to view the alert status, modify alert rules, and search alert history. • **Tools**: provides tools such as machine O&M, IDC shutdown, and clone progress.

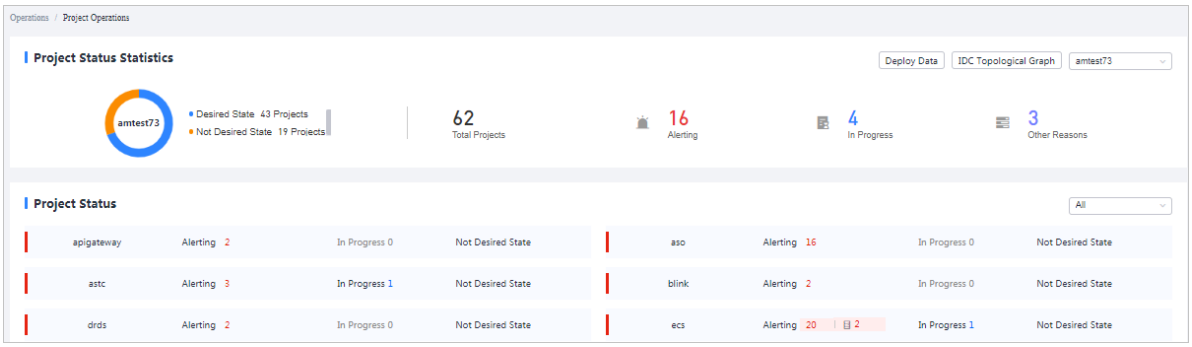
②	Top navigation bar	• Search box: supports global search. You can enter a keyword in the search box to search for clusters, services, and machines. • The following information is displayed when you move the pointer over the time: ◦ **TJDB Sync Time**: the time when the data on the current page is generated. ◦ **Desired State Calc Time**: the time when the desired-state data on the current page is calculated. The system processes data as fast as it can after the data is generated. Latency exists because Apsara Infrastructure Management is an asynchronous system. Time information helps explain why data on the current page is generated and determine whether the system is faulty. • **Back to Old Version**: allows you to return to the old version of the Apsara Infrastructure Management console. • **English (US)**: the current display language of the console. You can select another language from the drop-down list. You can select another language from the drop-down list. • Profile picture: allows you to select **Exit** from the drop-down list to log off your account.
③	Status bar of global resources	Displays the overview of global resources. • **Clusters**: displays the total number of clusters, the percentage of clusters that have reached the desired state, and the number of abnormal clusters. • **Service Instances**: displays the total number of instances, the percentage of instances that have reached the desired state, and the number of abnormal instances. • **Machines**: displays the total number of machines, the percentage of normal machines, and the number of abnormal machines. You can move the pointer over each section and then click**Details** to go to the Cluster Operations, Service Operations, or Machine Operations page.
④	Task status bar	Displays the information of tasks submitted within the last week. You can click the number next to a task state to go to the My Tasks page and view the task details. The top 5 latest tasks are displayed in the lower part of the section. You can click **Details** corresponding to each task to view the task details.
⑤	Quick Actions section	Displays links of the following common quick actions: • **Project Operations**: allows you to go to the Project Operations page. • **OAM Permission Management**: allows you to go to the Operation Administrator Manager (OAM) console. OAM is a centralized permission management platform in the Apsara Uni-manager Operations Console.
⑥	Show/hide button	Allows you to expand or collapse the left-side navigation pane to narrow or enlarge the workspace.

4.4.1.1.4. Project operations

This topic describes how to query a project and view its details.

Procedure

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



3. On the Project Operations page, perform the following operations:
   - Query a project

     In the upper-right corner of the **Project Status** section, enter the name of a project in the search box to search for the project. The search results include the number of alerts, the number of tasks in progress, and whether the project reaches the desired state.
   - View project details
     - Click the number next to **Alerting** corresponding to a project. In the Alert Information dialog box, view the metric name, metric type, and alert source. Click the alert source to view service details.
     - Click the number next to **In Progress** corresponding to a project. In the Tasks dialog box, view details about service upgrade and machine change.

4.4.1.1.5. Cluster operations

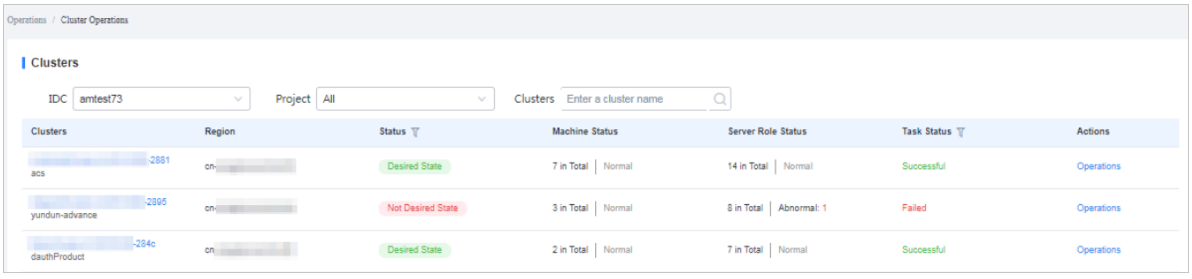
This topic describes the actions about cluster operations.

4.4.1.1.5.1. View the cluster list

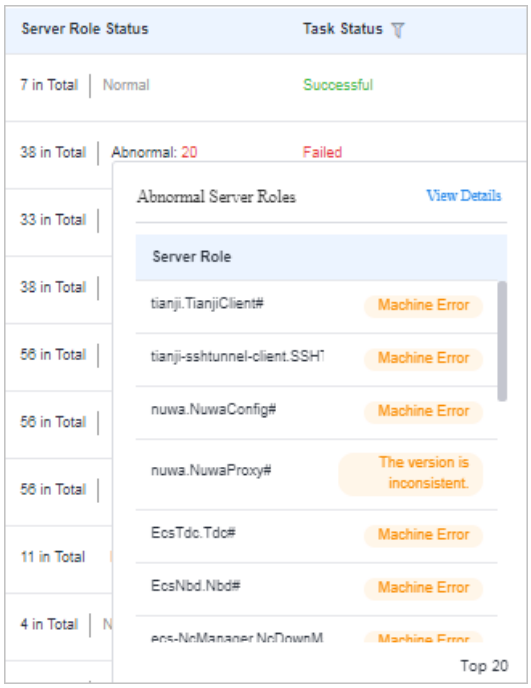
This topic describes how to view all clusters and their information.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the cluster list:
   - On the **Home** page, move the pointer over the **Cluster** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations > Cluster Operations**.



The following table describes the information displayed in the cluster list.

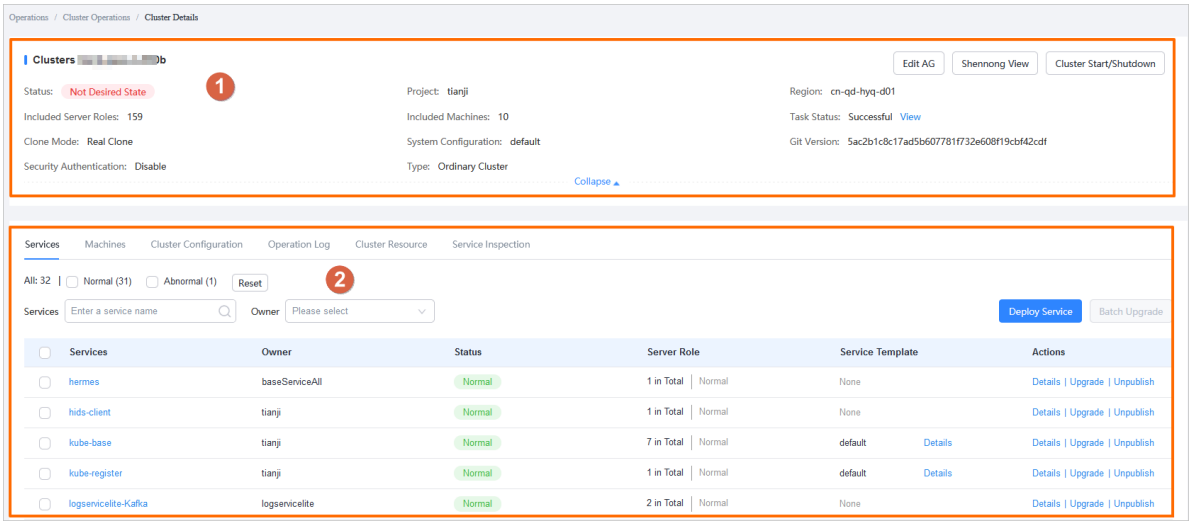
Item	Description
Cluster	The name of the cluster. Click the cluster name to view the cluster details.
Region	The region where the cluster is deployed.
Status	Specifies whether the cluster reaches the desired state. Click the icon to filter clusters. ◦ Desired State: The cluster has reached the desired state. ◦ Not Desired State: The cluster has reached the desired state for the first time but a server role has not reached the desired state due to undefined reasons.
Machine Status	The number of machines within the cluster and the machine status. Click the machine status to go to the Machines tab of the Cluster Details page.
Server Role Status	The number of server roles within the cluster and the server role status. Click a server role status to go to the Services tab of the Cluster Details page. Click **Abnormal** in the Server Role Status column to view all the abnormal server roles in the cluster in the displayed dialog box. Click **View Details** in the upper-right corner of the dialog box to go to the Services tab of the Cluster Details page. 
Task Status	The status of the task related to the cluster. Click the icon to filter clusters. Click the task status to view the task details.
Actions	The available operations. Click **Operations** to go to the **Cluster Details** page.

4.4.1.1.5.2. View details of a cluster

This topic describes how to view details of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. Select a project from the drop-down list or enter a cluster name to search for the cluster.
4. Click the cluster name or click **Operations** in the **Actions** column to go to the **Cluster Details** page.



Section	Item	Description
	Status	◦ **Desired State**: All clusters in a project have reached the desired state. ◦ **Not Desired State**: A project has reached the desired state for the first time but a server role has not reached the desired state due to undefined reasons.
	Project	The project to which the cluster belongs.
	Region	The region where the cluster is deployed.
	Included Server Roles	The number of server roles included in the cluster.
	Included Machines	The number of machines included in the cluster.
	Purpose	The purpose of the cluster. Click the icon. In the dialog box that appears, select a purpose from the drop-down list.

①	**Task Status**	The status of the task. Click **View** to view the task details. ◦ **Successful**: The task is successful. ◦ **Preparing**: Data is being synchronized and the task is not started. ◦ **In Progress**: The cluster has a changing task. ◦ **Paused**: The task is paused. ◦ **Failed**: This task failed. ◦ **Terminated**: The task is manually terminated.
	Clone Mode	◦ **Pseudo-clone**: The system is not cloned when a machine is added to the cluster. ◦ **Real Clone**: The system is cloned when a machine is added to the cluster.
	System Configuration	The name of the system service template used by the cluster.
	Git Version	The change version to which the cluster belongs.
	Security Authentication	The access control among processes. By default, security authentication is disabled in non-production environments. You can enable or disable security authentication to meet your business requirements.
	Type	◦ **Ordinary Cluster**: an operations unit of machine groups, in which multiple services can be deployed. ◦ **Virtual Cluster**: an operations unit of services, which can manage versions of software on machines within several physical clusters in a centralized manner. ◦ **RDS**: a type of cluster that renders special cgroup configurations based on some rules. ◦ **NETFRAME**: a type of cluster that renders special configurations for special scenarios of Server Load Balancer (SLB). ◦ **T4**: a type of cluster that renders special configurations for the mixed deployment of e-commerce. Apsara Stack provides only ordinary clusters.
②	**Services**	The status of each service within the cluster. You can also upgrade or unpublish a service. ◦ **Normal**: The service works normally. ◦ **Not Deployed**: The service is not deployed on machines. ◦ **Changing**: Some server roles in the service are changing. ◦ **Operating**: No server role is changing, but a server role is performing operations and maintenance (O&M). ◦ **Abnormal**: No server role is changing or the machines on which server roles are deployed are not performing O&M operations. However, the server role is in the **not good** state, or the version that the service runs on the machines is different from the desired version.

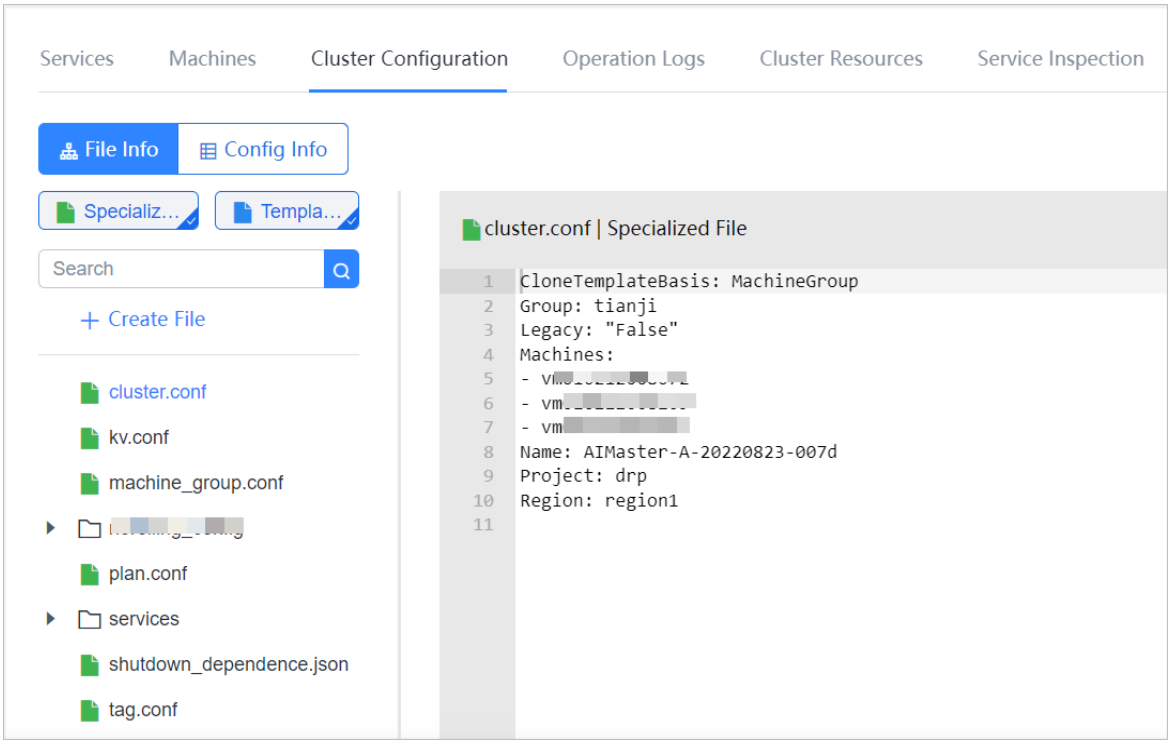
Machines	The running status and monitoring status of each machine within the cluster. You can also view details of server roles that are deployed on each machine.
Cluster Configuration	The configuration file used within the cluster.
Operation Logs	The operation logs. You can also view the version differences.
Cluster Resources	The details of resources that can be filtered.
Service Inspection	The inspection information of each service within the cluster.

4.4.1.1.5.3. View configuration information of a cluster

This topic describes how to view configuration files and folders of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the **Cluster Configuration** tab to view configuration files and folders:
   - Enter a cluster name in the search box in the upper-right corner of the page. Click **Operations** next to the found cluster. On the Cluster Details page, click the **Cluster Configuration** tab.
   - In the left-side navigation pane, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find a cluster and click **Operations** in the **Actions** column. On the Cluster Details page, click the **Cluster Configuration** tab.



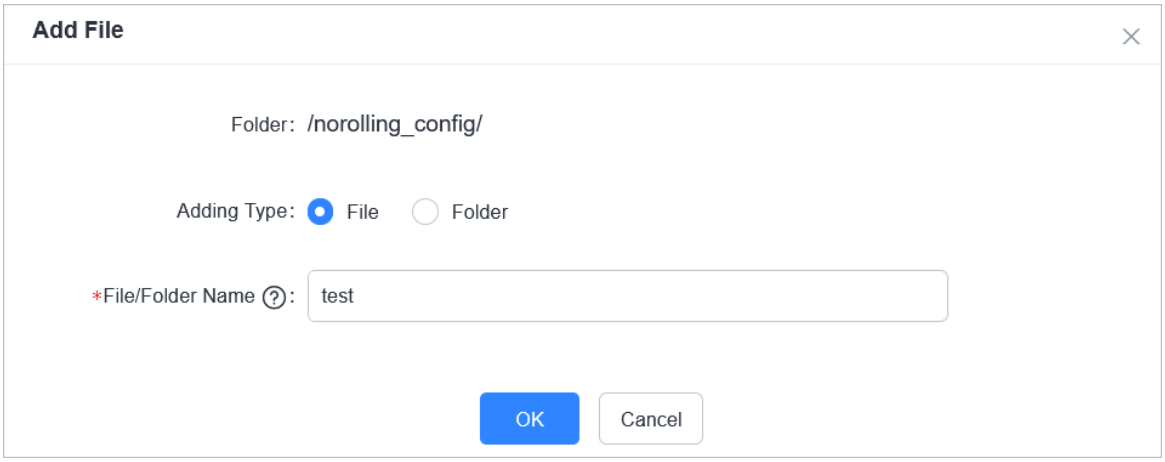
The following table describes configuration files and folders of a cluster.

Item	Description
cluster.conf	The configuration file of the cluster, including the cluster name, cluster type, and machines.
kv.conf	The file that stores the values used to replace template placeholders when configurations are rendered.
machine_group.conf	The file that stores information of machine groups within a cluster.
plan.conf	The file that defines dependencies between services and configuration upgrade parameters.
services	The folder where configurations of each service are stored.
shutdown_dependence.json	The shutdown dependency file.
tag.conf	The file that stores the tags used to calculate tag expressions when configurations are rendered.

3. On the **Cluster Configuration** tab, move the pointer over a folder, click the icon next to the folder name, and then select **Add File** to add a configuration file.

> **Note** You can also click **Create File** below the search box to add a file or folder to the directory.

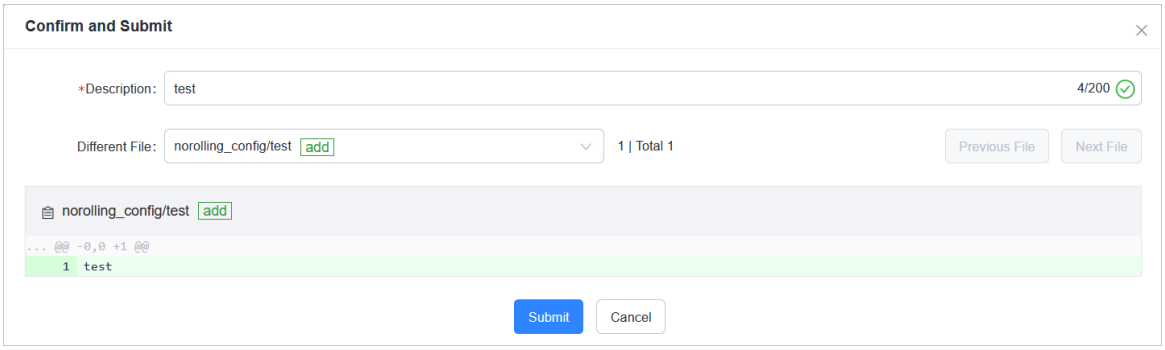
i. In the **Create File** dialog box, enter a file or folder name and click **OK**.



> **Note** After you enter a folder name and click **OK**, the folder is added.

ii. Enter configuration file information into the **Cluster File** text editor. Click **Preview and Submit**.

iii. In the **Confirm and Submit** dialog box, enter **Description** and click **Submit**.



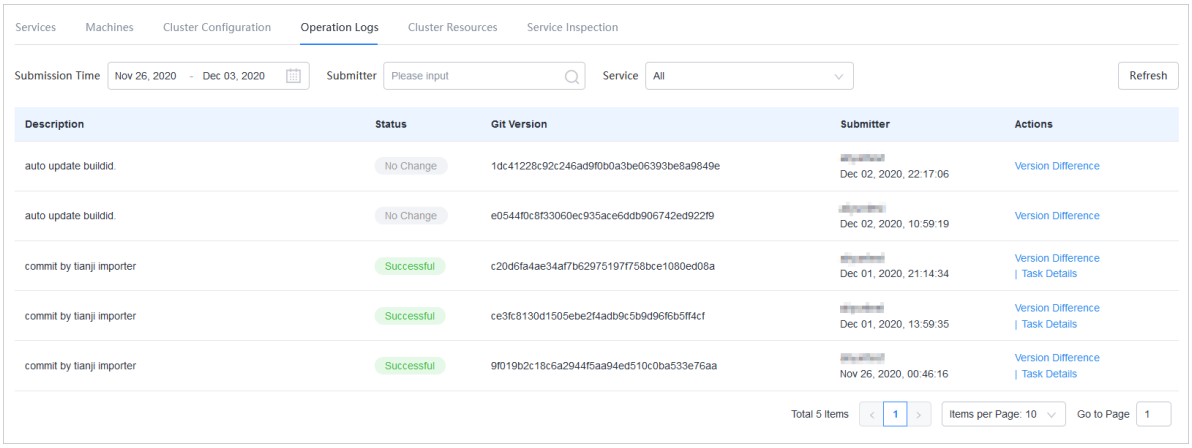
The configuration file is added. Click the **Operation Logs** tab to view related records.

4.4.1.1.5.4. View operation logs

This topic describes how to view differences between Git versions from operation logs.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the operation logs of a cluster:
   - Enter a cluster name in the search box in the upper-right corner of the page. Click **Operations** next to the found cluster. On the Cluster Details page, click the **Operation Logs** tab.
   - In the left-side navigation pane, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find a cluster and click **Operations** in the **Actions** column. On the Cluster Details page, click the **Operation Logs** tab.



3. View the version differences on the **Operation Logs** tab.
   i. Find the operation log that you want to view and click **Version Difference** in the **Actions** column.
   ii. Set **Configuration Type** to **Show Configuration** or **Cluster Configuration**.
      - **Show Configuration**: displays the cluster configuration merged with the template configuration.
      - **Cluster Configuration**: displays the cluster configuration.
        - Cluster configuration description: Each cluster contains its dedicated configurations, such as the list of machines.
        - Template configuration description: A template that has the same configurations can be used to deploy a service to multiple clusters.
   iii. Select a basic version below **Configuration Type**. Then, a difference file is displayed in the lower part of the page.
   iv. Select a difference file from the **Difference File** drop-down list to view the content of each difference file.

