ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

apsara base

Apsara Uni-manager Operations Console User Guide

Product Version: V3.18.1

Document Version: 20231215

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

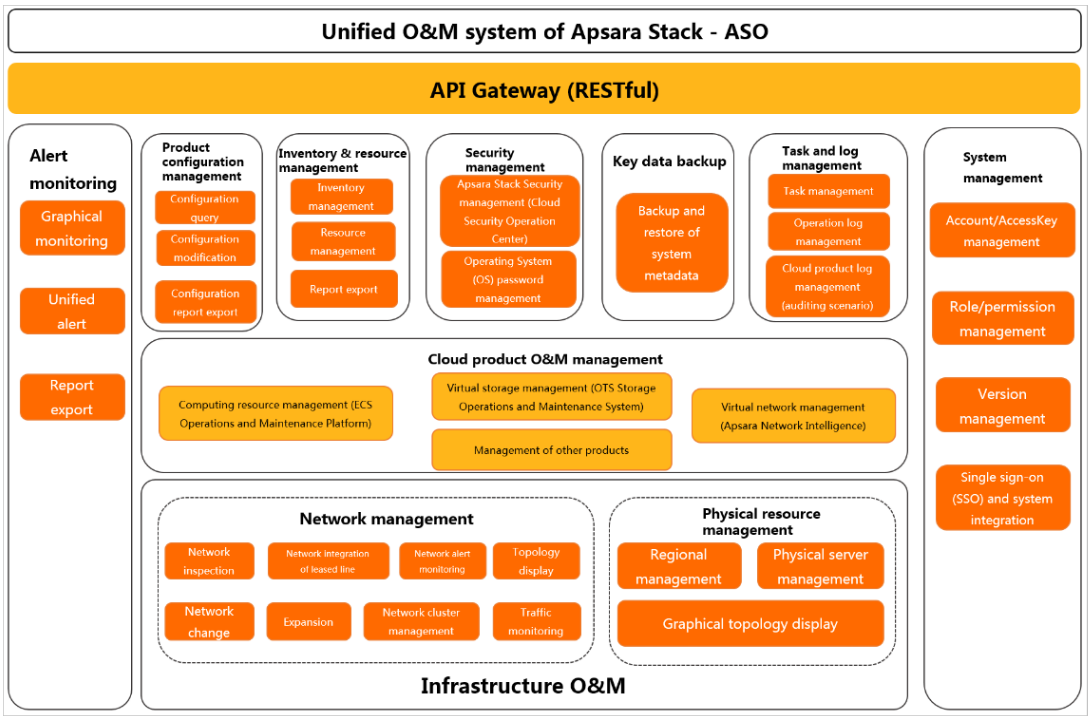
1.Overview

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


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

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 role administrator.

Procedure

1. The role administrator logs on to the Apsara Uni-manager Operations Console.
2. The role administrator creates a role to be assigned to the operations account. For more information about how to create a role, see Role management.
3. The role administrator creates a department to be assigned to the operations account. For more information about how to create a department, see Department management.
4. The role administrator creates an operations account and assigns the created role to the account. For more information, see User management.

   > ? **Note**
   >
   > If the role administrator wants to perform a more fine-grained permission control on the operations role, the role administrator can 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

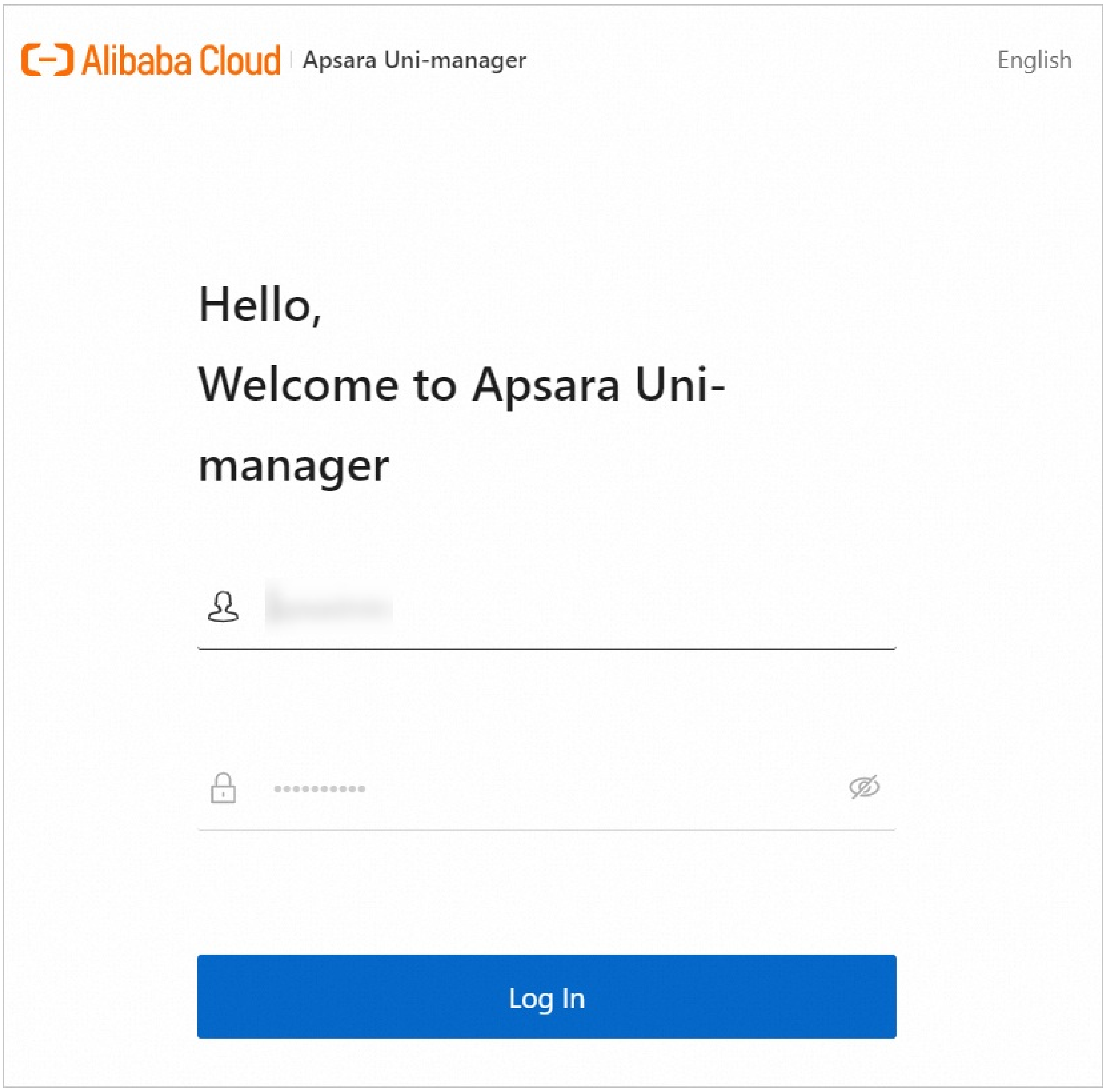
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment engineer or an administrator.

  The endpoint of the Apsara Uni-manager Operations Console is in the following format: *region-id*.ops.console.*intranet-domain-id*.

- A web 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.



Hello,

Welcome to Apsara Uni-manager

> **Note**
>
> You can click the current language in the upper-right corner to switch to another language. Simplified Chinese, English, and Traditional Chinese are supported.

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 engineer or an administrator.

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

   To enhance security, your password must meet the following requirements:

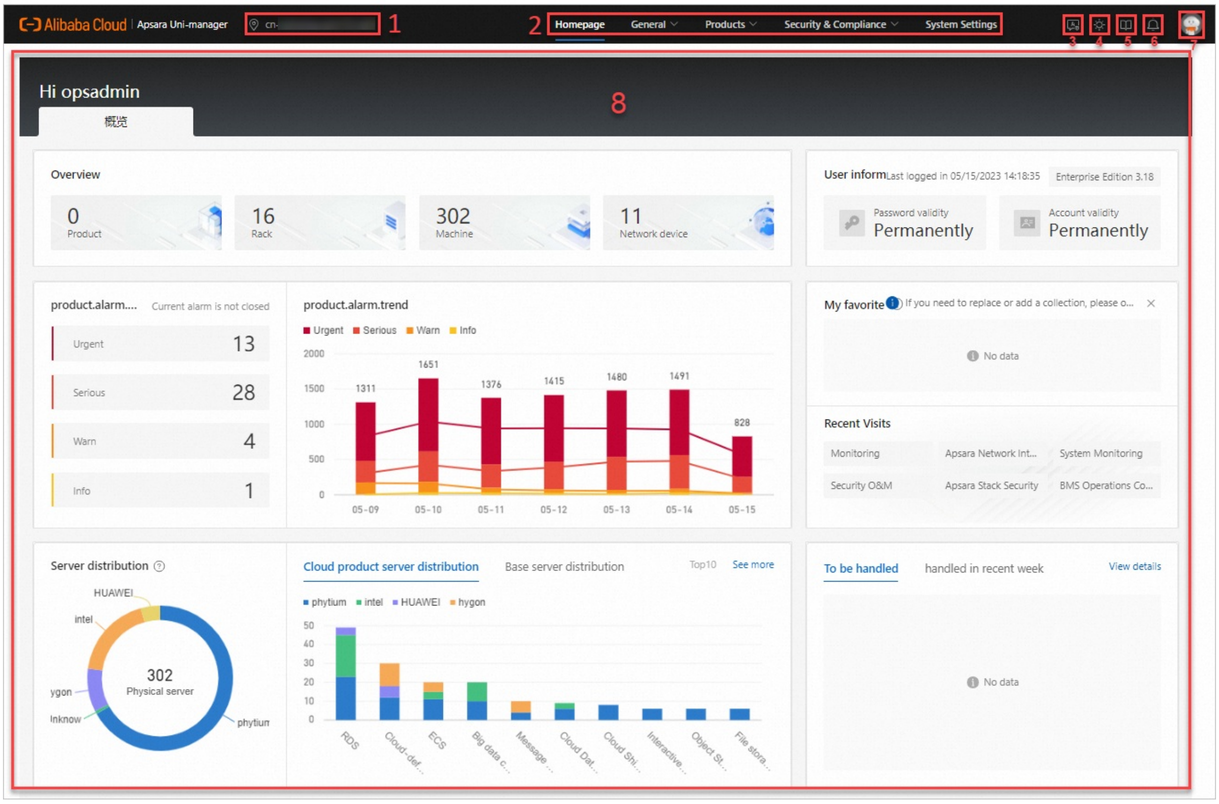
   - The password contains uppercase and lowercase letters.
   - The password contains digits.

- ○ The password contains at least one of the following special characters: ! @ # $ %
- ○ The password is 10 to 20 characters in length.

4. Click **Log On**.

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	Display mode	Click to switch the display mode of the console.

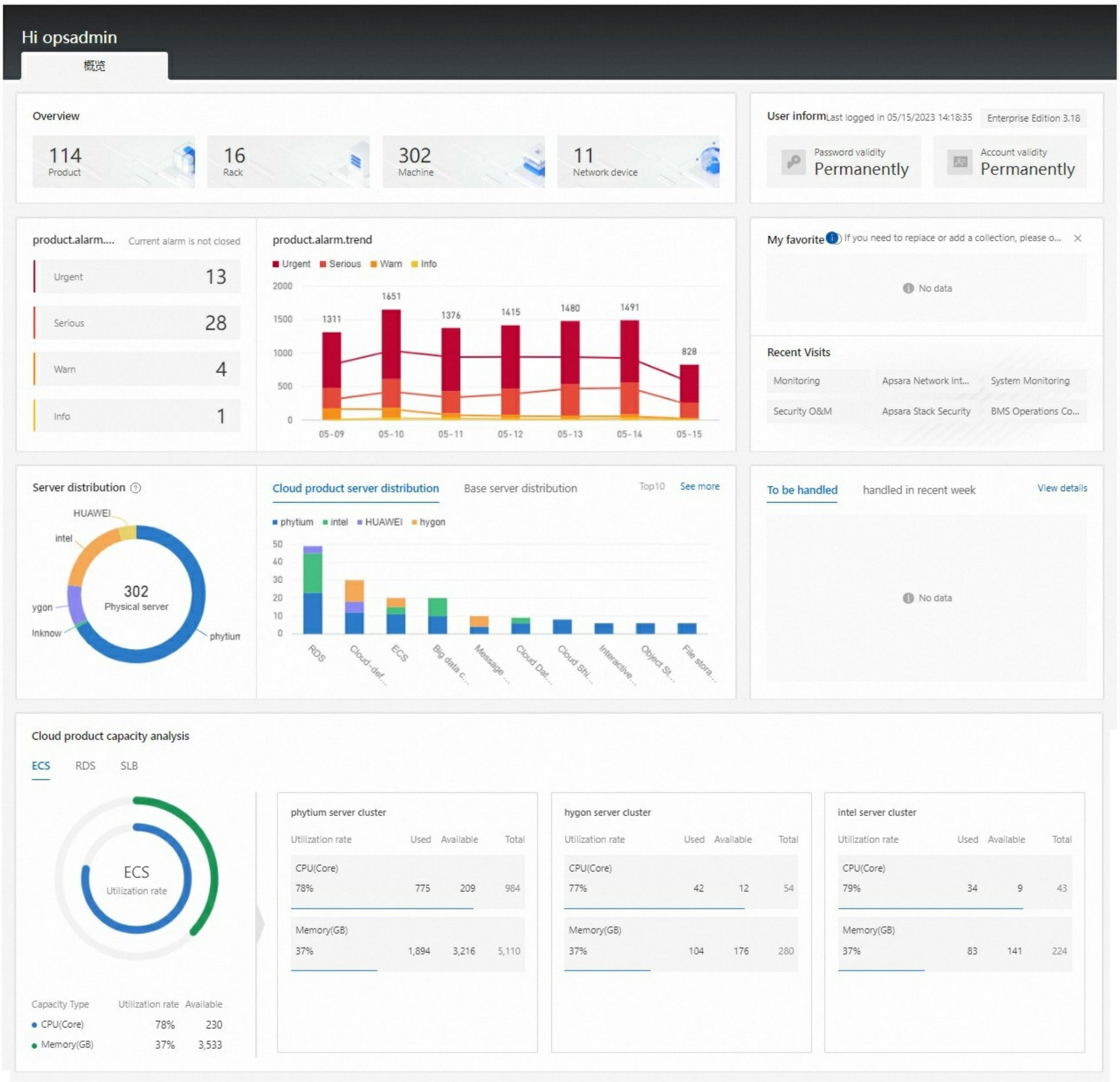
5	Help center	Click to view online documentation.
6	Message center	Click to view the approval notifications and alert notifications that are not handled on the **Approval Messages** and **Alert Messages** tabs.
7	User center	Click to choose **Personal information**, **View version information**, or **Log Out**.
8	Dashboard	View information and perform operations.

2.4. Homepage

On the homepage, you can view resource overview, event overview, the server distribution of multiple chip architectures, and the capacity analysis of cloud products.

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 following sections.

Section	Description
Overview	Displays the total number of products, the total number of racks, the total number of machines, and the total number of network devices.
User	Displays the user information of the current account, including the last logon time, password validity period, account validity period, and version information.
Alert Overview	◦ Displays the number of disabled alerts of each level. ◦ Displays the number of alerts of each level and the trend chart.

Quick access	This section consists of the My favorite and Recent Visits subsections. ∘ **My favorite**: displays the features that you regularly use in the top navigation bar. If you want to change or add features to My favorite, perform operations in the top navigation bar. ∘ **Recent Visits**: displays the menu bars that you recently visit.
Server distribution	∘ Physical server: displays the number of physical servers of each CPU type and the total number of physical servers. ∘ Cloud product server distribution: displays the number of cloud servers of each CPU type at the tenant side. ∘ Base server distribution: displays the number of base servers of each CPU type.
To be handled	∘ Displays the content and submission time of the workflows that require your approval. You can click **View details** in this section to go to the Pending my approval page. ∘ The **handled in recent week** tab displays the content and approval time of the workflows that you approved in the last seven days.
Cloud product capacity analysis	Displays the capacities of multiple cloud services such as Elastic Compute Service (ECS), ApsaraDB RDS, and Server Load Balancer (SLB).

3.General O&M

3.1. Alerts

This topic describes modules of the alert management feature.

Positioning

If exceptions or faults occur in cloud infrastructure or software on the cloud platform, alerts are triggered. The sources of alerts include monitored cloud products, the monitoring system, and objects that are monitored by the monitoring system. After alerts are generated, the alert information is displayed on the Alert Overview, Alerts, and Alert details pages from different dimensions. For example, the total number of alerts for each module of a product is displayed on the Alert Overview page, alerts are converged and the number of alerts is increased on the Alerts page, and the details of an alert is displayed on the Alert details page.

Benefits

The alert management feature allows the system to report alerts or collect monitoring data to match alert rules. This helps manage the alerts of cloud resources in various modules of the cloud platform in a centralized manner and efficiently troubleshoot faults to ensure business stability.

Modules

Module	Description
Alert Overview	Displays general information about alerts by region, alert source, alert trend, alert distribution, and cloud product.
Alerts	Displays information about all reported alerts, including disabled alerts. You can view the details of an alert, change the alert status, and export alert information on this page.
Alert Settings	Provides management features related to alerts, including policy management, alert template, notification management, alert blocking, and alert rule configuration.
Alert Packages	Allows you to upload an alert package to support hot replacement of alert data.

Alert sources

The following table lists the sources of alerts:

Original value	Source
tianjimon	Cluster monitoring system (TianjiMon)
tpcmon	Apsara Stack lightweight monitoring system (TPCMon)

dts	Data Transmission Service (DTS)
Bcmc#	Zone-disaster recovery system of Apsara Stack Resilience
DB	License for Apsara Stack products
asapi	Apsara Stack API operations
drds	PolarDB-X
asrbr-backup	Backup and recovery system of Apsara Stack Resilience
ascm	Apsara Uni-manager Management Console
dbs-dbs	Database Backup Service (DBS)
admin-server	admin-server
asd	Apsara Stack Doctor (ASD)
sds-management	sds-management
bcc	Apsara Bigdata Manager (BCC)
aso-inventory	Inventory monitoring system of Apsara Uni-manager Operations Console
OcpApiV2	ApsaraDB for OceanBase

3.1.1. Alert overview

This topic describes how to view alert overview by region, alert source, and service. You can also view alerts of a specific region and time point.

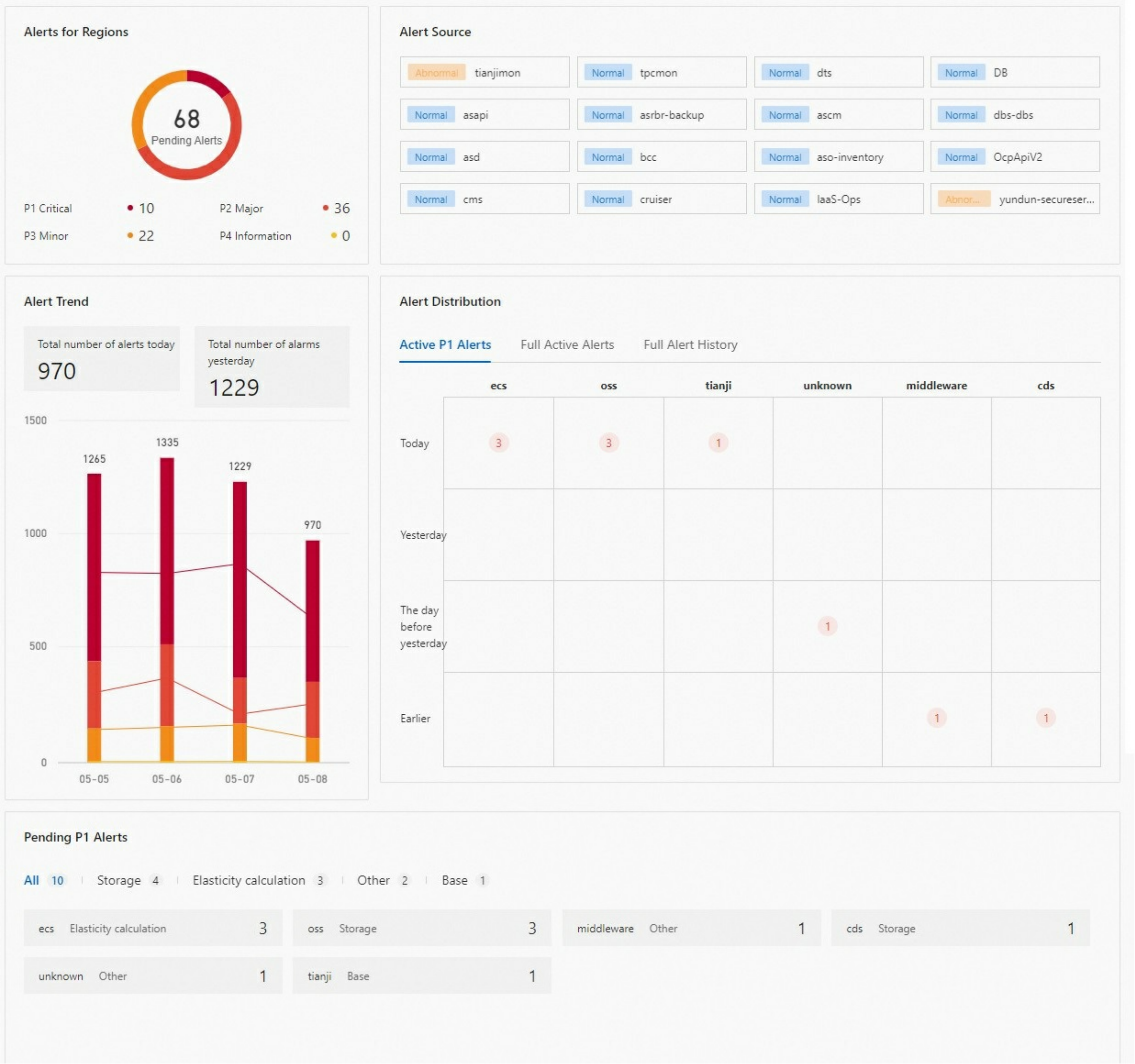
Prerequisites

System administrator permissions are granted.

Procedure

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

2. In the top navigation bar, choose **General** > **Alerts** > **Alert Overview**.
3. The Alert Overview page consists of five sections to provide alert statistics and analysis from different perspectives.



Alerts for Regions

68 Pending Alerts

P1 Critical	● 10	P2 Major	● 36
P3 Minor	● 22	P4 Information	● 0

Alert Source

Abnormal tianjimon	Normal tpcmon	Normal dts	Normal DB
Normal asapi	Normal asrbr-backup	Normal ascm	Normal dbs-dbs
Normal asd	Normal bcc	Normal aso-inventory	Normal OcpApiV2
Normal cms	Normal cruiser	Normal IaaS-Ops	Abnor... yundun-secureser...

Alert Trend

Total number of alerts today 970

Total number of alarms yesterday 1229

Alert Distribution

	ecs	oss	tianji	unknown	middleware	cds
Today	3	3	1			
Yesterday						
The day before yesterday				1		
Earlier					1	1

Pending P1 Alerts

All 10 | Storage 4 | Elasticity calculation 3 | Other 2 | Base 1

ecs	Elasticity calculation	3
oss	Storage	3
middleware	Other	1
cds	Storage	1
unknown	Other	1
tianji	Base	1

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

  Levels P1 to P4 alerts are displayed in different colors on the ring diagram. A larger area of a color on the ring diagram indicates more alerts of the corresponding level.
- The **Alert Source** section shows the status of each alert source.

  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 date.
  - Colors on each bar represent the alert levels. A darker color indicates a higher alert level.
  - A larger area of a color on a bar indicates more alerts of the corresponding levels.
  - If you move the pointer over a bar, the system shows the numbers of alerts of all levels for the day.
  - The line charts show the trend of different alert levels.

- The **Alert Distribution** section shows the quantities and levels of alerts of different services from the following dimensions: **Active P1 Alerts**, **Full Active Alerts**, and **Full Alert History**.

  A larger color block indicates more alerts of the corresponding level. When you move the pointer over a color block, the system shows the alert level and quantity.

- The **Pending P1 Alerts** section shows the cloud platforms that have pending P1 alerts and the quantity of corresponding alerts.

  Each tab is a product category. Click a tab to view the products that have pending P1 alerts and the corresponding alert quantity under the category.

What to do next

After you obtain the alert overview information based on your requirements, you can view alert details in the alert list.

3.1.2. Alerts

You can view the details of all current alerts and change the status of alerts if the system does not update the status in a timely manner. You can also specify custom conditions to search for specific alerts and export the alert information in the XLSX format.

Prerequisites

System administrator permissions are granted.

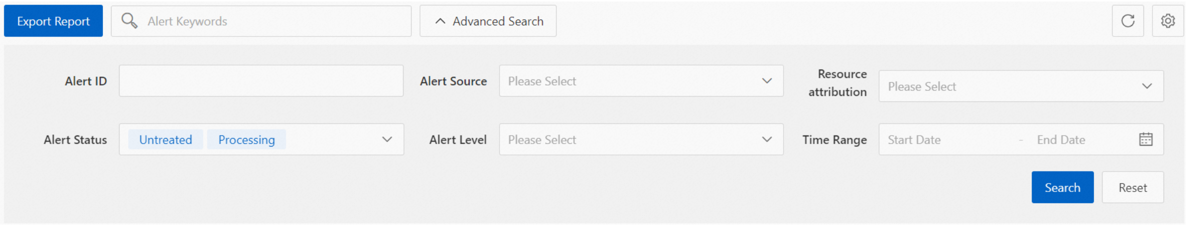
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Alerts** > **Alerts**.
3. By default, the **Not Disabled** tab is displayed. On this tab, you can view information such as **alert IDs**, **resources with alerts**, **alert levels**, **resource attribution**, **alert status**, **last alert time or duration**, **number of alerts**, and **alert source**.

   > **Note**
   >
   > You can also switch to the **Disabled** tab to view the disabled alert list.

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

   You can also click **Advanced Search** to filter alert data by **Alert ID**, **Alert Source**, **Resource attribution**, **Alert Status**, **Alert Level**, and **Time Range**.



Alert Status: Untreated Processing

> Note
>
> On the **Not Disabled** tab, the system does not display the disabled alerts by default. However, you can set **Alert Status** in **Advanced Search** to filter and display the disabled alerts. Similarly, on the **Disabled** tab, the system does not display the alerts that are not disabled by default. You can set **Alert Status** in **Advanced Search** to filter and display the alerts that are not disabled.

5. In the upper-left corner of the page, click **Export Report** to export alerts in the XLSX format.
6. Click the ID of an alert in the **Alert ID** column or click **Details** in the **Operation** column to go to the alert details page and view the details of the alert.
   - In the **Alert information** section, view the basic alert information.

     > Note
     >
     > - Move the pointer over **Details** next to **Detailed alert information**. The details of the alert are displayed.
     > - Click **Handle** or **Disable** to change the alert status.

   - In the **State timing diagram** section, view the alert monitoring metrics in a chart.
     - **1 Day**: shows the alert metrics of the day before the alert is triggered.
     - **1 Week**: shows the alert metrics of the week before the alert is triggered.
   - 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 status. In addition, the services, clusters, products, and physical machines to which the server roles belong are displayed.
7. After an alert is cleared, the system synchronizes the alert status regularly based on alert rules. If the system does not update the status of an alert in a timely manner after the alert is cleared, you can manually change the status of the alert to **Processing** or **Closed**.
   - Into **Processing**:
     - Single alert: On the **Alerts** page, find the alert whose status you want to change and click **Handel** in the **Operation** column. Then, the alert enters the **Processing** state.
     - Multiple alerts: Select the alerts whose status you want to change and click **Batch Handel** in the lower part of the page. Then, the alerts enter the **Processing** state.
   - Into Closed:
     - Single alert: On the **Alerts** page, find the alert whose status you want to change and click **Disable** in the **Operation** column. Then, the alert enters the **Closed** state. After you change the status of the alert, the alert is displayed on the **Disabled** tab.
     - Multiple alerts: Select the alerts whose status you want to change and click **Batch Disable** in the lower part of the page. Then, the alerts enter the **Closed** state. After you change the status of the alert, the alert is displayed on the **Disabled** tab.

3.1.3. Alert settings

Modules

Module	Description
Policy Management	You can configure alert notification contacts, contact groups, and static parameters.
Alert Templates	You can manage alert templates.
Alert Notification	You can configure alert notification channels to push alert notifications to parties of interests.
Alert Blocking	You can block alerts based on time range, resource ownership, cluster, service, server role, server, alert level, and alert source settings. You can also block specific alerts based on alert IDs.
Blocked Alerts	You can view blocked alerts and their details and associated blocking rules.
Alert Rule Settings	You can view rules that trigger alerts.