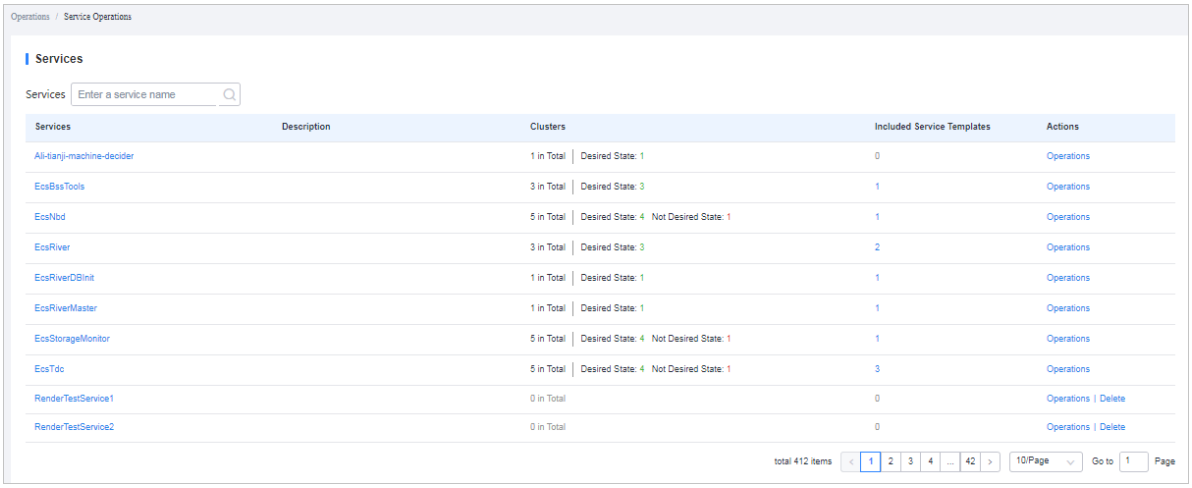
4.4.1.1.6. Service operations

4.4.1.1.6.1. View the service list

This topic describes how to view all services and their information.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the service list:
   - On the **Home** page, move the pointer over the **Service Instances** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations > Service Operations**.



The following table describes the information displayed in the service list.

Item	Description
Service	The name of the service. Click the service name to view the service details.
Clusters	The number of clusters in which the service is deployed and the cluster status.
Included Service Templates	The number of service templates that are included in the service.
Actions	◦ Click **Operations** to go to the Service Details page. ◦ Click **Delete** to delete the service. **Note** A service can be deleted only when the number of clusters in which the service is deployed is 0.

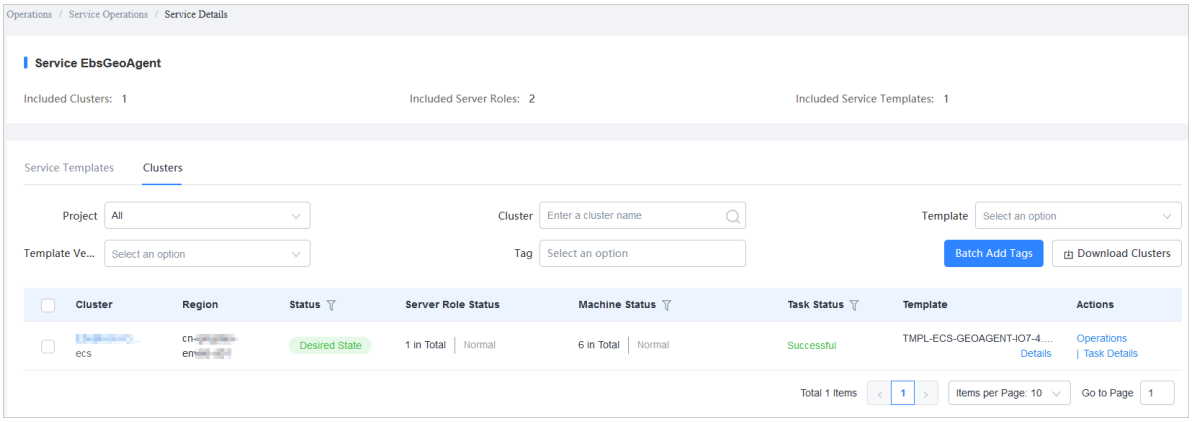
3. Enter a service name in the search box to search for the service.

4.4.1.1.6.2. View details of a server role

This topic describes how to view details of a server role.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Operations > Service Operations**.
3. Enter a service name in the search box to search for the service.
4. Click the service name or click **Operations** in the **Actions** column.
5. On the **Clusters** tab, click a state in the **Server Role Status** column to view the server roles included in a cluster.



6. Select the server role that you want to view.
   - Click the **Machines** tab to view details of the server role.

Item	Description
Machine	The machine where the server role is deployed. Click the machine name to view the machine details.
Actions	▪ Click **Metric** to view the server role, machine, and system service metrics. ▪ Click **Applications** to view application versions. ▪ Click **Terminal** to log on to the machine and perform operations. ▪ Click **Restart Server Role** to restart the server role.

   - Click the **Upgrade History** tab. Click **Details** in the **Actions** column to view details of a historical task.

4.4.1.1.6.3. Block hardware alerts

This topic describes how to block hardware alerts.

Background information

You must block hardware alerts in the following scenarios:

- Alerts are improperly triggered by hardware. In this case, you must block the alerts, and then cancel the block operation after no alerts are reported.
- Upgrades fail to reach the desired state due to hardware faults, and the hardware faults cannot be rectified at this time. In this case, you must block the alerts, and then cancel the block operation after the desired state is reached.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Operations** > **Service Operations**.
3. In the search box, enter **cruiser** to search for the cruiser service.
4. Find the cruiser service and click **Operations** in the **Actions** column.
5. Click the **Clusters** tab.
6. Click **Operations** in the **Actions** column corresponding to a cluster.

7. Click the **Cluster Configuration** tab. Open the `/user/ignore_monitor_config.json` file in **Cluster File**. Modify the configuration file.

   The following table describes information displayed in the configuration file.

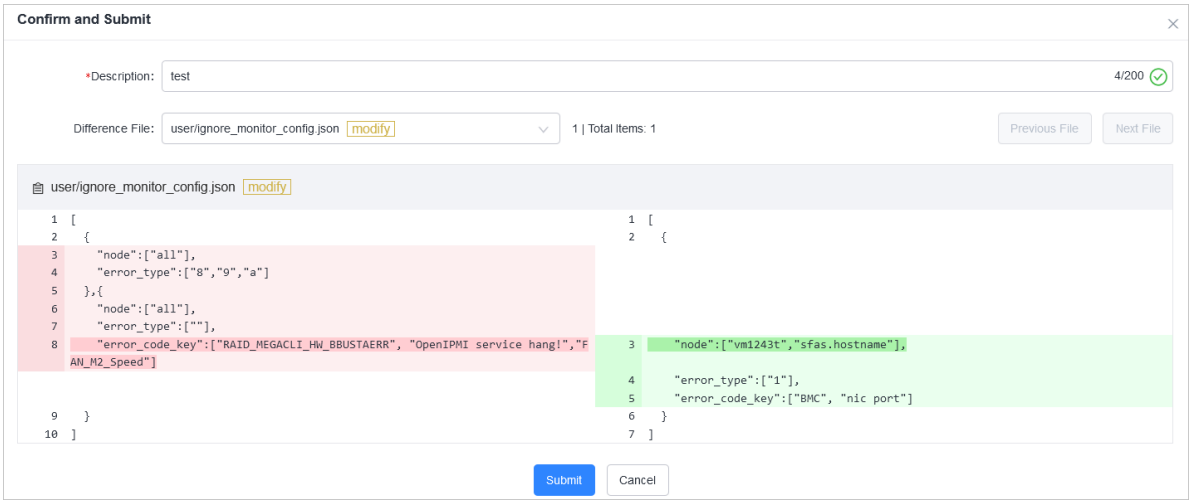
Item	Description	Remarks
node	The name of the machine where alerts are blocked. If you want to block alerts on all machines, set the parameter to `"all"`.	◦ All the node, error_type, and error_code_key parameters are in an array format. ◦ The node parameter is required. ◦ At least one of the error_type and error_code_key parameters is required.
error_type	The type of the fault that triggers alerts. Valid values: ◦ 0: LogicDrive fault ◦ 1: hard disk fault ◦ 2: memory fault	
error_code_key	The keyword that is used to block alerts. The keyword can be the error code or information.	

   Examples:

```
{
   "node":["vm1243t", "sfas.hostname"],
   "error_type":["1"]
   "error_code_key":["BMC", "nic port"]
 }
```

   In the preceding example, the alerts caused by hard disk faults are blocked on the vm1243t and sfas.hostname machines. The error information includes BMC and NIC port.

8. Click **Preview and Submit**.
9. In the **Confirm and Submit** dialog box, enter the description and click **Submit**.



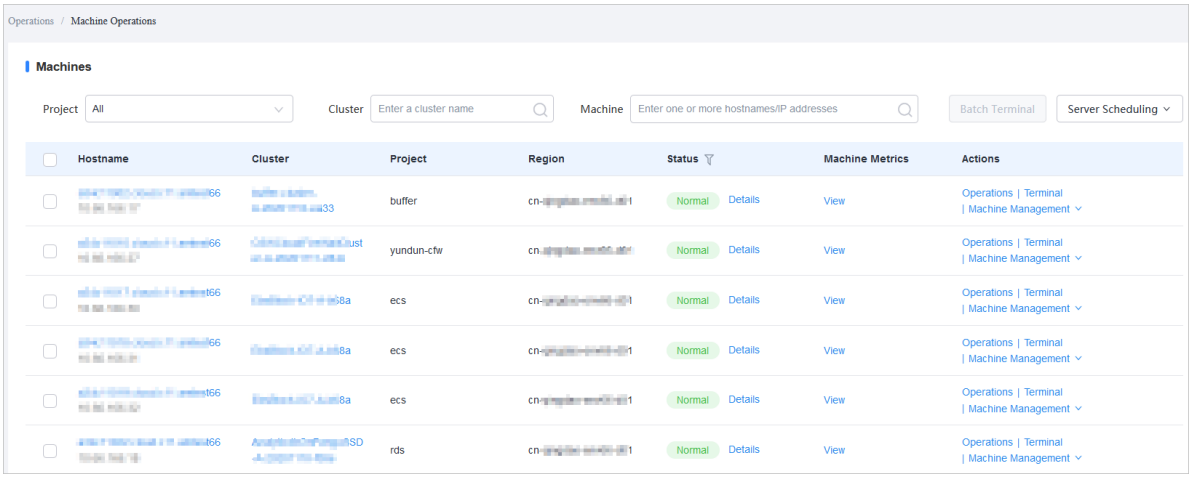
0. Click the **Operation Logs** tab to view related records.

4.4.1.1.7. Machine operations

This topic describes how to view the statistics of all machines.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the machine list:
   - On the **Home** page, move the pointer over the **Machine** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations > Machine Operations**.
3. Select a project from the drop-down list or enter a cluster or machine name to search for the machine.



Item	Description
Hostname	The hostname of the machine. Click a hostname to go to the Machine Details page.
Cluster	The cluster where the machine is deployed. Click a cluster name to go to the Cluster Details page.

Status	The status of the machine. Click the icon to filter machines. Click **Details**. Then, the **Status Details of Machine** dialog box appears.
Machine Metrics	The metrics of the machine. Click **View**. Then, the **Metrics** dialog box appears. Metrics are displayed on the **Server Role Metric**, **Machine Metrics**, and **System Service Monitor** tabs. You can view the status and update time of each metric. Enter a keyword in one of the search boxes in the upper-right corner to search for a server role or metric. You can also select the status in the upper-left corner to filter metrics.
Actions	◦ Click **Operations** to go to the Machine Details page. ◦ Click **Terminal** to log on to the machine and perform operations. You can select multiple machines and then click **Batch Terminal** in the upper-right corner to log on to multiple machines at a time. ◦ Click **Machine Management** to perform an out-of-band restart operation on the machine.

4.4.1.1.8. Machine repairs

If the CPU, memory, or system disk or a machine is damaged or the physical machine needs to be shut down for a long time, you can perform machine repairs on the **Machine Repair** page. Machine repairs stipulate standardized processes for repairs. You can perform operations such as preprocessing and approving server roles, starting repairs, completing repairs and cloning. These processes assist you undergoing repairs and serve the purpose of reducing complexity.

Background information

Machine repairs involve many steps and may contain non-standard operations. You may experience difficulties because you must check the machine status on many pages and perform operations with the command line. Standardized processes and console operations are designed to simplify machine repairs.

During repairs, your machines may be shut down for a very long period or encounter unrecoverable issue. You must back up your machines in advance to prevent data loss.

The process for a machine repair:

1. Before the repair: On the **Machine Repair** page, perform preprocessing and approval steps to migrate data. Manually migrate data that cannot be automatically migrated on the page. All services and all data on the machine are migrated.
2. During the repair: Shut down the faulty machine, replace the faulty hardware, and restart the machine.
3. After the repair: On the **Machine Repair** page, click Complete Repair or Complete Repair and Clone. Then, Apsara Infrastructure Management automatically redeploys services on the machine and restores the machine.

Prerequisites

The host name or IP address of the machine to be repaired is obtained.

Procedure

1. Log on to the Apsara Infrastructure Management console.

2. Go to the **Machine Repair** page.
   i. In the left-side navigation pane, choose **Operations > Machine Operations**.
   ii. On the **Machine Operations** page, search for the machine by entering its hostname or IP address, and click the hostname of the machine.
   iii. In the upper-right corner of the **Machine Details** page, select **Machine Repair** from the **Machine Management** drop-down list.
   iv. In the **Confirmation** dialog box, enter a `Repair` and click **OK**.
   v. After the status of the machine changes to **Repairing**, click **Details** to go to the **Machine Repair** page.
3. Perform preprocessing steps.
   i. On the **Machine Repair** page, click **Add SR for Preprocessing**.
   ii. In the **Add SR for Preprocessing** dialog box, select the server role and click **OK**.
4. Perform approval steps.
   i. In the **Components** section, view the status of server roles. When the server roles are all in the **Successful** state, click **Enter Approval Phase** at the lower part of the page. In the **Confirmation** message, click **OK**.

      Server role approval can be automatic approval or manual approval. When server roles are in the normal state, the system starts automatic approval. All server roles are automatically updated to the **Successful** state. You can initiate manual approval only when service roles are abnormal and remain in the **Pending** state for a long period.

      > ⚠ **Warning**
      > - Manual approval may cause data loss. If you can ensure that all data is migrated, manual approval is allowed.
      > - If some data needs to be manually migrated and processed, complete these steps before manual approval to prevent data loss.

      Manual approval procedure: Click **Manual Approval** in the **Actions** column corresponding to the server role. In the **Approve** dialog box, select **Approved** and click **OK**. After manual approval is complete, all server roles are updated to the **Successful** state.
   ii. In the **Server Roles for Approval** section, view the role status. When all roles are in the **done** state, click **Enter Repair Phase** at the lower part of the page.
   iii. In the **Machine Information** section, view machine information.
5. Shut down the machine and perform the repair. After the repair is complete, restart the machine and check whether the machine is normal.
   - If yes, proceed to the next step.
   - If no, contact technical support engineers.
6. Go to the **Machine Repair** page of the machine, and click Complete Repair or Complete Repair and Clone depending on whether you want to clear remaining data.

   > ⓘ **Note** We recommend that you select **Complete Repair and Clone** to clear remaining data after the machine repair is complete.

   - If you want to clear remaining data, click **Complete Repair and Clone**. In the **Confirmation** dialog box, enter `Clone` and click **OK**.
   - If not, click **Complete Repair**. In the **Confirmation** dialog box, click **OK**.

   Then, you are redirected to the **Machine Details** page. When the status of the machine

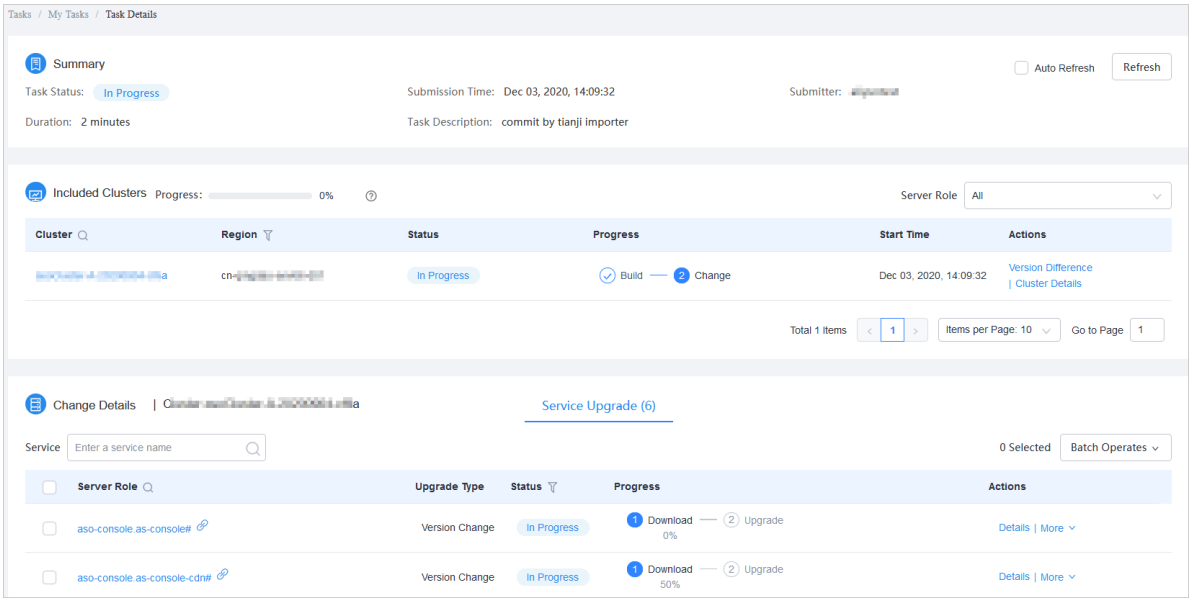
changes to **Normal**, the services are deployed and the machine becomes normal.

4.4.1.1.9. View tasks

This topic describes how to view the submitted tasks and their statuses.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the task list:
   - In the left-side navigation pane, choose **Tasks > My Tasks**.
   - In the left-side navigation pane, choose **Tasks > Related Tasks**.
3. (Optional) Click the icon in the **Status** column to filter tasks.
4. Find the task that you want to view and click the task name or **Details** in the **Actions** column.
5. View the status and progress of each cluster and server role on the **Task Details** page.



4.4.1.1.10. Reports

4.4.1.1.10.1. View reports

This topic describes how to view report data.

Background information

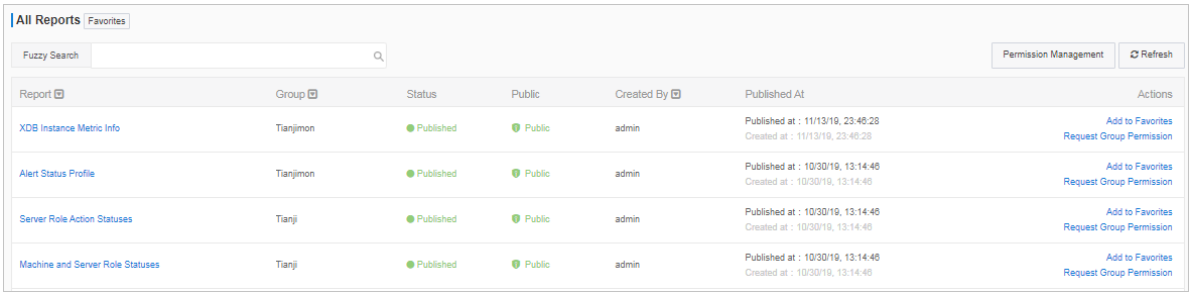
You can choose to view the following reports in the Apsara Infrastructure Management console:

- System reports: include default and common reports in the system.
- All reports: include system reports and custom reports.

Procedure

1. Log on to the Apsara Infrastructure Management console.

2. In the left-side navigation pane, click **Reports**. On the Reports page, click **Go** to go to the All Reports page.



The following table describes information about reports.

Item	Description
Report	The name of the report. Move the pointer over the down arrow next to Report and search by report name.
Group	The group to which the report belongs. Move the pointer over the down arrow next to Group and search by group name.
Status	Specifies whether the report is published. ◦ Published ◦ Not Published
Public	Specifies whether the report is public. ◦ Public: visible to all logon users. ◦ Private: visible only to the current logon user.
Created By	The person who creates the report.
Published At	The time when the report is created and published.
Actions	◦ Click **Add to Favorites** to add the report to your favorites. Then, you can view the report by choosing **Reports > Favorites** in the top navigation bar. ◦ Click **Request Group Permission** to go to the Operation Administrator Manager (OAM) console. You can then configure groups and permissions. For more information, see **OAM** in **Operations and Maintenance Guide**.

3. **Optional:**Enter a report name in the search box to search for the report.
4. Click the report name to go to the corresponding report details page.
   For more information about reports, see Appendix.

4.4.1.1.10.2. Add a report to favorites

This topic describes how to add frequently used reports to favorites. Then, you can find them on the Home or Favorites page.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click **Reports**. On the Reports page, click **Go** to go to the All Reports page.
3. Search for a report in the search box.
4. Click **Add to Favorites** in the **Actions** column corresponding to the report.
5. In the **Add to Favorites** dialog box, enter tags for the report.
6. Click **Add to Favorites**.

4.4.1.1.11. Monitoring center

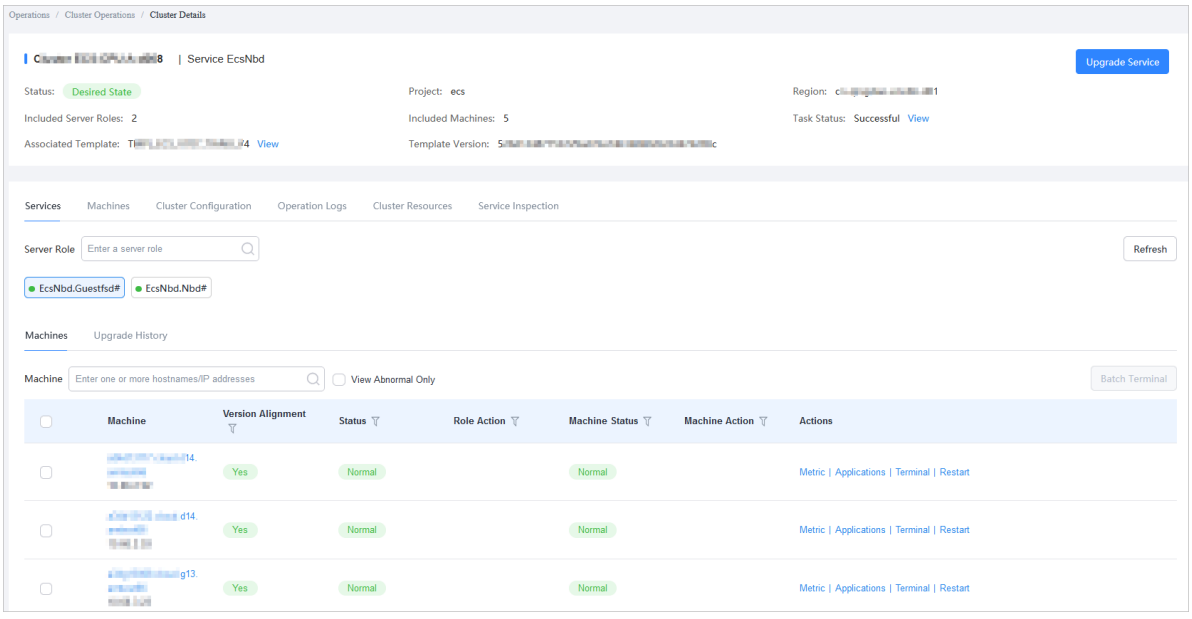
You can view the alert status, alert rules, and alert history in the monitoring center.