3.1.3.1. Policy management

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

Manage contacts

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

Procedure

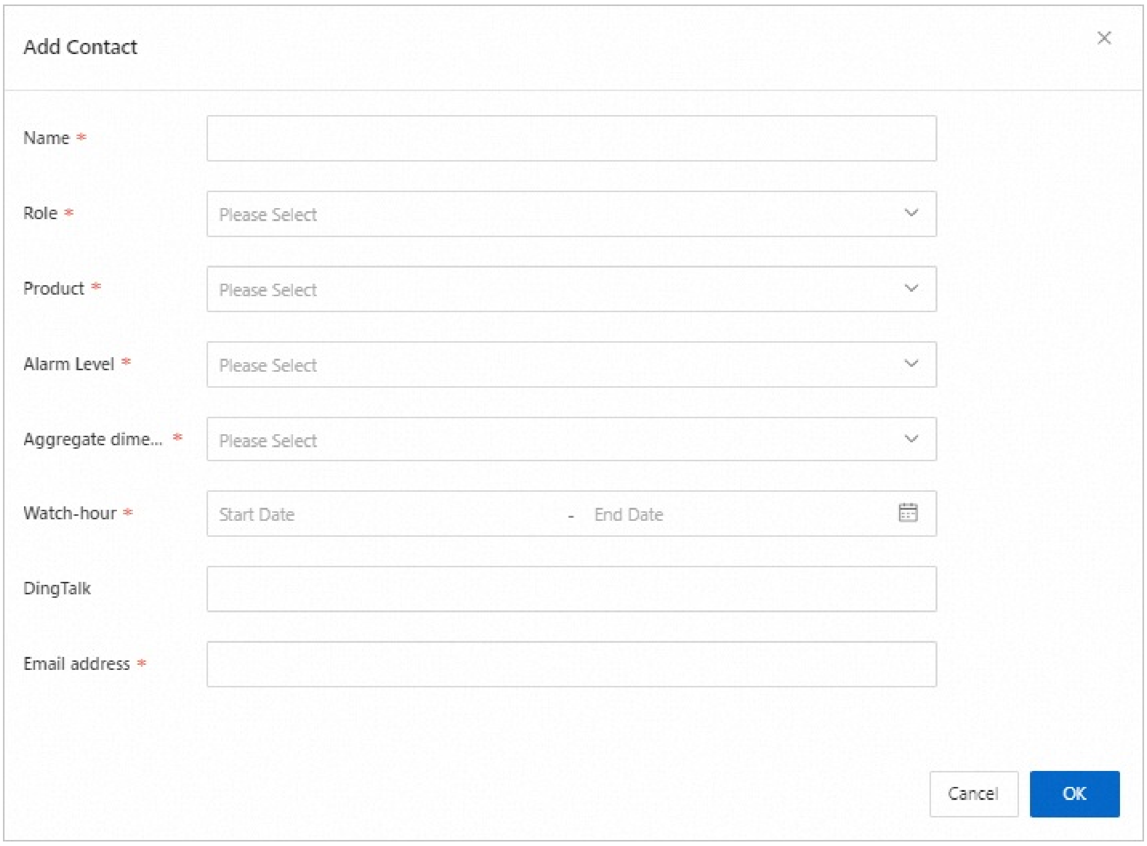
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Alerts** > **Alert Settings**.
3. In the left-side navigation pane, click **Policy Management**.
4. You can perform the following operations:
    - Query an alert contact

      In the upper-left corner of the Contact tab, select a product name and enter a contact name. The alert contacts that meet the filter conditions are displayed in the list.
    - Add an alert contact

      In the upper-left corner of the Contact tab, click **Add Contact**. In the **Add Contact** dialog box, configure the following parameters. Then, click **OK**.

Parameter	Description
Name	Enter a name for the contact.

Role	Select a role for the contact. ▪ Developer: a developer ▪ TAM: an O&M person
Product	Select the product for which you want to create the alert contact. You can select multiple products.
Alert Severity	Select alert levels. You can select multiple alert levels. ▪ P1: a critical alert ▪ P2: a major alert ▪ P3: a minor alert ▪ P4: a reminder alert
Aggregation Dimension	Select an alert push method. ▪ One By One ▪ Product ▪ Metrics ▪ Machine
Duty Hours	Select the start time and end time of the watch-hour of the new alert contact.
Email address	Enter the email address of the new alert contact.



Add Contact

Name *

Role * Please Select

Product * Please Select

Alarm Level * Please Select

Aggregate dime... * Please Select

Watch-hour * Start Date - End Date

DingTalk

Email address *

Cancel OK

- Modify an alert contact

  Find the alert contact whose information you want to modify and click **Modify** in the **Operation** column. In the **Modify Contact** dialog box, modify the information and click **OK**.

- Delete an alert contact

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

Manage contact groups

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

Procedure

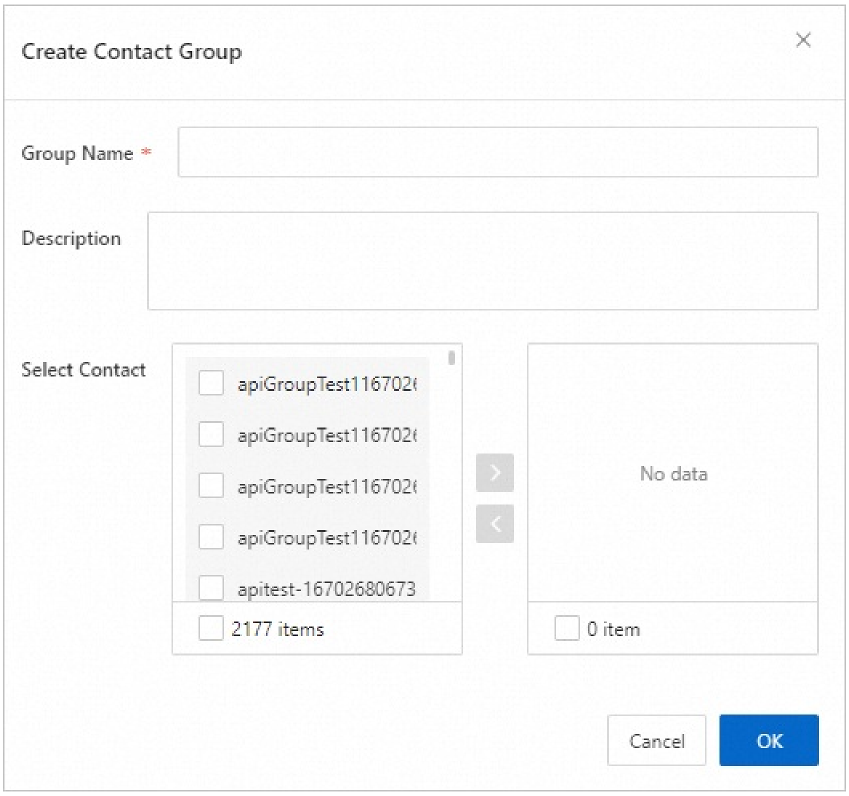
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Alerts** > **Alert Settings**.
3. In the left-side navigation pane, click **Policy Management**.
4. Click the **Contact Groups** tab.
5. You can perform the following operations:
   - Query an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

     Enter a group name in the **Group Name** search box to view alert contact groups that meet the search condition.

   - Add an alert contact group

     In the upper-left corner of the tab, click **Add Contact Group**. In the **Create Contact Group** dialog box that appears, set the following parameters and click **OK**.

Parameter	Description
Group Name	Enter a name for the alert contact group.
Description	Enter a description for the alert contact group.
Select Contact	Select contacts to add to the contact group.



Create Contact Group ×

Group Name *

Description

Select Contact

□ apiGroupTest116702

□ apiGroupTest116702

□ apiGroupTest116702

□ apiGroupTest116702

□ apitest-16702680673

□ 2177 items

No data

□ 0 item

- Modify an alert contact group

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

- Delete an alert contact group

  - 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** in the lower-left corner of the tab. In the message that appears, click **OK**.

Configure static parameters

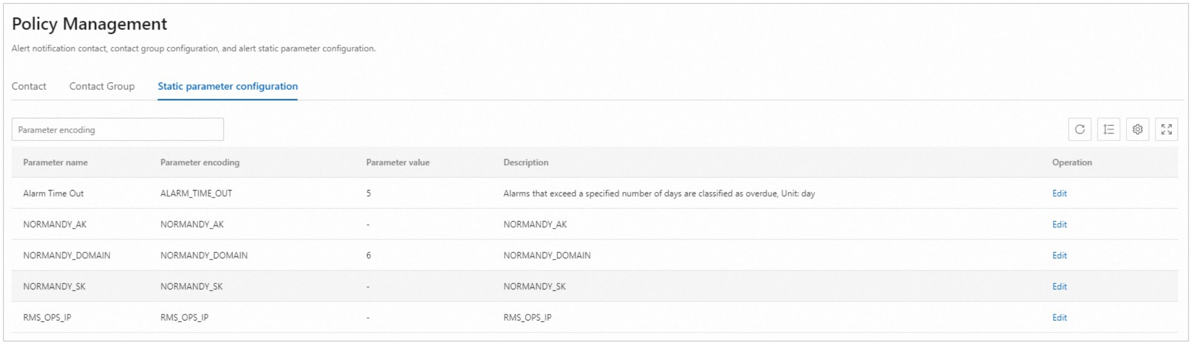
You can configure alert-related static parameters based on your business requirements.

Background information

You can configure parameters for only timeout alerts. You cannot add new configurations in the current version. By default, the system provides configurations for timeout alerts. You can modify the configurations 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 **Static Parameter Settings** tab.



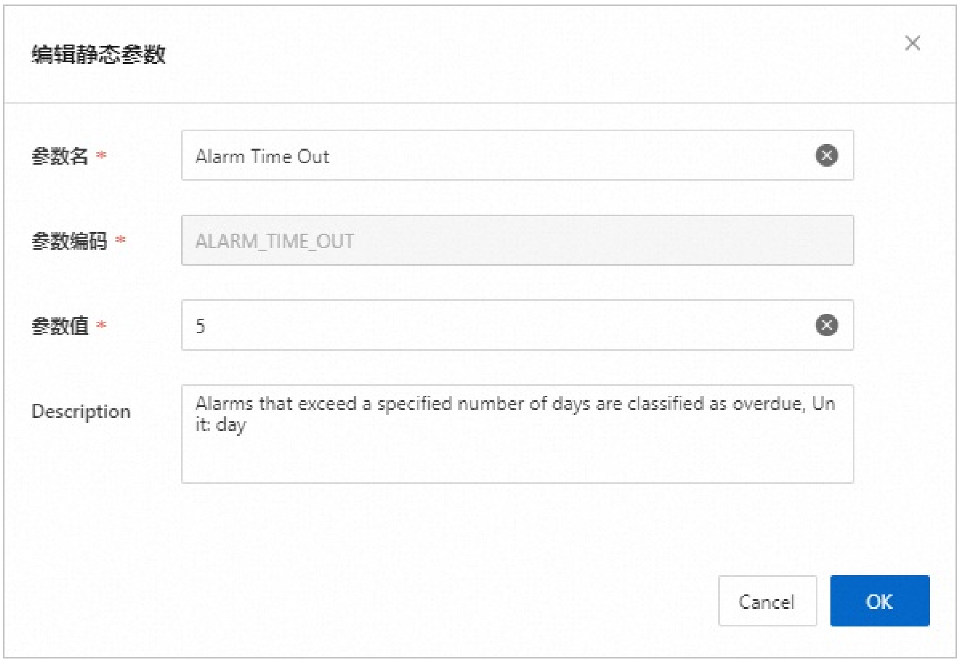
Policy Management

Alert notification contact, contact group configuration, and alert static parameter configuration.

Parameter name	Parameter encoding	Parameter value	Description	Operation
Alarm Time Out	ALARM_TIME_OUT	5	Alarms that exceed a specified number of days are classified as overdue, Unit: day	Edit
NORMANDY_AK	NORMANDY_AK	-	NORMANDY_AK	Edit
NORMANDY_DOMAIN	NORMANDY_DOMAIN	6	NORMANDY_DOMAIN	Edit
NORMANDY_SK	NORMANDY_SK	-	NORMANDY_SK	Edit
RMS_OPS_IP	RMS_OPS_IP	-	RMS_OPS_IP	Edit

5. Optional. In the search box in the upper-left corner of the tab, enter a parameter name to query static parameter configurations.
6. Find the static parameter that you want to modify and click **Edit** in the **Operation** column.
7. In the **Modify Static Parameters** dialog box, modify the **Parameter Name**, **Parameter Value**, and **Description** parameters.

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



编辑静态参数

参数名 * Alarm Time Out

参数编码 * ALARM_TIME_OUT

参数值 * 5

Description: Alarms that exceed a specified number of days are classified as overdue, Unit: day

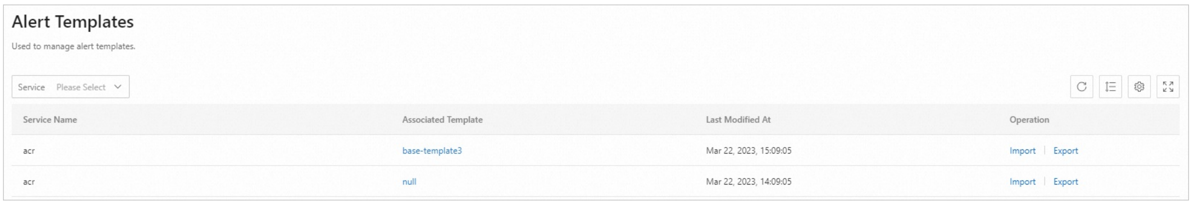
8. Click **OK**.

3.1.3.2. Alert templates

For Ant Financial Service products that are deployed on the PaaS platform, you can upload alert templates to configure or modify the rules that are used to 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. In the left-side navigation pane, click **Alert Templates**.
4. In the upper-left corner of the page that appears, select a service from the **Service** drop-down list. You can view detailed information about the service in the lower part of the page. Then, click the template in the Associated Template column to view detailed information about the template.



Alert Templates

Used to manage alert templates.

Service: Please Select

Service Name	Associated Template	Last Modified At	Operation
acr	base-template3	Mar 22, 2023, 15:09:05	Import | Export
acr	null	Mar 22, 2023, 14:09:05	Import | Export

5. Download alert templates.

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

6. Find the service that you want to manage and click **Import** in the **Operation**. In the **Import Templates** dialog box, click **Upload and Parse File**. Select the template and click **Open**. After the template is uploaded, click **OK**.

> ? **Note**
>
> You can also export a template.

3.1.3.3. Alert notification

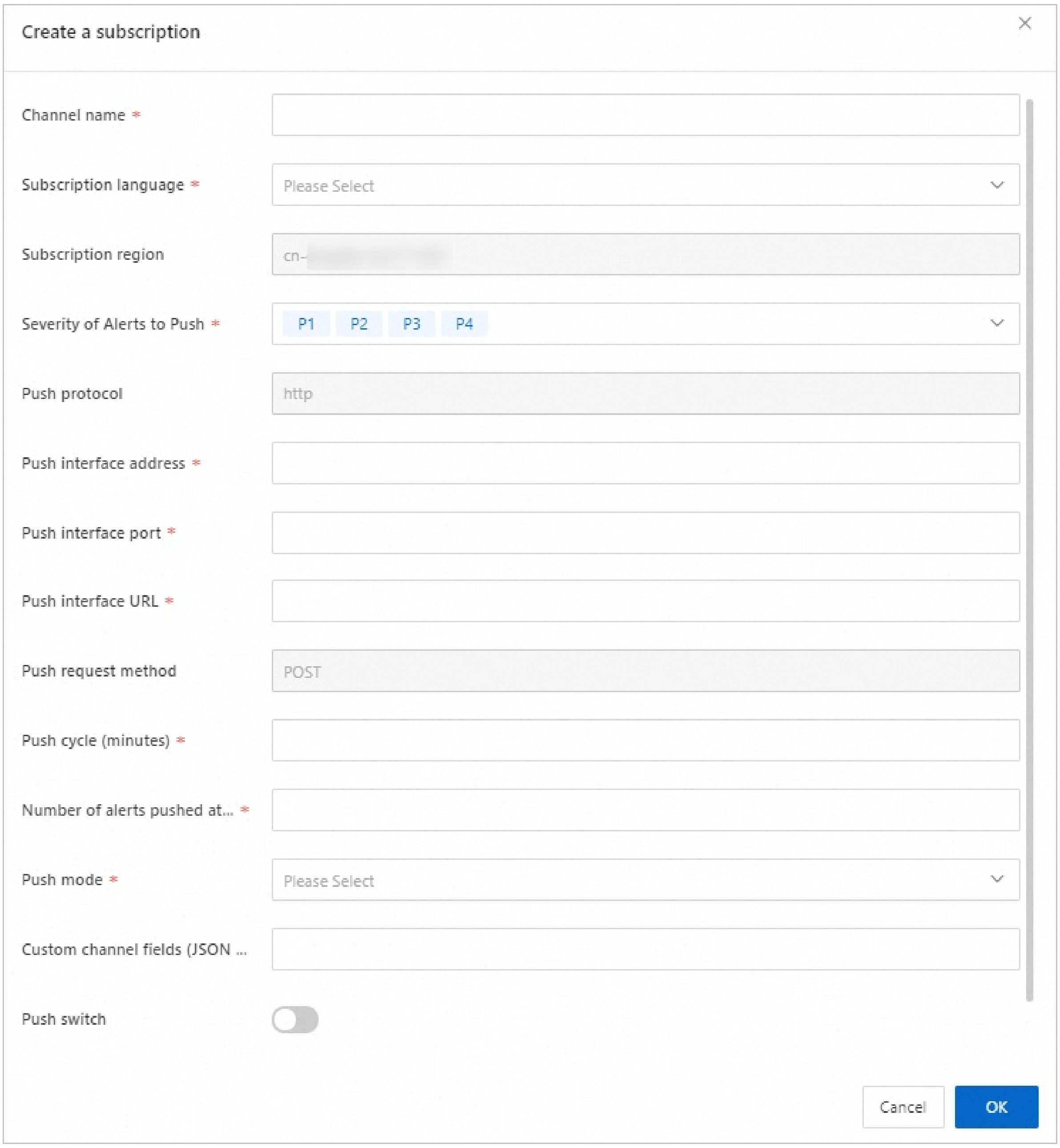
The alert notification feature allows you to configure alert notification channels and then push alerts to O&M engineers.

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 **Alert Notification**.
4. Click the **Subscription** tab. In the upper-left corner of the page that appears, click **Create a subscription**. In the dialog box that appears, configure the parameters and click **OK**. The following table describes the parameters.

Parameter	Description
Channel name	The name of the subscription channel.
Subscription language	The language in which you want to receive notifications. Valid values: Simplified Chinese and English.
Subscription region	By default, the region where the subscription resides is displayed.
Severity of Alerts to Push	The severity of alerts that you want to push. You can select multiple values.
Push protocol	The protocol that is used to push alerts. Only HTTP is supported.
Push interface address	The IP address of the push interface.
Push interface port	The port number of the push interface.
Push interface URL	The URL of the push interface.
Push request 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.

Number of alerts pushed at a time	The number of alerts that are 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.
Custom channel fields (JSON format)	The push receiver can use this field to create a custom identifier. The field must be in the JSON format.
Push switch	Specifies whether to push alerts. If you do not turn on the push switch in the Create a subscription dialog box, you can enable the push feature by turning on the switch in the **Push switch** column after you configure the subscription channel.



Create a subscription

Channel name *

Subscription language * Please Select

Subscription region cn-[redacted]

Severity of Alerts to Push * P1 P2 P3 P4

Push protocol http

Push interface address *

Push interface port *

Push interface URL *

Push request method POST

Push cycle (minutes) *

Number of alerts pushed at... *

Push mode * Please Select

Custom channel fields (JSON ...

Push switch

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

Related operations

Operation	Description

Modify notification channel settings	1. Find the notification channel that you want to manage, and click**Modify** in the **Operation** column. 2. In the dialog box that appears, modify the parameters and click**OK**. Note Turn on or turn off the switch in the**Push switch** column to enable or disable the notification channel.
Check the connectivity of a notification channel	Find the notification channel that you want to manage and click**Test** in the **Operation** column to check the connectivity of the notification channel.
Reset a notification channel	1. Find the notification channel that you want to manage and click**Reset** in the **Operation** column. 2. In the message that appears, click **Reset**.
Delete a notification channel	In the top navigation bar, click **System Settings**. In the left-side navigation pane, choose **Platform Settings** > **Notification Management** > **Channel Management**, find the notification channel that you want to delete, and then click Delete in the Operation column.

3.1.3.4. Alert masking

Alert masking allows you to mask alerts reported during a specified period of time, and mask alerts by product, cluster, service, service role, and machine. You can also mask alerts by alert ID.

Prerequisites

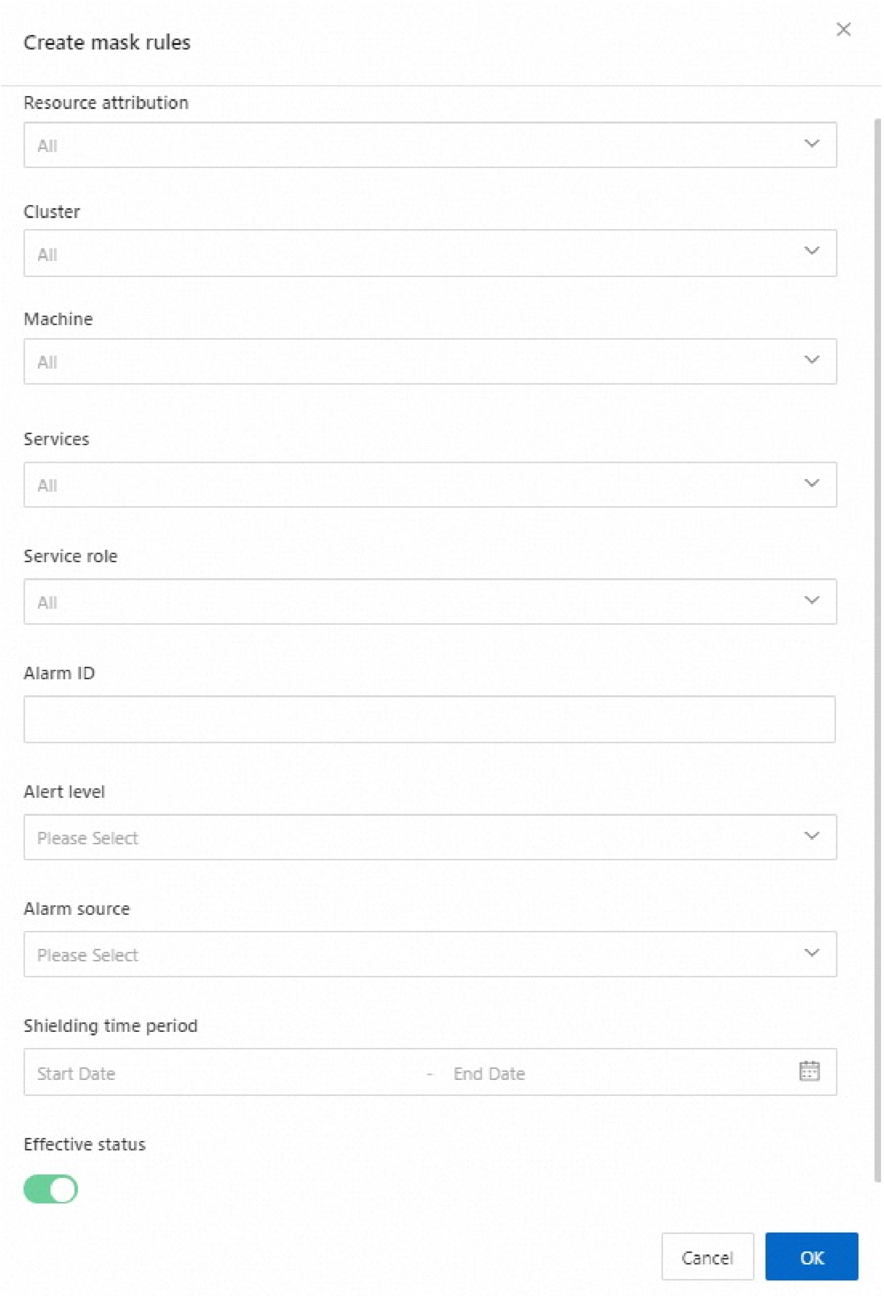
The permissions on the alert masking menu are obtained.

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 mask rules**. In the dialog box that appears, configure the filters to mask alerts and click **OK**.

Parameter	Description
Resource attribution	Optional. The name of the product to which the alert to be masked belongs.
Cluster	Optional. The name of the cluster to which the alert to be masked belongs.

Machine	Optional. The hostname of the ECS instance to be masked.
Services	Optional. The name of the service to which the alert to be masked belongs.
Service role	Optional. The service role of the alert to be masked.
Alarm ID	Optional. The ID of the alert to be masked.
Alert level	Optional. The level of the alert to be masked. Valid values: ◦ P1: critical ◦ P2: major ◦ P3: minor ◦ P4: info
Alarm source	Optional. The source of the alert to be masked.
Shielding time period	Optional. The time period during which the alert to be masked occurs.
Effective status	Required. Specifies whether the masking rule takes effect.



Create mask rules

Resource attribution: All

Cluster: All

Machine: All

Services: All

Service role: All

Alarm ID:

Alert level: Please Select

Alarm source: Please Select

Shielding time period: Start Date - End Date

Effective status: On

Related operations

Operation	Description

View alert masking rules	You can view available alert masking rules in the list or search for a masking rule by using Advanced Search. - Enter a keyword in the search box to filter masking rules. Fuzzy search is supported. - Click **Advanced Search** and filter rules by **Resource attribution**, **Cluster**, **Services**, **Service role**, and **Machine**. - In the **Effective status** column, filter masking rules that are **Open** or **Close**.
Modify an alert masking rule	1. Find the alert masking rule that you want to manage, and click **Edit** in the **Operation** column. 2. In the dialog box that appears, modify the parameters and click **OK**. **Note** You can enable or disable the alert masking rule by turning on or off the switch in the **Effective status** column.
Delete an alert masking rule	1. Find the masking rule that you want to delete and click **Delete** in the **Operation** column. 2. In the message that appears, click **OK**.

3.1.3.5. Masked alerts

You can view details of masked alerts and the associated alert masking rule.

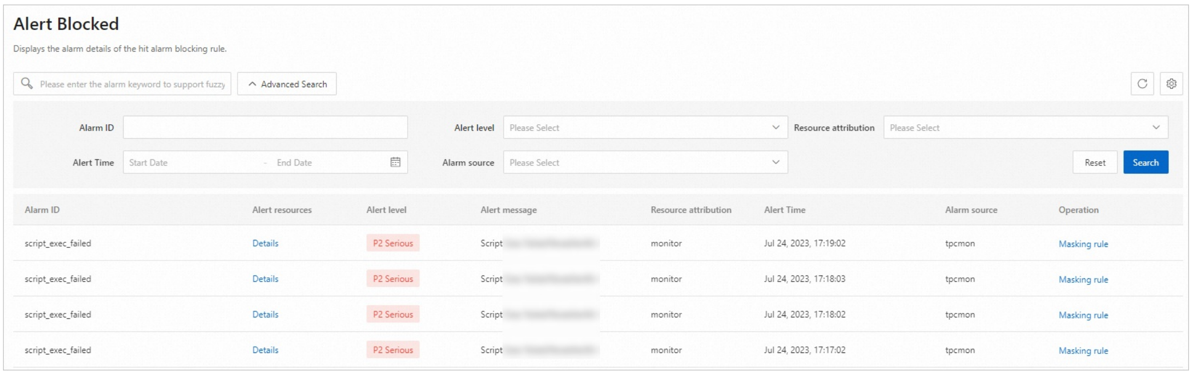
Prerequisites

- The permissions to view masked alerts are obtained.
- At least one alert masking rule is created 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**.

   For a masked alert, the following information is displayed: **Alert ID**, **Alert resources**, **Alert level**, **Alert message**, **Resource attribution**, **Alert Time**, **Alert source**, and the associated masking rule.



Alert Blocked

Displays the alarm details of the hit alarm blocking rule.

Alarm ID	Alert resources	Alert level	Alert message	Resource attribution	Alert Time	Alarm source	Operation
script_exec_failed	Details	P2 Serious	Script [redacted]	monitor	Jul 24, 2023, 17:19:02	tpcmon	Masking rule
script_exec_failed	Details	P2 Serious	Script [redacted]	monitor	Jul 24, 2023, 17:18:03	tpcmon	Masking rule
script_exec_failed	Details	P2 Serious	Script [redacted]	monitor	Jul 24, 2023, 17:18:02	tpcmon	Masking rule
script_exec_failed	Details	P2 Serious	Script [redacted]	monitor	Jul 24, 2023, 17:17:02	tpcmon	Masking rule

4. Enter a keyword to search for alerts. Fuzzy search is supported. You can also click **Advanced Search** and filter alerts by **Alert ID**, **Alert level**, **Resource attribution**, **Alert Time**, or **Alert source**.
5. Move the pointer over **Details** in the **Alert resources** column of an alert to view the alert details, including the product, cluster, service, server role, and host.
6. Find the alert that you want to manage and click **Masking rule** in the **Operation** column. A dialog box appears.
   - If the masking rule is not deleted, the details of the masking rule are displayed in the dialog box. You can modify the parameters in the dialog box and click **OK**.
   - If the masking rule is deleted, message **Masking rule has been deleted** appears.

3.1.3.6. Alert rule settings

This topic describes how to modify the settings of an alert rule, including the status and triggering conditions of an alert rule, and the number of times an alert rule is triggered. Compared with alert templates that have a complicated modification process, the alert rule setting feature allows you to view alert rule settings in an efficient manner and modify the settings of alert rules with a few clicks.

Background information

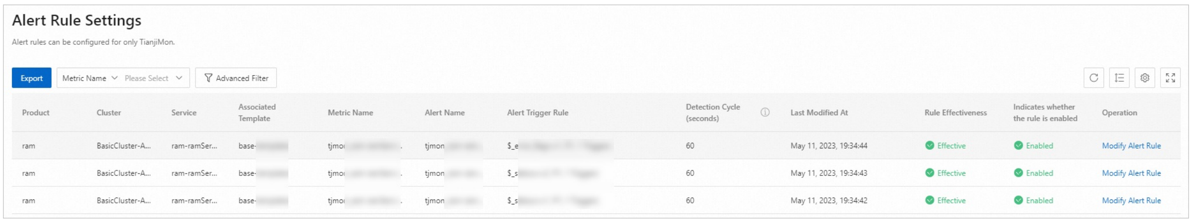
- Alert rules can be configured for only TianjiMon.
- Only alert rules that contain numbers can be modified.
- After a verified alert rule takes effect, all alerts that use the rule are affected. If the settings of an alert rule are improperly modified, risks may occur. The risks include a surge in the number of alerts and no generated 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 **Alert Rule Settings**.
4. Filter alert rules by **Metric Name**, **Product**, **Cluster**, **Service**, and **Rule Effectiveness**. The following table lists the parameters of alert rules.

Parameter	Description
Product	The product for which the alert rule is configured.

Cluster	The cluster for which the alert rule is configured.
Service	The service for which the alert rule is configured.
Associated Template	The template with which the alert rule is associated.
Metric Name	The name of the metric for which the alert rule is configured.
Alert Name	The name of the alert.
Alert Trigger Rule	The conditions that are used to trigger the alert rule.
Detection Cycle (seconds)	The interval at which the alert rule is executed. Unit: seconds.
Last Modified At	The time when the alert rule was last modified.
Rule Effectiveness	The status of the alert rule. Valid values:**Effective**, **Ineffective**, and **Verifying**.
Indicates whether the rule is enabled	Indicates whether the alert rule is enabled. Valid values:**Enabled** and **Disabled**.