4.4.1.1.11.1. View the status of a metric

This topic describes how to view the status of a metric.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Operations > Service Operations**.
3. Enter a service name in the search box to search for the service.
4. Click **Operations** in the **Actions** column corresponding to the service.
5. Click the **Clusters** tab.
6. Find the cluster that you want to view and click **Operations** in the **Actions** column.
7. On the **Services** tab, select a server role and click **Metrics** in the **Actions** column corresponding to a machine to view the server role, machine, and system service metrics.

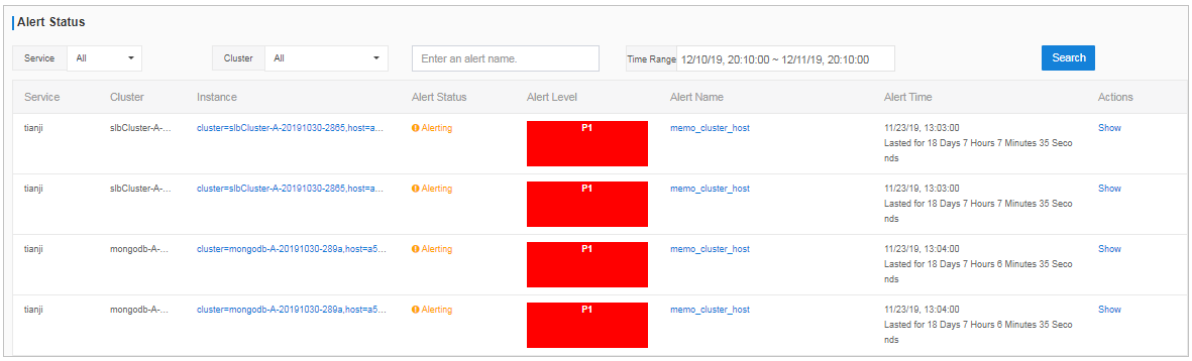


4.4.1.1.11.2. View the alert status

This topic describes how to view the alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert Status**.



4. Search for an alert by service name, cluster name, alert time range, or alert name.
5. View alert details on the **Alert Status** page. The following table describes the information about the alert status.

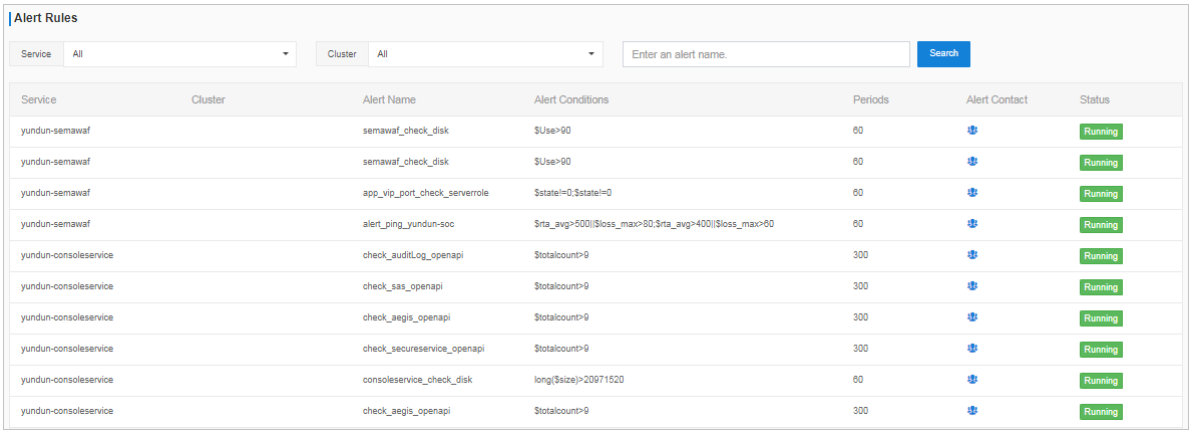
Item	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Instance	The name of the monitored instance. Click the name of an instance to view the alert history of the instance.
Alert Status	The state of the alert. Two alert states are available, which are**Normal** and **Alerting**.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ◦ P0: an alert that has been cleared ◦ P1: a critical alert ◦ P2: a major alert ◦ P3: a minor alert ◦ P4: a warning alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered and how long the alert lasts.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

4.4.1.1.11.3. View alert rules

This topic describes how to view the alert rules of a service.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert Rules**.



4. Search for alert rules by service name, cluster name, or alert name.
5. View alert rules on the **Alert Rules** page. The following table describes the information about alert rules.

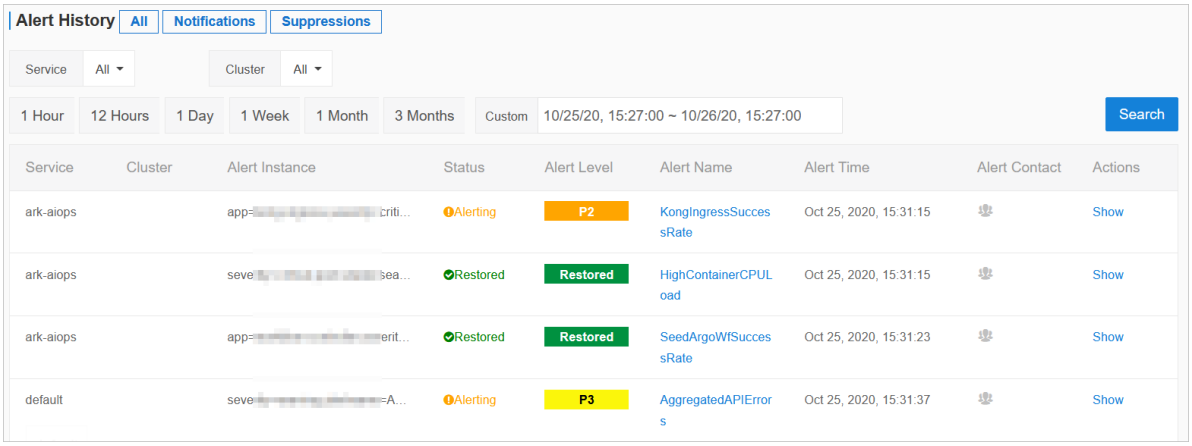
Item	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Alarm Name	The name of the alert.
Alert Conditions	The conditions that trigger the alert.
Periods	The frequency at which the alert rule is executed.
Alert Contact	The groups and members to notify when the alert is triggered.
Status	The status of the alert rule. ◦ **Running**: Click it to stop the alert rule. ◦ **Stopped**: Click it to execute the alert rule.

4.4.1.1.11.4. View alert history

This topic describes how to view the historical alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert History**.



4. Search for an alert by service name, cluster name, alert cycle, or alert time range.
5. View the alert history on the **Alert History** page. The following table describes the information about historical alerts.

Item	Description
Service	The name of the service to which the alert belongs.
Cluster	The name of the cluster where the service is deployed.
Alert Instance	The name of the instance where the alert is triggered.
Status	The state of the alert. Two alert states are available, which are**Normal** and **Alerting**.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ◦ P0: an alert that has been cleared ◦ P1: a critical alert ◦ P2: a major alert ◦ P3: a minor alert ◦ P4: a warning alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered.
Alert Contact	The groups and members to notify when the alert is triggered.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

4.4.1.1.12. Tools

4.4.1.1.12.1. Use machine operations tools

This topic describes how to use machine operations tools in typical scenarios.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Tools > Operation Tools > Machine Tools**. On the Machine Tools page, click **Go** to go to the Operation Tools page.
3. Select a scenario from the Operation Scene drop-down list.

Scenario	Description	Operation
Scene 1. NC Scale-out (with existing machines)	Scales out an SRG of the worker type.	Select a cluster from the Target Cluster drop-down list and an SRG from the Target SRG drop-down list. Select the machines to scale out in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 2. Host Scale-out (with existing machines)	Scales out DockerHost#Buffer of a cluster.	Select a cluster from the Target Cluster drop-down list. Select the machines to scale out in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 3. NC Scale-in	Scales in an SRG of the worker type.	Select a cluster from the Target Cluster drop-down list and an SRG from the Target SRG drop-down list. Select the machines to scale in in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 4. Host Scale-in	Scales in DockerHost#Buffer of a cluster.	Select a cluster from the Target Cluster drop-down list. Select the machines to scale in in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 5. VM Migration	Migrates virtual machines (VMs) from a host to another host.	Select a source host from the Source Host drop-down list and a destination host from the Destination Host drop-down list. Select the VMs to migrate in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.

Scene 6. Host Switching	Switches a standby host to the primary host.	Select a source host from the Source Host drop-down list and a destination host from the Destination Host drop-down list. Click **Submit**. In the message that appears, click **Confirm**.

4.4.1.1.12.2. Shut down a data center

This topic describes how to shut down up to 25 machines within all clusters of a data center in scenarios such as vehicle-mounted devices.

Prerequisites

- The total number of machines within all clusters of a data center cannot exceed 25.
- Your browser is connected with the machines on which Apsara Infrastructure Management is deployed over a smooth network. If a proxy is required to log on to the Apsara Infrastructure Management console, the proxy is not configured on a machine that you want to shut down.
- Your browser remains active while the machines are being shut down.
- Data related to operations such as scaling is not retained within the default cluster before the machines are shut down.

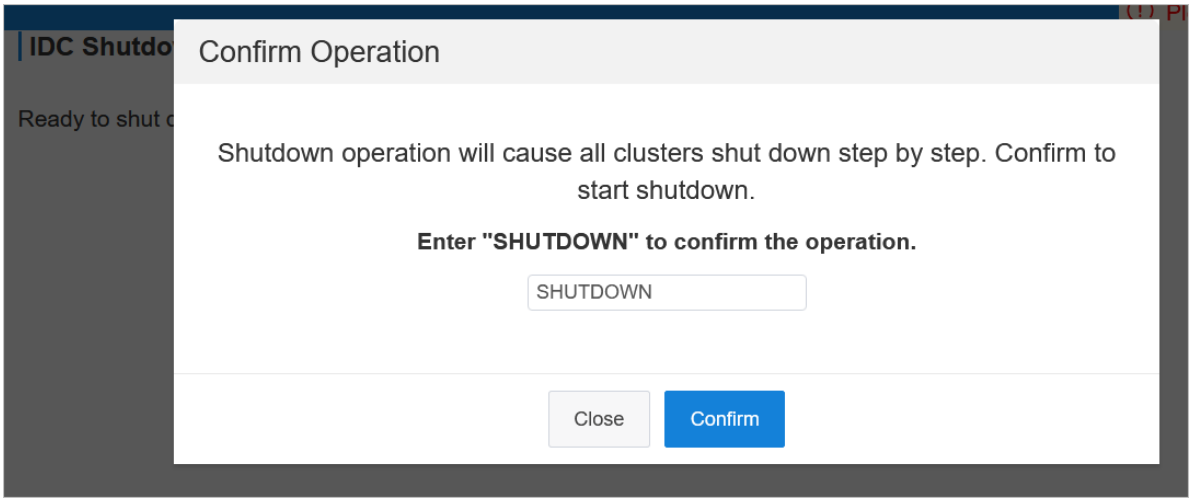
Background information

When you shut down a data center, business clusters are shut down first, and then the base cluster is shut down.

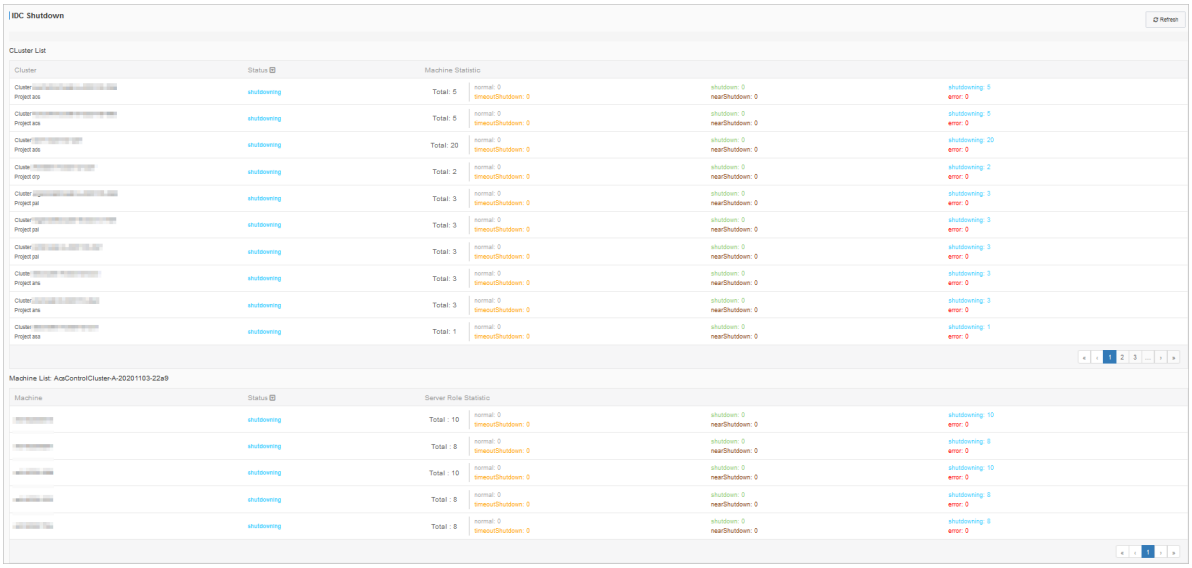
Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Tools > IDC Shutdown**. In the right-side workspace, click **Go**.
3. On the **IDC Shutdown** page, click **Start Shutdown**.
4. In the **Confirm Operation** message, enter `SHUTDOWN` and click **Confirm**.

> ⚠ **Warning**
>
> - The data center shutdown operation shuts down all services and machines and thus cause business interruption.
> - Backend services must communicate with the frontend shutdown page during the data center shutdown process. Do not close the shutdown page until the shutdown is complete.



5. View the data center shutdown progress and the statuses of clusters, machines, and server roles.



It takes a long time to shut down all clusters and machines within an environment. You can view the shutdown progress on the **IDC Shutdown** page. The following statuses are available for clusters, machines, and server roles:

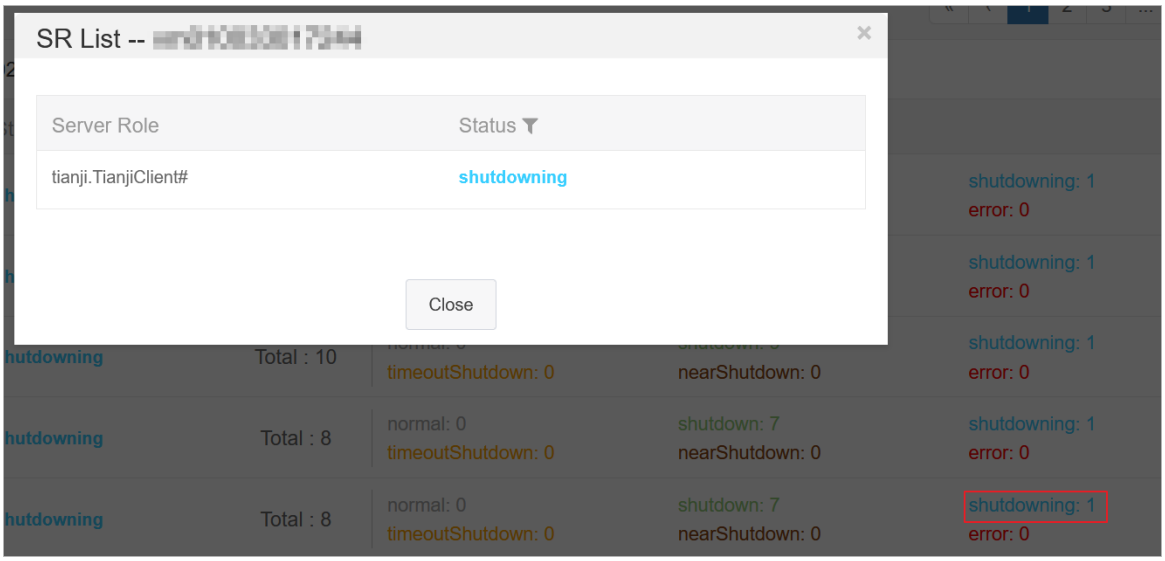
- **normal**: A cluster, machine, or server role is running normally.
- **shutdown**: A cluster, machine, or server role is shut down.
- **shutdowning**: A cluster, machine, or server role is being shut down.
- **timeoutShutdown**: The shutdown of a cluster, machine, or server role timed out.
- **nearShutdown**: A cluster, machine, or server role is about to be shut down.
- **error**: An error occurred while a cluster, machine, or server role is being shut down.

You can perform the following operations:

- View the data center shutdown progress: In the upper part of the **IDC Shutdown** page, view the data center shutdown progress.
- View the cluster status: In the **Cluster List** section, view the status of each cluster, the total number of machines within each cluster, and the number of machines in each state.
- View the machine status: In the **Cluster List** section, click a state corresponding to a cluster. In the **Machine List** section, view all machines in the corresponding state within the cluster, the total number of server roles on each machine, and the number of server

roles in each state.

- View the server role status: In the **Machine List** section, click a state corresponding to a machine. In the **SR List--xxx** message, view all server roles in the corresponding state on the machine.



> **Note**
>
> In the left-side navigation pane, click **Go**. On the **All Reports** page, enter the entire or part of **Machine Power On or Off Statuses of Clusters** in the **Fuzzy Search** search box. In the search results, click **Machine Power On or Off Statuses of Clusters** to view the status of each server role.

- Filter clusters or machines: In the **Cluster List** or **Machine List** section, click the filter icon in the **Status** column and select a state to filter all clusters or machines in the corresponding state.
- Refresh data: Click **Refresh** in the upper-right corner to refresh data.

If all clusters in the **Cluster List** section are displayed in the **shutdown** state, the data center shutdown operation succeeds. After the base cluster is shut down, the OPS1 server is also shut down. Then, the Apsara Infrastructure Management console is inaccessible.

6. After all base machines are shut down and inaccessible, go to the data center and confirm that all machines are powered off.

What to do next

If you want to use the machines in the future, power on each machine one by one in the data center and wait until all services reach the desired state.

4.4.1.1.12.3. View the clone progress

This topic describes how to go to the OS Provision console (Corner Stone) and check the progress, status, and errors about machine installation.

Prerequisites

The username and password used to log on to the OP Provision console are obtained from delivery personnel.

Background information

Apsara Infrastructure Management provides a quick entry to the OS Provision console, which allows you to view details about machine installation. You can then obtain the progress and status about machine installation and then locate the installation faults.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, choose **Tools > Clone Progress**.
3. On the logon page of the OS Provision console, enter **Username** and **Password**, and then click **Submit**.

4.4.1.1.13. Appendix

4.4.1.1.13.1. 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 name of the project.
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 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 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 status of the machine.
Machine Action	The action that Apsara Infrastructure Management asks the machine to perform, such as the clone action.

4.4.1.1.13.2. 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.

4.4.1.1.13.3. Machine info report

This report displays the states of machines and server roles on the machines.

Machine Status

This section displays all the machines currently managed by Apsara Infrastructure Management and their states. In the **Global Filter** section in the upper part 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 name of the machine.
IP	The IP address of the machine.
Machine Status	The status of the machine.
Machine Action	The action currently performed on the machine.
Machine Action Status	The status of the action.
State Desc	The description of the machine status.

Expected Server Role List

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.

Server Role	The name of the expected server role on the machine.

Abnormal Monitoring Status

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item.
Updated At	The updated time of the monitored item.

Server Role Version and Status on Machine

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Server Role	The name of the server role.
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.
State Desc	The description of the status.
ErrorMessage	The error message of the server role.

Monitoring Status

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Server Role	The name of the server role.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item.

Updated At	The updated time of the monitored item.

4.4.1.1.13.4. Rolling info report

This report displays the running and completed rolling tasks and the task-related states.

Rolling Tasks

This section displays the rolling tasks that are running. If no rolling tasks are running, no data is displayed in this section.

Item	Description
Cluster	The name of the cluster.
Git Version	The version of the change that triggers the rolling task.
Description	The description of the change entered by a user when the user submits the change.
Start Time	The start time of the rolling task.
End Time	The end time of the rolling task.
Submitted By	The ID of the user who submits the change.
Rolling Task Status	The current status of the rolling task.
Submitted At	The time when the change is submitted.

Server Role in Job

When you select a rolling task in the **Rolling Tasks** section, this section displays the rolling states of server roles related to the selected task. If no rolling tasks are selected, the states of server roles related to all historical rolling tasks are displayed.

Item	Description
Server Role	The name of the server role.
Server Role Status	The rolling status of the server role.
ErrorMessage	The error 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 for which the rolling task was approved by the decider.
Failure Rate	The proportion of machines on which the rolling task failed.

Success Rate	The proportion of machines on which the rolling task succeeded.

Server Role Rolling Build Information

This section displays the current and desired versions of each application in the server role during the rolling process.

Item	Description
App	The name of the application that requires rolling in the server role.
Server Role	The server role to which the application belongs.
From Build	The version of the application before the upgrade.
To Build	The version of the application after the upgrade.

Server Role Statuses on Machines

When you select a server role in the **Server Role in Job** section, this section displays the status of the server role on each machine.

Item	Description
Machine Name	The name of the machine on which the server role is deployed.
Expected Version	The desired version of the server role.
Actual Version	The current version of the server role.
State	The status of the server role.
Action Name	The ongoing action on the server role.
Action Status	The status of the action.

4.4.1.1.13.5. Machine RMA approval pending list

Some Apsara Infrastructure Management 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

This section displays the basic information of pending approval machines.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
IP	The IP address of the machine.

State	The 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

This section displays the information of server roles on the pending approval machines.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
Serverrole	The name of the server role.
State	The 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

This section displays the hard disk information of pending approval machines.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
Component	The hard disk on the machine.
State	The 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.

4.4.1.1.13.6. 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.

4.4.1.1.13.7. 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.

4.4.1.1.13.8. 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.

4.4.1.1.13.9. 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.
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.

4.4.1.1.13.10. Statuses of project components

This report displays the statuses of all abnormal server roles on machines within the current project. This report also displays the alert information of server roles and machines reported to Monitoring System.

Error State Component Table

This section displays the server roles that are not in the GOOD state or that are pending upgrade.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Service	The name of the service.
Server Role	The name of the server role.
Machine Name	The name of the machine.
Need Upgrade	Specifies whether the version has reached the desired state.
Server Role Status	The status of the server role.
Machine Status	The status of the machine.

Server Role Alert Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.

Service	The name of the service.
Server Role	The name of the server role.
Machine Name	The name of the machine.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.
Description	The description of the alert.
Updated At	The update time of the alert.

Machine Alert Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.
Machine Name	The name of the machine.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.
Description	The description of the alert.
Updated At	The update time of the alert.

Service Inspector Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.
Service	The name of the service.
Server Role	The name of the server role.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.
Description	The description of the alert.
Updated At	The update time of the alert.

4.4.1.1.13.11. 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.