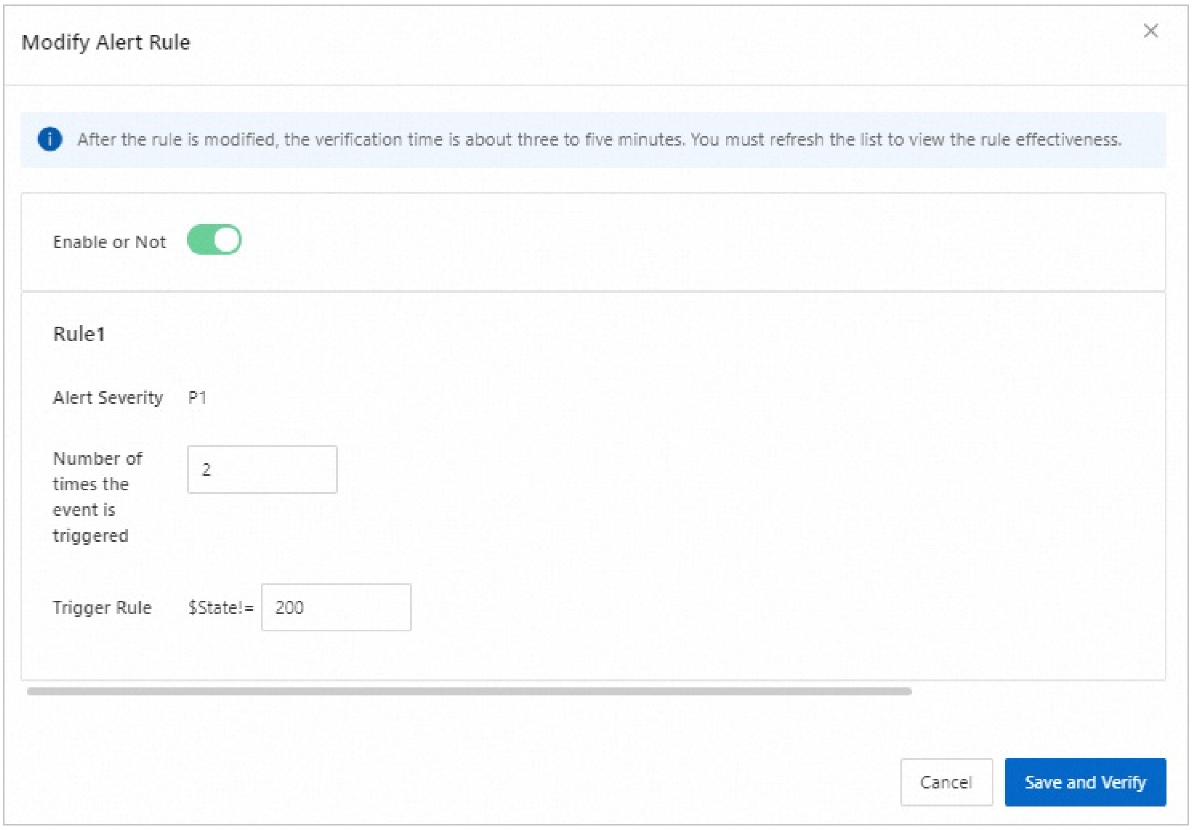


Alert Rule Settings

Alert rules can be configured for only TianjiMon.

Product	Cluster	Service	Associated Template	Metric Name	Alert Name	Alert Trigger Rule	Detection Cycle (seconds)	Last Modified At	Rule Effectiveness	Indicates whether the rule is enabled	Operation
ram	BasicCluster-A...	ram-ramSer...	base-[redacted]	tjmo[redacted]	tjmon[redacted]	$_e[redacted]	60	May 11, 2023, 19:34:44	Effective	Enabled	Modify Alert Rule
ram	BasicCluster-A...	ram-ramSer...	base-[redacted]	tjmo[redacted]	tjmon[redacted]	$_s[redacted]	60	May 11, 2023, 19:34:43	Effective	Enabled	Modify Alert Rule
ram	BasicCluster-A...	ram-ramSer...	base-[redacted]	tjmo[redacted]	tjmon[redacted]	$_s[redacted]	60	May 11, 2023, 19:34:42	Effective	Enabled	Modify Alert Rule

5. Find the alert rule that you want to manage and click **Modify Alert Rule** in the **Operation** column. In the dialog box that appears, turn on or turn off the Enable or not switch, configure the Number of times the event is triggered and Trigger Rule parameters, and then click **Save and Verify**.



Modify Alert Rule

After the rule is modified, the verification time is about three to five minutes. You must refresh the list to view the rule effectiveness.

Enable or Not: on

Rule1

Alert Severity: P1

Number of times the event is triggered: 2

Trigger Rule: $State!= 200

> **Note**
>
> After you modify the rule, the verification takes 3 to 5 minutes. Refresh the list to check whether the rule has taken effect.

6. In the upper-left corner of the Alert Rule Settings page, click **Export** to export alert rules that are displayed on the page.

3.1.4. Alert Packages

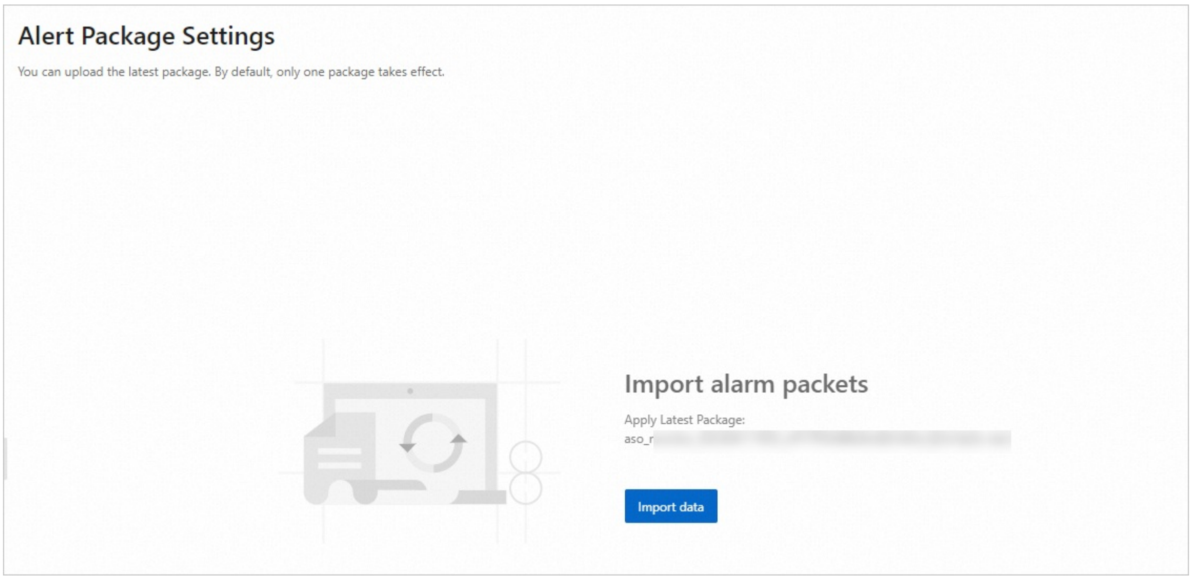
You can upload an alert package to support the hot replacement of alert data.

Background information

Uploading an alert package allows you to implement incremental configuration by using the hot replacement feature. With this feature, you do not need to suspend services, making onsite O&M more flexible. Acceptable package content includes an alert text localization file and alert handling suggestion KB file. A 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 data**. In the dialog box that appears, select a package and click **Open** to import the desired package. The system will display a message indicating whether the import succeeds or fails.



Alert Package Settings

You can upload the latest package. By default, only one package takes effect.

Import alarm packets

Apply Latest Package:
aso_r[redacted]

Important

The system supports TAR packages that are not larger than 200 MB. The system verifies the data of packages. Therefore, the alert packages must be prepared and generated by Apsara Stack O&M engineers.

3.2. Inspections

This topic describes the features related to inspection management.

Features

In the Apsara Uni-manager Operations Console, you can perform quick inspections in various inspection scenarios to help maintain the health of your business system and cloud services.

Feature	Description
All inspections	Multiple inspection scenarios are supported, including preset inspection scenarios and custom inspection scenarios.
Inspection dashboard	You can view the status of inspection tasks, data overview, distribution and trends of detected exceptions, inspection task records, issue details, and latest inspection report for the last seven days.
Inspection reports	You can view all inspection reports for the last seven days. The reports include the basic information about inspection tasks and the overview and details of inspection results.
Inspection scenarios	All inspection scenarios and inspection items are displayed.

Inspection records	All inspection records are displayed. You can view inspection reports and cancel a running inspection task.
Inspection items	You can view all inspection items and related inspection parameters and content.
Inspection packages	You can import or export the latest inspection package. After you import an inspection package, the inspection items of the product are updated to improve the inspection capabilities of the platform.

3.2.1. All inspections

This topic describes the inspections supported by the system in various scenarios. These inspections can help maintain the health of your business system and cloud services. You can perform inspections based on your business requirements.

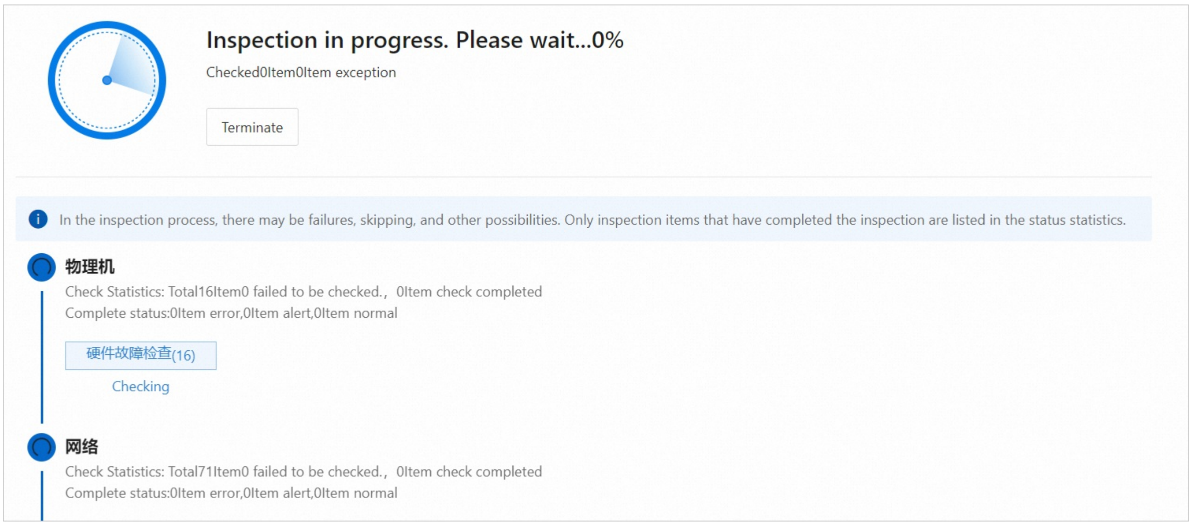
Prerequisites

- The system administrator permissions of the Apsara Uni-manager Operations Console are obtained.
- Custom inspection settings are configured before you enable a custom inspection. For more information, see Inspection scenario configuration.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Inspections** > **All Inspections**.
3. Perform a preset inspection or custom inspection.
4. Select an inspection that you want to perform and then start the inspection task.
   - If this is the first time you are performing this inspection, click **Check now**.
   - If this is not the first time you are performing this inspection, click **Re-check**.
   - If you want to perform a custom inspection, click **Custom inspection**, select an inspection scenario, and then click **Immediate inspection**.

5. After the inspection is started, the system displays the inspection progress in detail. To stop the inspection, click **Terminate**. In the message that appears, click **OK**.



Inspection in progress. Please wait...0%

Checked0Item0Item exception

Terminate

In the inspection process, there may be failures, skipping, and other possibilities. Only inspection items that have completed the inspection are listed in the status statistics.

物理机

Check Statistics: Total16Item0 failed to be checked.，0Item check completed

Complete status:0Item error,0Item alert,0Item normal

硬件故障检查(16)

Checking

网络

Check Statistics: Total71Item0 failed to be checked.，0Item check completed

Complete status:0Item error,0Item alert,0Item normal

6. After the inspection is complete, view the inspection results displayed on the page.

   - On the left side of the page, the total number of inspection items, the number of errors, warning, and normal items are also displayed for a successful inspection.

   - On the right side of the page, the distributions of errors, warnings, and normal items for each product or component are displayed. Move the pointer over the inspection results of a scenario to view each inspection item.

7. Click **View the complete report** to go to the **Inspection Reports** page to view the detailed inspection report.

3.2.2. Inspection dashboard

The **Inspection Dashboard** page displays the status of recent inspection tasks, data overview, distribution and trends of detected exceptions, inspection task records, issue details, and the latest inspection report.

Procedure

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

2. In the top navigation bar, choose **General** > **Inspections** > **Inspection Dashboard**.

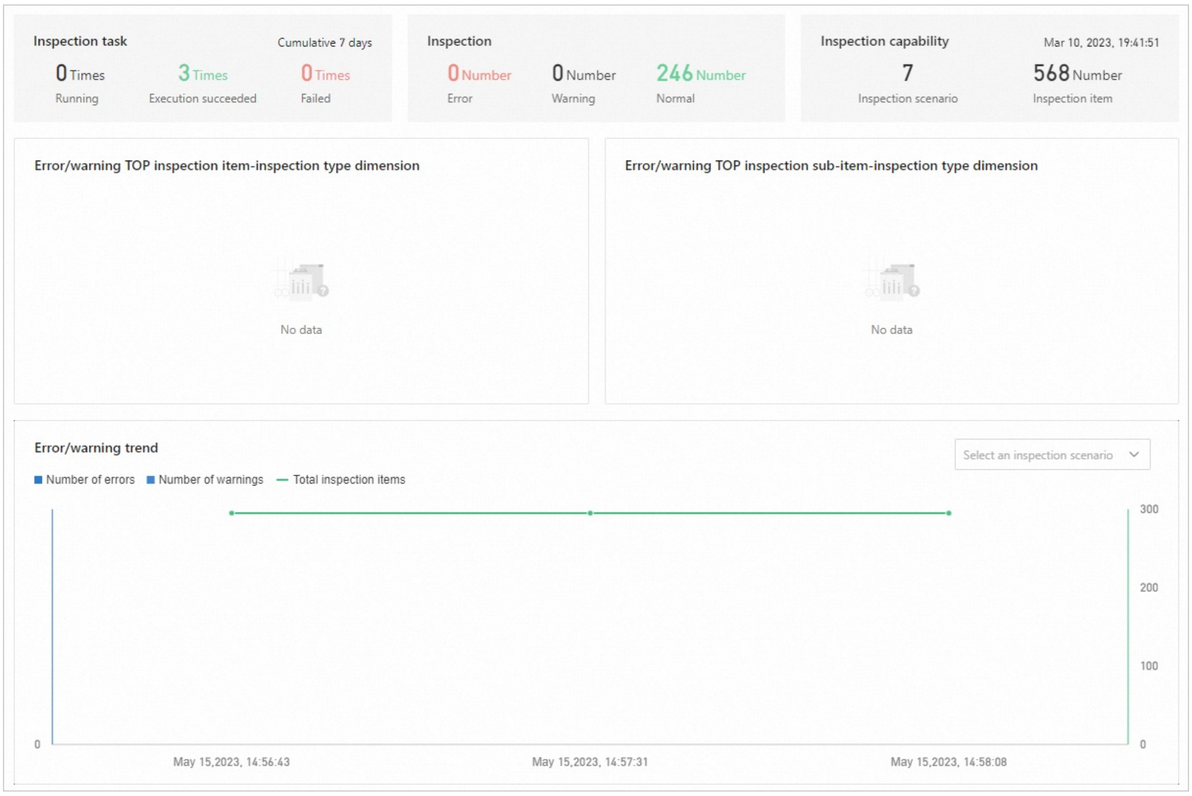
3. In the upper part of the page, view the following information:

   - The execution status of inspection tasks in the last seven days, the number of inspection errors of each type, and the inspection capabilities (the number of inspection scenarios and inspection items).

   - The number of inspection errors and the number of inspection warnings that are sorted by inspection item and sub-item.

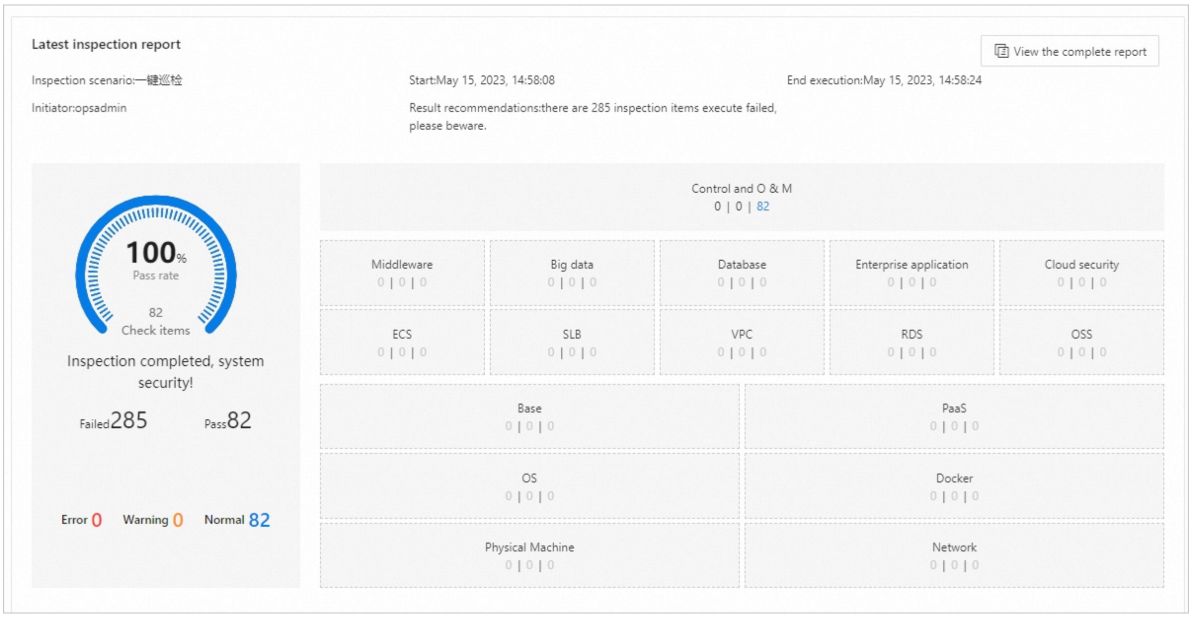
     > **Note**
     >
     > You can move the pointer over a row to view the numbers of errors and warnings for a specific item or sub-item.

   - The quantity trends of errors, warnings, and inspection items for an inspection scenario that you select from the **Error/warning trend** drop-down list.



4. In the **Inspection task records** section, view the inspection task records of the last seven days.
5. In the **Inspection** section, view the details of inspection issues in the last seven days.

   Click the number in the **Inspection item results** column of the desired inspection item. In the dialog box that appears, view the inspection result details.
6. In the **Latest inspection report** section, view the latest inspection report.


Latest inspection report

Inspection scenario:一键巡检

Initiator:opsadmin

Start:May 15, 2023, 14:58:08

Result recommendations:there are 285 inspection items execute failed, please beware.

End execution:May 15, 2023, 14:58:24

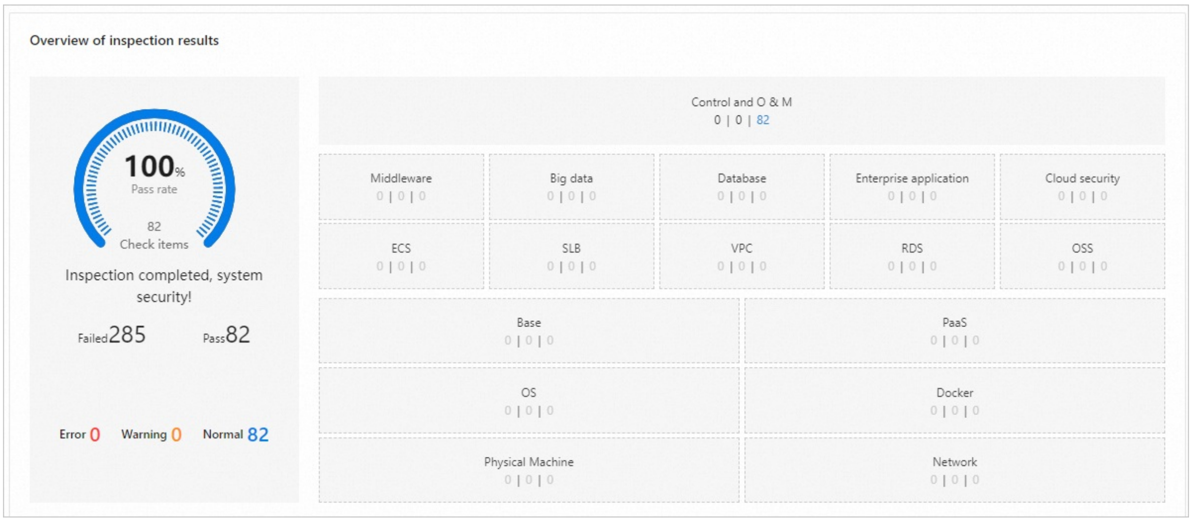
7. Click **View the complete report** to go to the **Inspection Report** page to view the detailed inspection report.

3.2.3. Inspection reports

You can view all recent inspection reports to check issues or faults of the system.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Inspections** > **Inspection Reports**.
3. Find the inspection report whose details you want to view. By default, the system displays the report of the latest inspection. You can search for an inspection report by scenario and time in the upper right corner of the **Inspection Report** page.
4. In the **Basic Information** section, view the scenario, start time, end time, initiator, and recommendations of the inspection.
5. In the **Overview of inspection results** section, view the overall pass rate, total number of inspection items, number of failed items, number of passed items, number of errors, number of warnings, and number of normal inspection items.



Overview of inspection results

100% Pass rate

82 Check items

Inspection completed, system security!

Failed285 Pass82

Error 0 Warning 0 Normal 82

Control and O & M
0 | 0 | 82

Middleware 0 | 0 | 0

Big data 0 | 0 | 0

Database 0 | 0 | 0

Enterprise application 0 | 0 | 0

Cloud security 0 | 0 | 0

ECS 0 | 0 | 0

SLB 0 | 0 | 0

VPC 0 | 0 | 0

RDS 0 | 0 | 0

OSS 0 | 0 | 0

Base 0 | 0 | 0

PaaS 0 | 0 | 0

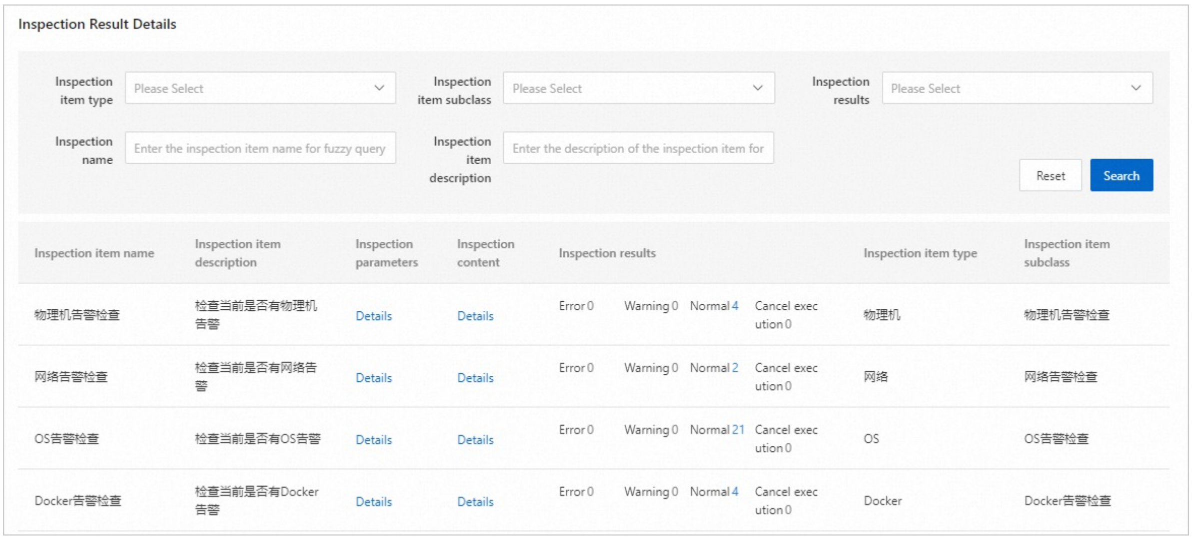
OS 0 | 0 | 0

Docker 0 | 0 | 0

Physical Machine 0 | 0 | 0

Network 0 | 0 | 0

6. In the **Inspection Result Details** section, view the details of each inspection item.
   - Filter inspection details by **Inspection item type**, **Inspection item subclass**, **Inspection results**, **Inspection name**, and **Inspection item description**.
   - Move the pointer over **Details** in the **Inspection parameters** and **Inspection content** columns to view the details.
   - Click the number in the **Inspection results** column to view the inspection results.



Inspection Result Details

Inspection item name	Inspection item description	Inspection parameters	Inspection content	Inspection results	Inspection item type	Inspection item subclass
物理机告警检查	检查当前是否有物理机告警	Details	Details	Error 0 Warning 0 Normal 4 Cancel execution 0	物理机	物理机告警检查
网络告警检查	检查当前是否有网络告警	Details	Details	Error 0 Warning 0 Normal 2 Cancel execution 0	网络	网络告警检查
OS告警检查	检查当前是否有OS告警	Details	Details	Error 0 Warning 0 Normal 21 Cancel execution 0	OS	OS告警检查
Docker告警检查	检查当前是否有Docker告警	Details	Details	Error 0 Warning 0 Normal 4 Cancel execution 0	Docker	Docker告警检查

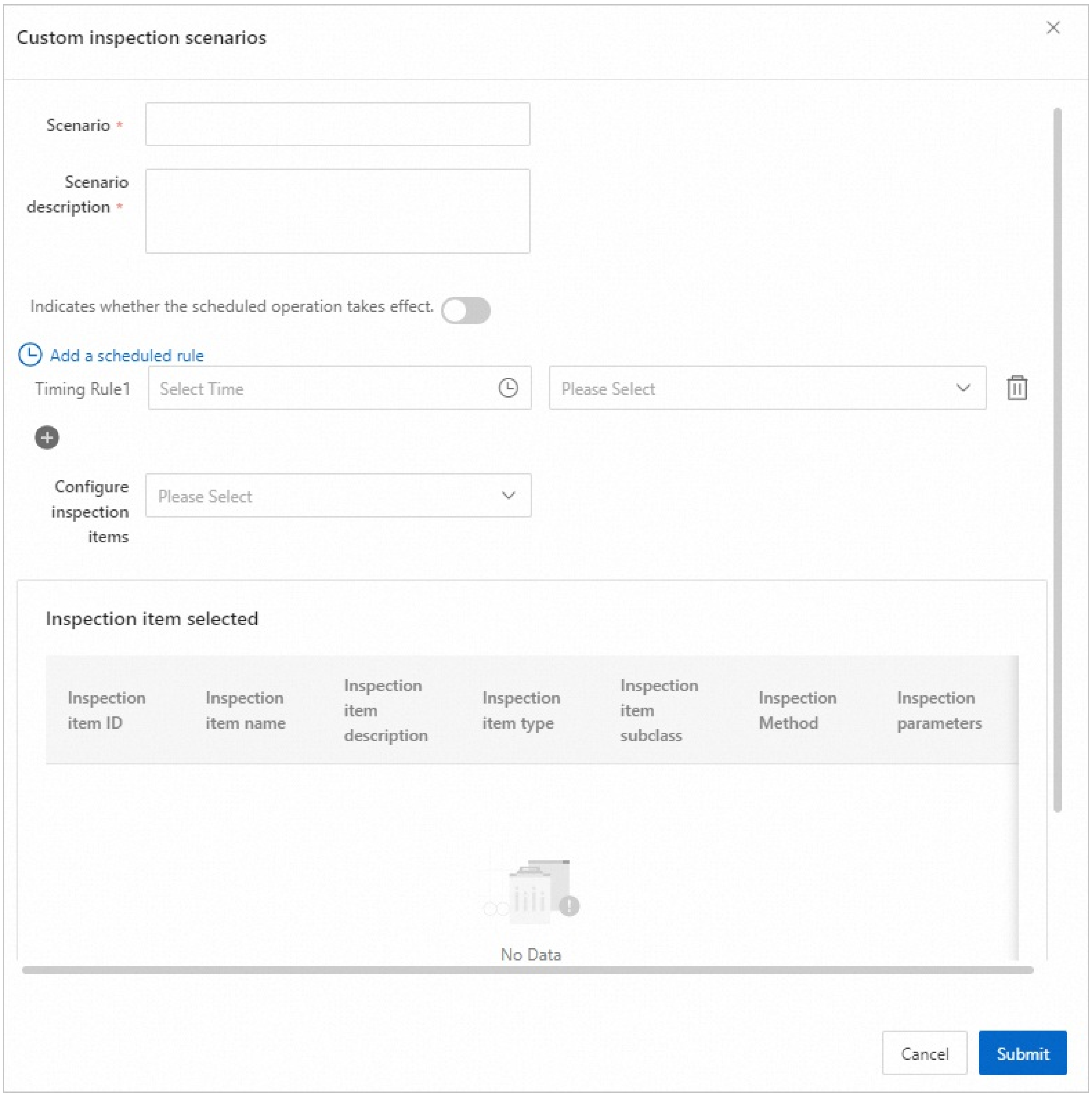
3.2.4. Inspection scenarios

This topic describes how to configure custom inspection scenarios and inspection items to make inspections more efficient.

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**. In the dialog box that appears, configure the following parameters and click **Submit**.

Parameter	Description
Scenario	Enter a name for the custom inspection scenario.
Scenario description	Enter a description for the custom inspection scenario.
Indicates whether the scheduled operation takes effect.	Specify whether to perform the custom inspection at a scheduled time point. If you turn on the switch, the scheduled rules you configure take effect. If you turn off the switch, the scheduled rules you configure do not take effect.
Add a scheduled rule	Specify the time and frequency for the custom inspection. You can click ⊕ to add multiple scheduled rules.
Configure inspection items	Select inspection items for the custom inspection scenario. After you select inspection items, the details of the inspection items are displayed in the lower part.