4.4.1.1.13.12. 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.
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.

4.4.1.1.13.13. 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.
Level	Whether the clone action performed by the machine is normal.
Clone Status	The current status of the clone action performed by the machine.

4.4.1.1.13.14. 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.

4.4.1.1.13.15. 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.

4.4.1.2. Apsara Infrastructure Management 1.0

4.4.1.2.1. Apsara Infrastructure Management

This topic describes the features and terms of Apsara Infrastructure Management.

4.4.1.2.1.1. Apsara Infrastructure Management overview

Apsara Infrastructure Management is a distributed data center management system. It can manage applications within clusters that contain multiple machines and provide basic features such as deployment, upgrade, scale-in, scale-out, and configuration change.

Apsara Infrastructure Management also provides data monitoring and report analysis features to facilitate end-to-end operations and maintenance (O&M) and management. In large-scale distributed scenarios, Apsara Infrastructure Management offers automatic O&M to improve O&M efficiency and system availability.

Apsara Infrastructure Management is composed of TianjiMaster and TianjiClient. TianjiClient is installed as an agent on a machine. TianjiMaster delivers the received commands to TianjiClient. Apsara Infrastructure Management uses components to implement different features and provides users with the APIServer and console.

Features

- Initializes networks within a data center.
- Manages server installation and maintenance processes.
- Deploys, scales, and upgrades cloud services.
- Manages cloud service configurations.
- Applies for cloud service resources.
- Repairs software and hardware faults.
- Monitors software and hardware infrastructure and business processes.

4.4.1.2.1.2. Terms

This topic describes the terms that are used in Apsara Infrastructure Management.

project

A group of clusters. A project provides services for users.

cluster

A group of physical machines. A cluster provides services logically and is used to deploy software of a project.

- A cluster belongs to only one product.
- You can deploy multiple services on a single cluster.

service

A group of software programs used to provide an independent set of features. A service is composed of one or more server roles. A service can be deployed within multiple clusters to provide service capabilities. For example, 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 within a cluster.

server role

One or more indivisible feature units of a service. A server role is composed of one or more applications. If a service is deployed within a cluster, all server roles of the service must be deployed on machines within the same cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same machine.

service role instance

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

application

A process component contained in a server role. Each application works independently. Applications are the minimum units that can be deployed and upgraded in Apsara Infrastructure Management Framework, and can be deployed on each machine. Typically, an application is an executable software program or Docker container.

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

rolling

A process in which Apsara Infrastructure Management Framework upgrades services and modifies cluster configurations based on the configurations updated by users. This process is called rolling.

service configuration template

A template that contains the same service configurations. A service configuration template can make it easy to write the same configurations to different clusters, and applies to large-scale deployment and upgrade scenarios.

associated service template

A file named template.conf in service configurations. The file declares that a specific version of a service configuration template is used by a service instance.

desired state

A state in which all hardware and software on each machine of a cluster work normally and all software programs are in the desired versions.

dependency

A dependency relationship between server roles in a service. Tasks are executed or configurations are upgraded based on the dependency relationship. For example, assume that A depends on B. In this case, A is downloaded after B is downloaded and upgraded after B is upgraded. By default, the dependency of configuration upgrade does not take effect.

upgrade

A way to change the current state of a service to the desired state. After a user submits a version change request, Apsara Infrastructure Management Framework can upgrade the service version to the desired version. An upgrade is performed on each server role, and aims to upgrade all machines to the desired version.

Before an upgrade starts, the current and desired states of a cluster are the same. When a user submits a version change request, the current state remains unchanged, but the desired state changes. A rolling task is generated to gradually approximate the current state to the desired state. When the upgrade ends, the current state is exactly the same as the desired state.

4.4.1.2.2. Log on to the Apsara Infrastructure Management console

This topic describes how to log on to the Apsara Infrastructure Management console.

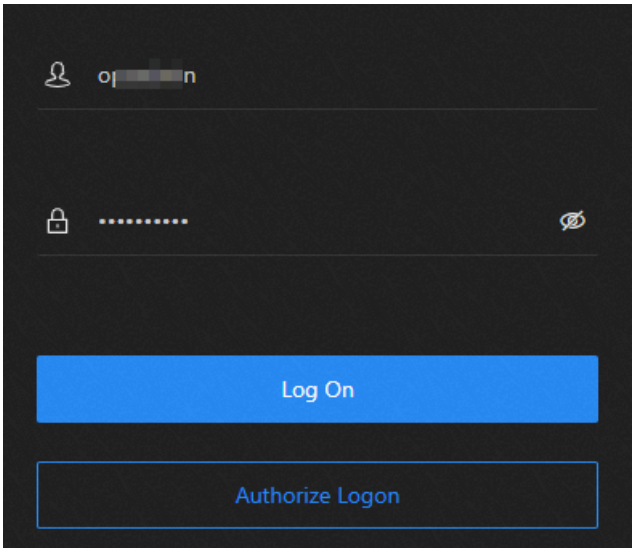
Prerequisites

- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The endpoint of the Apsara Uni-manager Operations Console is in the following format: *region-id*.ops.console.*intranet-domain-id*.
- We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the endpoint of the Apsara Uni-manager Operations Console. Press the Enter key.



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

3. Enter your username and password.

> **Note** Obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

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

To enhance security, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains at least one of the following special characters: ! @ # $ %
- The password is 10 to 20 characters in length.

4. Click **Log On**.

> **Note** If you want to authorize a third-party account to log on to the Apsara Uni-manager Operations Console, click **Authorize Logon**. You are navigated to the page on which you can authorize the third-party account to log on to the Apsara Uni-manager Operations Console. After you perform the operations as prompted, you are navigated to the logon page of the Apsara Uni-manager Operations Console.
>
> Before you can log on to the Apsara Uni-manager Operations Console by using the third-party account, you must complete the required configurations. For more information, contact Alibaba Cloud technical support.

5. In the top navigation bar, choose **Products** > **Base/Platforms** > **Apsara Infrastructure Management**.
6. When you enter the new version of Apsara Infrastructure Management, click **Back to Old Version** in the upper-right corner to go to the old version.

4.4.1.2.3. Webpage usage

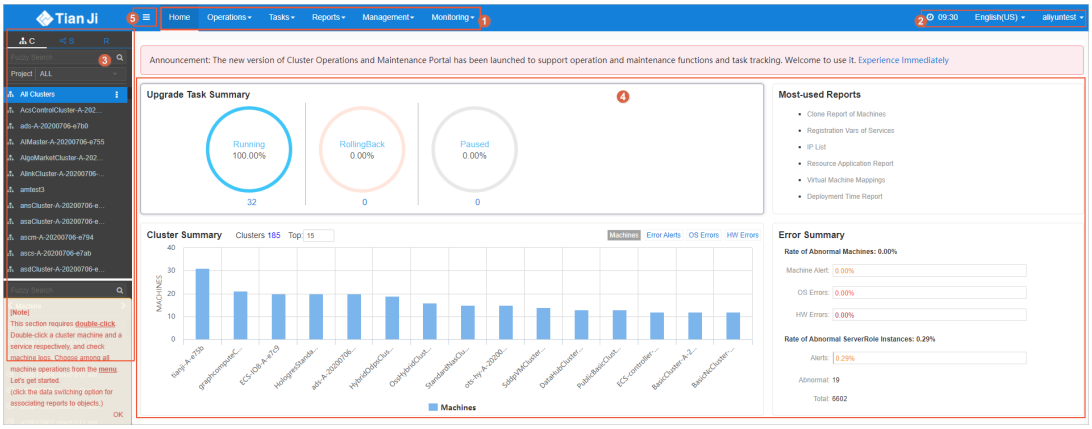
Before you perform operations on Apsara Infrastructure Management, you must learn about its webpages.

4.4.1.2.3.1. Instructions for the homepage

Log on to the Apsara Infrastructure Management console. This topic describes the basic operations and features available on the homepage.

Log on to the Apsara Infrastructure Management console. The homepage of the Apsara Infrastructure Management console appears, as shown in the following figure.

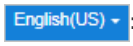
Figure 1. Homepage of the Apsara Infrastructure Management console



The Sections on the homepage table describes the functional sections on the homepage.

Table 1. Sections on the homepage

Section		Description
①	Top navigation bar	• **Operations**: the quick entrance to operations & maintenance (O&M) operations, which allows you to find operations and their objects. This menu consists of the following submenus: ◦ **Cluster Operations**: allows you to perform O&M and management operations on clusters based on your project permissions. For example, you can view the status of clusters. ◦ **Service Operations**: allows you to manage services based on your service permissions. For example, you can view the service list. ◦ **Machine Operations**: allows you to perform O&M and management operations on machines. For example, you can view the status of machines. • **Tasks**: Rolling tasks are generated after you modify configurations in the system. This menu allows you to view the running tasks, task history, and deployment of clusters, services, and server roles in all projects. • **Reports**: allows you to view monitoring data in tables and find specific reports by using fuzzy search. • **Monitoring**: monitors metrics during system operations and sends alert notifications for abnormal conditions. This menu allows you to view the alert status, modify alert rules, and search alert history.

②	Upper-right buttons	•  ◦ **TJDB Sync Time**: the time when the data on the current page is generated. ◦ **Desired State Calc Time**: the time when the desired-state data on the current page is calculated. The system processes data as fast as it can after the data is generated. Latency exists because Apsara Infrastructure Management is an asynchronous system. Time information helps explain why data on the current page is generated and determine whether the system is faulty. •  : the current display language of the console. You can select another language from the drop-down list. •  : your logon account. You can select **Logout** from the drop-down list to log out of your account.
③	Left-side navigation pane	In the left-side navigation pane, you can view the logical architecture of Apsara Infrastructure Management. The tabs allow you to view details and perform operations. For more information, see Instructions for the left-side navigation pane.
④	Workspace	The workspace shows a summary of tasks and other information. • **Upgrade Task Summary**: shows the numbers and proportions of running, rolling back, and suspended upgrade tasks. • **Cluster Summary**: shows the numbers of machines, error alerts, operating system errors, and hardware errors in each cluster. • **Error Summary**: shows metric values about the rate of abnormal machines and the rate of abnormal server role instances. • **Most-used Reports**: shows links of common statistical reports.
⑤	Show/hide button	Allows you to expand or collapse the left-side navigation pane to narrow or enlarge the workspace.

4.4.1.2.3.2. Instructions for the left-side navigation pane

The left-side navigation pane contains three tabs: **C** (cluster), **S** (service), and **R** (report). This topic describes how to use the tabs to view information.

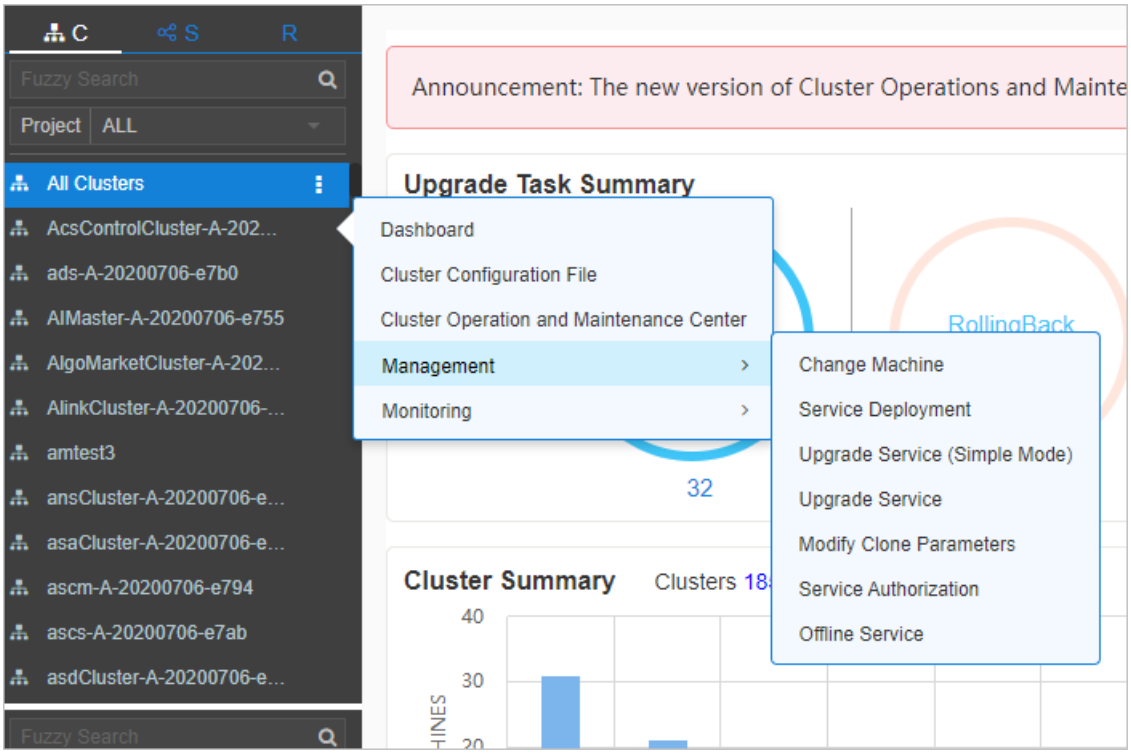
Cluster

You can search for clusters in a project and their information such as the cluster status, cluster operations and maintenance (O&M), service desired state, and logs by fuzzy match.

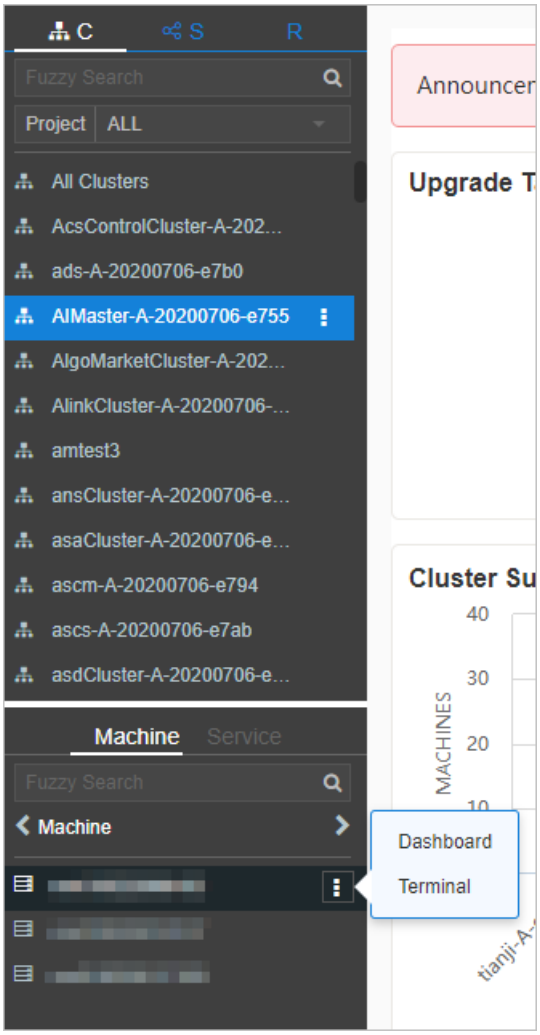
On the **C** tab of the left-side navigation pane, you can perform the following operations:

- Enter a cluster name or a part of a cluster name in the search box to filter clusters.
- Select a project from the **Project** drop-down list to view all clusters in the project.
- Move the pointer over the  icon next to a cluster and select menu items to perform

corresponding operations on the cluster.



- Click a cluster. All machines and services within the cluster are displayed in the lower part of the left-side navigation pane. Move the pointer over the icon next to a machine or service on the **Machine** or **Service** tab and select menu items to perform corresponding operations on the machine or service.



- Click the **Machine** tab. Double-click a machine to view information about all server roles on the machine. Double-click a server role to view applications, and then double-click an application to view log files.
- Click the **Service** tab. Double-click a machine to view information about all server roles on the machine. Double-click a server role to view machines, double-click a machine to view applications, and then double-click an application to view log files.
- Double-click a log file. Move the pointer over the log file, click the icon next to the log file, and then click **Download** to download the log file.

  Alternatively, move the pointer over a log file and click **View** next to the log file. The time-ordered log details are displayed on the **Log Viewer** page. You can search for log details by keyword.

Service

You can search for services and view information about services and service instances by fuzzy match.

On the **S** tab of the left-side navigation pane, you can perform the following operations:

- Enter a service name or a part of a service name in the search box to filter services.
- Move the pointer over the icon next to a service and select menu items to perform corresponding operations on the service.
- Click a service. All service instances within the service are displayed in the lower part of the

left-side navigation pane. Move the pointer over the icon next to a service instance and select menu items to perform corresponding operations on the service instance.

Report

You can search for reports by fuzzy match and view report details.

On the **R** tab of the left-side navigation pane, you can perform the following operations:

- Enter a report name or a part of a report name in the search box to filter reports.
- Click **All Reports** or **Favorites**. Corresponding groups are displayed in the lower part of the left-side navigation pane. Double-click a group to view all reports in the group. Double-click a report to view details of the report.

4.4.1.2.4. Cluster operations

This topic describes the actions about cluster operations.

4.4.1.2.4.1. View configuration information of a cluster

This topic describes how to view the basic information, deployment plan, and configuration information of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Operations > Cluster Operations**.
   The **Cluster Operations** page contains the following information:
   - Cluster

     The name of a cluster. Click a cluster name to go to the Cluster Dashboard page. For more information, see View dashboard information of a cluster.
   - Scale-in Scale-out

     The numbers of machines and server roles that are scaled in and out. Click a number to go to the Cluster Operation and Maintenance Center page. For more information, see View information of the cluster O&M center.
   - Abnormal Machine Count

     The number of machines that are not in the Good state within a cluster. Click the number to go to the Cluster Operation and Maintenance Center page. For more information, see View information of the cluster O&M center.
   - Final Status of Normal Machines

     Indicates whether a cluster has reached the desired state. Select **Clusters not Final** above the cluster list to view all clusters that have not reached the desired state. Click a link in the column to view desired state information. For more information, see View the desired state of a service.
   - rolling

     Specifies whether rolling tasks are running within a cluster. Select **Rolling Tasks** above the cluster list to view all clusters that have rolling tasks. Click rolling in the column to view rolling tasks. For more information see View rolling tasks.
3. Select a project from the drop-down list or enter a cluster name to search for the cluster.

4. Click the cluster name or click **Cluster Configuration** in the **Actions** column to go to the **Cluster Configuration** page.
   Cluster configuration description describes the parameters on the **Cluster Configuration** page. Table 1. Cluster configuration description

Section	Parameter	Description
Basic Information	**Cluster**	The name of the cluster.
	Project	The project to which the cluster belongs.
	Clone Switch	◦ **Pseudo-clone**: The system is not cloned when a machine is added to the cluster. ◦ **Real Clone**: The system is cloned when a machine is added to the cluster.
	Machines	The number of machines included in the cluster. Click View Clustering Machines to view the list of machines.
	Security Verification	The access control among processes. By default, security verification is disabled in non-production environments. You can enable or disable security verification based on your business requirements.
	Cluster Type	◦ RDS ◦ NETFRAME ◦ T4: a type of cluster that renders special configurations for the mixed deployment of e-commerce ◦ Default
Deployment Plan	**Service**	The service that is deployed within the cluster.
	Dependent Service	The service on which the current service depends.
Service Information	**Service Information**	The service that you want to view. Select a service from the drop-down list to view its configuration information.
	Service Template	The template that is used by the service.
	Monitoring Template	The monitoring template that is used by the service.
	Machine Mappings	The machines where server roles of the service are deployed.
	Software Version	The version of the software that is included in server roles of the service.
	Availability Configuration	The percentage of availability configuration for server roles of the service.

Deployment Plan	The deployment plan of server roles of the service.
Configuration Information	The configuration file that is used for the service.
Role Attribute	The server roles and their parameter information.

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

4.4.1.2.4.2. View dashboard information of a cluster

This topic describes how to view the basic information and related statistics of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the **Cluster Dashboard** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the icon next to the target cluster and select **Dashboard**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, click the name of the target cluster.
3. View all information about the cluster on the **Cluster Dashboard** page. The following table describes the information of a cluster, such as basic information, desired state information, rolling tasks, dependencies, resources, virtual machine (VM) mappings, and monitoring status.

Item	Description

Cluster Basic Information	The basic information about the cluster. ◦ **Project Name**: the name of the project. ◦ **Cluster Name**: the name of the cluster. ◦ **IDC**: the data center to which the cluster belongs. ◦ **Final Status Version**: the latest version of the cluster. ◦ **Cluster in Final Status**: specifies whether the cluster has reached the desired state. ◦ **Machines Not In Final Status**: the number of machines that have not reached the desired state. ◦ **Real/Pseudo Clone**: specifies whether the system is cloned when a machine is added to the cluster. ◦ **Expected Machines**: the number of machines that are expected within the cluster. ◦ **Actual Machines**: the number of machines that are deployed in the current environment. ◦ **Machines Not Good**: the number of machines that are not in the Good state within the cluster. ◦ **Actual Services**: the number of services that are deployed within the cluster. ◦ **Actual Server Roles**: the number of server roles that are deployed within the cluster. ◦ **Cluster Status**: specifies whether the cluster is starting or shutting down machines.
Machine Status Overview	The status of machines within the cluster.
Machines In Final State	The distribution of machines where services are deployed, based on whether the machines have reached the desired state.
Load-System	The statistics chart of the cluster system load.
CPU-System	The statistics chart of the CPU load.
Mem-Sytem	The statistics chart of the memory load.
Disk_usage-System	The statistics chart of the disk usage.
Traffic-System	The statistics chart of the system traffic.
TCP State-system	The statistics chart of the TCP request status.
TCP Retrans-System	The statistics chart of the TCP retransmission traffic.
Disk_IO-System	The statistics chart of the disk I/O information.

Service Instances	The service instances that are deployed within the cluster and their desired state information. ◦ **Service Instance**: the service instance that is deployed within the cluster. ◦ **Final Status**: specifies whether the service instance has reached the desired state. ◦ **Expected Server Roles**: the number of server roles that are expected to deploy in the service instance. ◦ **Server Roles in Final Status**: the number of server roles that have reached the desired state in the service instance. ◦ **Server Roles Going Offline**: the number of server roles that are being unpublished from the service instance. ◦ Actions: Click **Details** to go to the **Service Instance Information Dashboard** page. For more information about the service instance dashboard, see View dashboard information of a service instance.
Upgrade Tasks	The upgrade tasks within the cluster. ◦ **Cluster Name**: the name of the cluster. ◦ **Type**: the type of the upgrade task. Valid values: app and config. app indicates version upgrade, and config indicates configuration change. ◦ **Git Version**: the change version of the upgrade task. ◦ **Description**: the description of the change. ◦ **Rolling Result**: the result of the upgrade task. ◦ **Submitted By**: the user who submits the change. ◦ **Submitted At**: the time when the change is submitted. ◦ **Start Time**: the time when rolling starts. ◦ **End Time**: the time when the upgrade task ends. ◦ **Time Used**: the time consumed for the upgrade. ◦ Actions: Click **Details** to go to the **Rolling Task** page. For more information about rolling tasks, see View rolling tasks.
Cluster Resource Request Status	◦ **Version**: the version of the resource request. ◦ **Msg**: the error message. ◦ **Begintime**: the time when the resource request analysis starts. ◦ **Endtime**: the time when the resource request analysis ends. ◦ **Build Status**: the build status of resources. ◦ **Resource Process Status**: the resource request status of the version.