Custom inspection scenarios

Scenario *

Scenario description *

Indicates whether the scheduled operation takes effect.

Inspection item selected

Inspection item ID	Inspection item name	Inspection item description	Inspection item type	Inspection item subclass	Inspection Method	Inspection parameters

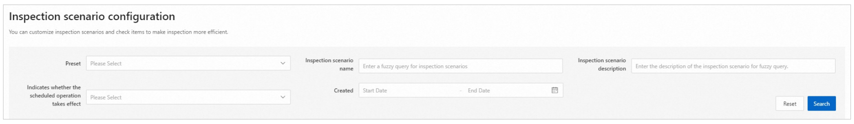
No Data

Related operations

Operation	Description

<table>
<tr>
<td>View the configurations of an inspection scenario</td>
<td>

1. You can view the configurations of all inspection scenarios. You can also filter the inspection scenario that you want to view by **Preset**, **Inspection scenario name**, **Inspection scenario description**, **Indicates whether the scheduled operation takes effect**, and **Created** or their combinations.



Inspection scenario configuration

You can customize inspection scenarios and check items to make inspection more efficient.

Preset
Please Select
Inspection scenario name
Enter a fuzzy query for inspection scenarios
Inspection scenario description
Enter the description of the inspection scenario for fuzzy query.
Indicates whether the scheduled operation takes effect
Please Select
Created
Start Date
End Date
Reset
Search

2. Click **Details** in the **Operation** column of the desired inspection scenario. In the dialog box that appears, view the configurations.
3. Move the pointer over **Details** in the **Inspection parameters** or **Inspection content** column to view the details of the inspection parameters or content.

</td>
</tr>
<tr>
<td>Modify an inspection scenario</td>
<td>

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

1. Click **Details** in the **Operation** column of the desired inspection scenario.
2. In the dialog box that appears, modify the parameters and click**Submit**.

</td>
</tr>
<tr>
<td>Delete an inspection scenario</td>
<td>

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

1. Click **Delete** in the **Operation** column of the desired inspection scenario.
2. In the message that appears, click **Delete**.

</td>
</tr>
</table>

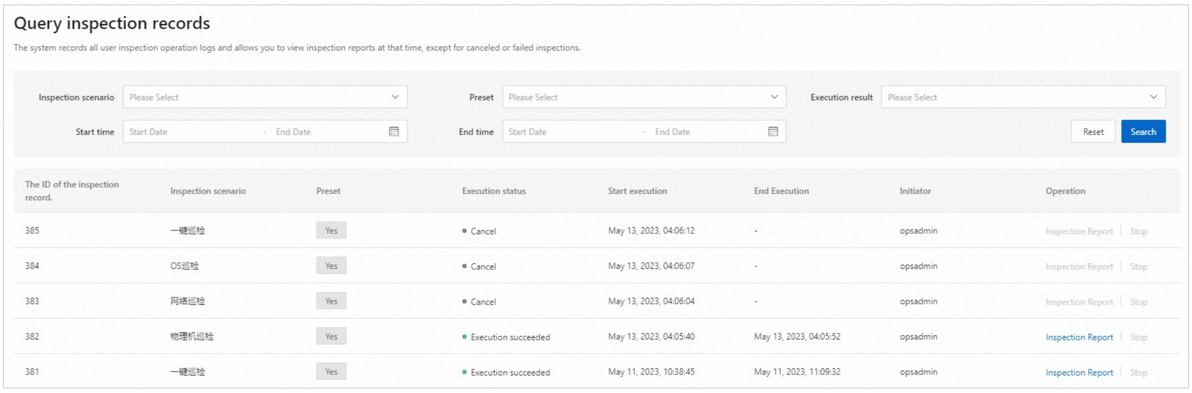
3.2.5. Inspection records

The **Inspection Records** page records all inspection operations performed by a user. You can filter inspection reports and view the report of a specific inspection task. You can also cancel inspection tasks that are in the Running state.

Procedure

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

3. View all inspection records. You can filter inspection records by **Inspection scenario**, **Preset**, **Execution result**, **Start time**, and **End time**.



Query inspection records

The system records all user inspection operation logs and allows you to view inspection reports at that time, except for canceled or failed inspections.

The ID of the inspection record.	Inspection scenario	Preset	Execution status	Start execution	End Execution	Initiator	Operation
385	一键巡检	Yes	● Cancel	May 13, 2023, 04:06:12	-	opsadmin	Inspection Report | Stop
384	OS巡检	Yes	● Cancel	May 13, 2023, 04:06:07	-	opsadmin	Inspection Report | Stop
383	网络巡检	Yes	● Cancel	May 13, 2023, 04:06:04	-	opsadmin	Inspection Report | Stop
382	物理机巡检	Yes	● Execution succeeded	May 13, 2023, 04:05:40	May 13, 2023, 04:05:52	opsadmin	Inspection Report | Stop
381	一键巡检	Yes	● Execution succeeded	May 11, 2023, 10:38:45	May 11, 2023, 11:09:32	opsadmin	Inspection Report | Stop

4. In the inspection record list, view information such as the **inspection record ID**, **inspection scenario**, **whether the scenario is preset**, **inspection execution status**, **inspection start time**, **inspection end time**, and **inspection initiator**.

5. Find the inspection record whose report you want to view and click **Inspection Report** in the **Operation** column to go to the **Inspection Report** page. On this page, you can view the details of the inspection report.

> **Note**
>
> If the **Execution status** column of an inspection record displays **Canceled** or **Failed**, you cannot view the report of the inspection record.

6. Find the inspection record that you want to manage and click **Stop** in the **Operation** column to cancel the inspection task.

3.2.6. Inspection items

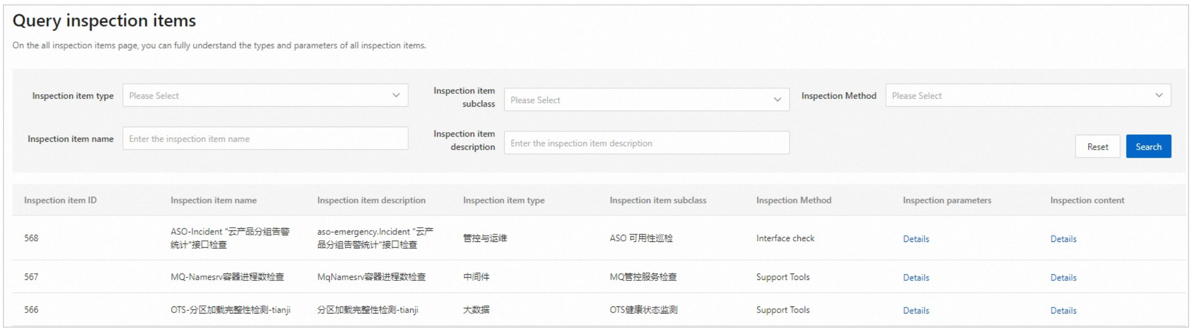
You can view the information about all inspection items. This helps you understand the types and parameters of the inspection items.

Procedure

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

2. In the top navigation bar, choose **General** > **Inspections** > **Inspection Items**.

3. View the information about all inspection items. You can also filter inspection items by specifying the **Inspection item type**, **Inspection item subclass**, **Inspection Method**, **Inspection item name**, and **Inspection item description** fields.



Query inspection items

On the all inspection items page, you can fully understand the types and parameters of all inspection items.

Inspection item ID	Inspection item name	Inspection item description	Inspection item type	Inspection item subclass	Inspection Method	Inspection parameters	Inspection content
568	ASO-Incident "云产品分组告警统计"接口检查	aso-emergency.Incident "云产品分组告警统计"接口检查	管控与运维	ASO 可用性巡检	Interface check	Details	Details
567	MQ-Namesrv容器进程数检查	MqNamesrv容器进程数检查	中间件	MQ管控服务检查	Support Tools	Details	Details
566	OTS-分区加载完整性检测-tianji	分区加载完整性检测-tianji	大数据	OTS健康状态监测	Support Tools	Details	Details

4. Move the pointer over **Details** in the **Inspection parameters** and **Inspection content** columns to view the details.

3.2.7. Inspection packages

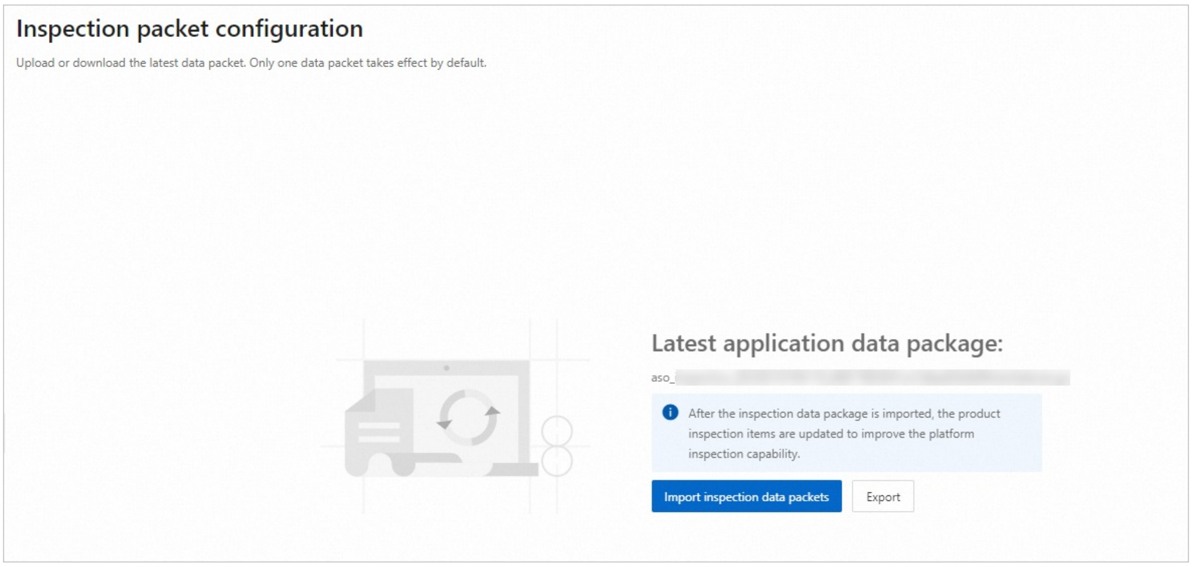
The topic describes how to import or export inspection packages that are designed for preset scenarios.

Background information

- This feature supports only packages that are provided by the Alibaba Cloud support team. Other packages will fail the validation.
- By default, only one inspection package is valid.

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 a package and click **Open** to import the package. After the inspection package is imported, the inspection items of the product are updated and the inspection capabilities of the platform are improved.



Inspection packet configuration

Upload or download the latest data packet. Only one data packet takes effect by default.

Latest application data package:

aso_[redacted]

After the inspection data package is imported, the product inspection items are updated to improve the platform inspection capability.

4. Click **Export** to export the inspection package to your computer.

3.3. Resource Management

This topic describes modules related to resource management.

Modules

Module	Description
Products	You can view all resources in the product dimension, including products, clusters, services, and components.
Data Centers	You can view all cloud platform resources in the data center dimension, including data centers, cabinets, and machines.

Resource Tags	You can use resource tags to demonstrate and manage specific resources based on your business requirements. You can bind, query, unbind, modify, and export resource tags on this page.
HDD Repairs	You can efficiently and securely complete the entire process of data disk replacement. • Prepare: After you initiate a disk replacement task, you must make preparations for it, including task reporting, task approving, and disk unmounting. • Maintenance: After the preparation for disk replacement is complete, you can start maintenance work, including disk replacement, disk installation, and inspection. • History: You can view disk replacement records, including related machines, replaced disks, and operation results.

3.3.1. Products

The Products tab displays products in two modes: list and hierarchy. You can switch between the modes to view the status of all products that are deployed in the environment and easily spot products that are not in the final state at a glance. Then, you can follow the on-screen instructions to identify the cause.

Modules

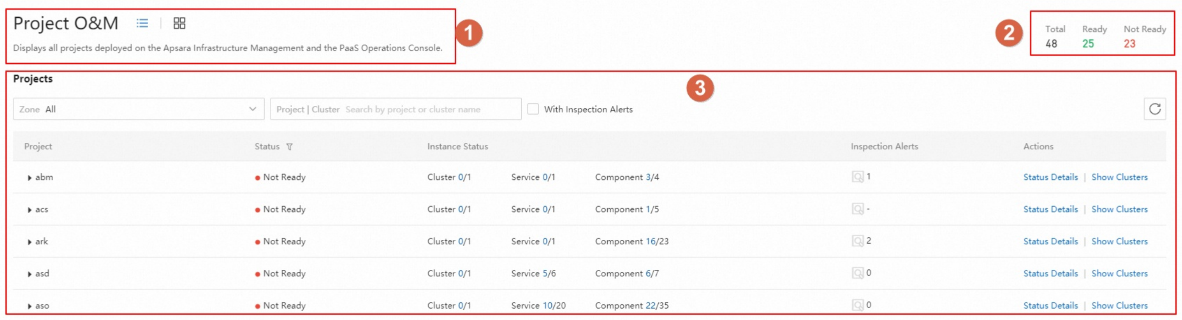
Module	Description
Product list	Displays product status and statistics in a list. The information includes the number of clusters.
Product hierarchy	Displays product status, statistics, and relationships in a hierarchical diagram.
View product details	You can view the basic product information, cluster instance list, and component list.
View cluster details	You can view the basic information about clusters and the application sets on the clusters.
View service component details	You can view the details of components clusters, including component status and final-state configurations.
View task details	You can view the details of a change task.

3.3.1.1. The list mode

This mode displays product status and resource statistics by product in a list. The data includes the numbers of clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General**>**Resources**>**Products**.
3. On the **Project O&M** page, view product status and cluster status.



Project O&M

Displays all projects deployed on the Apsara Infrastructure Management and the PaaS Operations Console.

Total	Ready	Not Ready
48	25	23

Projects

Zone All

Project | Cluster Search by project or cluster name

□ With Inspection Alerts

Project	Status	Instance Status			Inspection Alerts	Actions
abm	● Not Ready	Cluster 0/1	Service 0/1	Component 3/4	1	Status Details | Show Clusters
acs	● Not Ready	Cluster 0/1	Service 0/1	Component 1/5	-	Status Details | Show Clusters
ark	● Not Ready	Cluster 0/1	Service 0/1	Component 16/23	2	Status Details | Show Clusters
asd	● Not Ready	Cluster 0/1	Service 5/6	Component 6/7	0	Status Details | Show Clusters
aso	● Not Ready	Cluster 0/1	Service 10/20	Component 22/35	0	Status Details | Show Clusters

No.	Section	Description
1	Mode switching section	In this section, you can switch between the list mode and the hierarchy mode to view resource information. ◦ By default, the list mode is used. ◦ You can click the □ icon to switch to the hierarchy mode. This mode displays the relationships between products and their subordinate resources. ◦ You can click the □ icon to switch to list mode. This mode displays product status and statistics by product in a list. The information includes the numbers of clusters.
2	Overview section	In this section, you can view the total number of products deployed in the current environment and the number of products in each status. The product status can be **Ready** or **Not Ready**. **Note** A product consists of one or multiple clusters, service instances, and components, and the product status information is aggregated level by level from components to service instances and then to clusters.
3	List section	◦ In this section, you can view product names, status, instance status, and inspection alerts in a list. ◦ You can select a zone to view products and clusters in the zone. ◦ You can also perform a quick search for products or clusters. ◦ You can select **With Inspection Alerts** to view products for which inspection alerts are generated.

The following table describes the parameters in the list.

Parameter	Description
Project	The name of the product. You can click the icon on the left of the project name or click **Show Clusters** in the **Actions** column to view the clusters of the product.
Status	The status of the product or cluster. You can click the icon at the top of the list and select **Ready** or **Not Ready** to view resources by status.
Instance Status	The instance status. A product consists of one or multiple clusters, service instances, and components, and the product status information is aggregated level by level from components to service instances and then to clusters. This column shows the numbers of clusters, service instances, and components in the Ready state of a product, and the corresponding total numbers. You can click an item to view the names and status of resources at all levels. indicates the Ready state and indicates the Not Ready state. **Note** This design facilitates your checks of**Not Ready** state changes. For example, you fixed a product that is not in the Not Ready state. In this case, you can view whether the product is fixed on the current page without having to go to the details page of the product.
Inspection Alerts	The number of inspection items that the product failed in the last inspection task. ◦ - indicates that no inspection task is found. The reason may be no executed inspection task or query failure. ◦ 0 indicates that an inspection task is found and the product passed the inspection. ◦ Other numbers indicate the number of inspection items that the product failed. You can click the number to view the failed inspection items.
Actions	◦ This column provides the **Status Details** and **Show Clusters** options. The Status Details option navigates to the product details page. ◦ The Show Clusters option provides two further options:**Status Details** and **Cluster Details**. You can click Status Details to go to the product details page for more cluster options, or click Cluster Details to go to the cluster details page.

3.3.1.2. The hierarchy mode

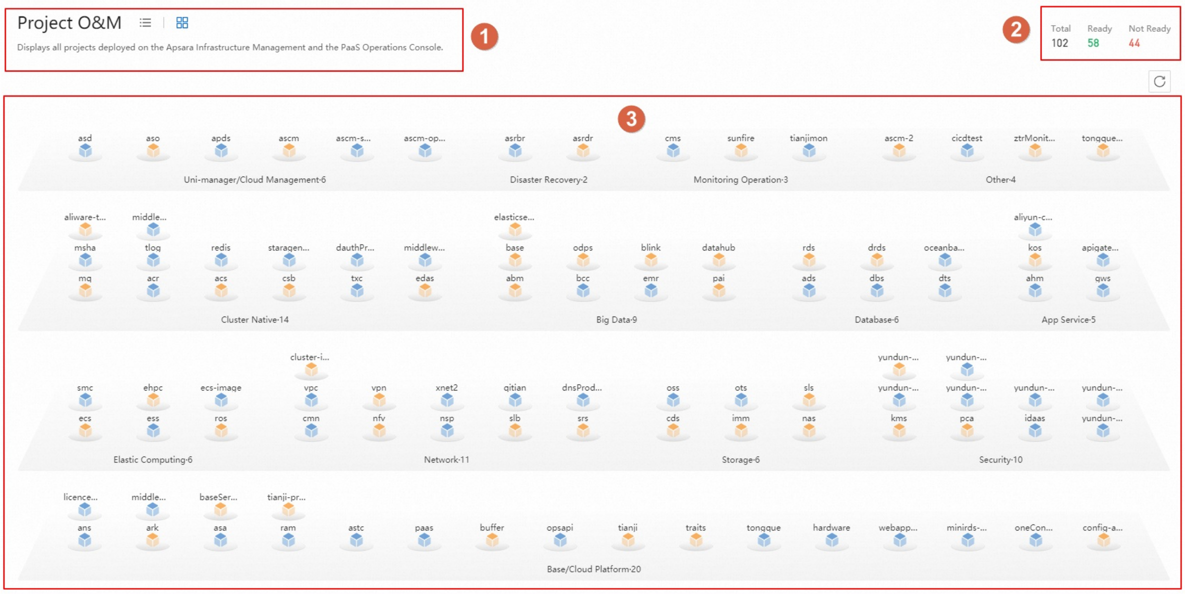
This mode displays product status and resource statistics by product in a hierarchy. The information includes the relationships between products and subordinate resources.

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 to switch to the hierarchy mode.



Project O&M

Displays all projects deployed on the Apsara Infrastructure Management and the PaaS Operations Console.

Total	Ready	Not Ready
102	58	44

No.	Section	Description
1	Mode switching section	In this section, you can switch between the list mode and the hierarchy mode to view resource information. - By default, the list mode is used. - You can click the □ icon to switch to the hierarchy mode. This mode displays the relationships between products and their subordinate resources. - You can click the □ icon to switch to list mode. This mode displays product status and statistics by product in a list. The information includes the numbers of clusters.
2	Overview section	In this section, you can view the total number of products deployed in the current environment and the number of products in each status. The product status can be **Ready** or **Not Ready**. **Note** A product consists of one or multiple clusters, service instances, and components, and the product status information is aggregated level by level from components to service instances and then to clusters.

3	Hierarchy section	The hierarchy consists of four layers. ◦ The layer at the top shows products on the cloud management platforms, monitoring, disaster recovery, and backup products. These products are displayed under the titles of Uni-manager, Disaster Recovery, Monitoring Operation, and Other. The Other title includes products that fail to fall into the preceding categories. ◦ The next layer shows PaaS products, including middleware, big data, database, application services, Internet of Things products. ◦ The next layer shows IaaS products, including elastic computing, network, storage and security products. ◦ The layer at the bottom shows infrastructure, including common components that enable other cloud products.

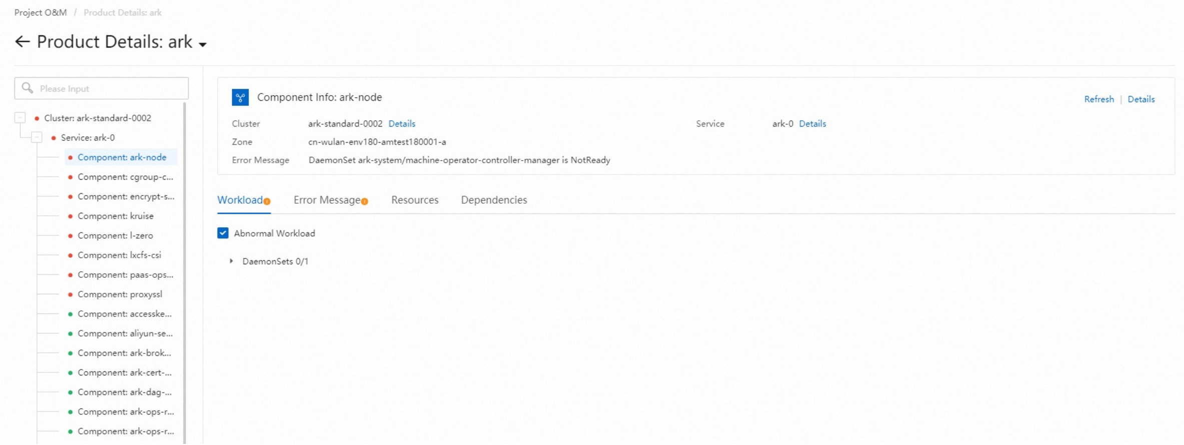
3.3.1.3. View the details of products

You can view the basic product information, cluster instance list, and component list.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Products**.
3. You can use one of the following methods to access the product details page:
   - On the Products page, find the product that you want to view in the list mode and click **Status Details** in the Actions column.
   - Find the product that you want to view in the hierarchy mode on the Product Dimensions page and click the product icon.
4. View product details

   The left-side area displays the status of each level by cluster, service, and component hierarchy. Select a cluster, service, or component. The right-side area displays the corresponding details.



Project O&M / Product Details: ark

← Product Details: ark

Please Input

- Cluster: ark-standard-0002
  - Service: ark-0
    - Component: ark-node
    - Component: cgroup-c...
    - Component: encrypt-s...
    - Component: kruise
    - Component: l-zero
    - Component: lxcfs-csi
    - Component: paas-ops...
    - Component: proxyssl
    - Component: accesske...
    - Component: aliyun-se...
    - Component: ark-brok...
    - Component: ark-cert-...
    - Component: ark-dag-...
    - Component: ark-ops-r...
    - Component: ark-ops-r...

Component Info: ark-node

Refresh | Details

Cluster: ark-standard-0002 Details

Service: ark-0 Details

Zone: cn-wulan-env180-amtest180001-a

Error Message: DaemonSet ark-system/machine-operator-controller-manager is NotReady

Workload | Error Message | Resources | Dependencies

☑ Abnormal Workload

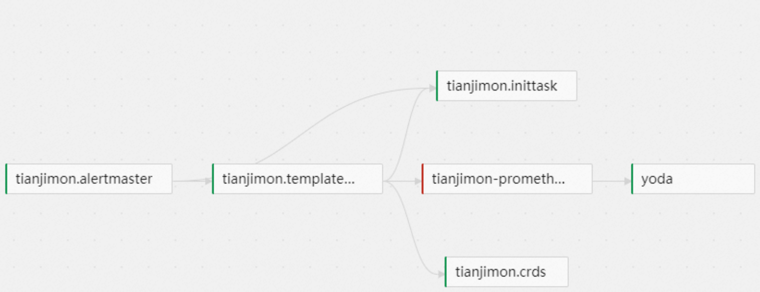
DaemonSets 0/1

Level	Description

Cluster	Displays the current cluster information, including the cluster name, status, statistics (the number of services in the Ready state and the total number of services in the current cluster), the zone to which the cluster belongs, and the error message.
Service	Displays the current service information, including the service name, cluster, status, statistics (the number of components in the Ready state and the total number of components), zone, and error information.
Component	Displays information about the current component, including the component name, cluster, service, zone, and error message. In the Component Information section, you can view the component resource list and dependency status of the product. The following table describes the differences between the product components deployed in Tianji and PaaS.

Product component information table for Tianji and PaaS deployment

Basic service	**Component parameters**	**Description**
	Instances	◦ Displays the status and version alignment of components deployed on machines. ◦ Provides operations such as diagnosis, monitoring, terminal login, and machine status panel. ▪ Click **Diagnose** in the **Actions** column to diagnose the cause of the abnormal status of the instance. ▪ Click **Monitor** in the **Actions** column. In the Component Monitoring panel, you can view the monitoring details of components, machines, and services. ▪ Click **Security Operations** in the **Actions** column to log on to the server. ◦ Click **Details** in the upper-right corner to go to the widget details page.
	Resources	◦ This section displays the resources that are used by the widget and their statuses. **Important** During the deployment phase, if the resource application is not completed, the component does not reach the final state. ◦ Click **Details** in the **Actions** column to view the resource status details, including the resource request parameters, resource request results, and error messages.

Tianji	**Dependency Status**	Displays the dependency status of the component. The left-right relationship is that the left-side component depends on the right-side component.  tianjimon.inittask tianjimon.alertmaster tianjimon.template... tianjimon-prometh... yoda tianjimon.crds ◦ The display mode supports **All Components** and **NotReady**. ▪ All Components: displays all components in the dependency tree. ▪ NotReady Related: displays the nodes that have not reached the final state in the dependency tree and their leaf nodes. If both nodes reach the final state, only the direct dependencies of the root node are displayed. ◦ You can select **Strong Dependency** or **Weak Dependency**. ▪ Strong dependency: If the dependency is not satisfied, the current startup status of the component will be directly affected. ▪ Weak dependency: If the dependency is not satisfied, the current component will still start, but some functions will be affected. For example, some configuration information that is not on the critical path. **Note** Components deployed through Tianji have only strong dependencies.
	Running Tasks	◦ Displays the 10 most recent tasks of the widget. ◦ Click **Details** in the Actions column to go to the task details page. You can view the task details, such as the task status, up time, and changes.
	Workload	◦ Displays the status of the workload used by the component. Workload directly affects the status of the component. ◦ Select **Abnormal Workload** to filter abnormal workloads. ◦ Click **Details** in the **Actions** column of a specific workload. On the component details page, find the component that you want to view and click **View YAML** in the **Actions** column.

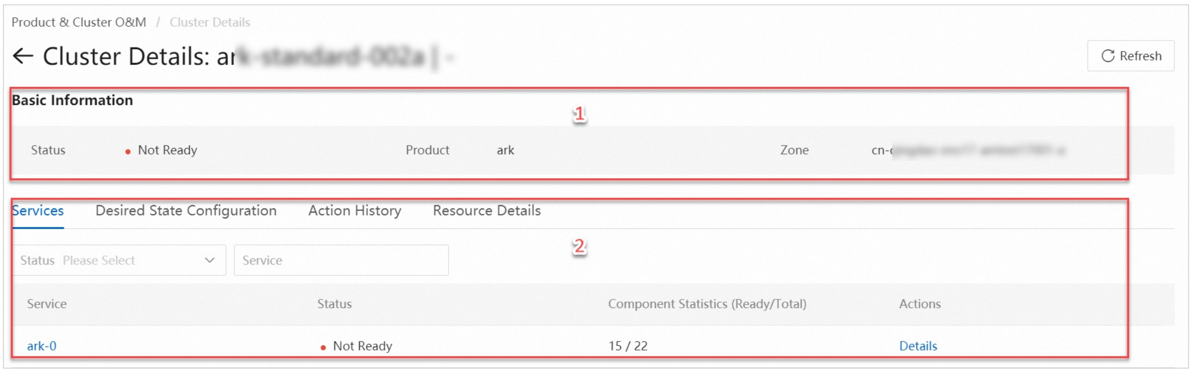
PaaS	**Error message**	When an exception occurs in a component deployed by using PaaS, an error message, such as a XXX Pod not ready, is reported in some cases to facilitate the user to investigate the problem.
	Resources	◦ This section displays the resources that are used by the widget and their statuses. **Important** During the deployment phase, if the resource application is not completed, the component does not reach the final state. ◦ Click **Details** in the **Actions** column to view the resource status details, including the resource request parameters, resource request results, and error messages.
	Dependency Status	Same as Tianji dependency status.

3.3.1.4. View the details of clusters

You can view the basic information about clusters and the application sets on the clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Products**.
3. In the Products section of the **Product Dimension** page, click **Cluster List** in the **Actions** column.
4. Find the cluster that you want to view and click **Cluster Details** in the **Actions** column.
5. View details of a cluster.



Product & Cluster O&M / Cluster Details

← Cluster Details: ar[redacted]

Basic Information

Status ● Not Ready   Product ark   Zone cn-[redacted]

Services | Desired State Configuration | Action History | Resource Details

Status Please Select   Service

Service	Status	Component Statistics (Ready/Total)	Actions
ark-0	● Not Ready	15 / 22	Details

No.	Section	Description
1	Basic Information	Displays the basic information of the cluster, including the cluster status, product, and zone.

2	Cluster Details	The details of clusters deployed through Tianji and PaaS are different, as shown in the following table.