Cluster Resource	◦ **Service**: the name of the service. ◦ **Service Role**: the name of the server role. ◦ **App**: the name of the application of the server role. ◦ **Name**: the name of the resource. ◦ **Type**: the type of the resource. ◦ **Status**: the status of the resource request. ◦ **Error_Msg**: the error message. ◦ **Parameters**: the parameters of the resource. ◦ **Result**: the result of the resource request. ◦ **Res**: the ID of the resource. ◦ **Reprocess Status**: the request status of AnyTunnel VIP addresses. ◦ **Reprocess Msg**: the error message reported when AnyTunnel VIP addresses are requested. ◦ **Reprocess Result**: the request result of AnyTunnel VIP addresses. ◦ **Refer Version List**: the version that uses the resource.
VM Mappings	The VMs within the cluster. VM information is displayed only when VMs are deployed within the cluster. ◦ **VM**: the hostname of the VM. ◦ **Currently Deployed On**: the hostname of the physical machine where the VM is deployed. ◦ **Target Deployed On**: the hostname of the physical machine where you expect to deploy the VM.
Service Dependencies	The dependency configuration of service instances and server roles within the cluster, and the desired state information of dependency services or server roles. ◦ **Service**: the name of the service. ◦ **Server Role**: the name of the server role. ◦ **Dependent Service**: the service on which the server role depends. ◦ **Dependent Server Role**: the server role on which the server role depends. ◦ **Dependent Cluster**: the cluster where the dependency server role is deployed. ◦ **Dependency in Final Status**: specifies whether the dependency server role has reached the desired state.

4.4.1.2.4.3. View information of the cluster O&M center

This topic describes how to view the status and statistics of services and machines within a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the **Cluster Operation and Maintenance**

Center page:

- In the left-side navigation pane, click the **C** tab. Move the pointer over the icon next to the target cluster and select **Cluster Operation and Maintenance Center**.
- In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Cluster Operation and Maintenance Center** in the Actions column.
- In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, click the name of the target cluster. On the **Cluster Dashboard** page, choose **Operations Menu > Cluster Operation and Maintenance Center**.

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

Item	Description
SR not in Final Status	All server roles that have not reached the desired state within the cluster. Click the number to view the list of server roles. Click a server role to view information of machines where the server role is deployed.
Running Tasks	Indicates whether rolling tasks are running within the cluster. Click **Rolling** to go to the **Rolling Task** page. For more information about rolling tasks, see View rolling tasks.
Head Version Submitted At	The time when the HEAD version is submitted. Click the time to view details.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ◦ **Preparing**: No new version is detected. ◦ **Waiting**: The latest version has been detected, but the analysis module has not started. ◦ **Doing**: The application to be changed is being analyzed. ◦ **done**: The desired state analysis succeeds. ◦ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state. Click a state to view related information.
Service	The service deployed within the cluster. Select a service from the drop-down list.
Server Role	The server role of a service within the cluster. Select a server role from the drop-down list. **Note** After you select a service and a server role, machines that are related to the service or the server role are displayed.

Total Machines	The total number of machines within the cluster or machines where the selected server roles are deployed.
Scale-in Scale-out	The numbers of machines and server roles that are scaled in and out.
Abnormal Machines	The numbers of machines in an abnormal state for the following reasons: ◦ **Ping Failed**: the number of machines that experience ping_monitor errors because TianjiMaster cannot ping the machines. ◦ **No Heartbeat**: the number of machines that experience TianjiClient or network errors because TianjiClient does not report data on a regular basis. ◦ **Status Error**: the number of machines that experience critical or fatal errors. Resolve problems based on alert information.
Abnormal Services	The number of machines that have abnormal services. The following rules are used to check whether a service has reached the desired state: ◦ Each server role on the machine is in the GOOD state. ◦ The actual version of each application of each server role on the machine is consistent with the HEAD version. ◦ Before the Image Builder builds an application of the HEAD version, Apsara Infrastructure Management cannot obtain the value of the HEAD version, and the desired state of the service is unknown. This process is called change preparation. The desired state of the service cannot be obtained when the preparation process is in progress or if the preparation fails.
Machines	All machines within the cluster or machines where the selected server roles are deployed. ◦ Click the Machine Search search box. In the dialog box that appears, enter one or more machines. Fuzzy match and batch search are supported. ◦ Click the name of a machine to view its physical information in the Machine Information dialog box. Click **DashBoard** to go to the **Machine Details** page. For more information about machine details, see View dashboard information of a machine. ◦ Move the pointer over the **Final Status** or **Final SR Status** column and click **Details** to view the machine status and system service information, as well as status information and error messages of server roles on the machine. ◦ Before you filter machines by service and service role, move the pointer over the **Running Status** column and click **Details** to view status information and error messages of the machine. After you filter machines by service and service role, move the pointer over the **SR Running Status** column and click **Details** to view status information and error messages of server roles on the machine. ◦ Click **Error**, **Warning**, or **Good** in the **Monitoring Statistics** column to view machine and server role metrics. ◦ Click **Terminal** in the **Actions** column to log on to the machine and perform operations. ◦ Click **Machine Operation** in the **Actions** column to perform reboot, out-of-band reboot, or reclone operations on the machine.

4.4.1.2.4.4. View the desired state of a service

This topic describes how to check whether a service within a cluster has reached the desired state and how to view desired state details.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the **Service Final Status Query** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the icon next to the target cluster and choose **Monitoring > Service Final Status Query**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Service Final Status Query** in the Actions column.
3. View information on the **Service Final Status Query** page.

Item	Description
Project Name	The name of project to which the cluster belongs.
Cluster Name	The name of the cluster.
Head Version Submitted At	The time when the HEAD version is submitted.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ◦ **Preparing**: No new version is detected. ◦ **Waiting**: The latest version has been detected, but the analysis module has not started. ◦ **Doing**: The application to be changed is being analyzed. ◦ **done**: The desired state analysis succeeds. ◦ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state.
Cluster Rolling Status	Indicates whether the cluster has reached the desired state. If a rolling task is running, its task information is displayed.
Cluster Machine Final Status Statistics	The status of all machines within the cluster. Click**View Details** to go to the **Cluster Operation and Maintenance Center** page and view machine details. For more information about the operations and maintenance (O&M) center, see View information of the cluster O&M center.

Final Status of Cluster SR Version	The desired state of services within the cluster. **Note** This section includes only the services that have not reached the desired state due to version inconsistency or status exceptions. For other services that fail to reach the desired state due to machine errors, see desired state information of machines within the cluster.
Final Status of SR Version	The number of machines that have not reached the desired state. The number is displayed if server roles have rolling tasks.

4.4.1.2.4.5. View operation logs

This topic describes how to view differences between Git versions from operation logs.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the **Cluster Operation Logs** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the icon next to the target cluster and choose **Monitoring > Operation Logs**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Operation Logs** in the Actions column.
3. On the **Cluster Operation Logs** page, click **Refresh** in the upper-right corner to view the Git version, description, submission information, and task status.
4. **Optional:**On the **Cluster Operation Logs** page, view differences between versions.
   i. Find the target operation log and click **View Release Changes** in the **Actions** column.
   ii. On the **Version Difference** page, configure the following parameters:
      - **Select Base Version**: Select a basic version.
      - **Configuration Type**: Select **Extended Configuration** or **Cluster Configuration**. **Extended Configuration** allows you to view differences between the merging results of cluster and template configurations. **Cluster Configuration** allows you to view differences between cluster configurations.
   iii. Click **Obtain Difference**.

   Difference files are displayed.
   iv. Click each difference file to view its difference details.

4.4.1.2.5. Service operations

This topic describes the actions about service operations.

4.4.1.2.5.1. View the service list

This topic describes how to view all services and their information.

Procedure

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

3. View the information on the **Service Operations** page.

Item	Description
Service	The name of the service.
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.
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.

4.4.1.2.5.2. View dashboard information of a service instance

This topic describes how to view the basic information and related statistics of a service instance.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click the **S** tab.
3. Enter a service name in the search box to search for the service.
4. Click the service name to view service instances of the service.
5. Move the pointer over the icon next to the target service instance and select **Dashboard**.
6. View information on the **Service Instance Information Dashboard** page.

Item	Description

Service Instance Summary	The basic information about the service instance. ◦ **Cluster Name**: the name of the cluster where the service instance is deployed. ◦ **Service Name**: the name of the service to which the service instance belongs. ◦ **Actual Machines**: the number of machines that are deployed in the current environment. ◦ **Expected Machines**: the number of machines that are expected for the service instance. ◦ **Target Total Server Roles**: the number of server roles that are expected for the service instance. ◦ **Actual Server Roles**: the number of server roles that are deployed in the current environment. ◦ **Template Name**: the name of the service template that is used by the service instance. ◦ **Template Version**: the version of the service template that is used by the service instance. ◦ **Schema**: the name of the service schema that is used by the service instance. ◦ **Monitoring System Template**: the name of the Monitoring System template that is used by the service instance.
Server Role Statuses	The status of server roles in the service instance.
Machine Statuses for Server Roles	The status of machines where server roles are deployed.
Service Monitoring Information	◦ **Monitored Item**: the name of the metric. ◦ **Level**: the level of the metric. ◦ **Description**: the description of the metric. ◦ **Updated At**: the time when the data is updated.
Service Alert Status	◦ **Alarm Name** ◦ **Instance Information** ◦ **Alert Start** ◦ **Alert End** ◦ **Alert Duration** ◦ **Alert Level** ◦ **Occurrences**: the number of occurrences of the alert.

Server Role List	◦ **Server Role** ◦ **Current Status** ◦ **Expected Machines** ◦ **Machines In Final Status** ◦ **Machines Going Offline** ◦ **Rolling Task Status** ◦ **Time Used**: the time that is used for the execution of rolling tasks. ◦ **Actions**: Click **Details** to go to the View dashboard information of a server role page.
Service Alert History	◦ **Alert Name** ◦ **Alert Time** ◦ **Instance Information** ◦ **Alert Level** ◦ **Contact Group**
Service Dependencies	The dependency configuration of service instances and server roles, and the desired state information of dependency services or server roles. ◦ **Server Role**: the name of the server role. ◦ **Dependent Service**: the service on which the server role depends. ◦ **Dependent Server Role**: the server role on which the server role depends. ◦ **Dependent Cluster**: the cluster where the dependency server role is deployed. ◦ **Dependency in Final Status**: specifies whether the dependency server role has reached the desired state.

4.4.1.2.5.3. View dashboard information of a server role

This topic describes how to view the basic information and related statistics of a service instance.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click the **S** tab.
3. Enter a service name in the search box to search for the service.
4. Click the service name to view service instances of the service.
5. Move the pointer over the icon next to the target service instance and select **Dashboard**.
6. In the **Server Role List** section of the **Service Instance Information Dashboard** page, click **Details** in the **Actions** column.
7. View information on the **Service Instance Information Dashboard** page.

Item	Description
Server Role Summary	The basic information about the server role. ◦ **Project Name**: the name of the project to which the server role belongs. ◦ **Cluster Name**: the name of the cluster where the server role is deployed. ◦ **Service Instance**: the name of the service instance to which the server role belongs. ◦ **Server Role**: the name of the server role. ◦ **In Final Status**: indicates whether the server role reaches the desired state. ◦ **Expected Machines**: the number of machines that are expected within the server role. ◦ **Actual Machines**: the number of actual machines within the server role. ◦ **Machines Not Good**: the number of machines whose status is not Good. ◦ **Machines with Role Status Not Good**: the number of server roles whose status is not Good. ◦ **Machines Going Offline**: the number of machines that are going offline. ◦ **Rolling**: indicates whether a running rolling task exists. ◦ **Rolling Task Status**: the current status of the rolling task. ◦ **Time Used**: the time that is used for the execution of rolling tasks.
Machine Final Status Overview	The statistical chart of the current status of the server role.
Server Role Monitoring Information	◦ **Updated At**: the time when the data is updated. ◦ **Monitored Item**: the name of the metric. ◦ **Level**: the level of the metric. ◦ **Description**: the description of the metric.

Machine Information	◦ **Machine Name**: the hostname of the machine. ◦ **IP**: the IP address of the machine. ◦ **Machine Status**: the status of the machine. ◦ **Machine Action**: the action that is being performed on the machine. ◦ **Server Role Status**: the status of the server role. ◦ **Server Role Action**: the action that is being performed on the server role. ◦ **Current Version**: the current version of the server role on the machine. ◦ **Target Version**: the expected version of the server role on the machine. ◦ **Error Message**: the error message. ◦ **Actions**: ▪ Click **Terminal** to log on to the machine and perform operations. ▪ Click **Restart** to restart the server roles on the machine. ▪ Click **Details** to go to the **Machine Details** page. For more information about the machine details, see View dashboard information of a machine. ▪ Click **Machine System View** to go to the **Machine Info Report** page. For more information about the machine info report, see Machine info report. ▪ Click **Machine Operation** in the Actions column to perform reboot, out-of-band reboot, or reclone operations on the machine.
Server Role Monitoring Information of Machines	◦ **Updated At**: the time when the data is updated. ◦ **Machine Name**: the name of the machine. ◦ **Monitored Item**: the name of the metric. ◦ **Level**: the level of the metric. ◦ **Description**: the description of the metric.
VM Mappings	The VMs within the cluster. VM information is displayed only when VMs are deployed within the cluster. ◦ **VM**: the hostname of the VM. ◦ **Currently Deployed On**: the hostname of the physical machine where the VM is deployed. ◦ **Target Deployed On**: the hostname of the physical machine where you expect to deploy the VM.

Service Dependencies	The dependency configuration of service instances and server roles, and the desired state information of dependency services or server roles. ◦ **Dependent Service**: the service on which the server role depends. ◦ **Dependent Server Role**: the server role on which the server role depends. ◦ **Dependent Cluster**: the cluster where the dependency server role is deployed. ◦ **Dependency in Final Status**: specifies whether the dependency server role has reached the desired state.

4.4.1.2.6. Machine operations

This topic describes the actions about machine operations.

4.4.1.2.6.1. View dashboard information of a machine

This topic describes how to view the basic information and related statistics of a machine.

Procedure

1. Log on to the Apsara Infrastructure Management console.
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 to search for the machine.
4. Move the pointer over next to the machine and select **Dashboard**.
5. On the **Machine Details** page, view all the information of the machine. The following table describes the information of a machine.

Item	Description
Load-System	The statistics chart of the cluster system load.
CPU-System	The statistics chart of the CPU load.
Mem-System	The statistics chart of the memory load.
Disk Usage-System	The statistics chart of the disk usage.
Traffic-System	The statistics chart of the system traffic.
TCP State-System	The statistics chart of the TCP request status.
TCP Retrans-System	The statistics chart of the TCP retransmission traffic.
DISK IO-System	The statistics chart of the disk I/O information.

Machine Summary	◦ **Project Name**: the name of the project to which the machine belongs. ◦ **Cluster Name**: the name of the cluster to which the machine belongs. ◦ **Machine**: the name of the machine. ◦ **SN**: the serial number of the machine. ◦ **IP**: the IP address of the machine. ◦ **IDC**: the data center of the machine. ◦ **Room**: the room in the data center where the machine is located. ◦ **Rack**: the rack where the machine is located. ◦ **Unit in Rack**: the location of the rack. ◦ **Warranty**: the warranty of the machine. ◦ **Purchase Date**: the date when the machine is purchased. ◦ **Machine Status**: the status of the machine. ◦ **Status**: the hardware status of the machine. ◦ **CPUs**: the number of CPUs for the machine. ◦ **Disks**: the disk size. ◦ **Memory**: the memory size. ◦ **Manufacturer**: the manufacturer of the machine. ◦ **Model**: the model of machine. ◦ **os**: the operating system of the machine. ◦ **part**: the disk partition.
Server Role Status of Machine	The distribution of the current status of all server roles on the machine.
Machine Monitoring Information	◦ **Monitored Item**: the name of the metric. ◦ **Level**: the level of the metric. ◦ **Description**: the description of the metric. ◦ **Updated At**: the time when the data is updated.
Machine Server Role Status	◦ **Service instance** ◦ **Server Role** ◦ **Server Role Status** ◦ **Server Role Action** ◦ **Error Message** ◦ **Target Version** ◦ **Current Version** ◦ **Actual Version Update Time** ◦ **Actions**: ▪ Click **Details** to go to the **Server Role Dashboard** page. For more information about the server role dashboard, see View dashboard information of a server role. ▪ Click **Restart** to restart the server roles on the machine.

Application Status in Server Roles	◦ **Application Name**: the name of the application. ◦ **Process Number** ◦ **Status**: the status of the application. ◦ **Current Build ID**: the ID of the current package version. ◦ **Target Build ID**: the ID of the expected package version. ◦ **Git Version** ◦ **Start Time** ◦ **End Time** ◦ **Interval**: the interval between the time when Apsara Infrastructure Management detects that the process exits and the time when Apsara Infrastructure Management fixes the process. ◦ **Information Message**: the normal output logs. ◦ **Error Message**: the error message.

4.4.1.2.7. Monitoring center

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

4.4.1.2.7.1. Modify an alert rule

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

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Operations > Service Operations**.
3. Enter a service name in the search box to search for the service.
4. Find the service and then click **Management** in the **Actions** column.
5. Click the **Monitoring Template** tab.
6. Find the monitoring template and then click **Edit** in the Actions column.
7. Configure the monitoring parameters.
8. Click **Save Changes**.

   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 deployed.

4.4.1.2.7.2. View the status of a monitoring instance

This topic describes how to view the status of a monitoring instance.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Operations > Service Operations**.
3. (Optional)Enter a service name in the search box to search for the service.
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.

4.4.1.2.7.3. View the alert status

This topic describes how to view the alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Monitoring > Alert Status**.
3. Search for an alert by service name, cluster name, alert name, or alert time range.
4. View alert details on the **Alert Status** page. The following table describes the information of the alert.

Item	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Instance	The name of the monitored instance. Click the name of an instance to view the alert history of the instance.
Alert Status	Two alert states are available, which are Normal and Alerting.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ◦ P0: an alert that has been cleared ◦ P1: a critical alert ◦ P2: a major alert ◦ P3: a minor alert ◦ P4: a warning alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered and how long the alert lasts.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

4.4.1.2.7.4. View alert rules

This topic describes how to view alert rules.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Monitoring > Alert Rules**.
3. Search for alert rules by service name, cluster name, or alert name.

4. View alert rules on the **Alert Rules** page. The following table describes the information about alert rules.

Item	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Alarm Name	The name of the alert.
Alert Conditions	The conditions that trigger the alert.
Periods	The frequency at which the alert rule is executed.
Alert Contact	The groups and members to notify when the alert is triggered.
Status	The status of the alert rule. ◦ **Running**: Click it to stop the alert rule. ◦ **Stopped**: Click it to execute the alert rule.

4.4.1.2.7.5. View alert history

This topic describes how to view the historical alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Monitoring > Alert History**.
3. Search for an alert by service name, cluster name, alert cycle, or alert time range.
4. View the alert history on the **Alert History** page. The following table describes the information of historical alerts.

Item	Description
Service	The name of the service to which the alert belongs.
Cluster	The name of the cluster where the service is deployed.
Alert Instance	The name of the instance where the alert is triggered.
Status	Two alert states are available, which are Normal and Alerting.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ◦ P0: an alert that has been cleared ◦ P1: a critical alert ◦ P2: a major alert ◦ P3: a minor alert ◦ P4: a warning alert

Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered.
Alert Contact	The groups and members to notify when the alert is triggered.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

4.4.1.2.8. Tasks and deployment summary

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

4.4.1.2.8.1. View rolling tasks

This topic describes how to view rolling tasks and their status.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Operations > Cluster Operations**.
3. Select **Rolling Tasks** to view all clusters that have rolling tasks.
4. Click **rolling** in the **Rolling** column.
5. On the **Rolling Task** page. view the information of change tasks and change details.
   Table 1. Information of change tasks

Item	Description
Change Version	The source version of the rolling task.
Description	The description of the change.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ◦ **Preparing**: No new version is detected. ◦ **Waiting**: The latest version has been detected, but the analysis module has not started. ◦ **Doing**: The application to be changed is being analyzed. ◦ **done**: The desired state analysis succeeds. ◦ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state.
Blocked Server Role	The server role that is blocked by dependencies in the rolling task.
Submitter	The person who submits the change.

Submitted At	The time when the change is submitted.
Actions	Click **View Difference** to go to the **Version Difference** page. For more information, see View operation logs. Click **Stop** to terminate the rolling task. Click **Pause** to suspend the rolling task.

Table 2. Information of change details

Item	Description
Service name	The name of the service that has changes.
Status	The current status of the service. The rolling status of a service is an aggregation result of rolling statuses of multiple server roles. Services can be in one of the following states: ◦ **succeeded**: A task succeeds. ◦ **blocked**: A task is blocked. ◦ **failed**: A task fails.
Server Role Status	The status of the server role. Click**>** to the left of a service name to view the rolling task status of each server role in the service. Server roles can be in one of the following states: ◦ **Downloading**: A task is being downloaded. ◦ **Rolling**: A rolling task is in progress. ◦ **RollingBack**: A rolling task fails and is performing rollback.
Depend On	The services on which the service depends, or the server roles on which the server role depends.
Actions	Click **Stop** to terminate the change of the server role. Click **Pause** to suspend the change of the server role.

4.4.1.2.8.2. View running tasks

This topic describes how to view running tasks.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Tasks > Running Tasks**.
3. Search for running tasks by cluster name, server role name, task status, task submitter, Git

version, or time range.

4. Find the task, move the pointer over the **Rolling Task Status** column, and then click **View Tasks** to go to the **Rolling Task** page. For more information about rolling task details, see View rolling tasks.

4.4.1.2.8.3. View task history

This topic describes how to view historical tasks.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. In the top navigation bar, choose **Tasks > History Tasks**.
3. Search for historical tasks by cluster name, Git version, submitter, or time range.
4. Find the task and click **Details** in the **Actions** column to go to the **Rolling Task** page. For more information about rolling task details, see View rolling tasks.

4.4.1.2.8.4. 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.

Procedure

1. Log on to the Apsara Infrastructure Management console.
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: 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 desired state for one time yet.
     - Green: in the desired state. It indicates that all clusters in the project have reached the desired state.
     - Orange: not in the desired state. It indicates that a server role does not reach the desired state for some reason after the project reaches the desired state for the first time.
   - Configure the global clone parameter clone_mode.
     - **normal**: enables clone.
     - **block**: disables clone.
   - Configure the global dependency parameter dependency_check_level.
     - **normal**: checks all configured dependencies.
     - **ignore**: does not check dependencies.
     - **ignore_service**: checks only indicates dependencies at the server role level and ignores dependencies at the service level, including the server role dependencies across services.
3. Click the **Deployment Details** tab to view the deployment details.

   The following table describes the information on the tab.