Cluster Details Table

Basic service	Parameter	Description
Tianji	**Services**	- Displays the services deployed in the current cluster and the service status. - Click **Details** in the Actions column to go to the Component Details page and view the component details.
	Machines	- Displays the list and status of machines that can be used by the current cluster. - Click **View** in the **Machine Monitoring** column to view component monitoring, machine monitoring, and system service monitoring information.
	Divide instances into groups	- Displays planning information between machines and components. For example, what is the role of a machine group, what machines it contains, and what components it can be used by. - Click a machine name in the **Associated Machine** column to view the machine details. - Click a component name in the **Associated Components** column to view the component details.
	Desired State Configuration.	Displays the final-state configuration file of the cluster.
	Action History	- Displays the change history of the cluster. - Click **Task Details** in the Actions column to go to the task details page.
	Resource Details	- Displays the resource list applied by each component in the cluster. - Click **Versions** in the Actions column to view the versions of the resource.
	Test result report	- Displays the list of test reports of services under the cluster. - Click **Details** in the Actions column to view the details of service failure cases, successful cases, and skipped cases.

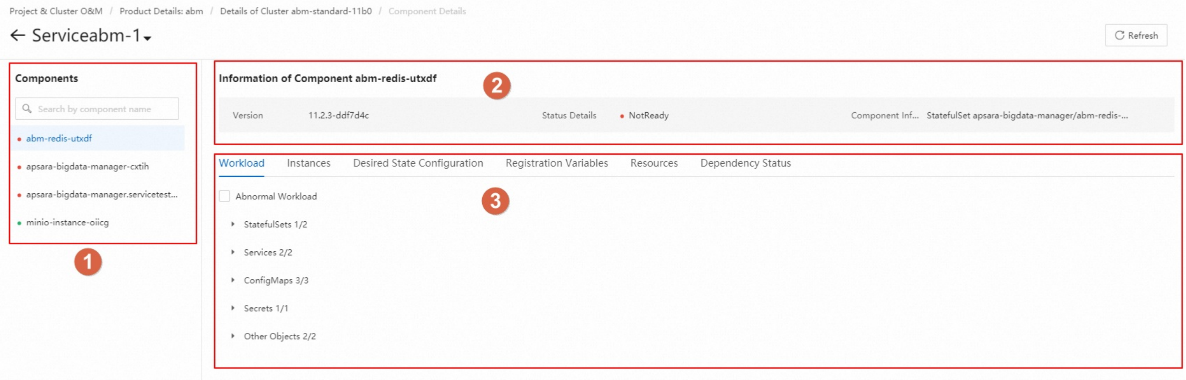
PaaS	**Services**	◦ Displays the services deployed in the current cluster and the service status. ◦ Click **Details** in the Actions column to go to the Component Details page and view the component details.
	Desired-State Configuration.	Displays the final-state configuration file of the cluster.
	Action History	◦ Displays the change history of the cluster. ◦ Click **Task Details** in the Actions column to view the task details. **Note** Cluster changes mainly refer to the final state changes, excluding machine operations such as machine maintenance in the cluster.
	Resource Details	Displays the resource list applied by each component in the cluster.

3.3.1.5. View the details of components

You can view the details of components in clusters, including component status and desired-state configurations.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Products**.
3. On the Products page, find the product that you want to view and click **Show Clusters** in the **Actions** column.
4. Find the cluster that you want to view and click **Cluster Details** in the **Actions** column.
5. On the **Services** tab of the cluster details page, click the name of a service or click **Details** in the **Actions** column.
6. View the details of a service component. The following figure shows an example of a service component.



Information of Component abm-redis-utxdf

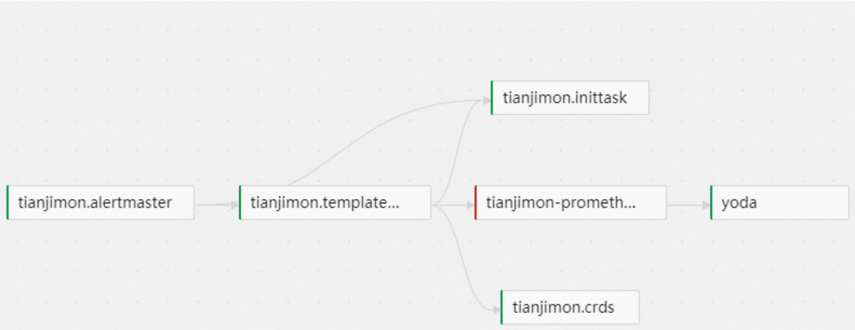
Version 11.2.3-ddf7d4c Status Details ● NotReady Component Inf... StatefulSet apsara-bigdata-manager/abm-redis-...

No.	Section	Description
1	Components	○ Displays the list of components under the service. ○ Click the component to view the basic information and details of the component in the right-side section.
2	Basic component information	Displays the current widget name, version, status details, and widget information.
3	Component details	The components deployed through Tianji and PaaS have different details, as shown in the following table.

Component details table for Tianji and PaaS deployment

Basic service	Parameter	Description

Tianji	**Instances**	- Displays the status of the component deployed on the machine, including whether the version of the component on the machine is aligned, whether there is an action in progress, and the machine status. **Note** Version inconsistency indicates that the currently running version is inconsistent with the version set in the final state. The upgrade may be in progress, failed, or is about to be upgraded (the final state version has been modified, but it is not the turn of the component upgrade). - On the page that appears, click **Diagnosis** in the Actions column. Tianji initially diagnoses the cause of the version inconsistency or the status is not Good. **Note** **Diagnosis** is displayed only when the versions are inconsistent or the status is not Good. - Choose **Component Information** > **Monitoring** in the Actions column to view the details of component monitoring (critical), machine monitoring, and system service monitoring. - Choose **Component Information** > **Apps** in the Actions column to view the apps and versions of the component on the machine. **Note** ▪ _tianji_config is a special app that indicates the configuration file that is sent to the machine. ▪ The_tianji_config version can be used as a version number of the configuration file content. If the configuration file content changes, the version number changes. If the configuration file content remains unchanged, the version number also remains unchanged. ▪ Other apps are user programs. - Choose **Component Information** > **Status Details** in the Actions column to view the detailed status of the component on the machine, such as the description status. - Click **Security Operations** in the Actions column to log on to the server. - Choose **Actions** > **Restart** in the Actions column to restart the app process of the component.
	Desired State Configuration	View the final-state configuration of the component, including the consolidation file.
	Change History	- A component deployed through Tianji displays the change tasks related to this component. - Click **Details** in the Actions column to view the task details.

Registration Variables	Displays the variables registered by the component and can be used by other components. For example, the endpoint of a program.
Resources	◦ Displays information about the resources that the widget applies to. ◦ Click **Versions** in the Actions column to view resource versions.
Dependency Status	Displays the dependency status of the component. The left-right relationship is that the component on the left depends on the component on the right. The following figure shows the architecture.  tianjimon.inittask tianjimon.alertmaster tianjimon.template... tianjimon-prometh... yoda tianjimon.crds ◦ The display mode supports **All Components** and **NotReady**. ▪ All Components: displays all components in the dependency tree. ▪ NotReady Related: displays the nodes that have not reached the final state in the dependency tree and their leaf nodes. If both nodes reach the final state, only the direct dependencies of the root node are displayed. ◦ You can view **strong dependencies** or **weak dependencies**. ▪ Strong dependency: If the dependency is not satisfied, the current startup status of the component will be directly affected. ▪ Weak dependency: If the dependency is not satisfied, the current component will still start, but some functions will be affected. For example, some configuration information that is not on the critical path.
Workload	◦ Displays the basic workload information of the component. ◦ For Deployments, StatefulSets, and DaemonSets workloads, the page displays information about the pods to which the workloads apply and provides the ability to log on to the containers deployed on the pods. ◦ Click **View in YAML** in the **Actions** column to view the original configuration and running information of the workload.
Instances	◦ This section displays the pods that are applied for by the workload and the statuses of Kubernetes nodes. ◦ Click **Security Operations** in the Actions column to log on to the server.

PaaS	**Desired State Configuration**	Displays the final-state configuration of the widget.
	Registration Variables	Displays the variables registered by the component and can be used by other components. For example, the endpoint of a program.
	Resources	Displays information about the resources that the widget applies to.
	Dependency Status	Displays the dependency data of a component on other components. Same as Tianji dependency status.

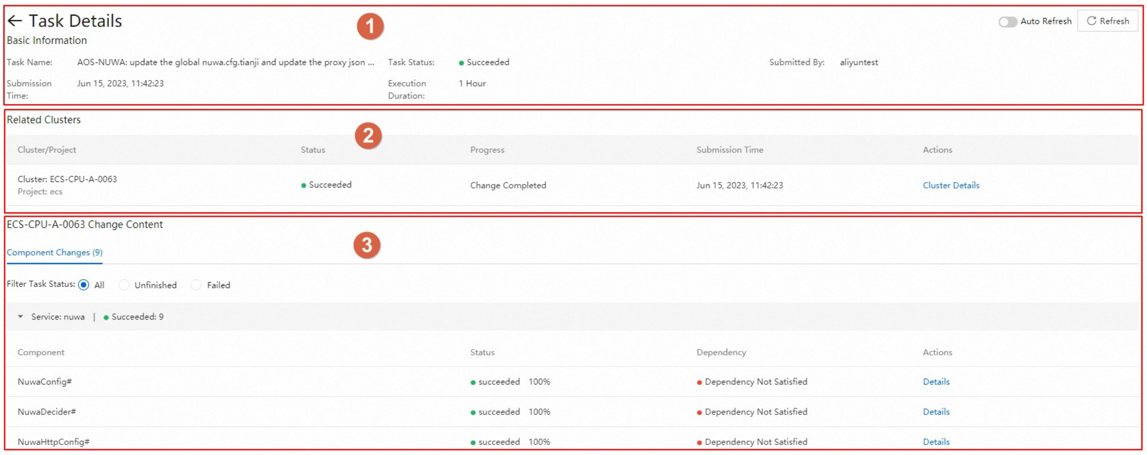
3.3.1.6. View the details of a task

You can view details of historical change tasks on the Action History tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Products**.
3. On the Product page, find the product that you want to view and click **Show Clusters** in the **Actions** column.
4. Find the cluster that you want to view and click **Cluster Details** in the **Actions** column.
5. On the page that appears, click the **Action History** tab.
6. Find the task that you want to view and click **Task Details** in the **Actions** column.
7. View the details of the task.

    - ### Tianji task details



Basic Information

Task Name: AOS-NUWA: update the global nuwa.cfg.tianji and update the proxy json ...
Task Status: ● Succeeded
Submitted By: aliyuntest
Submission Time: Jun 15, 2023, 11:42:23
Execution Duration: 1 Hour

Related Clusters

Cluster/Project	Status	Progress	Submission Time	Actions
Cluster: ECS-CPU-A-0063 Project: ecs	● Succeeded	Change Completed	Jun 15, 2023, 11:42:23	Cluster Details

ECS-CPU-A-0063 Change Content

Service: nuwa | ● Succeeded: 9

Component	Status	Dependency	Actions
NuwaConfig#	● succeeded 100%	● Dependency Not Satisfied	Details
NuwaDecider#	● succeeded 100%	● Dependency Not Satisfied	Details
NuwaHttpConfig#	● succeeded 100%	● Dependency Not Satisfied	Details

No.	Section	Description

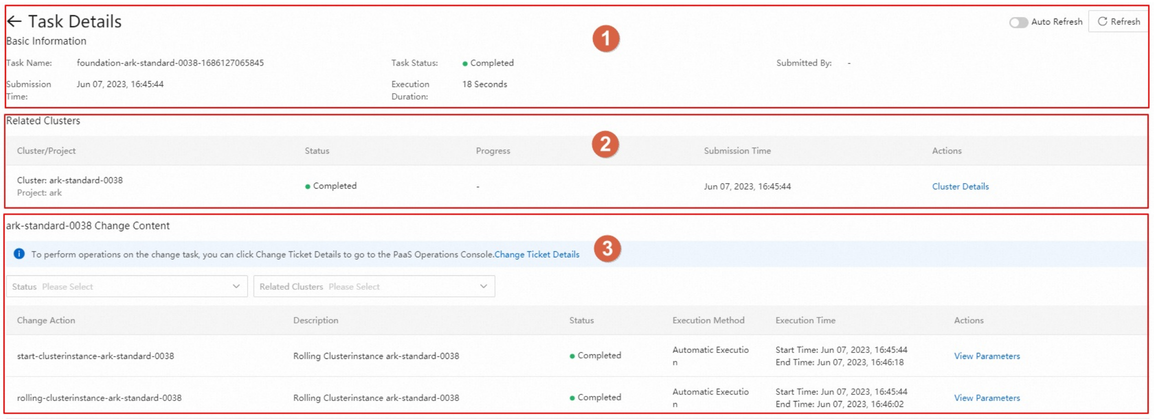
1	Basic Information	Displays basic information about the task, such as task name, task status, submitter, submission time, and execution duration.
2	Related Clusters	Displays the clusters that are related to the task. You can submit a task to change multiple clusters. In most cases, an Apsara Stack task is associated with one cluster. ▪ **Cluster/Product**: the cluster that is changed and the product to which the cluster belongs. ▪ **Status**: the status of the task. ▪ Failed ▪ Terminated ▪ Running ▪ Paused ▪ Succeeded ▪ Waiting ▪ **Progress**: the status of the task in progress. In most cases, you must build the task before you submit it. ▪ The building states include Waiting, Doing, Done, and Failed. **Note** Tianji calculates the change content based on the final status. For example, Tianji determines whether to update the version and the version that is updated to. ▪ The task change states include Waiting for Change, Changing, Change Completed, and Change Failed. ▪ **Submission Time**: the time when the task is submitted. ▪ **Actions**: Click **Cluster Details** to view the cluster details.
3	Change Content	Displays the changes of a cluster. **Component Changes**: the version change of a component. Displays the version change status of all components based on services. This section displays the number of components of each service. Click the icon on the left of the service name to view the change details of each component. For more information, see the following table.

Component change

Parameter	Description

Component	The components of the service.
Status	The following content describes the component states: ▪ Building: The component is being built. ▪ Build Failed: The component failed to be built. ▪ Waiting: The component is waiting to be changed. ▪ Running: The component is being changed. ▪ Paused: The change is paused. ▪ Rolling Back: The change is being rolled back. ▪ Rolling Back Prepared: The rollback is being prepared. ▪ Downloading: The program and configurations are being downloaded. ▪ Ready: The dependencies are being updated. ▪ Download Timeout: The download timed out. ▪ Succeeded: The change is complete. ▪ Failed: The change failed. ▪ Blocked: The component is not updated because the dependencies failed to be changed. ▪ Obstructed: The change is blocked by a previous task. ▪ Terminated: The task is terminated. ▪ Rolling Back Failed: The rollback failed. ▪ Rolled Back: The rollback is successful. ▪ Resource Checking: The resources are being checked. ▪ Resource Apply Failed: The resources failed to be applied. ▪ Su Paused: The canary release is paused. If you specify canary release rules, you must specify the interval at which the canary release is paused. ▪ Su Binary Paused: The version change is paused when no canary release is performed. ▪ Su Failed Paused: The canary release failed. In this case, the change is paused. You must determine whether to resume the change. ▪ Precheck: The component update is being prechecked. The precheck is performed before the download. ▪ Precheck Failed: The precheck failed. ▪ Postcheck: The component is being checked after the task is complete. ▪ Postcheck Failed: The post-check failed.
Dependency	Displays the dependencies required for component update. You can update the component only after the dependencies are updated. You can view the dependencies to locate the task blockage.
Actions	Click **Details** in the **Actions** column to view the change details of the component.

◦ PaaS task details



← Task Details

Basic Information

Task Name: foundation-ark-standard-0038-1686127065845

Task Status: ● Completed

Submitted By: -

Submission Time: Jun 07, 2023, 16:45:44

Execution Duration: 18 Seconds

Related Clusters

Cluster/Project	Status	Progress	Submission Time	Actions
Cluster: ark-standard-0038 Project: ark	● Completed	-	Jun 07, 2023, 16:45:44	Cluster Details

ark-standard-0038 Change Content

To perform operations on the change task, you can click Change Ticket Details to go to the PaaS Operations Console.Change Ticket Details

Status Please Select

Related Clusters Please Select

Change Action	Description	Status	Execution Method	Execution Time	Actions
start-clusterinstance-ark-standard-0038	Rolling Clusterinstance ark-standard-0038	● Completed	Automatic Execution	Start Time: Jun 07, 2023, 16:45:44 End Time: Jun 07, 2023, 16:46:18	View Parameters
rolling-clusterinstance-ark-standard-0038	Rolling Clusterinstance ark-standard-0038	● Completed	Automatic Execution	Start Time: Jun 07, 2023, 16:45:44 End Time: Jun 07, 2023, 16:46:02	View Parameters

No.	Section	Description
1	Basic Information	Displays basic information about the task, such as task name, task status, submitter, submission time, and execution duration.
2	Related Clusters	Displays the clusters that are related to the task. You can submit a task to change multiple clusters. In most cases, an Apsara Stack task is associated with one cluster. - **Cluster/Product**: the cluster that is changed and the product to which the cluster belongs. - **Status**: the status of the PaaS task. - Failed - Processing - Suspended - Waiting - Completed - **Progress**: the status of the task in progress. - **Submission Time**: the time when the task is submitted. - **Actions**: Click **Cluster Details** in the Actions column to view the details of the cluster.

3	Change Content	The change content includes the change action, description, status, execution method, and execution time. **Note** To perform operations on a change task, click**Change Ticket Details** above the change list to go to the PaaS console. The following content describes the change states: ▪ Failed ▪ Processing ▪ Suspended ▪ Waiting ▪ Completed Click **View Parameters** in the Actions column to view the parameter names and values.

3.3.2. Data centers

This topic describes the modules of the data center module.

Modules

Module	Description
Query of data center details	The data center module provides resource information of data centers, racks, and machines hierarchically to help you better understand the overall resource distribution and exception details.
Security O&M	The security O&M feature allows you to remotely log on to a server to perform O&M operations.
Machine monitoring	The machine monitoring feature allows you to view the monitoring information of physical servers and fix alerts.
Machine management	The machine management feature allows you to restart, repair, clone, and shut down servers. This feature also allows O&M personnel to send commands to servers by using GUIs and to control, manage, or maintain servers.
Favorites	You can add resource tags of data centers, racks, and machines to favorites for easy search and usage. This feature helps you better manage and utilize various resources and improve work efficiency.
Data export	The data export feature allows you to export server data by data center, rack, or machine to your computer in the XLS format for backup and query purposes.

Refresh	The refresh feature allows you to reload the content of the Machines page for update and troubleshooting purposes.

3.3.2.1. View the details of a data center

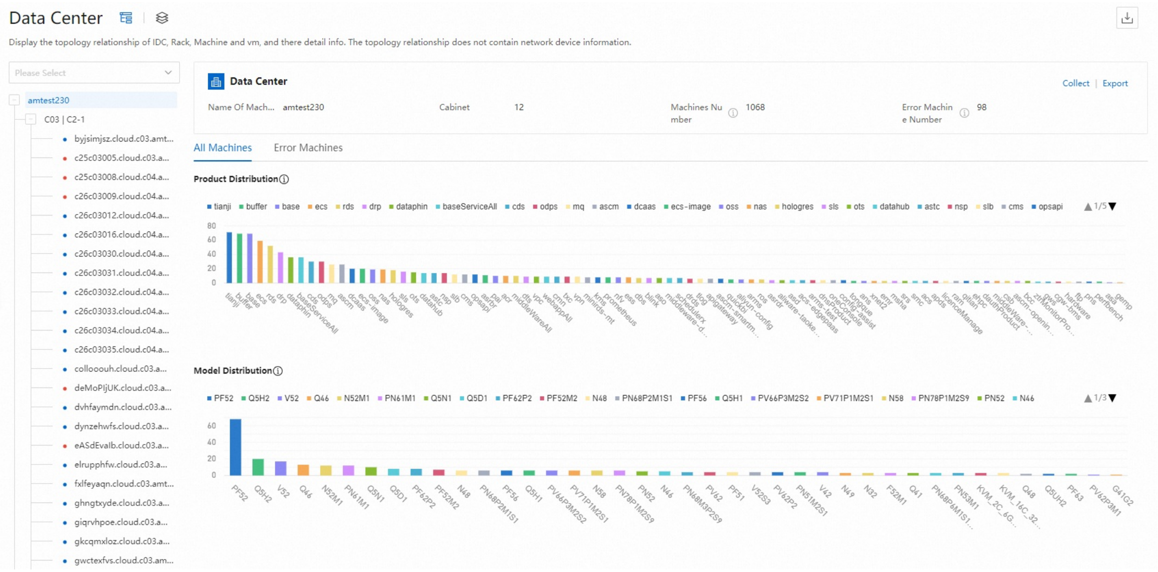
The data center dimension provides resource information of data centers, racks, and machines hierarchically to help you better understand the overall resource distribution and exception details.

Procedure

1. Go to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Data Centers**.
3. View the details of a data center

   - Click on the right of Data Center to expand the left-side structure tree and view the hierarchical relationships of data centers.

     Data center hierarchy diagram



Data Center

Display the topology relationship of IDC, Rack, Machine and vm, and there detail info. The topology relationship does not contain network device information.

Please Select

- amtest230
  - C03 | C2-1
    - byjsimjsz.cloud.c03.amt...
    - c25c03005.cloud.c03.a...
    - c25c03008.cloud.c04.a...
    - c26c03009.cloud.c04.a...
    - c26c03012.cloud.c04.a...
    - c26c03016.cloud.c04.a...
    - c26c03030.cloud.c04.a...
    - c26c03031.cloud.c04.a...
    - c26c03032.cloud.c04.a...
    - c26c03033.cloud.c04.a...
    - c26c03034.cloud.c04.a...
    - c26c03035.cloud.c04.a...
    - collooouh.cloud.c03.a...
    - deMoPIjUK.cloud.c03.a...
    - dvhfaymdn.cloud.c03.a...
    - dynzehwfs.cloud.c03.a...
    - eASdEvalb.cloud.c03.a...
    - elrupphfw.cloud.c03.a...
    - fxlfeyaqn.cloud.c03.amt...
    - ghngtxyde.cloud.c03.a...
    - giqrvhpoe.cloud.c03.a...
    - gkcqmxloz.cloud.c03.a...
    - gwctexfvs.cloud.c03.am...

Data Center

Collect | Export

Name Of Mach... amtest230

Cabinet 12

Machines Number 1068

Error Machine Number 98

All Machines | Error Machines

Product Distribution

tianji buffer base ecs rds drp dataphin baseServiceAll cds odps mq ascm dcaas ecs-image oss nas hologres sls ots datahub astc nsp slb cms opsapi
1/5
80
60
40
20
0
tianji buffer base ecs rds drp dataphin baseServiceAll cds odps mq ascm dcaas ecs-image oss nas hologres sls ots datahub astc nsp slb cms opsapi asrbr pai acr middleWareAll dts vpc webappAll cmn txc vpn minirds-mt kms prometheus nfv ess dbs blink aso middleware-d... schedulerx drds tlog apigateway ascm-smartm... quickbi aliyun-config ams ros asrdr aliware-taoke... asd acs-edgepaas ams-test dnsProduct oneConsole config-assist longque ans xnet2 emr msha srs smc acs apds licenceManage ram qitian ehpc dauthProduct middleWare-... csb ascm-openin... bcc ztMonitorPro... gws cgw-bms hardware ftp pns perfbench asa gemp

Model Distribution

PF52 Q5H2 V52 Q46 N52M1 PN61M1 Q5N1 Q5D1 PF62P2 PF52M2 N48 PN68P2M1S1 PF56 Q5H1 PV66P3M2S2 PV71P1M2S1 N58 PN78P1M2S9 PN52 N46
1/3
60
40
20
0
PF52 Q5H2 V52 Q46 N52M1 PN61M1 Q5N1 Q5D1 PF62P2 PF52M2 N48 PN68P2M1S1 PF56 Q5H1 PV66P3M2S2 PV71P1M2S1 N58 PN78P1M2S9 PN52 N46 PN68M3P2S9 PV62 PF51 V52S3 PV62P2 PN51M2S1 V42 N49 N32 F52M1 Q41 PN68P6M1S1 PN53M1 KVM_2C_6G... KVM_16C_32... Q48 Q5UH2 PF63 PV62P3M1 G41G2

Click in the upper-right corner of the page to save the server data in the XLS format on your local computer.

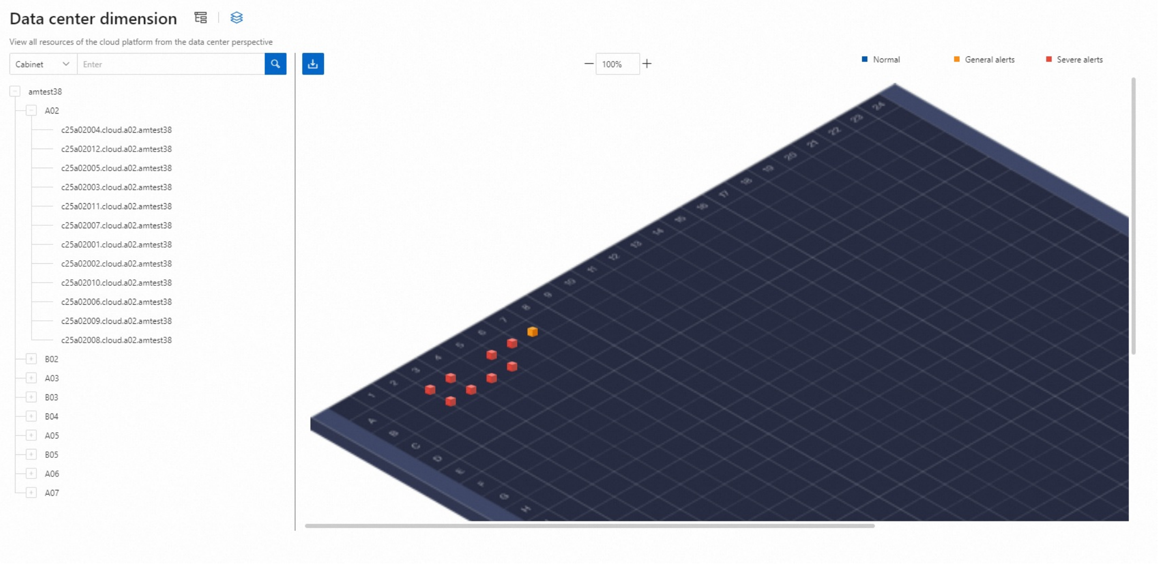
The left-side area is displayed in order by IDC, Rack | Room, physical machine, and virtual machine. Select IDC, Rack | Room, physical machine, or virtual machine. The right-side area displays the corresponding details. Click **Favorites** in the Actions column. In the **Resource Tags** section, you can view the added nodes. Click **Export** to save the server data in the. xls format on your on-premises machine.

Level	Description

IDC	▪ In the upper part of the section on the right, the name of the data center, the number of cabinets in the data center, the number of machines (including physical machines and virtual machines), and the number of abnormal machines (including physical machines and virtual machines) are displayed. ▪ Click the **All Machines** or **Error Machines** tab to view the **Product Distribution** and **Model Distribution** of the data center.
Rack | Room	▪ In the upper part of the section on the right, the name of the cabinet, the number of machines (including physical machines and virtual machines), and the number of abnormal machines (including physical machines and virtual machines) are displayed. ▪ Click the **All Machines** or **Error Machines** tab to view the **Product Distribution** and **Model Distribution** of the cabinet.
Physical/Virtual Machines	▪ The upper part of the section on the right side displays the basic information of the physical machine, including the IP address, status, machine action, cluster, IDC, SN, model, Kubernetes node status (if the machine is a Kubernetes node, the node status is displayed), and host (if the machine is a virtual machine, the host is displayed). ▪ Click the **Components**, **Virtual Machines**, **Taints**, and **Tags** tabs to view the details. ▪ **Components**: displays a list of components deployed on the machine, including the status, actions, and monitoring of the components. **Note** ▪ For components deployed through PaaS, pods related to the components running on the machine are displayed. ▪ You can restart the processes of components that are deployed by using Tianji. ▪ **VMs**: displays the VMs that are started on the host. This is displayed only when the machine is a host. ▪ **Taints**: displays the taint information of the Kubernetes node and allows you to add or delete taint information. This field is displayed only when the machine is a Kubernetes node. ▪ **Tags**: displays the tags of Kubernetes nodes. You can add or delete tags. This field is displayed only when the machine is a Kubernetes node.

- Click ≋ on the right of the data center dimension to expand the left-side structure tree and view the resource distribution from the data center perspective.

  Data Center Perspective



Data center dimension

View all resources of the cloud platform from the data center perspective

Cabinet | Enter

- amtest38
  - A02
    - c25a02004.cloud.a02.amtest38
    - c25a02012.cloud.a02.amtest38
    - c25a02005.cloud.a02.amtest38
    - c25a02003.cloud.a02.amtest38
    - c25a02011.cloud.a02.amtest38
    - c25a02007.cloud.a02.amtest38
    - c25a02001.cloud.a02.amtest38
    - c25a02002.cloud.a02.amtest38
    - c25a02010.cloud.a02.amtest38
    - c25a02006.cloud.a02.amtest38
    - c25a02009.cloud.a02.amtest38
    - c25a02008.cloud.a02.amtest38
  - B02
  - A03
  - B03
  - B04
  - A05
  - B05
  - A06
  - A07

Section	Description
Left	▪ In the upper part of the left-side area, you can select the cabinet, hostname, IP address, SN, and data center from the cabinet drop-down list to quickly search and query. ▪ The left-side area is displayed in order by data center, cabinet, and machine level. Select the target node and the corresponding perspective information is displayed in the right-side area.
Right	▪ In the right-side section, you can view the resource distribution in the left-side data center, cabinet, and machine perspective. You can also view the alert status of resources. ▪ 🟦Blue indicates that the resource is running normally. ▪ 🟧Orange indicates a normal alert. ▪ 🟥Red indicates a critical alert. ▪ Click ⤓ to save the detailed server data locally in. xls format for easy reference. ▪ Click the + or - icon to enlarge or reduce the size of the module display in the view. ▪ Move the pointer over a module in the view to view the number of alerts and the location of the machine. Click it to go to the corresponding alert status details panel and view the alert status of the machine.

3.3.2.2. Security O&M

The security O&M feature allows you to remotely log on to a server 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**.
3. Click ☰ to expand the structure tree on the left and click the desired machine.
4. In the upper-right corner of the page that appears, click **Security O&M**.
5. Perform the following O&M operations:
   i. After you log on to your server, enter Linux commands in the command-line interface (CLI) to perform O&M operations.
   ii. Click **Upload File**. The **File Upload** dialog box appears. You can use one of the following methods to upload a file:
      - 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 click **Upload**.
   iii. Click **File Download**. The **File Download** dialog box appears. Configure the **File Directory** and **File Name** parameters and click **Download** to download the file to the configured directory. If you do not configure a 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 that you want to upload is larger than 200 MB, use the `split` and `cat` commands to split and merge the file.