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. A project can be in one of the following states: ◦ **Final**: All clusters in a project have reached the desired state. ◦ **Deploying**: The project has not reached the desired state for one time yet. ◦ **Waiting**: Some services of the project depend on server roles or service instances that are being deployed, and other service instances or server roles in the project have already been deployed. ◦ **Non-final**: A server role does not reach the desired state for some reason after the project reaches the desired state for the first time. ◦ **Inspector Warning**: An error is detected on service instances in the project during the inspection.
Start Time	The time when Apsara Infrastructure Management starts the deployment.
Progress	The proportion of server roles that reach the desired state to all the server roles in the current environment.
Deployment Status	The time marked Final indicates the deployment duration for the following states: Final, Deploying, Waiting, and Inspector Warning. The time marked Non-final indicates the duration before the final status is reached. You can click a time value to view the details.
Deployment Progress	The proportion of clusters, services, and server roles that reach the final status to the total clusters, services, and server roles in the project. Move the pointer over the blank area at the right of the data of roles and then click **Details** to view the deployment statuses of clusters, services, and server roles. The deployment statuses are indicated by icons, which are the same as those used for status statistics.
Resource Application Progress	**Total** indicates the total number of resources related to the project. The application progress can be in one of the following states: ◦ **Done**: the number of resources that have been applied for. ◦ **Doing**: the number of resources that are being applied for and retried. The number of retries (if any) is displayed next to the number of resources. ◦ **Block**: the number of resources whose applications are blocked by other resources. ◦ **Failed**: the number of resources whose applications failed.
Inspector Error	The number of inspection alerts for the current product.
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 corresponding to a product to view service instances that are dependent on other service instances and the current deployment states of the depended service instances.

4.4.1.2.9. Reports

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

4.4.1.2.9.1. View reports

This topic describes how to view report data.

Background information

You can choose to view the following reports in the Apsara Infrastructure Management console:

- System reports: include default and common reports in the system.
- All reports: include system reports and custom reports.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. You can go to the report list in one of the following 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**.

   The following table describes information about reports.

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

3. **Optional:**Enter a report name in the search box to search for the report.
4. Click the report name to go to the corresponding report details page.
   For more information about reports, see Appendix.Appendix

4.4.1.2.9.2. Add a report to favorites

This topic describes how to add frequently used reports to favorites. Then, you can find them on the Home or Favorites page.

Procedure

1. Log on to the Apsara Infrastructure Management console.
2. Use one of the following methods to go to the report list:
   - In the top navigation bar, choose **Reports > System Reports**.
   - In the top navigation bar, choose **Reports > All Reports**.
3. Search for a report in the search box.
4. Click **Add to Favorites** in the **Actions** column corresponding to the report.
5. In the **Add to Favorites** dialog box, enter tags for the report.
6. Click **Add to Favorites**.

4.4.1.2.10. Appendix

4.4.1.2.10.1. Project component info report

This report displays the name and status for each type of project components, including services, server roles, and machines.

Item	Description
Project	The name of the project.
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 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 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 status of the machine.
Machine Action	The action that Apsara Infrastructure Management asks the machine to perform, such as the clone action.

4.4.1.2.10.2. IP list

This report displays the IP addresses of physical machines and Docker applications.

IP List of Physical Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The hostname of the machine.
IP	The IP address of the machine.

IP List of Docker Applications

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The hostname of the machine.
Docker Host	The Docker hostname.
Docker IP	The Docker IP address.

4.4.1.2.10.3. Machine info report

This report displays the states of machines and server roles on the machines.

Machine Status

This section displays all the machines currently managed by Apsara Infrastructure Management and their states. In the **Global Filter** section in the upper part 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 name of the machine.
IP	The IP address of the machine.
Machine Status	The status of the machine.
Machine Action	The action currently performed on the machine.
Machine Action Status	The status of the action.
State Desc	The description of the machine status.

Expected Server Role List

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Server Role	The name of the expected server role on the machine.

Abnormal Monitoring Status

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item.
Updated At	The updated time of the monitored item.

Server Role Version and Status on Machine

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.
Server Role	The name of the server role.
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.
State Desc	The description of the status.
ErrorMessage	The error message of the server role.

Monitoring Status

You can select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The name of the machine.

Server Role	The name of the server role.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item.
Updated At	The updated time of the monitored item.

4.4.1.2.10.4. Rolling info report

This report displays the running and completed rolling tasks and the task-related states.

Rolling Tasks

This section displays the rolling tasks that are running. If no rolling tasks are running, no data is displayed in this section.

Item	Description
Cluster	The name of the cluster.
Git Version	The version of the change that triggers the rolling task.
Description	The description of the change entered by a user when the user submits the change.
Start Time	The start time of the rolling task.
End Time	The end time of the rolling task.
Submitted By	The ID of the user who submits the change.
Rolling Task Status	The current status of the rolling task.
Submitted At	The time when the change is submitted.

Server Role in Job

When you select a rolling task in the **Rolling Tasks** section, this section displays the rolling states of server roles related to the selected task. If no rolling tasks are selected, the states of server roles related to all historical rolling tasks are displayed.

Item	Description
Server Role	The name of the server role.
Server Role Status	The rolling status of the server role.
ErrorMessage	The error 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 for which the rolling task was approved by the decider.
Failure Rate	The proportion of machines on which the rolling task failed.
Success Rate	The proportion of machines on which the rolling task succeeded.

Server Role Rolling Build Information

This section displays the current and desired versions of each application in the server role during the rolling process.

Item	Description
App	The name of the application that requires rolling in the server role.
Server Role	The server role to which the application belongs.
From Build	The version of the application before the upgrade.
To Build	The version of the application after the upgrade.

Server Role Statuses on Machines

When you select a server role in the **Server Role in Job** section, this section displays the status of the server role on each machine.

Item	Description
Machine Name	The name of the machine on which the server role is deployed.
Expected Version	The desired version of the server role.
Actual Version	The current version of the server role.
State	The status of the server role.
Action Name	The ongoing action on the server role.
Action Status	The status of the action.

4.4.1.2.10.5. Machine RMA approval pending list

Some Apsara Infrastructure Management 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

This section displays the basic information of pending approval machines.

Item	Description

Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
State	The 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

This section displays the information of server roles on the pending approval machines.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
Serverrole	The name of the server role.
State	The 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

This section displays the hard disk information of pending approval machines.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Hostname	The hostname of the machine.
Component	The hard disk on the machine.
State	The 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.

4.4.1.2.10.6. Registration vars of services

This report displays values of all service registration variables.

Item	Description
Service	The service name.
Service Registration	The service registration variable.
Cluster	The cluster name.
Update Time	The updated time.

4.4.1.2.10.7. Virtual machine mappings

Use the global filter to display the virtual machines of a specific cluster.

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

Item	Description
Project	The project name.
Cluster	The cluster name.
VM	The hostname of the virtual machine.
Currently Deployed On	The hostname of the physical machine on which the virtual machine is currently deployed.
Target Deployed On	The hostname of the physical machine on which the virtual machine is expected to be deployed.

4.4.1.2.10.8. Service inspector report

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

Service Inspector: Data is available only for services with inspection configured.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Description	The contents of the inspection report.

Level	The level of the inspection report.

4.4.1.2.10.9. Resource application report

In the **Global Filter** section, select the project, cluster, and machine from the **project**, **cluster**, and **machine** drop-down lists and then click **Filter** on the right to display the corresponding resource application data.

Change Mappings

Item	Description
Project	The project name.
Cluster	The cluster name.
Version	The version where the change occurs.
Resource Process Status	The resource application status in the version.
Msg	The exception message.
Begintime	The start time of the change analysis.
Endtime	The end time of the change analysis.

Changed Resource List

Item	Description
Res	The resource ID.
Type	The resource type.
Name	The resource name.
Owner	The application to which the resource belongs.
Parameters	The resource parameters.
Ins	The resource instance name.
Instance ID	The resource instance ID.

Resource Status

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.

Server Role	The server role name.
APP	The application of the server role.
Name	The resource name.
Type	The resource type.
Status	The resource application status.
Parameters	The resource parameters.
Result	The resource application result.
Res	The resource ID.
Reprocess Status	The status of the interaction with Business Foundation System during the VIP resource application.
Reprocess Msg	The error message of the interaction with Business Foundation System during the VIP resource application.
Reprocess Result	The result of the interaction with Business Foundation System during the VIP resource application.
Refer Version List	The version that uses the resource.
Error Msg	The exception message.

4.4.1.2.10.10. Statuses of project components

This report displays the statuses of all abnormal server roles on machines within the current project. This report also displays the alert information of server roles and machines reported to Monitoring System.

Error State Component Table

This section displays the server roles that are not in the GOOD state or that are pending upgrade.

Item	Description
Project	The name of the project.
Cluster	The name of the cluster.
Service	The name of the service.
Server Role	The name of the server role.
Machine Name	The name of the machine.
Need Upgrade	Specifies whether the version has reached the desired state.
Server Role Status	The status of the server role.
Machine Status	The status of the machine.

Server Role Alert Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.
Service	The name of the service.
Server Role	The name of the server role.
Machine Name	The name of the machine.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.
Description	The description of the alert.
Updated At	The update time of the alert.

Machine Alert Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.
Machine Name	The name of the machine.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.
Description	The description of the alert.
Updated At	The update time of the alert.

Service Inspector Information

When you select a row in the **Error State Component Table** section, this section displays the corresponding information.

Item	Description
Cluster	The name of the cluster.
Service	The name of the service.
Server Role	The name of the server role.
Monitored Item	The name of the server role metric.
Level	The severity level of the alert.

Description	The description of the alert.
Updated At	The update time of the alert.

4.4.1.2.10.11. Relationship of service dependency

This report displays the dependencies among server roles. Use the global filter to display the data of a specific cluster in the list.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Dependent Service	The service on which the server role depends.
Dependent Server Role	The server role on which the server role depends.
Dependent Cluster	The cluster to which the dependent server role belongs.
Dependency in Final Status	Whether the dependent server role reaches the final status.

4.4.1.2.10.12. Check report of network topology

This report checks if network devices and machines have wirecheck alerts.

Check Report of Network Topology

Checks if network devices have wirecheck alerts.

Item	Description
Cluster	The cluster name.
Network Instance	The name of the network device.
Level	The alert level.
Description	The description about the alert information.

Check Report of Server Topology

Checks if servers (machines) have wirecheck alerts.

Item	Description
Cluster	The cluster name.

Machine Name	The server (machine) name.
Level	The alert level.
Description	The description about the alert information.

4.4.1.2.10.13. Clone report of machines

This report displays the clone progress and status of machines.

Clone Progress of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.
Machine Status	The running status of the machine.
Clone Progress	The progress of the current clone process.

Clone Status of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.
Machine Action	The action performed by the machine, such as the clone action.
Machine Action Status	The status of the action performed by the machine.
Machine Status	The running status of the machine.
Level	Whether the clone action performed by the machine is normal.
Clone Status	The current status of the clone action performed by the machine.

4.4.1.2.10.14. Auto healing/install approval pending report

The list structure is the same as the machine RMA approval pending list, whereas this view is used for the approval during the installation. For more information, see Machine RMA approval pending list.

4.4.1.2.10.15. Machine power on or off statuses of clusters

After a cluster starts or shuts down machines, you can view the related information in this report.

Cluster Running Statuses

If a cluster is starting or shutting down machines, the corresponding data is available in this list. No data indicates that no cluster has machines shut down.

Item	Description
Project	The project name.
Cluster	The cluster name.
Action Name	The startup or shutdown action that is being performed by the cluster.
Action Status	The status of the action.

Server Role Power On or Off Statuses

Displays the power on or off statuses of server roles in the cluster selected in the **Cluster Running Statuses** section.

Select a row in the **Cluster Running Statuses** section to display the information of the corresponding cluster in the list.

Item	Description
Cluster	The cluster name.
Server Role	The server role name.
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.

4.4.2. Obtain the Prometheus domain name

This topic describes how to obtain the Prometheus domain name from the OPS1 server terminal when Prometheus is used for service monitoring.

Procedure

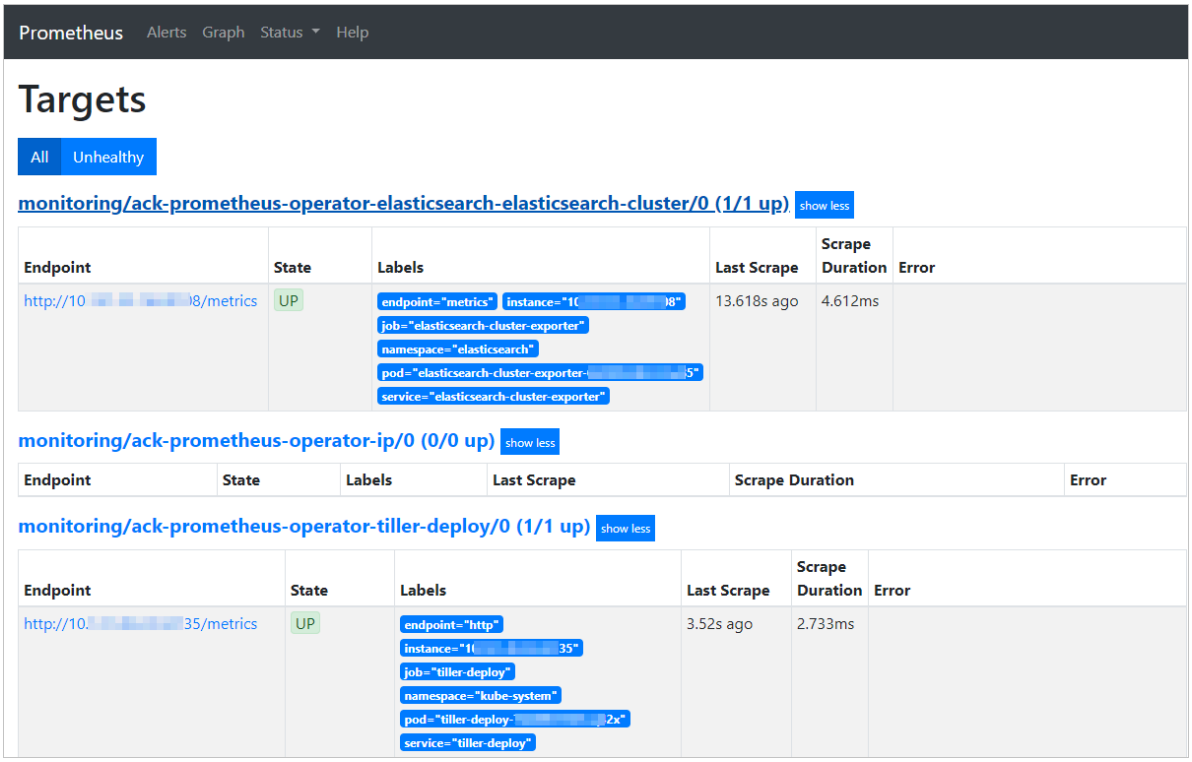
1. Log on to the OPS1 server terminal as the root user.
2. Run the following command to query the Prometheus domain name:

   ```
   kubectl get ing -n monitoring | grep tianjimon-prometheus-prome-prometheus | awk '{pr
   int $2}' | cut -d',' -f1
   ```

   A similar output is displayed:

   ```
   prometheus.tianjimon.cn-xxxx-envxx-d01.intra.envxx.shuguang.com
   ```

3. Replace the `<prometheus-domain>` value in the address `http://<prometheus-domain>/targets` with the domain name `prometheus.tianjimon.cn-xxxx-envxx-d01.intra.envxx.shuguang.com` that is obtained in the preceding step to obtain the endpoint `http://prometheus.tianjimon.cn-xxxx-envxx-d01.intra.envxx.shuguang.com/targets` of collection services in Prometheus.
4. Access the endpoint `http://prometheus.tianjimon.cn-xxxx-envxx-d01.intra.envxx.shuguang.com/targets` to view the collection services in Prometheus.



> **Note** If a collection service is displayed in red, the service is abnormal and its metrics cannot be collected. You must troubleshoot the service.

5.Security compliance

5.1. Operation log audit

You can check the resource usage and running status of all modules on the platform by viewing logs.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, click **Operation Log Audit**.
4. On the **Operation Logs** page, perform the following operations:
   - Query logs

     In the upper part of the page, enter a username and select a time range. Click **Search** to view related logs in the list below.
   - Delete logs

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

     Select the logs that you want to export and click the icon. If you do not select logs,

     when you click the icon, all displayed logs are exported.

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

5.2. Server password management

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

Background information

The Server Passwords module provides the following features:

- The system automatically collects information of all the servers in the Apsara Stack environment.
- Server passwords are periodically updated.
- You can configure the expiration period and length of a password.
- You can manually update the passwords of one or more servers at a time.
- The system records the history of server password updates.

- You can search for server passwords by product, hostname, or IP address.

Procedure

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

   The **Manage Passwords** tab shows the passwords of all servers in the current Apsara Stack environment.
4. You can perform the following operations:
   - Query a server

     On the **Manage Passwords** tab, select a product or hostname to query a specified server. Alternatively, click Advanced and enter an IP address in the IP field, and then click **Search** to query a specified server. You can choose Advanced > **Reset** to clear the previous search conditions.
   - Query a password
     a. On the **Manage Passwords** tab, find the server whose password you want to query.
     b. Click the icon in the **Password** column. The server password in plaintext is displayed and is converted into cipher text 10 seconds later. Alternatively, click the icon to show the password in cipher text.
   - Update a password
     a. On the **Manage Passwords** tab, find the server whose password you want to update.
     b. Click **Update Passwords** in the **Actions** column.
     c. In the dialog box that appears, specify **Password** and **Confirm Password**, and click **OK**.

        The password of the server is updated.
   - Update passwords at a time
     a. On the **Manage Passwords** tab, select servers whose passwords you want to update.
     b. Click **Batch Update** at the bottom of the page.
     c. In the dialog box that appears, specify **Password** and **Confirm Password**, and click **OK**.

        The passwords of the selected servers are updated.
   - Query the update history of server passwords

     Click the **History Password** tab. Select a product, hostname, or IP address, and then click Search to view the update history of server passwords in the search results.
   - Query the historical passwords of a server
     a. On the **History Password** tab, find the server whose historical passwords you want to query.
     b. Click the icon in the **Password** column. The server password in plaintext is displayed and is converted into cipher text 10 seconds later. Alternatively, click the icon to show the password in cipher text.
   - Query and modify the password configuration policy

a. Click the **Configuration** tab and view and modify the metadata of server password management, including the initial password, password length, and retry times. where:
   - **Initial Password** indicates the password assigned when the server password management module was deployed in the Apsara Stack environment. This parameter is required to modify the password of a server in the Apsara Stack environment.
   - **Password Length** indicates the length of passwords updated by the system.
   - **Retry Times** indicates the number of failed password updates before the system stops trying.
   - **Status** indicates whether the configuration takes effect. By default, the switch is turned off. To show the status, turn on  .

b. Click **Save**.

5.3. AccessKey pair management

The AccessKey Pairs module allows you to view the details about the AccessKey pairs of a user with a specified UID, create tasks for AccessKey pair rotation, and generate a new AccessKey pair to replace the AccessKey or SecretKey configuration of the corresponding cluster.

The base service AccessKey pairs of all user nodes that are preset in the Apsara Stack environment are the same. Base service AccessKey pairs are used by service accounts and preset accounts of the platform. If an AccessKey pair is leaked, all Apsara Stack customers are affected and extremely high risks are caused. Therefore, the rotation update of preset AccessKey pairs must be supported.

5.3.1. View AccessKey pair information

The AccessKey Pairs module allows you to query the details about the AccessKey pairs of a user such as the UID, username, enabled AccessKey pair, effective time, number of AccessKey pairs, and number of active clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > AccessKey Pairs**.

   The **AccessKey Management** page displays the information about the AccessKey pairs of all users in the current Apsara Stack environment.
4. Search for a user with a specified UID: In the upper part of the page, select UID, Username, or User AccessKey ID from the drop-down list, enter the corresponding information in the search box, and then click **Search**.
5. View the following details about the AccessKey pairs of the user:
   - The **Basic Information** and **AccessKey List** of the current user.

     On the **UID Details** page, perform the following steps:

     a. Find the UID whose details you want to view and click **Details** in the **Actions** column. The **UID Details** page appears.

     b. In the **Basic Information** section, view the username, number of active clusters, enabled AccessKey pair, and effective time.

     c. In the **Access Key List** section, view the AccessKey pairs, status, effective time, number of active clusters, and number of requests in the last 15 days of the current user.

- Active clusters and all clusters that correspond to the enabled AccessKey pairs of the current user.
  - On the **AccessKey Management** page, perform the following steps:
    a. On the right side of the page, find the cluster whose details you want to view and click the number of active clusters in the **Active Cluster** column.
    b. In the AccessKey Active Cluster dialog box that appears, view the names, products, and effective times of active clusters.
    c. Click **View All Clusters** to view the names, products, and effective time of all clusters.
  - On the **UID Details** page, perform the following steps:
    a. Find the UID whose details you want to view and click **Details** in the **Actions** column. The UID Details page appears.
    b. In the **AccessKey List** section, click **View Active Cluster** in the **Actions** column. You can also click the number of active clusters in the **Active Cluster** column.
    c. In the AccessKey Active Cluster dialog box that appears, view the names, products, and effective time of active clusters.
    d. Click **View All Clusters** to view the names, products, and effective time of all clusters.

5.3.2. Create AccessKey ID rotation tasks

The Create AccessKey ID Rotation Task feature implements the rotation update of preset AccessKey IDs to prevent the leakage of AccessKey IDs that might affect all Apsara Stack users. The procedure to create an AccessKey ID rotation task consists of four steps: create an AccessKey ID, enable an application, disable the old AccessKey ID, and complete the task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > AccessKey Pairs**.
4. In the upper-left corner of the page, click **Create AccessKey ID Rotation Task**. The **Create AccessKey ID Rotation Task** page appears.

> **Note**
> - During the creation of the AccessKey ID rotation task, the **Task Records** section on the right side of the page records every step that you perform.
> - You can click **Previous** to return to the previous step.
> - You can click **Back** to return to the AccessKey Management page. On the **Historical Tasks** page, you can view the details of the unfinished AccessKey ID rotation task. For more information, see View historical tasks.

The procedure to create an AccessKey ID rotation task consists of four steps: create an AccessKey ID, enable an application, disable the old AccessKey ID, and complete the task. The following table describes the steps.