3.3.2.3. Monitor a server

The machine monitoring feature allows you to view the monitoring information of physical servers 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**.
3. Click ☰ to expand the structure tree on the left and click the desired machine.
4. In the upper-right corner of the page, click **Machine Monitor**.
5. The **Monitoring Information** tab is displayed by default. Select a metric from the drop-down list in the upper-right corner of the chart, select a time range, and then click the 🔍 icon. You can view the monitoring charts of CPU utilization, system load, disk usage, memory usage, host traffic, and disk I/O.

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

When you view a statistical chart, click the ⬇ icon to download the monitoring information to your local computer.

6. 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**.

3.3.2.4. Machine management

The machine management feature allows you to restart, repair, clone, and shut down servers. This feature also allows O&M personnel to send commands to servers by using GUIs and to control, manage, or maintain servers.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Data Centers**.
3. In ☰ mode, display the machine tree on the left and click the target machine.
4. Click the buttons in the upper-right corner of the page to perform operations on the machine.

Operation	**Procedure**
Restart	In the upper-right corner of the page, choose**Machine Management** > **Restart**. In the dialog box that appears, click **OK**.
Repair and Clone	ⓘ **Note** You can click Repair and Clone or Power Off Repair based on your business requirements. Click Repair and Clone for machines that must be cloned before installing the operating system, such as the system disk. Click Power Off Repair for machines that can be repaired without cloning, such as the memory. i. In the upper-right corner of the page, choose**Machine Operations** > **Repair and Clone** or **Power Off Repair**. ii. In the dialog box that appears, enter**REPAIR** and click**OK**. iii. Click **Repair Details** next to Status Metrics to go to the Machine Repair page.

Power Off Repair	iv. Perform the precheck. In the Precheck step, click **Execute Pre Check** in the upper-right corner and click **OK**. The system automatically performs a precheck to ensure that the machine repair can be executed in a secure manner. **Note** If the precheck fails, click **Retry** in the upper-right corner to try again. v. Approve the repair. a. After the precheck is complete, click **Enter Approval Phase** in the lower-right corner of the page. In the dialog box that appears, click **OK**. b. In the Approve step, view the components that need to be approved and click **Approve** in the Actions column. c. In the dialog box that appears, enter **APPROVED** and click **OK**. **Important** Then, Action Status is changed from pending to approved. After Action Status is changed to approved, the action that you specified is automatically executed. Manually setting Action Status to approved instead of using the Decider program is a high risk operation. Data loss may occur. You must contact technical support for confirmation. vi. Repair the machine. a. After the repair is approved, click **Start Repair** in the lower-right corner of the page. In the dialog box that appears, click **OK**. b. On the page that appears, machine information such as the name, IP, and SN of the machine and the project to which the machine belongs is displayed. You can repair the machine offline based on your business requirements. vii. Perform the post-check. a. After the machine is repaired, click **Go to Post-check** in the lower-right corner of the page. In the dialog box that appears, click **OK**. b. In the Post-check step, click **Execute Post-check** in the upper-right corner. In the dialog box that appears, click **OK**. **Note** If the post-check operation fails, click **Retry** in the upper-right corner to try again. c. After the post-check is complete, click **Complete Repair** in the lower-right corner of the page. d. In the dialog box that appears, enter **FINISHREPAIR** and click **OK**. The machine is repaired.

3.3.2.5. Add a resource to favorites

You can add resource tags of data centers, racks, and machines to favorites for easy search and usage. This feature helps you better manage and utilize various resources and improve work efficiency.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Data Centers**.
3. In the ☰ mode, expand the structure tree on the left and select the target node.

- If you select a data center node, click **Add to Favorites** next to the data center information. The data center information is displayed in the Watchlist section on the Resource Tags page.
- If you select a rack node, click **Add to Favorites** next to the rack information. The rack information is displayed in the Watchlist section on the Resource Tags page.
- If you select a machine node, click **Add to Favorites** next to the machine information. The machine information is displayed in the Watchlist section on the Resource Tags page.

> **Note**
>
> After you add a resource to favorites, you can click **Remove from Favorites** to remove the resource from favorites.

3.3.2.6. Export

You can export server data to your computer and save the data in XLS format for backup and easy search by the following dimensions: data center, rack, and machine.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** >**Resources** >**Data Centers**.
3. Click ☰ to expand the structure tree on the left and click the desired node.
   - If you click a data center node, click **Export** in the upper-right corner of the data center details section to export server data to your computer and save the data in XLS format.
   - If you click a rack node, click **Export** in the upper-right corner of the **Cabinet** section to export server data to your computer and save the data in XLS format.
   - If you click a machine node, click **Export** in the upper-right corner of the machine details page to export server data to your computer and save the data in XLS format.

3.3.2.7. Refresh

The refresh feature allows you to reload the content of a specific machine for update and troubleshooting purposes.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** >**Resources** >**Data Centers**.
3. Click ☰ to expand the structure tree on the left and click the desired machine node.
4. Click **Refresh** in the upper-right corner of the machine details section to refresh the machine information.

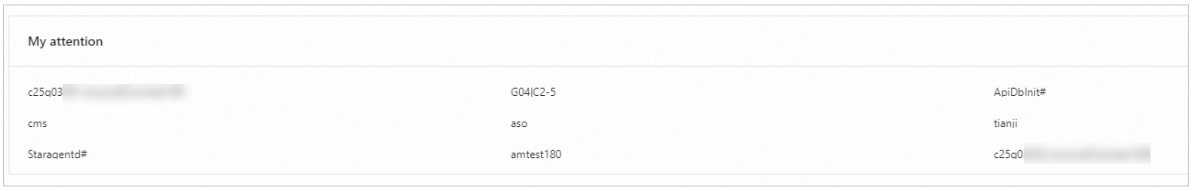
3.3.3. Resource tags

The Resource Tags module allows you to use tags to view and manage resources that you care about in a centralized manner.

My attention

You can add nodes in the **Products** or **Data Centers** module to your favorites. These nodes are then displayed on the **Resource tag** page.

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Data Centers**.
3. In hierarchy mode, expand the left-side navigation tree, select a node, and click **Collect**.
4. View the added node on the **Resource tag** page. You can click a node to view its details.



My attention

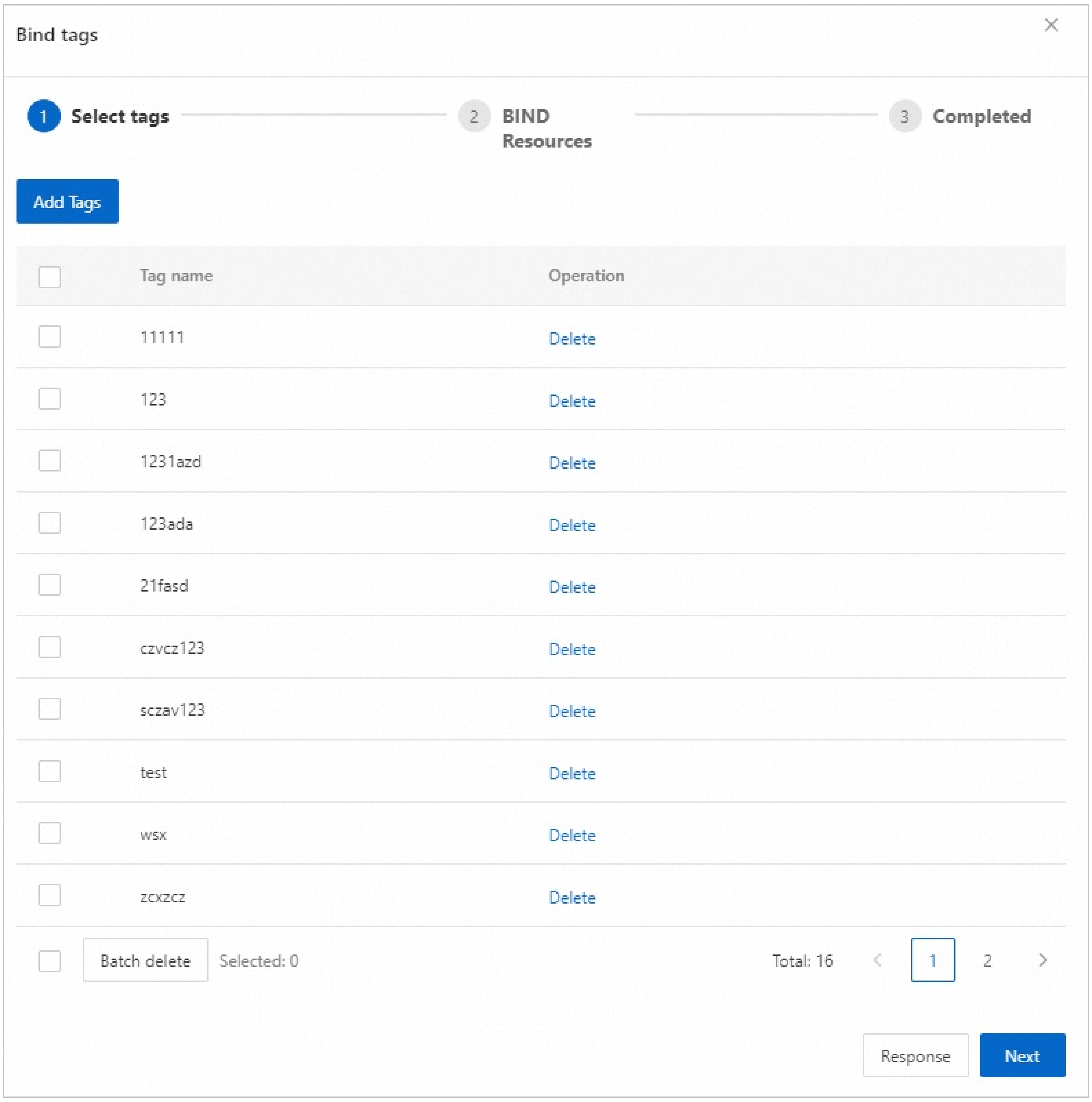
c25q03[redacted]	G04IC2-5	ApiDbInit#
cms	aso	tianji
Staragentd#	amtest180	c25q0[redacted]

Resource List

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

Procedure

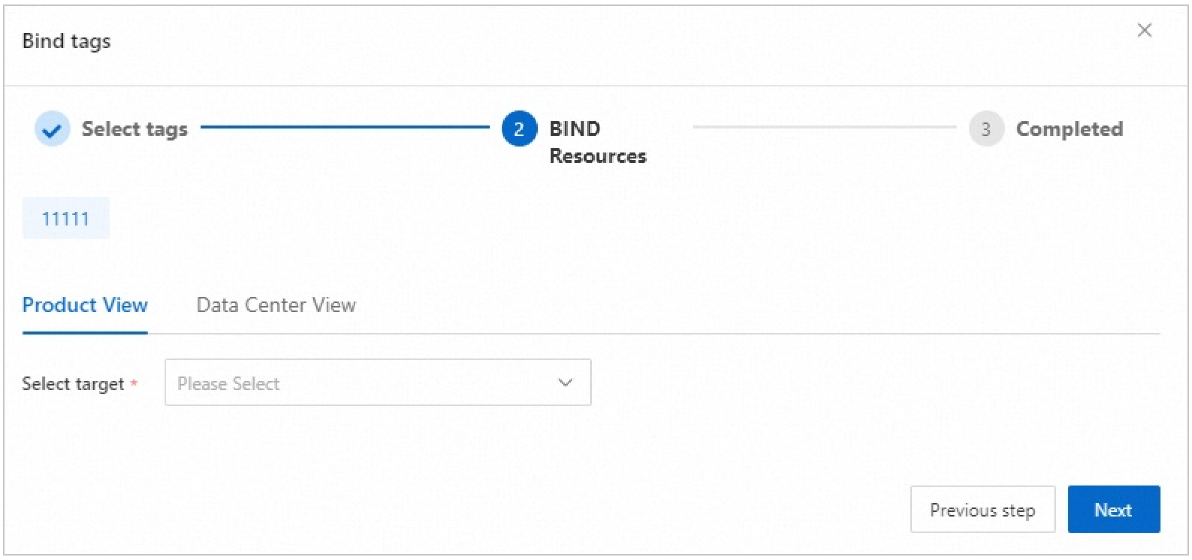
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Resources** > **Resource Tags**.
3. On the page that appears, click **Bind tags** in the Resource List section. In the dialog box that appears, select one or more tags in the **Select tags** step and click **Next**.



□	Tag name	Operation
□	11111	Delete
□	123	Delete
□	1231azd	Delete
□	123ada	Delete
□	21fasd	Delete
□	czvcz123	Delete
□	sczav123	Delete
□	test	Delete
□	wsx	Delete
□	zcxzcz	Delete

> **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. In the **BIND Resources** step, select one or more tags that you want to bind and click **Next**.



Bind tags

Select target * Please Select

> **Note**
>
> - You can select resources by clicking the **Product View** or **Data Center View** tab.
> - You can select multiple resources. However, the resources must be at the same level.

5. In the **Completed** step, confirm the information and then click **Complete**.

Related operations

Operation	Description
View resource tags	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.
Unbind tags from resources	You can unbind tags from resources based on your business requirements. Select the resources that you want to manage and click **Unbind tags**. In the message that appears, click**OK**.
Delete a resource tag	You can delete resource tags that are no longer required. 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**.
Export resource tags	You can export all resource tags in the list. Click**Export**. In the dialog box that appears, select a download URL and click **Download**. **Note** If you want to import only some of the resource tags, select the resource tags that you want to export and click **Export**. In the dialog box that appears, select a download URL and click **Download**.

3.3.4. HDD repairs

The HDD repair feature allows you to replace data disks. If a fault occurs in a data disk, the system confirms the status of the disk, uninstalls the disk, and then confirms that the business is not affected before performing subsequent operations. After the disk is replaced, the system formats, mounts, and restores the disk to provide the storage capacity.

Modules

Module	Description
Prepare	After you initiate a disk replacement task, you must make preparations for it, including task reporting, task approving, and disk unmounting.
Maintenance	After you complete the preparations that are required to replace a disk, you can replace the disk and perform a health check on the new disk.
History	You can view a list of all repair records to learn repaired machines and HDDs, and the repair results.

3.3.4.1. Preparation

After you initiate a disk replacement task, you must make preparations for it, including task reporting, task approving, and disk unmounting.

Prerequisites

If you want to use the disk replacement feature to replace a disk online, the following conditions must be met:

- The disk is a data disk that is used by Apsara Distributed File System and provides storage capabilities to users.
- No other files are stored on the disk.
- Cloud services that support disk replacement, such as Apsara Infrastructure Management, Elastic Compute Service (ECS), and ODPS, are deployed on the machine in which the disk resides.
- The disk is marked as abnormal in Apsara Distributed File System.

The system checks and confirms whether the preceding conditions are met during the maintenance. If the preceding conditions are not met, the disk replacement is not triggered or errors are reported during the precheck.

Background information

- If you ignore the error messages and forcibly replace the disk, data loss may occur.
- You can use the disk replacement feature to handle only damaged disks that are reported by Apsara Distributed File System.
- You can use the disk replacement feature to replace only damaged data disks. If you do not replace the disks with new disks, the maintenance process is interrupted.
- The data disks of Apsara Infrastructure Management, ODPS, Object Storage Service (OSS), and Simple Log Service can be repaired.

Procedure

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

   By default, the **Preparation** tab appears. You can query disk replacement tasks by progress or machine name.
3. Perform operations based on the task status in different phases.

   The preparation process is divided into the following phases: Report, Approval, and Unmounting. The task can be in one of the following states in each of the three phases: not started (displayed in gray), in progress (displayed in blue), completed (displayed in green), and failed (displayed in red). The following table lists the corresponding operations that can be performed in these states.

Report	Approval	Unmounting	Executable operation
In progress	Not started	Not started	Cancel the task
Completed	Not started	Not started	Start to repair the disk and cancel the task
Failed	Not started	Not started	Cancel the task
Completed	In progress	Not started	Select manual approval by clicking **Approval Details**
Completed	Completed	In progress	None
Completed	Completed	Disk unmounting completed but silence period not ended	None
Completed	Completed	Disk unmounting completed and silence period ended	Prepare to replace the disk

   Related operations:

   - Cancel the disk replacement task: Click **Cancel**. In the message that appears, click **OK**.
   - Start to repair the disk:

     Click **Start Repair**:

     - If a QR code is required for approval, the system pops up the QR code. You can use the DingTalk mini program ASLM Mobile to scan the QR code to obtain the authorization code. Then, enter the authorization code. The system proceeds to the next step after the verification is passed.

    - If a QR code is not required for approval, click **OK** in the dialog box that appears to start to repair the disk. After that, the software enters the automatic approval phase.

  - Manually approve a disk replacement task: If **Approval Details** is displayed in the **Actions** column, click **Approval Details**. In the dialog box that appears, click **Approval** in the **actions** column of the service role that you want to manage. In the dialog box that appears, enter **APPROVED** in the Enter APPROVED to confirm your operation field. Then, click **OK**.

    > **Important**
    >
    > Before approval, make sure that business data on the disk is backed up.

  - Prepare for disk replacement: Click **Prepare for Replacement**. The disk replacement task enters the repair phase and is displayed on the **Repair** tab.

    The time period displayed under **Unmounting** is the silence period. You can change the disk only if the value is larger than 7 days.

3.3.4.2. Repair

After you complete the preparations that are required to replace a disk, you can replace the disk and perform a health check on the new disk.

Prerequisites

If you want to use the disk replacement feature to replace a disk online, the following conditions must be met:

- The disk is a data disk that is used by Apsara Distributed File System and provides storage capabilities to users.
- No other files are stored on the disk.
- Cloud services that support disk replacement, such as Apsara Infrastructure Management, Elastic Compute Service (ECS), and ODPS, are deployed on the machine in which the disk resides.
- The disk is marked as abnormal in Apsara Distributed File System.
- The preparations that are required to replace the disk are complete.

The system checks and confirms whether the preceding conditions are met during the maintenance. If the preceding conditions are not met, the disk replacement is not triggered or errors are reported during the precheck.

Background information

- If you ignore the error messages and forcibly replace the disk, data loss may occur.
- You can use the disk replacement feature to handle only damaged disks that are reported by Apsara Distributed File System.
- You can use the disk replacement feature to replace only damaged data disks. If you do not replace the disks with new disks, the maintenance process is interrupted.
- The data disks of Apsara Infrastructure Management, ODPS, Object Storage Service (OSS), and Simple Log Service can be repaired.

Procedure

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

2. In the top navigation bar, choose **General** > **Resources** > **HDD Repairs**.
3. Click the **Repair** tab.

   You can query disk replacement tasks by progress or machine name.
4. Perform operations based on the task status in different phases.

   The maintenance process is divided into the following phases: Disk Replacement, Disk Formatting & Mounting, and Health Check.

   - Disk Replacement: replaces the failed disk.
   - Disk Formatting & Mounting: checks the basic information about the new disk and perform initialization operations such as formatting and mounting.
   - Health Check: waits for the related business system to check the new disk. After the check is passed, the new disk is used. If the check is not passed, contact technical support to troubleshoot the issue.

   The task can be in one of the following states in each of the three phases: not started (displayed in gray), in progress (displayed in blue), completed (displayed in green), and failed (displayed in red). The following table describes the corresponding operations that can be performed in these states.

Disk Replacement	Disk Formatting & Mounting	Health Check	Executable operation
Not started	Not started	Not started	Start to replace the disk
In progress	Not started	Not started	Complete the disk replacement
Completed	In progress	Not started	Replace the disk again
Completed	Failed	Not started	Replace the disk again
Completed	Completed	In progress	None
Completed	Completed	Failed	None

   Related operations:

   - Start to replace the disk: Click **Start Changing**.
   - Complete the disk replacement: Click **Complete Replacement**.
   - Replace the disk again: Click **Re-change Disk**.

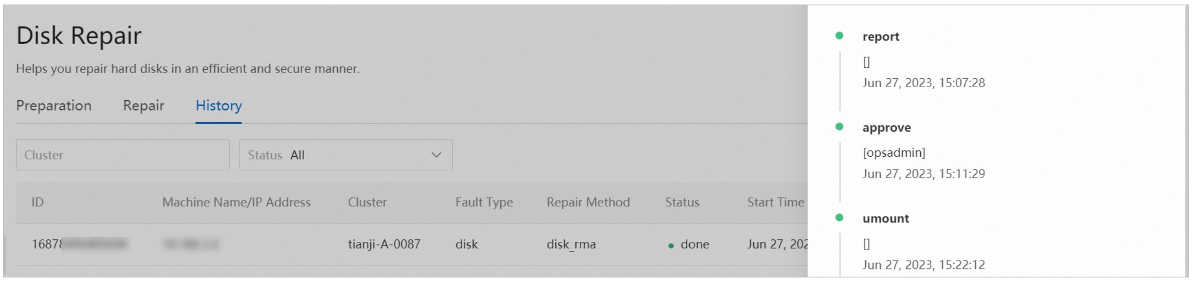
3.3.4.3. History

You can view a list of all repair records to learn repaired machines and HDDs, and repair results.

Procedure

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

   You can view disk replacement tasks by cluster and status.
4. Find the disk replacement task that you want to manage and click **Details** in the **Actions** column. In the panel that appears, you can view the task execution status, including the details of each step beginning from the report.



Disk Repair

Helps you repair hard disks in an efficient and secure manner.

ID	Machine Name/IP Address	Cluster	Fault Type	Repair Method	Status	Start Time
1687[redacted]	[redacted]	tianji-A-0087	disk	disk_rma	● done	Jun 27, 202

report
[]
Jun 27, 2023, 15:07:28

approve
[opsadmin]
Jun 27, 2023, 15:11:29

umount
[]
Jun 27, 2023, 15:22:12

3.4. Capacity management

This topic describes the features related to capacity management.

Features

The capacity management features allow you to predict capacity trends and perform operations such as scale-out based on the available product capacity and usage habits.

Feature	Description
Capacity Analytics	Displays the capacity usage of core services, unexpected capacity usage of each cloud service, distribution of cloud services by status and services whose capacity usage reached the warning threshold, and prediction of capacity usage trends.
ECS Capacity	Displays the capacity usage and usage trends of ECS resources. This allows you to perform O&M operations based on your business requirements.
SLB Capacity	Displays the capacity usage and usage trends of SLB resources. This allows you to perform O&M operations based on your business requirements.
OSS Capacity	Displays the capacity usage and usage trends of OSS resources. This allows you to perform O&M operations based on your business requirements.
Tablestore Capacity	Displays the capacity usage and usage trends of Tablestore resources. This allows you to perform O&M operations based on your business requirements.

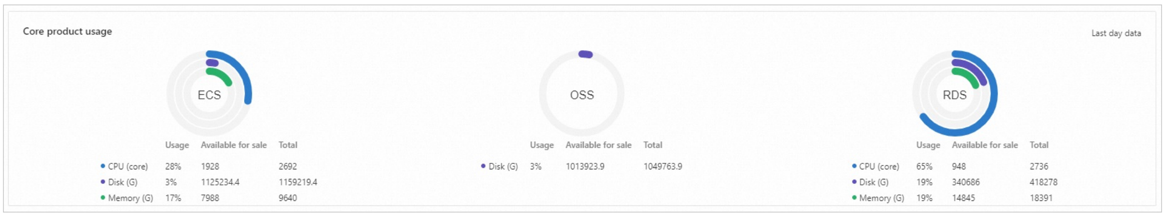
Log Service Capacity	Displays the capacity usage and usage trends of Simple Log Service resources. This allows you to perform O&M operations based on your business requirements.
EBS Capacity	Displays the capacity usage and usage trends of EBS resources. This allows you to perform O&M operations based on your business requirements.
NAS Capacity	Displays the capacity usage and usage trends of NAS resources. This allows you to perform O&M operations based on your business requirements.
RDS Capacity	Displays the capacity usage and usage trends of RDS resources. This allows you to perform O&M operations based on your business requirements.

3.4.1. Capacity analysis

This topic describes how to view the trends of available capacity and the prediction of capacity usage for various cloud products.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General O&M** > **Capacity Management** > **Capacity Analysis**.
3. On the current page, you can view the core product usage, clusters with abnormal cloud product capacity, product statistics, and forecast view.
    - Core product usage: displays the capacity usage of core cloud products.



Core product usage

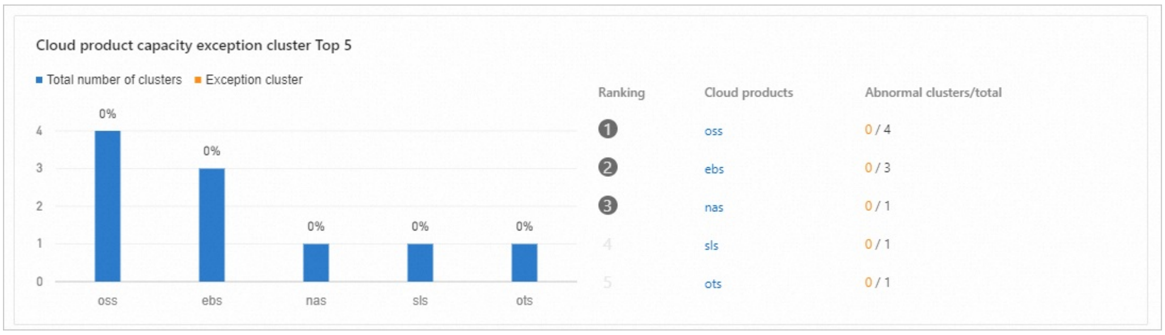
Last day data

	Usage	Available for sale	Total
● CPU (core)	28%	1928	2692
● Disk (G)	3%	1125234.4	1159219.4
● Memory (G)	17%	7988	9640

	Usage	Available for sale	Total
● Disk (G)	3%	1013923.9	1049763.9

	Usage	Available for sale	Total
● CPU (core)	65%	948	2736
● Disk (G)	19%	340686	418278
● Memory (G)	19%	14845	18391

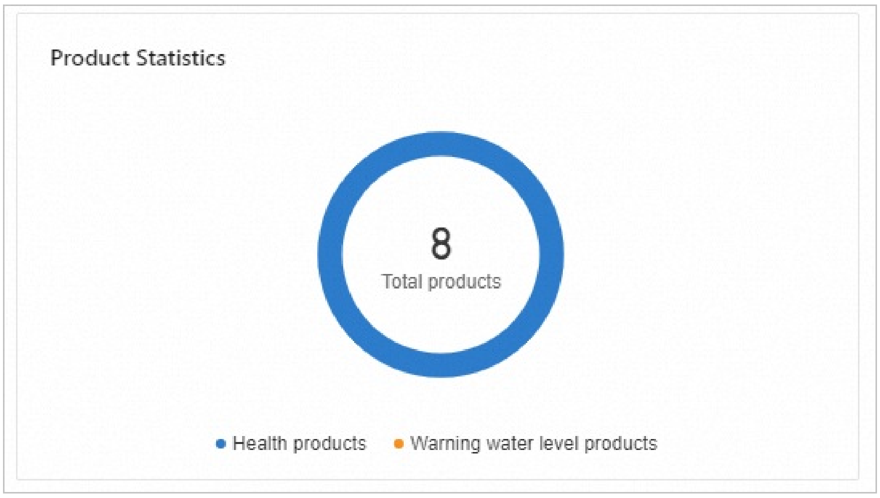
    - Cloud product capacity exception cluster Top 5: displays the proportions of clusters with unexpected high capacity usage for the top 5 cloud products. Move the pointer over a bar in the column chart to view the total number of clusters and the number of clusters with unexpected high capacity usage. Click the name of a cloud product in the Cloud products column. The corresponding product capacity page appears.



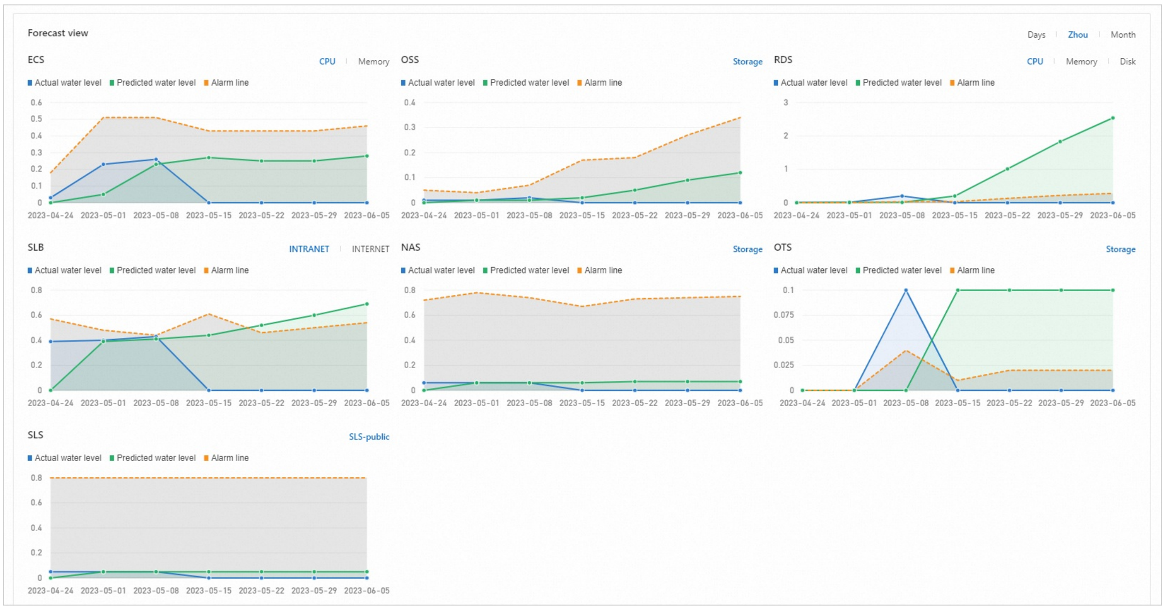
Cloud product capacity exception cluster Top 5

Ranking	Cloud products	Abnormal clusters/total
1	oss	0 / 4
2	ebs	0 / 3
3	nas	0 / 1
4	sls	0 / 1
5	ots	0 / 1

- Product Statistics: displays the number of healthy products, the number of products whose capacity usage reaches their warning thresholds, and the total number of products.



- Forecast view: displays the trends of actual usage, predicted usage, and alert thresholds for capacity metrics of each cloud product.



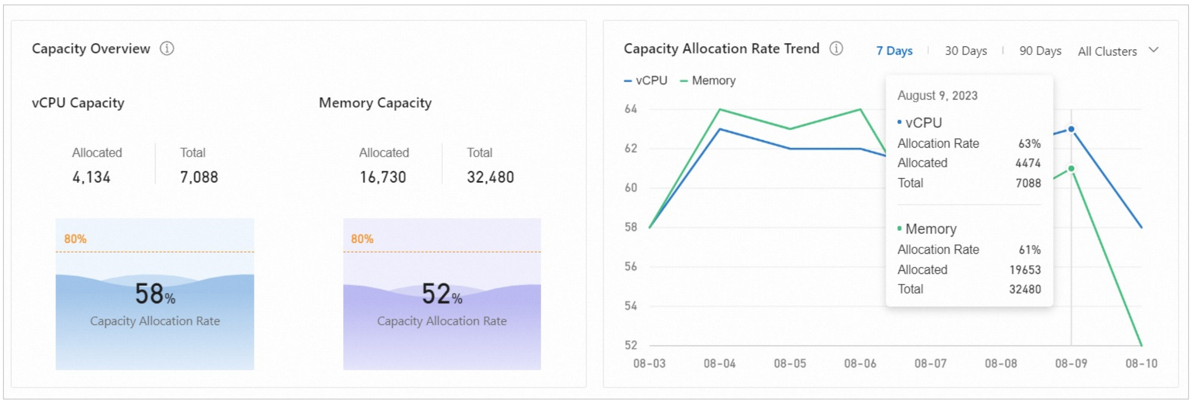
  - You can click **Day**, **Week**, or **Month** to view the available capacity of the service within the specified time range.
  - Click a capacity metric on the right side of a product name to view the corresponding capacity.
  - Move the pointer over a curve. Capacity information at a specific time point is displayed.

3.4.2. ECS capacity

By viewing the ECS capacity, you can learn about the capacity usage and usage trends of the current ECS product-related resources, so that you can perform related O&M operations based on your actual needs.

Procedure

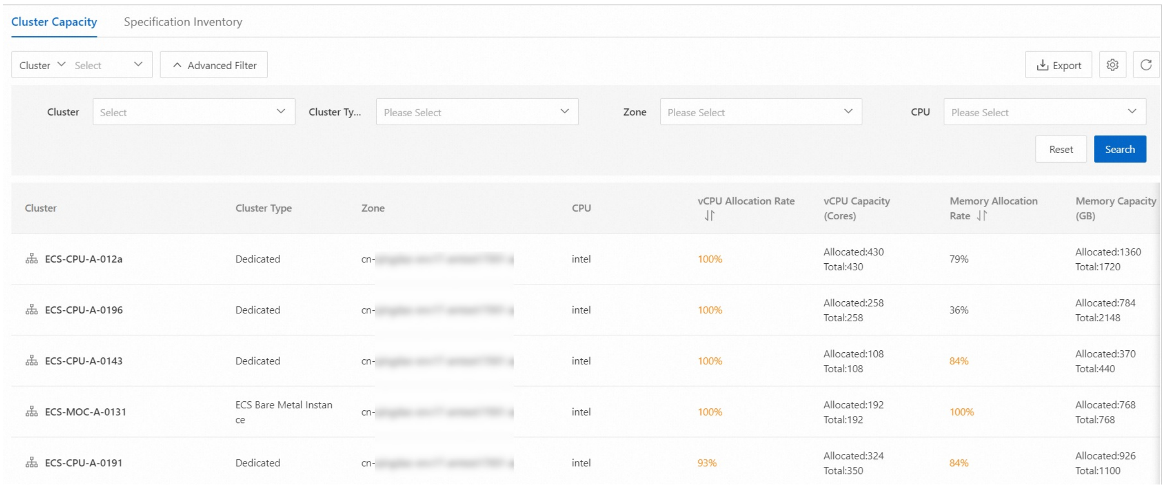
1. Log to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General O&M** > **Capacity** > **ECS Capacity**.
3. In the upper part of the page, view the **Capacity Overview** and **Capacity Allocation Rate Trend** of the ECS instance.
   - The **Capacity Overview** section displays the **vCPU Capacity** and **Memory Capacity** of all clusters, including the total amount, allocated capacity, and capacity allocation rate.
   - The **Capacity Allocation Rate Trend** section displays the trend charts of the vCPUs and memory allocation rates of all clusters or a single cluster in different time periods. Move the pointer over a node to view the data of the corresponding time node.



4. On the **Cluster Capacity** tab, click **Advanced Filter** to filter ECS instances by **Cluster**, **Cluster Type**, **Zone**, and **CPU Processor**.
   - Click the **vCPU Allocation Rate** or **Memory Allocation Rate** column. The capacity details list can be sorted in ascending or descending order.

> ⓘ **Note**
>
> When the distribution rate exceeds the water level warning threshold (80%), the value is highlighted. The water level warning threshold cannot be customized.

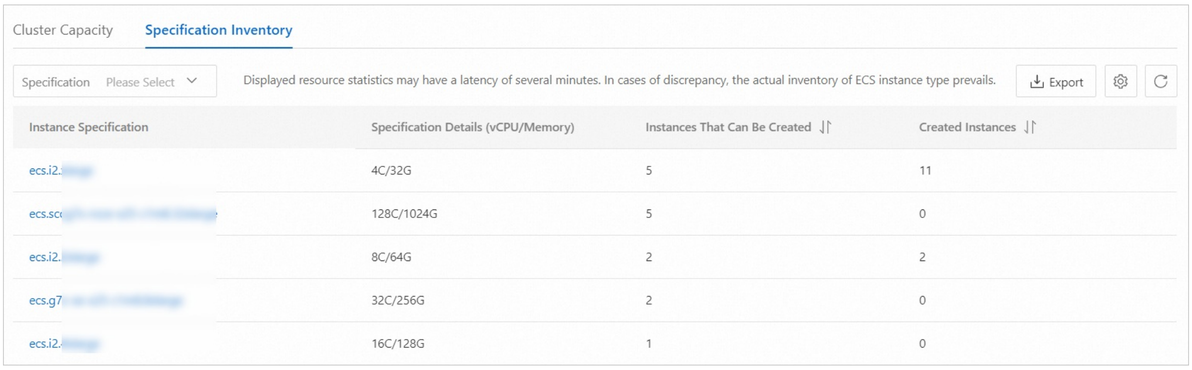
   - Click **Export** to export the cluster capacity data to your on-premises machine.



Cluster	Cluster Type	Zone	CPU	vCPU Allocation Rate	vCPU Capacity (Cores)	Memory Allocation Rate	Memory Capacity (GB)
ECS-CPU-A-012a	Dedicated	cn-[redacted]	intel	100%	Allocated:430 Total:430	79%	Allocated:1360 Total:1720
ECS-CPU-A-0196	Dedicated	cn-[redacted]	intel	100%	Allocated:258 Total:258	36%	Allocated:784 Total:2148
ECS-CPU-A-0143	Dedicated	cn-[redacted]	intel	100%	Allocated:108 Total:108	84%	Allocated:370 Total:440
ECS-MOC-A-0131	ECS Bare Metal Instance	cn-[redacted]	intel	100%	Allocated:192 Total:192	100%	Allocated:768 Total:768
ECS-CPU-A-0191	Dedicated	cn-[redacted]	intel	93%	Allocated:324 Total:350	84%	Allocated:926 Total:1100

5. On the **Inventory** tab in the lower part of the page, you can query the details of the instance type by **specification**. Fuzzy search is supported.
   - Click the **Created ()** or **Created ()** column. The list of instance types can be sorted in ascending or descending order.

- Click the name of the **instance type** to view the cluster details within the instance type.
- Click **Export** to export the specifications and inventory data to your on-premises machine.



Displayed resource statistics may have a latency of several minutes. In cases of discrepancy, the actual inventory of ECS instance type prevails.

Instance Specification	Specification Details (vCPU/Memory)	Instances That Can Be Created	Created Instances
ecs.i2.[redacted]	4C/32G	5	11
ecs.sc[redacted]	128C/1024G	5	0
ecs.i2.[redacted]	8C/64G	2	2
ecs.g7[redacted]	32C/256G	2	0
ecs.i2.[redacted]	16C/128G	1	0

3.4.3. SLB Capacity

You can view the Server Load Balancer (SLB) capacity to learn the usage and trend of SLB resources. This helps you perform O&M operations based on your business requirements.

Procedure

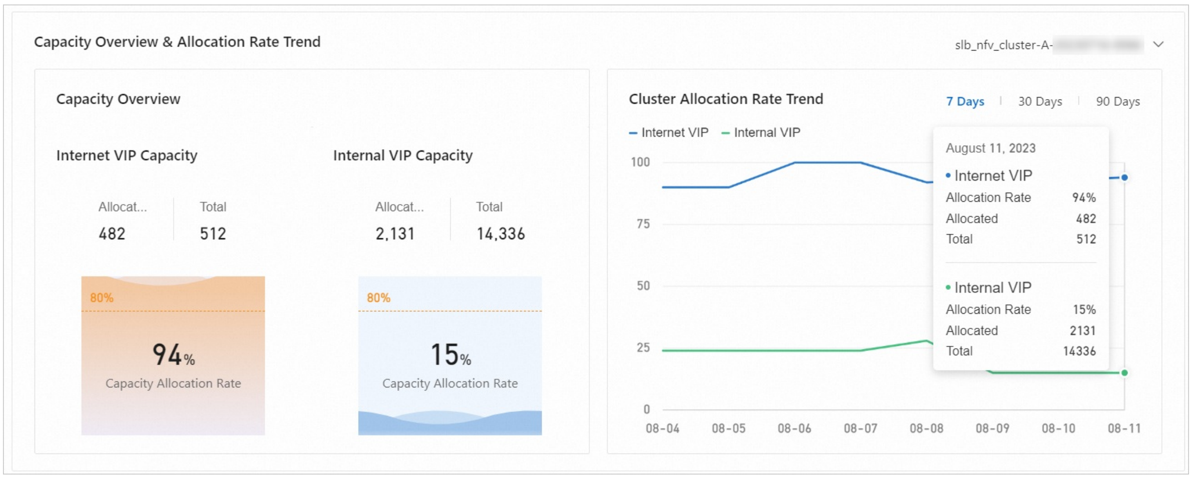
1. Go to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Capacity** > **SLB Capacity**.
3. In the upper-right corner of the page, select the target cluster to view the capacity data of different clusters.

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

4. In the upper part of the page, view the **Capacity Overview** and **Cluster Allocation Rate Trend** of the SLB instance.
   - The **Capacity Overview** section displays the **Internet VIP Capacity** and **Internal VIP Capacity** of the cluster. The information includes the total capacity, allocated capacity, and capacity allocation rate.

     > **Note**
     >
     > When the capacity allocation rate exceeds the warning threshold (80%), the value is highlighted. The warning threshold cannot be customized.

   - The **Cluster Allocation Rate Trend** section displays the trend charts of the allocation rates of public and internal VIPs in different time periods. Move the pointer over a node to view the data of the corresponding time node.


Capacity Overview & Allocation Rate Trend

slb_nfv_cluster-A-

Capacity Overview

Internet VIP Capacity

Allocat...	Total
482	512

94% Capacity Allocation Rate

Internal VIP Capacity

Allocat...	Total
2,131	14,336

15% Capacity Allocation Rate

Cluster Allocation Rate Trend

August 11, 2023

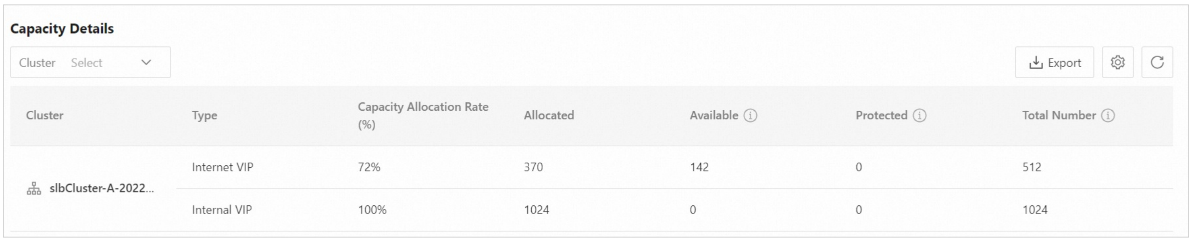
Internet VIP

Allocation Rate	94%
Allocated	482
Total	512

Internal VIP

Allocation Rate	15%
Allocated	2131
Total	14336

5. In the **Capacity Details** section, you can view the capacity details of the cluster by **Cluster**. Click **Export** to export the data to your computer.


Capacity Details

Cluster Select

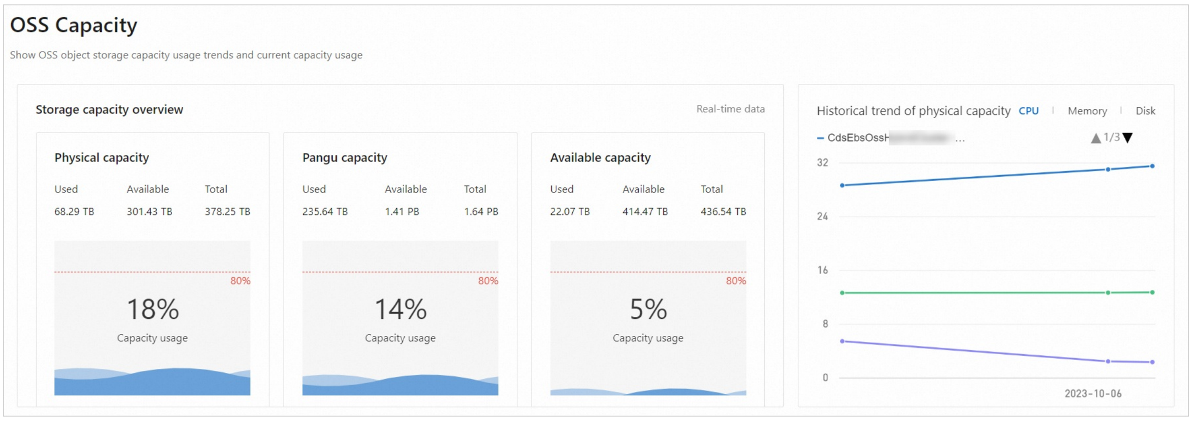
Cluster	Type	Capacity Allocation Rate (%)	Allocated	Available ⓘ	Protected ⓘ	Total Number ⓘ
slbCluster-A-2022...	Internet VIP	72%	370	142	0	512
	Internal VIP	100%	1024	0	0	1024

3.4.4. OSS capacity

You can view the Object Storage Service (OSS) capacity to learn the usage and availability of OSS resources. This helps you perform O&M operations based on your business requirements.

Procedure

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


OSS Capacity

Show OSS object storage capacity usage trends and current capacity usage

Storage capacity overview

Real-time data

Physical capacity

Used	Available	Total
68.29 TB	301.43 TB	378.25 TB

18% Capacity usage

Pangu capacity

Used	Available	Total
235.64 TB	1.41 PB	1.64 PB

14% Capacity usage

Available capacity

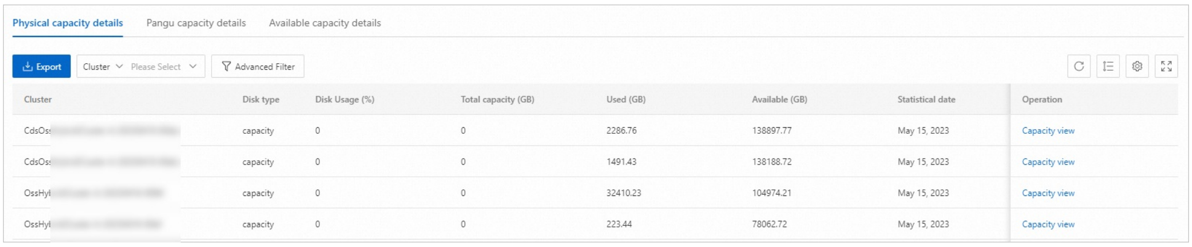
Used	Available	Total
22.07 TB	414.47 TB	436.54 TB

5% Capacity usage

Historical trend of physical capacity

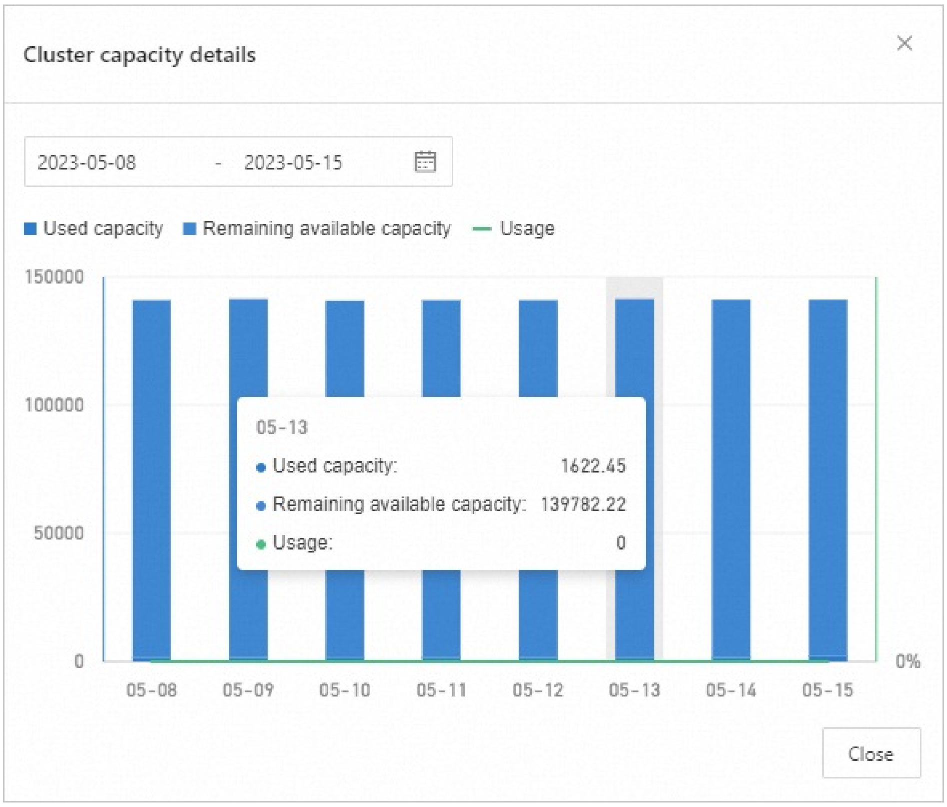
- In the left-side section of the **OSS Capacity** page, view the information about **Physical capacity**, **Pangu capacity**, and **Available capacity**.
- In the right-side section of the **OSS Capacity** page, view the trend charts of **Physical capacity**, **Pangu capacity**, and **Available capacity** in different dimensions. Move the pointer over a node to view the capacity data at a specific time point.

4. On the **Physical capacity details**, **Pangu capacity details**, and **Available capacity details** tabs in the lower part of the **OSS Capacity** page, filter the capacity details by **Cluster** or **Date**.



Cluster	Disk type	Disk Usage (%)	Total capacity (GB)	Used (GB)	Available (GB)	Statistical date	Operation
CdsOs[redacted]	capacity	0	0	2286.76	138897.77	May 15, 2023	Capacity view
CdsOs[redacted]	capacity	0	0	1491.43	138188.72	May 15, 2023	Capacity view
OssHy[redacted]	capacity	0	0	32410.23	104974.21	May 15, 2023	Capacity view
OssHy[redacted]	capacity	0	0	223.44	78062.72	May 15, 2023	Capacity view

5. Click **Capacity view** in the **Operation** column of the desired cluster to view the capacity trend chart of the cluster over a period of time. Move the pointer over the trend chart to view the capacity data at specific time points.



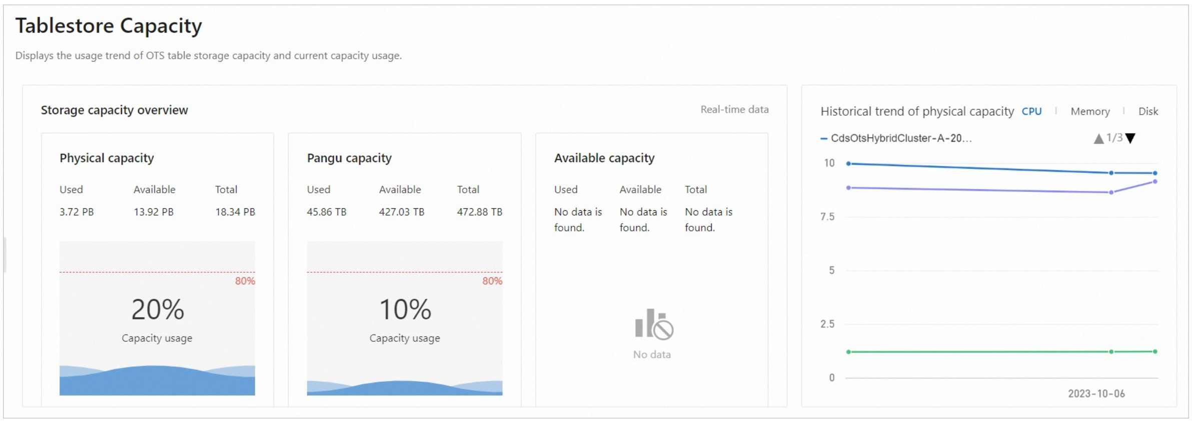
6. Click **Export** to export the capacity details to your computer.

3.4.5. Tablestore capacity

You can view the Tablestore capacity to learn the usage and availability of Tablestore resources. This helps you perform O&M operations based on your business requirements.

Procedure

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



Tablestore Capacity

Displays the usage trend of OTS table storage capacity and current capacity usage.

Storage capacity overview

Real-time data

Physical capacity

Used	Available	Total
3.72 PB	13.92 PB	18.34 PB

Pangu capacity

Used	Available	Total
45.86 TB	427.03 TB	472.88 TB

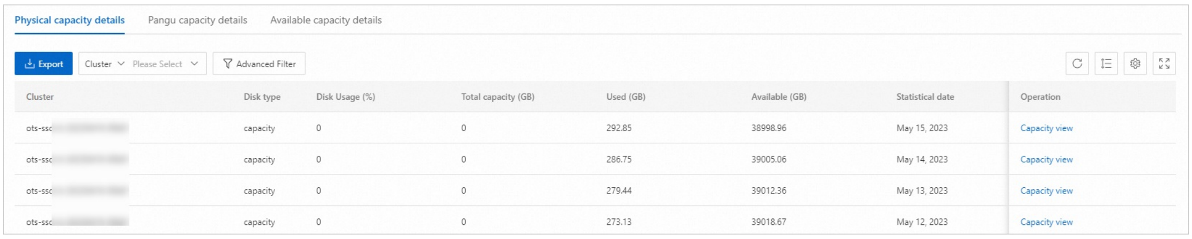
Available capacity

Used	Available	Total
No data is found.	No data is found.	No data is found.

No data
Historical trend of physical capacity
CPU
Memory
Disk
CdsOtsHybridCluster-A-20...
1/3
10
7.5
5
2.5
0
2023-10-06

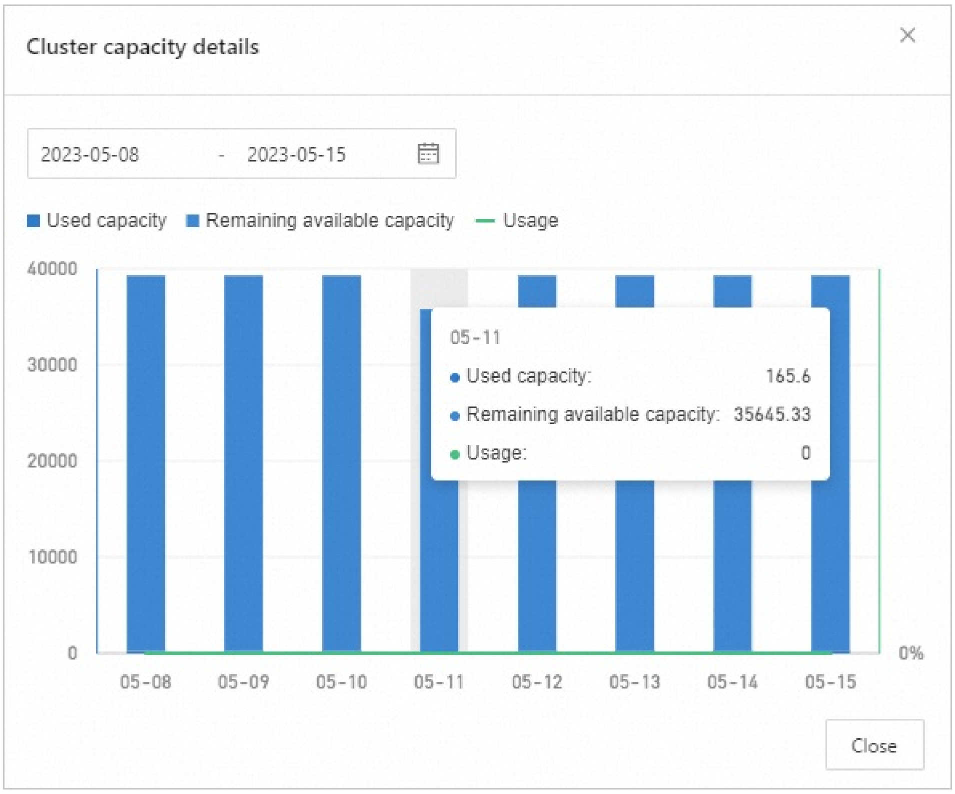
- On the **Tablestore Capacity** page, view the information about **Physical capacity**, **Pangu capacity**, and **Available capacity**.
- In the right-side section of the **Tablestore Capacity** page, view the trend charts of **Physical capacity**, **Pangu capacity**, and **Available capacity** in different dimensions. Move the pointer over a node to view the capacity data of multiple clusters at a specific time point.

4. On the **Physical capacity details**, **Pangu capacity details**, and **Available capacity details** tabs in the lower part of the **Tablestore Capacity** page, filter the capacity details by **Cluster** or **Date**.



Cluster	Disk type	Disk Usage (%)	Total capacity (GB)	Used (GB)	Available (GB)	Statistical date	Operation
ots-ssc[redacted]	capacity	0	0	292.85	38998.96	May 15, 2023	Capacity view
ots-ssc[redacted]	capacity	0	0	286.75	39005.06	May 14, 2023	Capacity view
ots-ssc[redacted]	capacity	0	0	279.44	39012.36	May 13, 2023	Capacity view
ots-ssc[redacted]	capacity	0	0	273.13	39018.67	May 12, 2023	Capacity view

5. Click **Capacity view** in the **Operation** column of the desired cluster to view the trend chart of the cluster over a period of time. Move the pointer over the trend chart to view the capacity data at specific time points.


Cluster capacity details

2023-05-08 - 2023-05-15

05-11
● Used capacity: 165.6
● Remaining available capacity: 35645.33
● Usage: 0

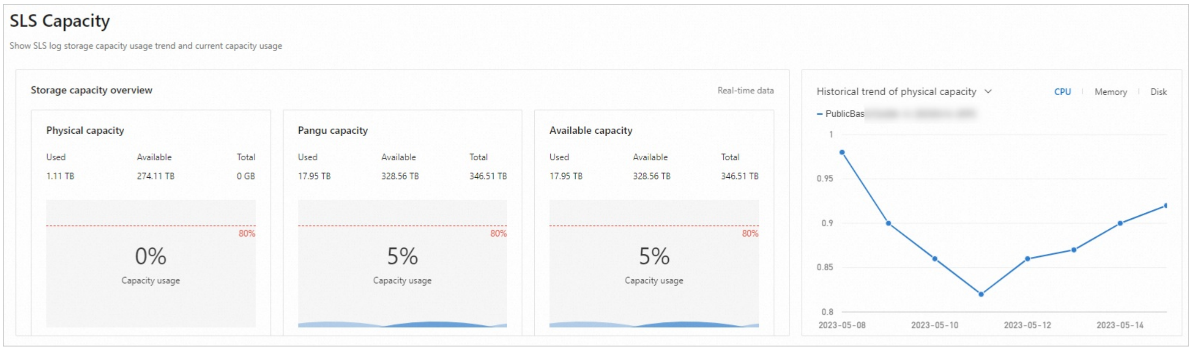
6. Click **Export** to export the capacity details to your computer.

3.4.6. Simple Log Service capacity

You can view the Simple Log Service capacity to learn the usage and availability of Simple Log Service resources. This helps you perform O&M operations based on your business requirements.