No.	Step	Operation

1	**Create Access Key ID**.	In the **Select UID** list, select the enabled AccessKey ID of the user and click **Create**. The enabled AccessKey ID that you selected is displayed in the **Create AccessKey ID** list. You can also undo the operation. In the **Create AccessKey ID** list, select the enabled AccessKey ID of the user and click **Recall**. The enabled AccessKey ID that you selected is displayed in the **Select UID** list.
2	**Validate Application**	In the lower-right corner of the page, click **Next:Validate Application**. The list of clusters to be rolled is displayed. ⚠ **Warning** The environment may be unavailable when you roll clusters. Proceed with caution. Rolling clusters is a risky operation. We recommend that you roll one cluster at a time. ◦ Roll clusters ⓘ **Note** Rolling: an operation defined in the Apsara Infrastructure Management to trigger service updates. ▪ Roll one cluster Find the cluster that you want to roll and click **Rolling** in the **Operation** column. After the cluster is rolled, **Has Rolling** is displayed in the **State** column. ▪ Roll multiple clusters at a time In the lower part of the page, select all clusters and click **Rolling**. After the cluster is rolled, **Has Rolling** is displayed in the **State** column. ◦ Rollback rolling In the lower part of the page, select all clusters and click **Rollback Rolling**. The system rolls the clusters by using the previous AccessKey or SecretKey instead of the current AccessKey or SecretKey. You can click **View task details** in the **Operation** column of the cluster list. On the **Cluster Operations** page of the Apsara Infrastructure Management, you can view the details of the cluster.
3	**Disable old Access Key**	⚠ **Warning** The environment may be unavailable when you disable the old AccessKey ID. Proceed with caution. Disabling the old AccessKey ID is a risky operation. We recommend that you disable one AccessKey ID at a time. i. When all clusters are in the **Has Rolling** state, click **Next:Disable Old AccessKey ID**. The old AccessKey IDs are displayed. ii. Disable old AccessKey IDs ▪ Disable one AccessKey ID Find the user whose AccessKey ID you want to disable and click **Disable** in the **Operation** column. After the AccessKey ID is disabled, **Disabled** is displayed in the State column. ▪ Disable multiple AccessKey IDs at a time Select the AccessKey IDs of all users and click **Disable**. After the AccessKey IDs are disabled, **Disabled** is displayed in the state column.
4	**Complete Task**	In the lower-right corner of the page, click **Complete Task**.

5.3.3. View historical tasks

The Historical Tasks feature allows you to view the operation logs of historical rotation tasks and resume unfinished tasks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > AccessKey Pairs**.
4. In the upper-left corner of the page, click **History Tasks**.
5. In the historical task list, view the task ID, initiator, initiation time, duration, as well as status and stage of task creation.

   > **Note** You can select a start date and an end date in the upper-left corner of the page, and click **Search** to view the historical tasks within the specified time range.

6. **Optional:** Find the task and click **Details** in the **Actions** column to go to the **Create AccessKey Rotation ID Task** page. You can continue to create a rotation task. For more information, see Create AccessKey ID rotation tasks.

5.4. Platform encryption

5.4.1. SM4-based metadatabase disk encryption

SM4-based metadatabase disk encryption refers to the use of the SM4 encryption algorithm recognized by China's State Cryptography Administration (SCA) to encrypt important data on the platform. It encrypts data stored in tables. You can use the Apsara Uni-manager Operations Console to enable disk encryption for important data on the platform based on the SM4 encryption algorithm.

5.4.1.1. Enable SM4-based metadatabase disk encryption

The Disk Encryption for Metadatabase (SM4) module allows you to encrypt important data on the platform by using the SM4 cryptographic algorithm that is recognized by the State Cryptography Administration.

Prerequisites

The aso-mgr and aso-opr services have reached the desired state.

Background information

After the metadatabase disk encryption feature is enabled, the service may not reach the desired state.

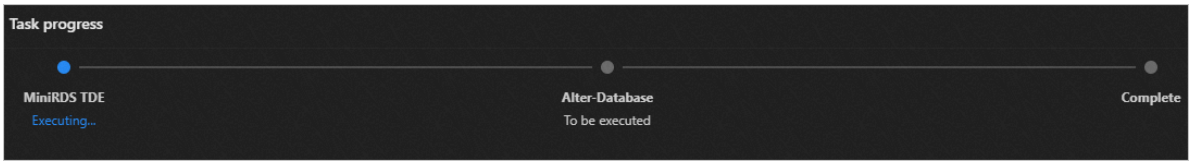
Procedure

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

2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Disk Encryption for Metadatabase (SM4)**.

> ⚠ **Warning** To avoid temporary inaccessibility to the Apsara Uni-manager Operations Console and Apsara Uni-manager management Console, unavailability of UMMAK, AAS, and RAM services, and interruption of the management business, we recommend that you enable transparent data encrytpion (TDE) during the maintenance window. This feature cannot be disabled after it is enabled.

4. If the information of the application that you want to manage is not shown, click the name of the application.
5. Find the application and turn on the switch in the **Actions** column. In the dialog box that appears, click **OK**.
6. In the **Task Progress** progress bar, view the task progress. If a step fails, an error message is displayed. The progress is updated in real time.



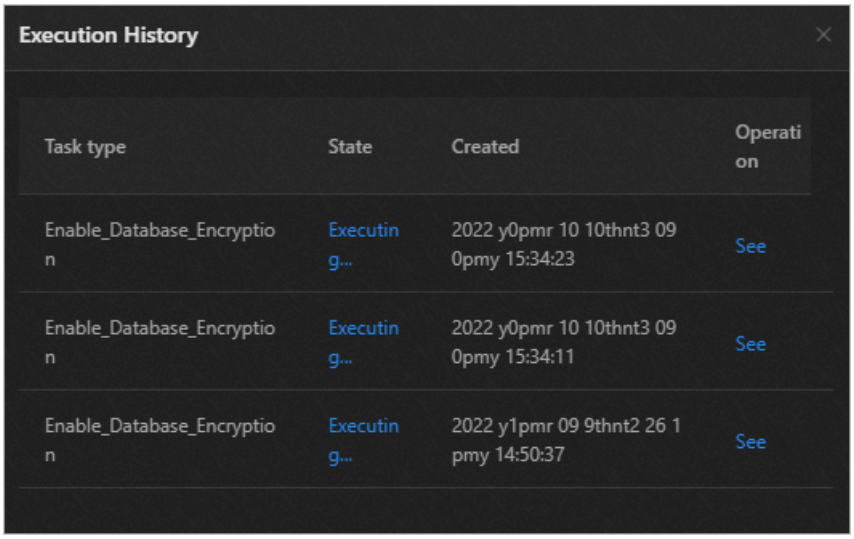
7. **Optional:** The **Reload** button appears below the step that fails. Click the button to execute the step again.
8. After encryption is enabled, the deployment task of changing the configuration for the key-value pairs of the product is triggered. You can query the task details on Apsara Infrastructure Management. Perform the following steps to query the task details:
   i. Log on to the Apsara Infrastructure Management console.
   ii. In the left-side navigation pane, choose **Operations > Cluster Operations**.
   iii. Find the cluster and click **Operations** in the **Actions** column.
   iv. On the **Cluster Details** page, click the **Operations Logs** tab.
   v. Find the ASO update commit log entry and click **Version Difference** in the **Actions** column. On the **Version Differences** page, view the details.

5.4.1.2. View execution history

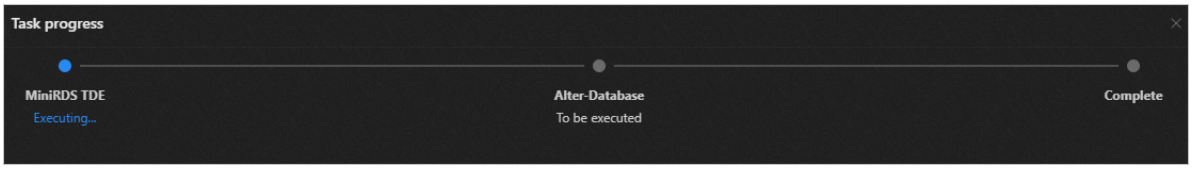
You can view the execution history of encryption operations for a service.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Disk Encryption for Metadatabase (SM4)**.
4. If the information of the application that you want to view is not shown, click the name of the application.
5. Click **See** in the **Execution History** column.
6. In the panel that appears, view the execution history.



7. Find the task and click **See** in the **Operation** column. In the progress bar that appears, view the task execution details.



5.4.2. Transmission encryption for metadatabase and platform access

The Transmission Encryption for Metadatabase and Platform Access module encrypts the transmission paths when important data is written to a disk. This module also encrypts access links to the Apsara Uni-manager Operations Console and Apsara Uni-manager Management Console, as well as the access links that are called by APIs.

5.4.2.1. Enable or disable transmission encryption with one click

This topic describes how to enable or disable transmission encryption for the metadatabase and platform access of all applications with one click.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Transmission Encryption for Metadatabase and Platform Access** .

> ⚠ **Warning** Transmission encryption for metadatabase and platform access includes the Secure Sockets Layer (SSL)-based encryption for metadata access and HTTPS-based encryption for Apsara Uni-manager Operations Console and Apsara Uni-manager Management Console access. If you switch between enabling and disabling encryption, your access to UMMAK, RAM, OAM, and AAS services is unavailable, and your access to the Apsara Uni-manager Operations Console, Apsara Uni-manager Management Console, IDaaS, and POP is interrupted. Proceed with caution.

4. In the upper-left corner of the page, turn on or turn off **Enable or disable transmission encryption with one click**. In the message that appears, click **OK**.
5. In the upper-right corner of the page, click **View tasks**. In the panel that appears, view the progress of enabling or disabling transmission encryption.

> ⓘ **Note** You can turn on or off **Automatic Update** based on your business requirements.

5.4.2.2. Enable or disable transmission encryption for a single application

This topic describes how to enable or disable transmission encryption for a single application.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Transmission Encryption for Metadatabase and Platform Access** .
4. If the information of the application for which you want to enable or disable transmission encryption is not shown, click the name of the application.

> ⚠ **Warning** Transmission encryption for metadatabase and platform access includes the Secure Sockets Layer (SSL)-based encryption for metadata access and HTTPS-based encryption for Apsara Uni-manager Operations Console and Apsara Uni-manager Management Console access. If you switch between enabling and disabling encryption, your access to UMMAK, RAM, OAM, and AAS services is unavailable, and your access to the Apsara Uni-manager Operations Console, Apsara Uni-manager Management Console, IDaaS, and POP is interrupted. Proceed with caution.

5. Find the application and turn on or turn off the switch in the **Actions** column. In the dialog box that appears, click **OK**.

5.4.2.3. View execution history

This topic describes how to view the execution history of product encryption operations.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Transmission Encryption for Metadatabase and Platform Access** .

4. If the information of the application that you want to view is not shown, click the name of the application.
5. Click **See** in the **Execution History** column.
6. In the panel that appears, view the execution history.
7. Find the task and click **See** in the **Operation** column. In the progress bar that appears, view the task execution details.

5.4.2.4. View a certificate

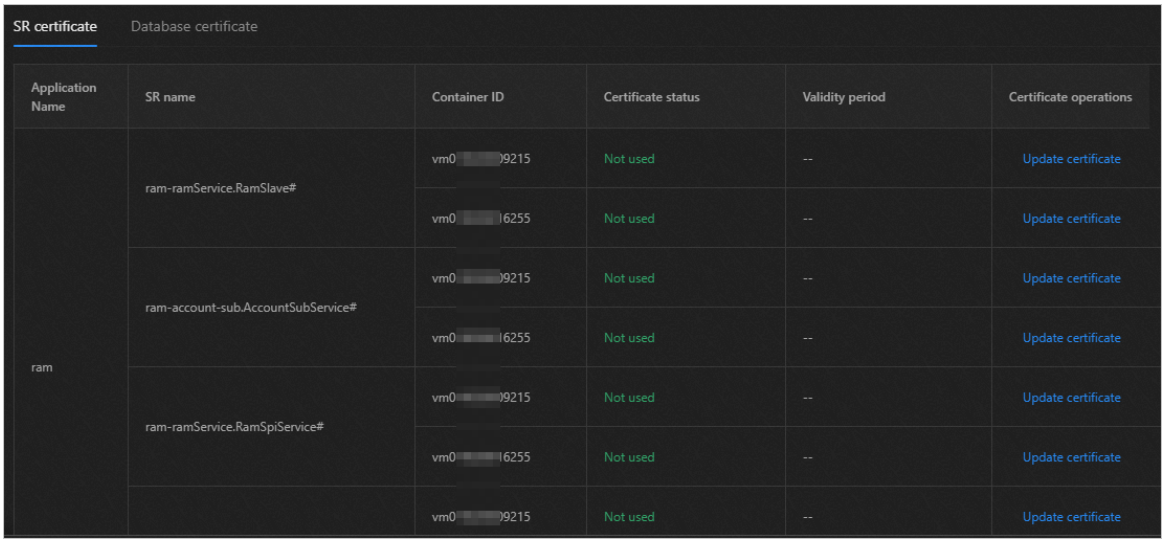
After you enable transmission encryption for metadatabase and platform access, you need to use a certificate to access the database. This topic describes how to view the status of the certificate.

Procedure

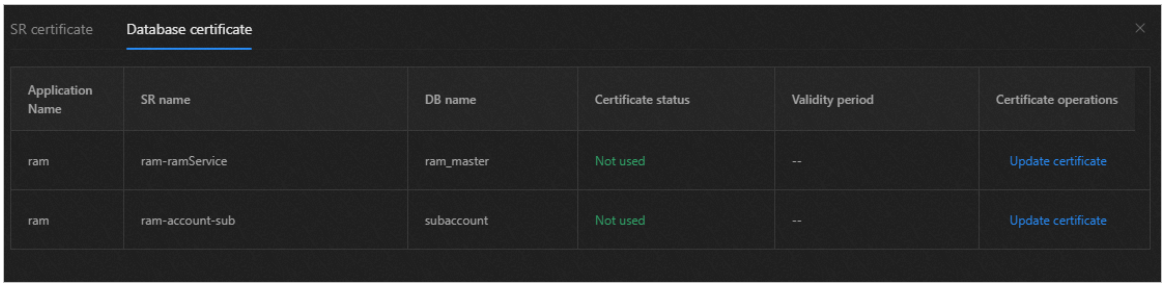
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Transmission Encryption for Metadatabase and Platform Access** .
4. Find the application whose certificate you want to view and click **Certificate** on the right of the application name. On the page that appears, you can view the details about the certificate.

> **Note** The certificate can be in one of the following statuses: **Normal**, **About to Expire**, **Expired**, **Initializing**, and **Not used**.
>
> - **Normal**: The certificate is used as expected.
> - **About to expire**: The certificate will expire in 15 days or less.
> - **Expired**: The certificate has expired.
> - **Initializing**: The code of the Apsara Uni-manager Operations Console is being initialized or an error occurred when the code is being initialized. When the deployment of the Apsara Uni-manager Operations Console reaches the desired state, the status of the certificate becomes Not used or Normal.
> - **Not used**: For some applications, you must pull the certificate during initialization. After the certificate is pulled, the status of the certificate is Normal. For some applications, you must pull the certificate after you enable encryption. The status of the certificate is Not used because the certificate is not pulled before encryption is enabled.

i. On the **SR certificate** tab, view the certificate details of the service role (SR) that uses SSL to access the database.



ii. Click the **Database certificate** tab to view the details about the database certificate.



5.4.2.5. Renew a certificate

If the status of a certificate is Expired or About to expire, you can renew the certificate by updating its validity period.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Security & Compliance**.
3. In the left-side navigation pane, choose **Passwords & Encryption > Platform Encryption > Transmission Encryption for Metadatabase and Platform Access** .
4. Find the application whose certificate you want to renew and click **Certificate** on the right of the application name. On the page that appears, view the details about the certificate.

   > ⚠ **Warning** If you renew a service role (SR) certificate, the service is expected to be interrupted for 30 minutes. Therefore, we recommend that you renew the certificate during the maintenance window.

5. On the **SR certificate** or **Database certificate** tab, click **Update certificate** in the **Certificate operations** column. In the dialog box that appears, click **OK**. After the certificate is updated, the message **Updated** appears.

6.System settings

6.1. Default operations roles

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

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

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

6.2. User permissions

6.2.1. User management

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

Prerequisites

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

- A department has been created.
- A custom role, if required, has been created.

Procedure

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

   In the left-side navigation pane, click **User Permissions > Users**. By default, the **Users** tab appears.
3. On the **Users** tab, perform the following operations:
   - Query a user

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

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

(Optional) Click **Reset** to clear the filter conditions.

- Add a user

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

  Click **Add** in the upper part of the page. On the **Add User** panel, specify parameters such as **Username** and **Password**, and click **OK**.

  The added user is displayed in the user list.

- Modify a user

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

  In the user list, find the user that you want to modify and click **Modify** in the **Actions** column. On the **Modify User** panel, modify the parameters and click **OK**.

- Delete a user

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

  > **Note**
  >
  > Deleted users are displayed on the **Recycle Bin** tab. To restore a deleted user, click the **Recycle Bin** tab. Find the user that you want to restore and click **Recover** in the **Actions** column. In the message that appears, click **OK**.

- Attach a logon policy

  In the user list, select the user to which you want to attach a logon policy and click **Modify Logon Policy** in the lower part of the page. In the dialog box that appears, select the logon policy to attach and click **OK**.

- Query the personal information of the current user

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

  On the **User Profile** page, you can also change the password that the current user uses to log on to the Apsara Uni-manager Operations Console.

- Logon settings

Move the pointer over the profile picture in the upper-right corner of the page and click **Logon setting**. On the **Logon Settings** page, you can modify the logon timeout period and validity period of the current account. You can also specify whether to allow multi-terminal logon.

6.2.2. User group management

The User Groups module enables you to add multiple users to a user group and add the same roles to the group as an administrator for centralized management. You can create, edit, and delete a user group, add users to and delete users from a created user group, as well as add and modify the roles of a user group by using this module.

6.2.2.1. Create a user group

This topic describes how to create a user group.

Procedure

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

   > **Note** You can add multiple roles to a user group.

6. Click **OK**.

6.2.2.2. Edit a user group

This topic describes how to modify the name of a created user group.

Procedure

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

6.2.2.3. Delete a user group

This topic describes how to delete an existing user group.

Prerequisites

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

Procedure

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

6.2.2.4. Manage users

This topic describes how to add users to or delete users from a created user group.

Procedure

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

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

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

6.2.2.5. Add a role

This topic describes how to add one or more roles to a user group.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **User Permissions** > **User Groups**.
4. **Optional:** Select a department name, enter a user group name, and then click **Search**. You can also click **Advanced**, enter a username, select a role, and then click **Search**. If you have specified filter conditions, you can click **Reset** to remove the conditions.
5. In the user group list, find the user group to which you want to add a role and click **Add Role** in the **Actions** column.

6. Select a role from the **Role** drop-down list.
7. Click **OK**.

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

6.2.2.6. Modify the role of a user group

This topic describes how to modify the role of a user group.

Prerequisites

The role information has been added to the user group.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **User Permissions > User Groups**.
4. **Optional:** Select a department name, enter a user group name, and then click **Search**. You can also click **Advanced**, enter a username, select a role, and then click **Search**. If you have specified filter conditions, you can click **Reset** to remove the conditions.
5. In the list of user groups, find the user group whose role you want to modify and click **Add Role** in the **Actions** column.
6. Select a role from the **Role** drop-down list.
7. Click **OK**.

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

6.2.3. Role management

You can set custom roles in the Apsara Uni-manager Operations Console to implement more flexible and efficient permission control. The Apsara Uni-manager Operations Console separates read and write permissions. You can bind specific read and write permissions to a role based on your business requirements.

Background information

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

Procedure

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

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

In the upper-left corner of the page, enter a role name in the **Role** search box and click **Search** to view the role information in the list. You can move the pointer over the **Permission Details** column to view the basic information about the role.

- Add a role

  > **Note**
  > - Only users who have the security officer role of the Apsara Uni-manager Operations Console can add a role in the console.
  > - You can bind the added role to a user and use the user to log on to the Aspara Uni-manager Operations Console. In this way, you can control access permissions of the user on specific menus.

  a. In the upper-left corner of the page, click **Add**.
  b. In the **Add Role** panel, configure the parameters.
     - In the **Role Name** field, enter the name of the role that you want to add.
     - In the **Role Description** field, enter a brief description of the new role.
     - Select roles from the **Base Role** drop-down list to specify the basic roles of the OAM system for underlying authentication.
     - In the **Menu** section, select the menus that are accessible to the role.
  c. Click **OK**.
- Modify a role

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

  a. Find the role that you want to modify and click **Edit** in the **Actions** column.
  b. In the **Edit Role** panel, update the parameters.
- Delete a role

  > **Important** Before you delete a role, make sure that the role is not bound to a user. Otherwise, the role cannot be deleted.

  a. Find the role that you want to delete and click **Delete** in the **Actions** column.
  b. In the dialog box that appears, click **OK**.

6.2.4. Department management

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

Background information

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

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

Procedure

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

On the **Department Management** page, you can view the tree structure of all created departments and the information about all users in each department.

4. **Optional:** In the upper-left corner of the page, enter a department name in the search box and click the search icon to find the department that you want to manage.
5. Perform the following operations:
   - Add a department

     In the catalog tree on the left, select the department to which you want to add a sub-department and click **Add Department**. In the **Add Department** dialog box, set Department Name, and click **OK**. Then, you can view the created department in the catalog tree.
   - Modify a department

     In the catalog tree on the left, select the department that you want to modify and click **Modify Department**. In the **Modify Department** dialog box, set Department Name, and click **OK**.
   - Delete a department

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

     In the catalog tree on the left, select the department that you want to delete and click **Delete Department**. In the message that appears, click **OK**.
   - Add a user to a department

     In the catalog tree on the left, select the department to which you want to add a user, click **Create User**. In the **Add User** dialog box, configure Username, Password, Confirm Password, Logon Policy, Role, and optional parameters such as Display Name, Logon Policy, Role, Department, Mobile Number, and Email Addresses. Click **OK**.

     After a user is added, you can choose **User Permissions** > **Users** in the left-side navigation pane to view the information about the user.
   - Add a user group to a department

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

     After a user group is added, you can choose **User Permissions** > User Groups to view the information about the user group.

6.2.5. Manage regions

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

Background information

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

Relationship between departments and regions:

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

Procedure

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

6.2.6. Two-factor authentication

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

Background information

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

This authentication method is 2-step verification and uses a password and a mobile app to provide a two-layer protection for accounts. You can obtain the logon key after you configure users in the Apsara Uni-manager Operations Console, and then enter the key in the Google Authenticator app on your mobile phone. The app generates a verification code for your logon based on the time and key.

Procedure

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

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

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

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

6.2.7. Logon policies

As an administrator, you can configure logon policies to manage the logon time and logon IP addresses of users.

Background information

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

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **User Permissions > Logon Policies**.
4. On the **Logon Policies** page, you can perform the following operations:
   - Query a policy

     In the upper-left corner of the page, enter a policy name in the **Policy Name** search box and click **Search** to view the policy information in the list.
   - Add a policy

     Click **Add Policy**. In the panel that appears, set the parameters and click **OK**.
   - Modify a policy

     Find the policy that you want to modify and click **Modify** in the **Actions** column. In the **Modify Policy** panel, modify the parameters and click **OK**.
   - Delete a policy

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

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

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

     > **Important**
     >
     > After a policy is disabled, users who are bound to the policy cannot log on to the Aspara Uni-manager Operations Console.
   - Enable a policy

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

6.2.8. Logon settings

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

Background information

To make your system more secure, you can modify the logon settings based on your scenario.

Procedure

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

       For example, User A uses the current account to go to another console from the Apsara Uni-manager Operations Console. At the same time, User B uses the current account to log on to the Apsara Uni-manager Operations Console. The system disables the logon of User A only after User A returns to the Apsara Uni-manager Operations Console.
     - **Forbid Multi-Terminal Logon in O&M**: The current account is not allowed to log on to the Apsara Uni-manager Operations Console or the console redirected from the Apsara Uni-manager Operations Console from multiple terminals.
5. Click **Save**.
6. Click the **Account Validity Period** tab and set **Account Validity (Days)**.

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

6.2.9. Personal information

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

Background information

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

Procedure

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

6.3. Platform settings

6.3.1. Menu settings

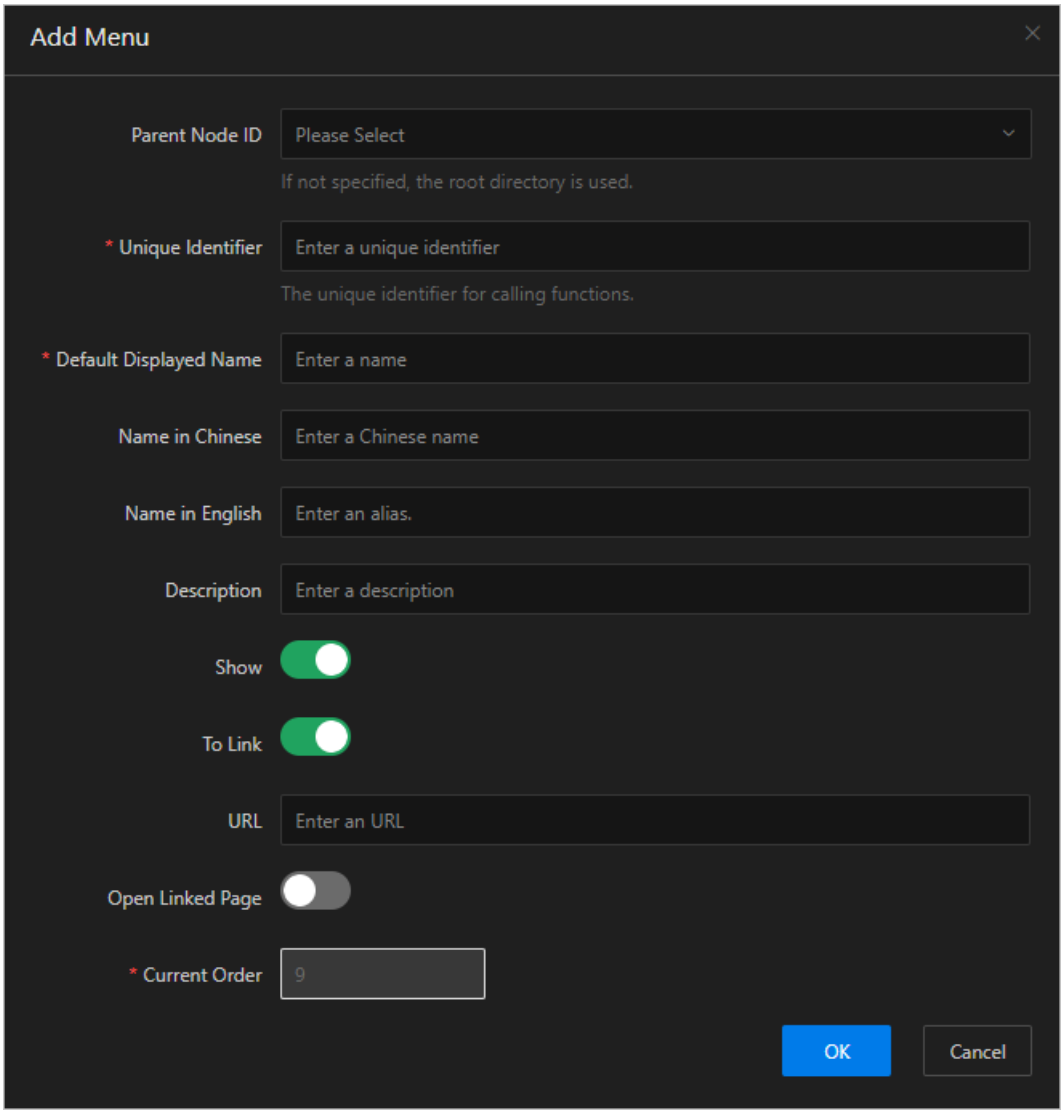
The Menu Settings module allows you to add, hide, modify, or delete a menu based on your business requirements.

6.3.1.1. Add a main menu

This topic describes how to add a main menu.

Procedure

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



The following table describes the parameters.

Parameter	Description
Parent Node ID	The parent menu. This parameter does not need to be specified when you add a main menu.
Unique Identifier	The unique identifier that is used to invoke functions. It can be 5 to 20 characters in length.
Default Display Name	The default display name of the menu.
Name in Chinese	The menu name in Chinese. In the Chinese language environment, if the Chinese name of the menu is specified, the default display name of the menu is the specified Chinese name.
Name in English	The menu name in English. In the English language environment, if the English name of the menu is specified, the default display name of the menu is the specified English name.
Description	The description of the menu.

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

6. Click **OK**.

Result

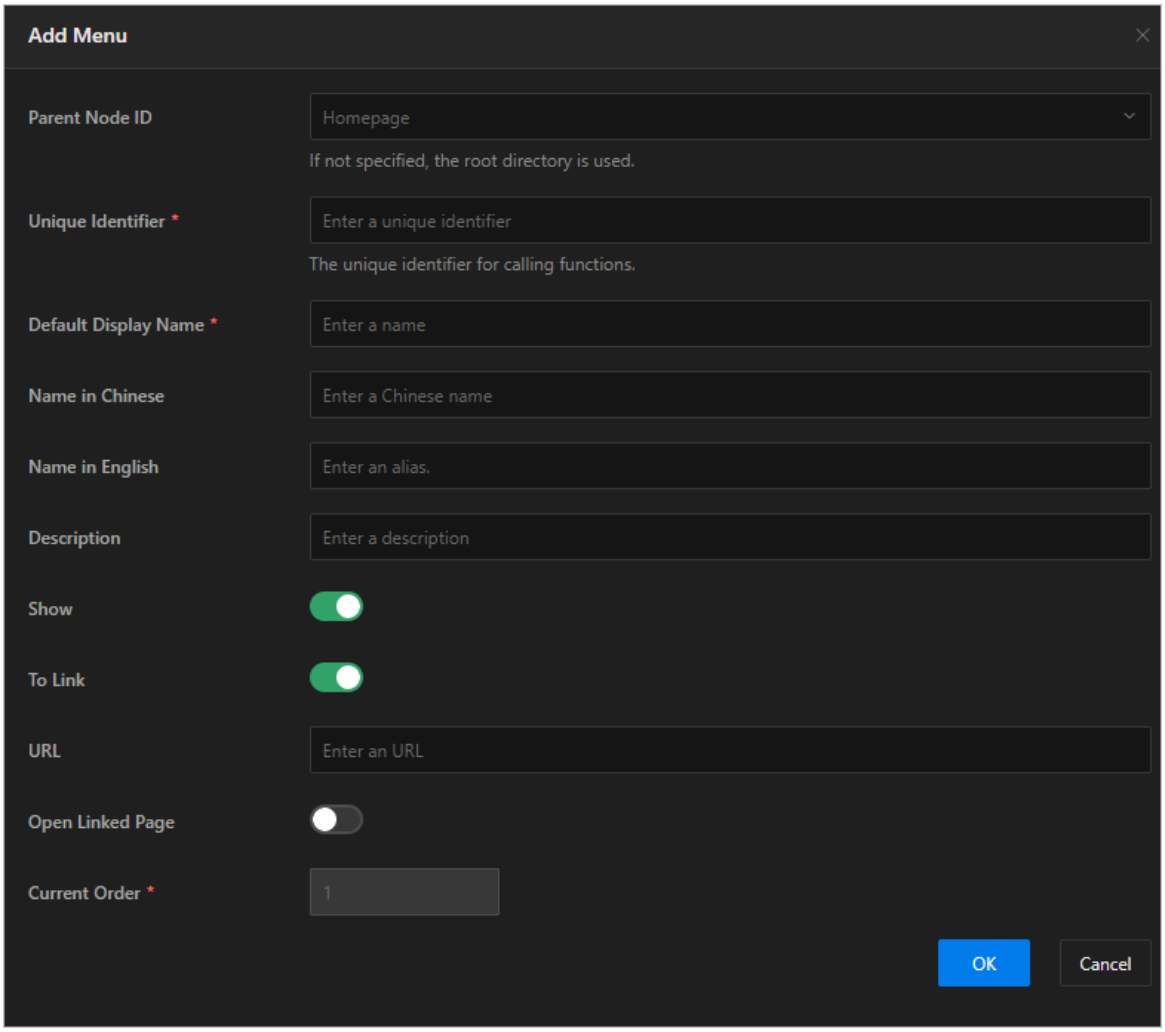
After you have added a main menu, you can view the menu in the menu list and the top navigation bar.

6.3.1.2. Add a submenu

This topic describes how to add a submenu.

Procedure

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



The following table describes the parameters.

Parameter	Description
Parent Node ID	The menu to which the submenu belongs.
Unique Identifier	The unique identifier that is used to invoke functions. It can be 5 to 20 characters in length.
Default Display Name	The default display name of the submenu.
Name in Chinese	The submenu name in Chinese. In the Chinese language environment, if the Chinese name of the submenu is specified, the default display name of the submenu is the specified Chinese name.
Name in English	The submenu name in English. In the English language environment, if the English name of the submenu is specified, the default display name of the submenu is the specified English name.
Description	The description of the submenu.
Show	Specifies whether to show the submenu after it is added. You can turn on or off **Show**. By default, Show is turned on.

To Link	Specifies whether to go to another page when you click the submenu. You can turn on or off **To Link**. By default, To Link is turned off.
URL	This parameter appears only when **To Link** is turned on. Set this parameter to the URL to go to when you click the submenu. ▪ If the URL of a page within the current system is used, enter the absolute path or a relative path of the page. Example: /aso/aso-alarm/dashboard. ▪ If the URL of a third-party system is used, enter the absolute path of the page. Example: http://example.com/TaskManageTool/#/taskView.
Open Linked Page	Specifies whether to open the link in a new page after you click the submenu. You can turn on or off **Open Linked Page**. By default, the switch is off.
Menu Type	The type of the menu. When you create a submenu, you do not need to configure this parameter.
Current Order	The order of the submenu under the selected menu. You cannot configure the order in the panel. You can modify the configuration on the **Menus** page after you create the submenu.

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

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

6.3.1.3. Hide a menu

This topic describes how to hide a menu.

Prerequisites

> **Important** Only custom menus and submenus can be hidden. After a menu or submenu is hidden, cascading menus beneath the menu or submenu are also hidden.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **Platform Settings > Menus**.
4. In the menu list, find the menu or submenu that you want to modify and click **Modify** in the **Actions** column.
5. In the Modify Menu panel, turn off **Show** and click **OK**.

6.3.1.4. Modify a menu

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

Prerequisites

> **Important** Only custom menus and submenus can be modified. Built-in menus and submenus can only be sorted.

Procedure

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

6.3.1.5. Delete a menu

This topic describes how to delete a menu or submenu that you no longer need.

Prerequisites

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

Procedure

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

6.3.2. Authorization information

The Authorization Information module allows customers, field engineers, and O&M engineers to query services that are experiencing authorization problems and troubleshoot the problems. It also supports threshold configuration, usage monitoring, and alert notifications.

6.3.2.1. View authorization information

The Authorization Information module allows users, field engineers, and O&M engineers to query services that are experiencing authorization problems and troubleshoot the problems.

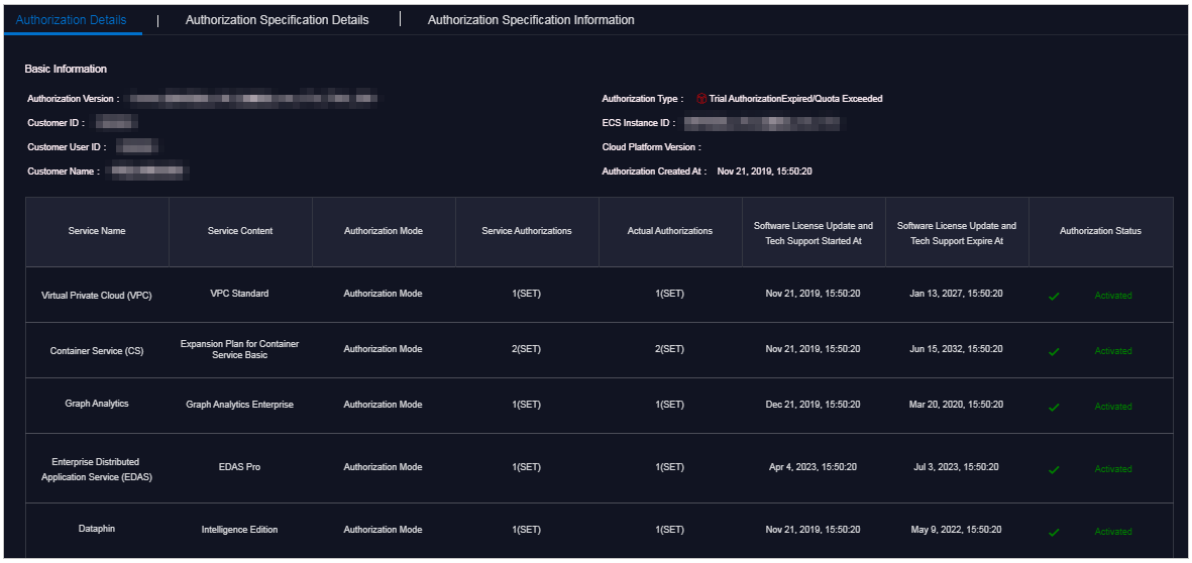
Prerequisites

The logon users are granted the administrator permissions. Only users who are granted the administrator permissions can view the trial authorization information or enter the authorization code to view the formal authorization information on the **Authorization Details** tab.

If you are not granted the administrator permissions, a message appears indicating that you have insufficient permissions when you access this tab.

Procedure

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



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

> **Note** For formal authorization, you must enter the authorization code to view the authorization information. You can obtain the authorization code from the authorization letter appended to the project contract or by contacting the business manager (CBM) of your project.

   - On the **Authorization Details** tab, view the authorization information.
     - In the **Basic Information** section, you can view the authorization information in the current Apsara Stack environment, including the authorization version, authorization type, customer ID, cloud instance ID, customer UID, cloud platform version, customer name, and authorization creation time.
     - You can select an authorization status from the **Select authorization status** drop-down list and click **Query** to view the authorization details.

     The following table describes the basic authorization information.

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

Authorization Type	Indicates the current authorization type and authorization status.
	▪ The following authorization types are available:
	  ▪ **Trial Authorization**
	  ▪ **Formal Authorization**
	▪ The following authorization statuses are available:
	  ▪ **Not activated**
	  ▪ **About to expire**
	  ▪ **Taking effect**
	  ▪ **Expired**
	  ▪ **Expired|Excess**

Customer Name	The name of the customer who purchased the Apsara Stack service.
Customer ID	The unique ID of the customer.
UID	The unique ID of the user.
Instance ID	The ECS instance ID in the deployment planner of the field environment.
Cloud Platform Version	The Apsara Stack version of the current cloud platform.
Authorization Created At	The start time of the authorization.

Apsara Stack Product Authorization Details (Data Center)	The authorization information of cloud services within different regions, including the service name, service content, current authorization mode, service authorization quantity, actual authorization quantity, software license update and technical support start time, software license update and technical support end time, and real-time product authorization status.
	If the following items appear in the **Authorization Status** column of a service, take note of them.
	▪ **RENEW Service Expired**
	  Specifies that the customer must renew the subscription as soon as possible. Otherwise, field operations services (including ticket processing) are terminated.
	▪ **Specification Quota Exceeded**
	  Specifies that the specifications deployed for a service have exceeded the contract quota, and the customer must scale up the service as soon as possible.

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

  The following table describes the authorization specification information.

Item	Description
Service Name	The name of an authorized service.

Authorization Specification Name	The specification name of an authorized service.
Authorized Specifications	The total number of current authorizations of a specification for a service.
Maximum specification	The maximum authorizations of a specification for a service.
Authorization Specification Status	The current authorization status of a specification for a service.
Threshold settings	Threshold: the percentage between the current authorizations of a specification for a service and the maximum authorizations of a specification for a service. For more information, see Set a threshold.

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

  Select values from the **Authorization Specification Level**, **Data Center ID**, and **Service Name** drop-down lists, select a time range, and then click **Search**. You can view specification authorization statistics of a service, including the maximum number of specifications within the specified time range, the occurrence time for the maximum specification, the minimum number of specifications within the specified time range, the occurrence time for the minimum specification, and the average number of specifications within the specified time range.

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

6.3.2.2. Set a threshold

This section describes how to set a threshold to trigger alerts. When a threshold is exceeded, an alert is triggered. You can view the alert on the Alerts page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **Platform Settings > Authorization Information**.
   The **Authorization Details** tab appears.
4. In the upper-left corner of the page, click the **Authorization Specifications Details** tab to set the thresholds for Apsara Stack services at the data center level and region level.

   > **Note** Threshold: the percentage (%) between the current number of authorized specifications and the maximum number of authorized specifications.

   - Set a threshold in the **Apsara Stack Product Authorization Specifications Details (Data Center)** section.

     a. To set the threshold for a single product, select the product for which you want to set the threshold, and click **Threshold settings** in the **Threshold settings** column. To set the thresholds for multiple products, select the products for which you want to set

thresholds. In the upper-right corner of the section, click **Configure batch thresholds at the data center level**.

b. In the **Threshold configuration** dialog box, turn on **Threshold Level switch**. In the **Threshold Level (%)** field, enter a value or click the arrows.

c. Click **OK**.

- Set a threshold in the **Apsara Stack Product Authorization Specifications Details (Region)** section. Follow the preceding steps to set the thresholds at the region level.

6.4. API management

The API Management module is used to view and manage product information and API information registered on OpsAPI Gateway.

6.4.1. Namespace management

6.4.1.1. View a namespace

The Namespace Management module allows you to view the information of services registered on OpsAPI Gateway, including the name and description of a namespace.

Prerequisites

The OpsAPI has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs > Namespace Management**.
4. View the information about services that are currently registered on OpsAPI Gateway. Alternatively, enter a namespace name in the **namespace** field and click **Search** to view the information about the service.

   > **Note** Click **Clear** to clear the search conditions.

5. Find the namespace that you want to manage and click **Details** in the **Operation** column. In the dialog box that appears, view the name and description of the namespace.
6. Find the namespace that you want to manage and click **Manage APIs** in the **Operation** column. The **Manage APIs** page appears. You can query all API operations of the service on this page.

6.4.1.2. Delete a namespace

This topic describes how to delete a namespace that is currently registered with OpsAPI Gateway.

Prerequisites

OpsAPI has reached the desired state.

Procedure

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

3. In the left-side navigation pane, choose **APIs > Namespace Management**.
4. Find the namespace that you want to delete and click **Delete** in the **Operation** column. In the dialog box that appears, click **OK**.

> **Note** The Delete operation takes effect only on the page and does not affect the actual running of the API for the product.

6.4.2. API management

6.4.2.1. View an API

This topic describes how to view the API information of a product that is registered with OpsAPI Gateway.

Prerequisites

OpsAPI has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs > API Management**.
4. View the API information of a product that is registered with OpsAPI Gateway. You can also enter an API name in the **API name** field, select a namespace and state from the **Belongs namespace** and **State** drop-down lists, and click **Search** to view the information about the API.

> **Note** Click **Clear** to clear the search conditions.

5. Find the API that you want to view and click **Preview** in the **Operation** column. In the dialog box that appears, view the basic information, service information, and parameters of the API.

6.4.2.2. Unpublish and re-publish APIs

You can unpublish an API that is in the **Online** state. After the API is unpublished, the state of the API changes to **Offline**. You can also re-publish an offline API.

Prerequisites

The OpsAPI has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs > API Management**.
4. Find the API that you want to unpublish and click **Offline** in the **Operation** column. In the message that appears, click **OK**.

   > **Note** The offline API operation takes effect only on the page and does not affect the actual running of the API for the service.

5. Find the offline API that you want to re-publish and click **Re-launch** in the **Operation** column.

6.4.2.3. Upgrade APIs

When the configuration data of an API needs to be urgently modified, you can upgrade the API to generate a subset of the API and modify the API configuration data of the subset. After the modification, the subset is launched to overwrite the configuration data in the original API.

Prerequisites

The OpsAPI has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs > API Management**.
4. Find the API that you want to upgrade and click **Upgrade** in the **Operation** column. After that, a subset is generated and is shown below the API column. The subset is in the **Configuring** state.
5. Click the  icon on the left of the API name. In the **Operation** column of the subset, click **Configuration**. In the dialog box that appears, configure the basic information and click **Next**.

   > **Note**
   > - API name: the API code that is used to register the service with OpsAPI gateway. Fuzzy query is supported.
   > - API belongs namespace: the name of the service.
   > - Maximum QPS: the maximum number of queries per second.

6. In the dialog box that appears, configure the parameters and click **Next**.
7. In the dialog box that appears, configure the parameters and click **Submitted**.
   You can specify whether to transparently pass input and output API parameters. You can also add, edit, and delete input and output API parameters.

- Add: Click **New**. In the dialog box that appears, set the parameters and click **OK**.
- Edit: In the **Operation** column, click **Editing**. In the dialog box that appears, modify the parameters and click **OK**.
- Delete: In the **Operation** column, click **Delete**. In the message that appears, click **OK**.

> **Note** After the parameters are configured and submitted, the state of the subset changes to **Debugging**. Only the subset in the **Debugging** state can be published. If only the save operation is performed after the parameters are configured, the subset is in the **Configuring** state and cannot be published.

8. In the **Operation** column of the subset, click **Online**. The original API data is overwritten by the subset. The version number of the original API is increased by 1. The subset information is no longer displayed on the page.

6.4.2.4. Delete an API

This section describes how to delete an API on the page.

Prerequisites

OpsAPI has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs > API Management**.
4. Find the API that you want to delete and click **Delete** in the **Operation** column. In the message that appears, click **OK**.

> **Note** The Delete API operation takes effect only on the page and does not affect the actual running of the API for the service.

6.5. Region Management

The Region Management module allows you to manage regions. You can use the same platform to perform O&M on different data centers by setting regions.

6.5.1. Add regions

If the current environment involves multiple regions, the multi-region configuration administrator and super administrator can add regions. After you add regions, you can switch to different data centers in the same console and view information or perform operations.

Prerequisites

Before you add regions, confirm the following information:

- The networks between regions are connected and the regions share accounts that have the same usernames and passwords.
- You are granted the permissions of a multi-region configuration administrator or a super administrator.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **Others > Regions**.
4. In the upper part of the page, click **Add**.
5. Configure the parameters and click **OK**.

Parameter	Description
Cloud Name	The name of the new data center.
Region Console URL	The console URL of the region. Make sure that the console URL is valid. Otherwise, an error message is returned.
Longitude	The geographic longitude of the region. This parameter is optional.
Latitude	The geographic latitude of the region. This parameter is optional.

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

6.5.2. Modify the region configuration

The Regions module allows a region configuration administrator or a super administrator to modify a region configuration.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **Others > Regions**.
4. Find the region that you want to modify and click **Modify** in the **Actions** column.
5. In the dialog box that appears, modify the parameters and click **OK**.