Procedure

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


SLS Capacity

Show SLS log storage capacity usage trend and current capacity usage

Storage capacity overview

Real-time data

Physical capacity

Used	Available	Total
1.11 TB	274.11 TB	0 GB

0% Capacity usage

Pangu capacity

Used	Available	Total
17.95 TB	328.56 TB	346.51 TB

5% Capacity usage

Available capacity

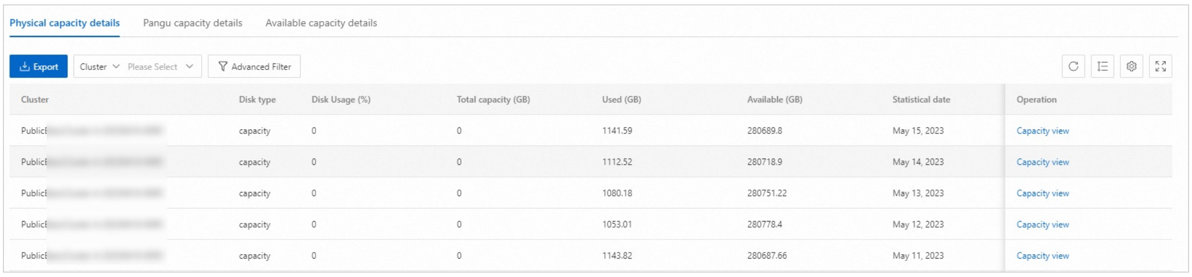
Used	Available	Total
17.95 TB	328.56 TB	346.51 TB

5% Capacity usage

Historical trend of physical capacity

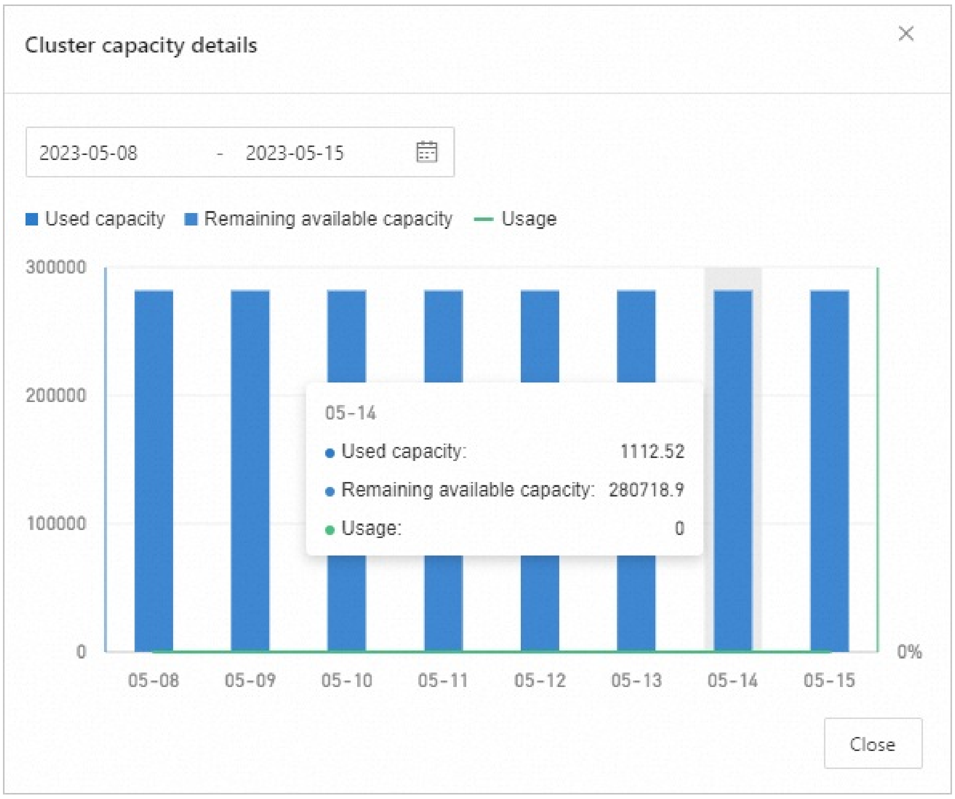
- On the **SLS Capacity** page, view the information about **Physical capacity**, **Pangu capacity**, and **Available capacity**.
- In the right-side section of the **SLS Capacity** page, view the trend charts of **Physical capacity**, **Pangu capacity**, and **Available capacity** in different dimensions. Move the pointer over a node to view the capacity data at a specific time point.

4. On the **Physical capacity details**, **Pangu capacity details**, and **Available capacity details** tabs in the lower part of the **SLS Capacity** page, filter the capacity details by **Cluster** or **Date**.



Cluster	Disk type	Disk Usage (%)	Total capacity (GB)	Used (GB)	Available (GB)	Statistical date	Operation
Public[redacted]	capacity	0	0	1141.59	280689.8	May 15, 2023	Capacity view
Public[redacted]	capacity	0	0	1112.52	280718.9	May 14, 2023	Capacity view
Public[redacted]	capacity	0	0	1080.18	280751.22	May 13, 2023	Capacity view
Public[redacted]	capacity	0	0	1053.01	280778.4	May 12, 2023	Capacity view
Public[redacted]	capacity	0	0	1143.82	280687.66	May 11, 2023	Capacity view

5. Click **Capacity view** in the **Operation** column of the desired cluster to view the trend chart of the cluster over a period of time. Move the pointer over the trend chart to view the capacity data at specific time points.



Cluster capacity details

2023-05-08 - 2023-05-15

05-14
- Used capacity: 1112.52
- Remaining available capacity: 280718.9
- Usage: 0

6. Click **Export** to export the capacity details to your computer.

3.4.7. EBS capacity

By viewing the EBS Elastic Block Storage capacity, you can learn about the capacity usage and usage trends of EBS-related resources, so that you can perform relevant O&M operations based on your actual needs.

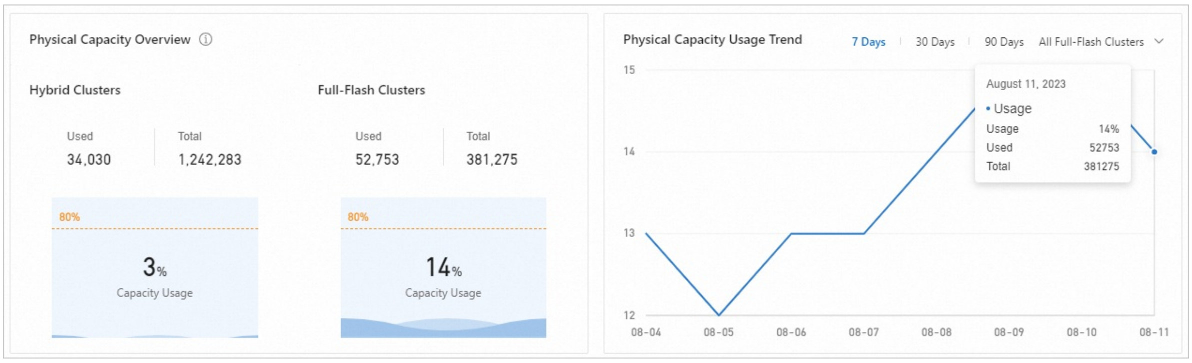
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General O&M** > **Capacity Management** > **EBS Capacity**.
3. In the upper part of the page, view **Physical Capacity Overview** and **Physical Capacity Utilization Trend**.

- The **Physical Capacity Overview** section displays the capacity of **Hybrid Flash Clusters** and **Full Flash Clusters**, including the total capacity, used capacity, and capacity utilization.

  > **Note**
  >
  > When the capacity usage exceeds the warning threshold (80%), the value is highlighted. The warning threshold cannot be customized.

- **Physical Capacity Utilization Trend** displays the trend chart of the physical capacity utilization of all flash clusters, all hybrid flash clusters, or a single cluster in different time periods. Move the pointer over a node to view the data of the corresponding time node.



Physical Capacity Overview

Hybrid Clusters

Used	Total
34,030	1,242,283

3% Capacity Usage

Full-Flash Clusters

Used	Total
52,753	381,275

14% Capacity Usage

Physical Capacity Usage Trend

7 Days | 30 Days | 90 Days | All Full-Flash Clusters

August 11, 2023

• Usage

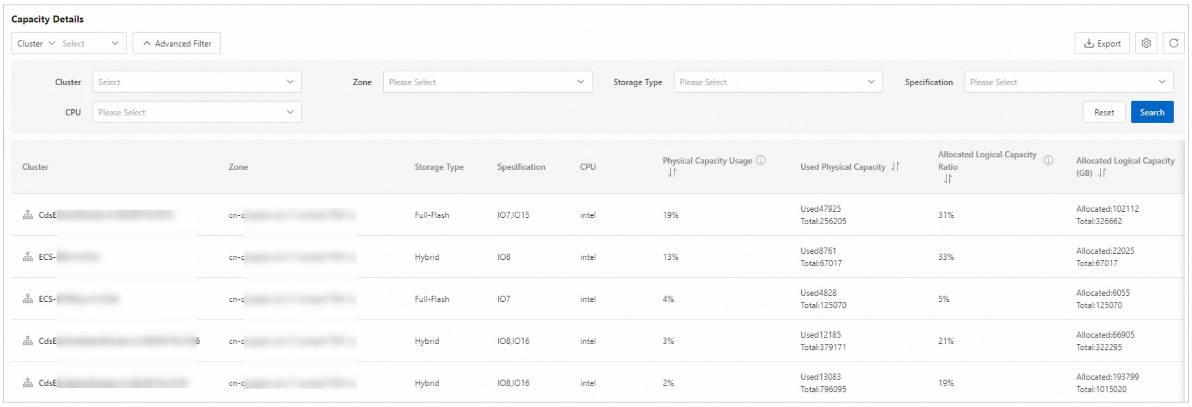
Usage	14%
Used	52753
Total	381275

4. In the **Capacity Details** section, you can view the capacity details of the cluster by **Cluster**, **Zone**, **Storage Type**, **Specification**, and **CPU /Processor**.

   - Click the **Physical Capacity Usage**, **Logical Capacity Allocation Rate**, or **Logical Capacity Allocation Amount** column in the **Physical Capacity Usage**,. The list can be sorted in ascending or descending order.

     > **Note**
     >
     > - Physical capacity: The physical capacity of the disk is occupied after data is actually written to it.
     > - Logical capacity: After a disk is created, it occupies the logical capacity.

   - Click **Export** to export the capacity details to your computer.



Capacity Details

Cluster Select | Advanced Filter | Export

Cluster: Select | Zone: Please Select | Storage Type: Please Select | Specification: Please Select

CPU: Please Select | Reset | Search

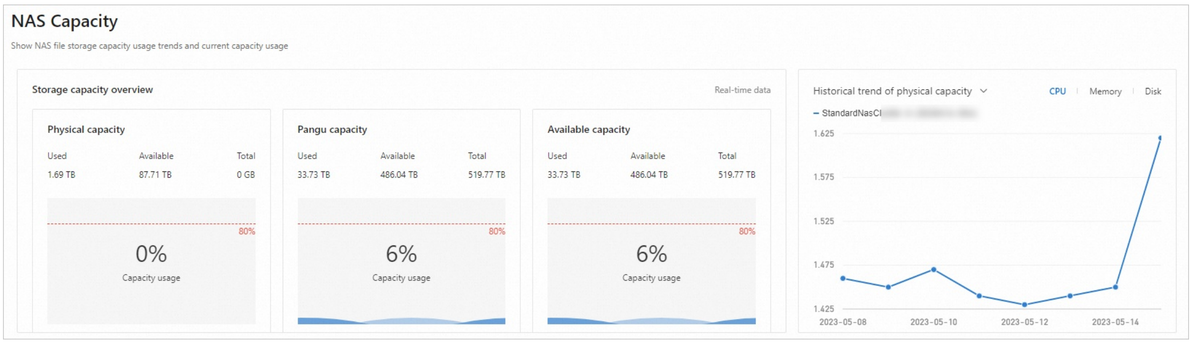
Cluster	Zone	Storage Type	Specification	CPU	Physical Capacity Usage	Used Physical Capacity	Allocated Logical Capacity Ratio	Allocated Logical Capacity (GB)
CdsE[redacted]	cn-c[redacted]	Full-Flash	IO7,IO15	intel	19%	Used47925 Total:256205	31%	Allocated:102112 Total:326662
ECS-[redacted]	cn-c[redacted]	Hybrid	IO8	intel	13%	Used8761 Total:67017	33%	Allocated:22025 Total:67017
ECS-[redacted]	cn-c[redacted]	Full-Flash	IO7	intel	4%	Used4828 Total:125070	5%	Allocated:6055 Total:125070
CdsE[redacted]6	cn-c[redacted]	Hybrid	IO8,IO16	intel	3%	Used12185 Total:379171	21%	Allocated:66905 Total:322295
CdsE[redacted]	cn-c[redacted]	Hybrid	IO8,IO16	intel	2%	Used13083 Total:796095	19%	Allocated:193799 Total:1015020

3.4.8. 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 the NAS capacity.



NAS Capacity

Show NAS file storage capacity usage trends and current capacity usage

Storage capacity overview

Real-time data

Physical capacity

Used	Available	Total
1.69 TB	87.71 TB	0 GB

80%

0%

Capacity usage

Pangu capacity

Used	Available	Total
33.73 TB	486.04 TB	519.77 TB

80%

6%

Capacity usage

Available capacity

Used	Available	Total
33.73 TB	486.04 TB	519.77 TB

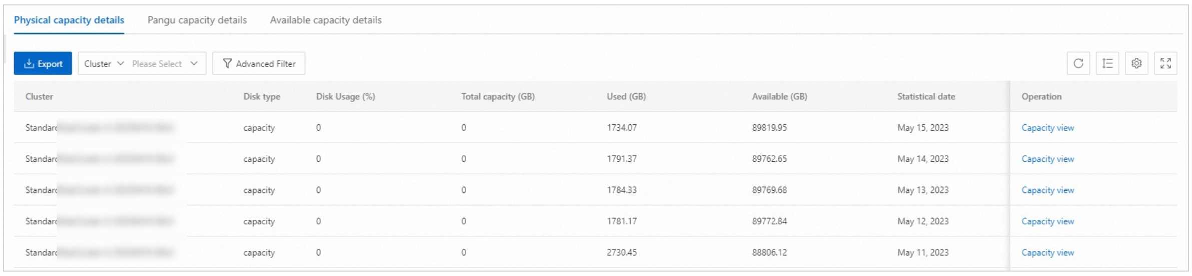
80%

6%

Capacity usage

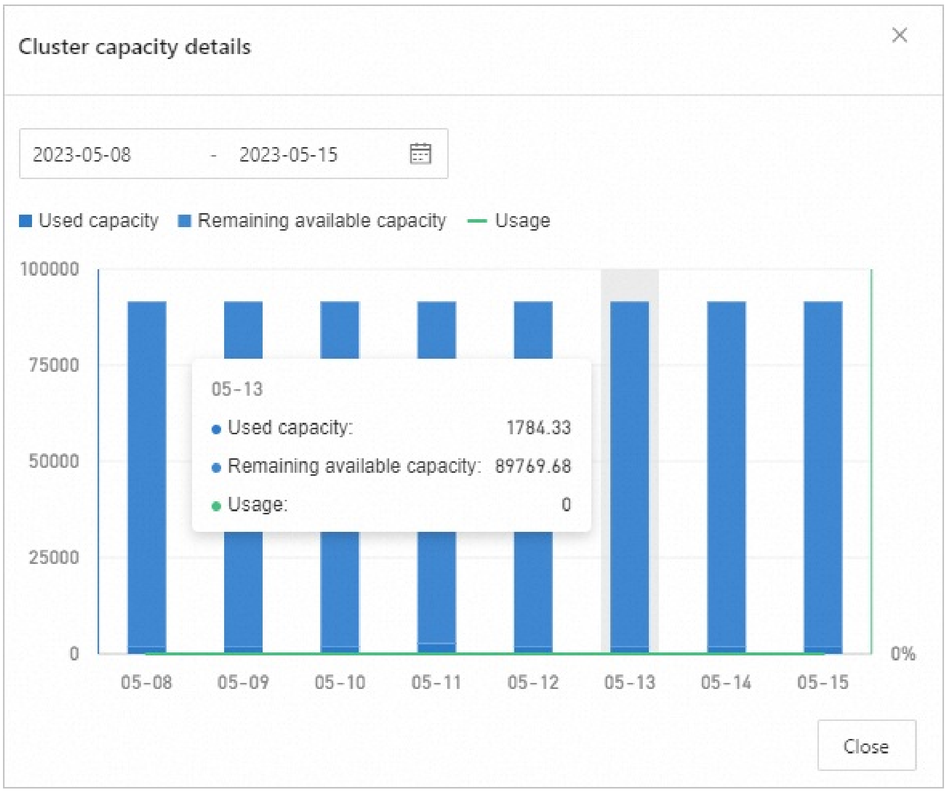
   - On the **NAS Capacity** page, view the information about**Physical capacity**, **Pangu capacity**, and **Available capacity**.
   - In the right-side section of the **NAS Capacity** page, view the trend charts of **Physical capacity**, **Pangu capacity**, and **Available capacity** in different dimensions. Move the pointer over a node to view the capacity data of different clusters at a specific time point.

4. On the **Physical capacity details**, **Pangu capacity details**, and **Available capacity details** tabs in the lower part of the **NAS Capacity** page, filter the capacity details by **Cluster** or **Date**.



Cluster	Disk type	Disk Usage (%)	Total capacity (GB)	Used (GB)	Available (GB)	Statistical date	Operation
Standar[redacted]	capacity	0	0	1734.07	89819.95	May 15, 2023	Capacity view
Standar[redacted]	capacity	0	0	1791.37	89762.65	May 14, 2023	Capacity view
Standar[redacted]	capacity	0	0	1784.33	89769.68	May 13, 2023	Capacity view
Standar[redacted]	capacity	0	0	1781.17	89772.84	May 12, 2023	Capacity view
Standar[redacted]	capacity	0	0	2730.45	88806.12	May 11, 2023	Capacity view

5. Click **Capacity view** in the **Operation** column of the desired cluster to view the trend chart of the cluster over a period of time. Move the pointer over the trend chart to view the capacity data at specific time points.



6. Click **Export** to export the capacity details to your computer.

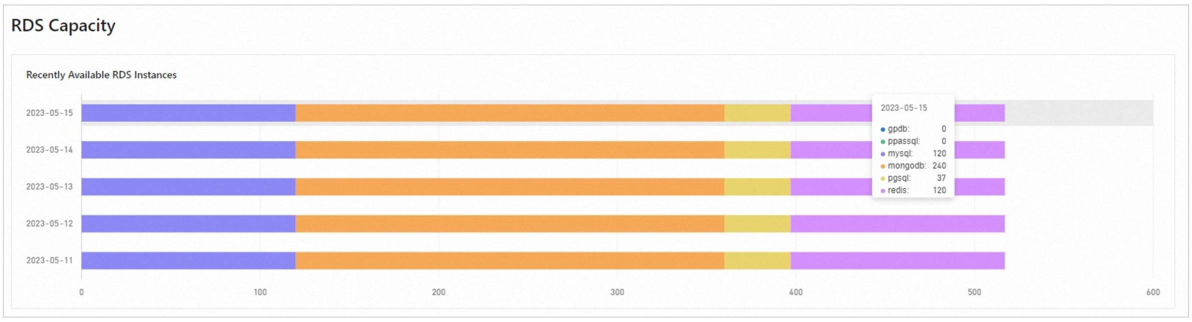
3.4.9. RDS capacity

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

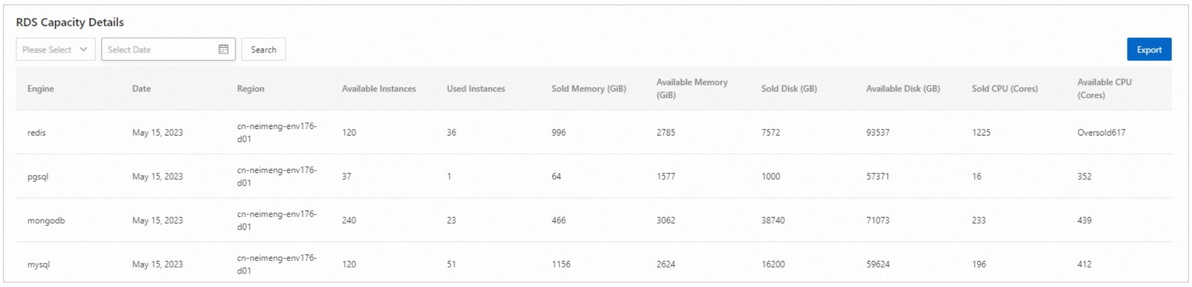
Procedure

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

   The **Recently Available RDS Instances** section shows the capacities of RDS of different engines within the last five days. Different colors indicate RDS of different engines. You can move the pointer over the bar to view the specific capacity data of RDS of different engines.



4. In the **RDS Capacity Details** section, query RDS capacities by **Engine** and **Date**.



Engine	Date	Region	Available Instances	Used Instances	Sold Memory (GiB)	Available Memory (GiB)	Sold Disk (GB)	Available Disk (GB)	Sold CPU (Cores)	Available CPU (Cores)
redis	May 15, 2023	cn-neimeng-env176-d01	120	36	996	2785	7572	93537	1225	Oversold617
pgsql	May 15, 2023	cn-neimeng-env176-d01	37	1	64	1577	1000	57371	16	352
mongodb	May 15, 2023	cn-neimeng-env176-d01	240	23	466	3062	38740	71073	233	439
mysql	May 15, 2023	cn-neimeng-env176-d01	120	51	1156	2624	16200	59624	196	412

5. Click **Export** to export the capacity details to your computer.

3.5. Change Management

This topic describes the modules related to change management.

Modules

Module	Description
Operation Orchestration Service	This module automates O&M for data centers. GUI-based operations are provided to help you perform 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.
Log Cleanup	This module clears specific logs in specific containers or physical servers.
Security O&M	This module supports black-screen logons, remote O&M, and high-risk operation interception, approval, and audit.
Plan Center	This module manages preset O&M actions.
Process Approval	This module provides approval and management features for O&M workflows.

3.5.1. Log cleanup

This topic describes the modules of the log cleanup module. This module allows you to clear logs from a specified container (Docker) or physical machine (virtual machine or bare metal).

Modules

Module	Description
Rules	You can manage log cleanup rules by performing operations such as rule import, query, modification, export, and deletion.

Plans	You can execute log cleanup plans, including obtaining the usage data of containers or physical servers and clearing log.
Records	You can view detailed log cleanup records.

3.5.1.1. Rule management

This topic describes how to import log cleanup rules. If log cleanup rules for containers or physical servers are available on your on-premises machine, you can batch import the log cleanup rules. This topic also describes operations that you can perform on the imported rules.

Background information

- Imported rules are incrementally added.
- You must check the values of the Product, Service, ServerRole, SrcPath, MatchFile, Threshold, and Method parameters to determine whether a cleanup rule already exists. If all values in the environment are the same as the values that are specified in the rule that you want to import, the rule already exists. If a rule already exists, the rule cannot be imported.
- Before you import a rule, you must contact technical support to obtain an encryption sequence.
- After you import a rule, special characters such as spaces, carriage returns, line feeds, and tabs in the rule are automatically deleted.
- The maximum disk usage range that is 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 the rule. We recommend that you set the Maximum Disk Usage parameter to 75%.
- Make sure that the cleanup methods that are specified by the rules that you want to import are tested and can be executed as expected. Otherwise, exceptions may occur when you use the methods to clear 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**. Click **Select a file to upload** . Then, select the XLS or XLSX file that you want to import and click **Open** to import log cleanup rules.

   After you import rules, the corresponding execution plans are asynchronously generated.

Related operations

Operation	Description

Export log cleanup rules	You can batch export multiple log cleanup rules for containers or physical servers. 1. Click the **Container** tab or the **Physical Machines** tab. 2. To export log cleanup rules for containers or physical servers, perform the following operations: ◦ Click **Export** to export all log cleanup rules. ◦ Click **Advanced Filter** and select a product from the **Product** drop-down list, a service from the **Service** drop-down list, and a server role from the **Server Roles** drop-down list. Then, click **Search**. In the search result, select the cleanup rules that you want to export and click **Export**. **Note** By default, no options are available in the Product, Service, and Service role drop-down lists. The first time you specify the fields, you must enter a product, service, and server role and select cleanup rules based on search results. In subsequent queries, the system shows all available options in the drop-down lists.

Modify log cleanup rules	You can modify log cleanup rules based on your business requirements. 1. Click the **Container** tab or the **Physical Machines** tab. 2. Find the log cleanup rule that you want to modify and click**Modify** in the **Actions** column. 3. In the panel that appears, configure the **Maximum Disk Usage** parameter and specify whether to enable **Automatic Deletion**. **Note** ◦ The maximum disk usage range that is 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** parameter to 75%. ◦ You can specify whether to enable the automatic deletion feature for a log cleanup rule by turning on or turning off the switch in the **Automatic Deletion** column of the log cleanup rule on the **Rules** page. You can also specify whether to enable the automatic deletion feature for multiple cleanup rules. 4. Click **OK**. **Note** • Select multiple log cleanup rules and click**Enable Automatic Clearance** or **Disable Automatic Clearance** to enable or disable the automatic deletion feature for the log cleanup rules at the same time. • After you modify a log cleanup rule, the execution plans for the rule are not modified. At 02:00:00 every day, the system cleans up existing execution plans and generates new execution plans based on the current log cleanup rules.

Delete log cleanup rules	You can delete log cleanup rules based on your business requirements 1. Click the **Container** tab or the **Physical Machines** tab. 2. Find the log cleanup rule that you want to delete and click**Delete** in the **Actions** column. 3. Read the message that appears and click **OK**. **Note** After you delete a log cleanup rule, the execution plans for the rule are not deleted. At 02:00:00 every day, the system cleans up existing execution plans and generates new execution plans based on the current log cleanup rules.
Obtain execution plans	1. Click the **Containers** or **Physical Machines** tab. 2. Find the log cleanup rule that you want to manage and click**Execution Plans** in the **Actions** column. On the **Execution Plans** page, view the execution plans of the cleanup rule.

3.5.1.2. Plans

This topic describes the execution plans of log cleanup rules, including how to query the disk usage of containers or physical machines and how to clear logs in execution plans.

Procedure

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, filter plans by **Product**, **Service**, and **Service role**.

   > **Note**
   >
   > By default, no options are available in the Product, Service, and Service role drop-down lists. The first time you specify the fields, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system displays all available options in the drop-down lists.

6. Perform the following operations to query the disk usage of containers or physical machines:
   - Find the execution plan that you want to manage and click **Query Usage** in the **Actions** column. In the message that appears, click **OK**. Then, refresh the page and view the disk usage in the **Disk Usage** column.
   - Select the execution plans that you want to manage and click **Batch Query Usage** in the lower-left part of the page. In the message that appears, click **OK**. Then, refresh the page and view the disk usage in the **Disk Usage** column.
7. Perform the following operations to clear logs in execution plans:
   - Find the execution plan that you want to manage and click **Execute Clearance** in the **Actions** column. In the message that appears, click **OK**.

- Select the execution plans that you want to manage and click **Batch Clear**. In the message that appears, click **OK**.

> **Note**
>
> The log cleanup operation is an asynchronous operation. If you want to view the log cleanup results, go to the **Records** page.

8. Find the execution plan that you want to manage and click **Cleanup Records** in the **Actions** column. The **Records** page appears.

3.5.1.3. Records

This topic describes how to view the detailed records of log cleanup operations.

Procedure

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. View the following information at the top of the page.
   - Each time you perform a log cleanup operation, the values of **Clear Operations**, **Server Roles**, and **Machines** are increased by one.
   - The value of **Log Files to clear** shows the number of log files that match all the available cleanup rules and that can be cleaned up, rather than the number of log files that have been cleaned up.
   - The value of **Cleared Capacity (GB)** shows the accumulated available space after you clean up logs.
5. (Optional) In the upper part of the tab, filter records by **Product**, **Service**, and **Service role**.

> **Note**
>
> By default, no options are available in the Product, Service, and Service role drop-down lists. The first time you specify the fields, you must enter a product, service, and server role and select the corresponding search result. In subsequent queries, the system displays all available options in the drop-down lists.

6. Click **View Details** in the **View Details** column of the desired cleanup record to view the detailed cleanup information.

3.5.2. Security O&M

This topic describes the modules of the Security O&M module.

Modules

Module	Description

Fast Arrival	You can log on to a virtual machine, host, container, or switch in the Apsara Stack environment and run commands to perform operations. You can also view environment metadata, OOB information, and cluster configurations.
Audit	You can view command operation records, file upload and download records, authorization information, and video playbacks on the fast arrival feature.
Rules	This module provides features such as high-risk command interception, double-verification prompt, and approved rule management.
Settings	When a project is connected to Apsara Stack Online, you can use this module to configure the worker IP address and port number that Apsara Uni-manager Operations Console needs to access and the IP address of the remote operations center that is allowed access.

3.5.2.1. Fast arrival

You can log on to machines in the Apsara Stack environment such as virtual machines (VMs), hosts, containers, and switches and run commands to perform operations. You can also view environment metadata, out-of-band (OOB) information, and cluster configurations.

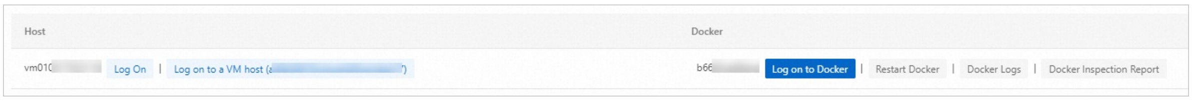
Server role logon

You can log on to a VM, host, or container where a server role is deployed to perform related operations.

Procedure

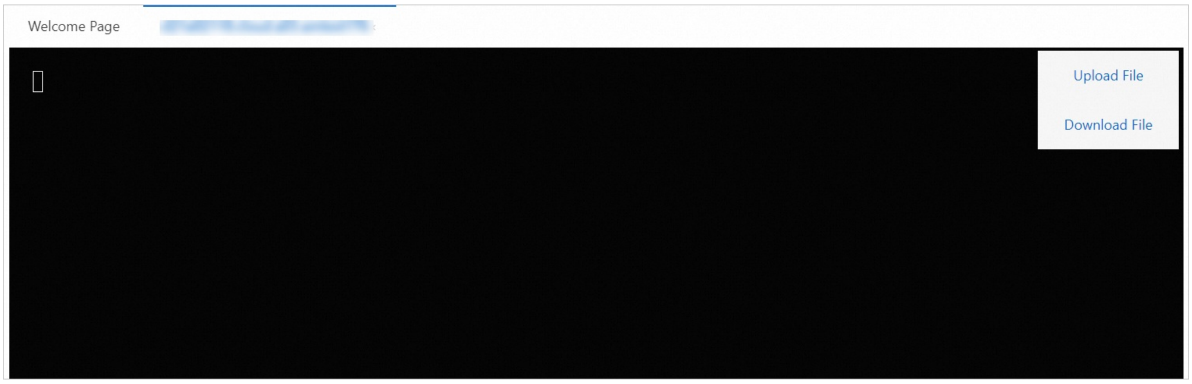
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Security O&M**.

   By default, the **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Select a server role name from the **Server Role** drop-down list. Fuzzy search is supported.
4. In the **Host** column, click a logon option to log on to the VM or host where the server role is deployed.
   - **Login**: log on to the VM where the server role is deployed.
   - **Log on to a VM host** : log on to the host of the VM where the server role is deployed.



Host	Docker
vm010[redacted] Log On | Log on to a VM host ([redacted])	b66[redacted] Log on to Docker | Restart Docker | Docker Logs | Docker Inspection Report

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



- Click **Upload** in the upper-right corner of the CLI window. You can use one of the following methods to upload a file:
  - 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**.
- Click **Download File** in the upper-right corner of the CLI window. The **Download File** dialog box appears. Configure the **File Directory** and **File Name** parameters and then click **Download** to download the file to the default download folder used by your local browser.

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

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

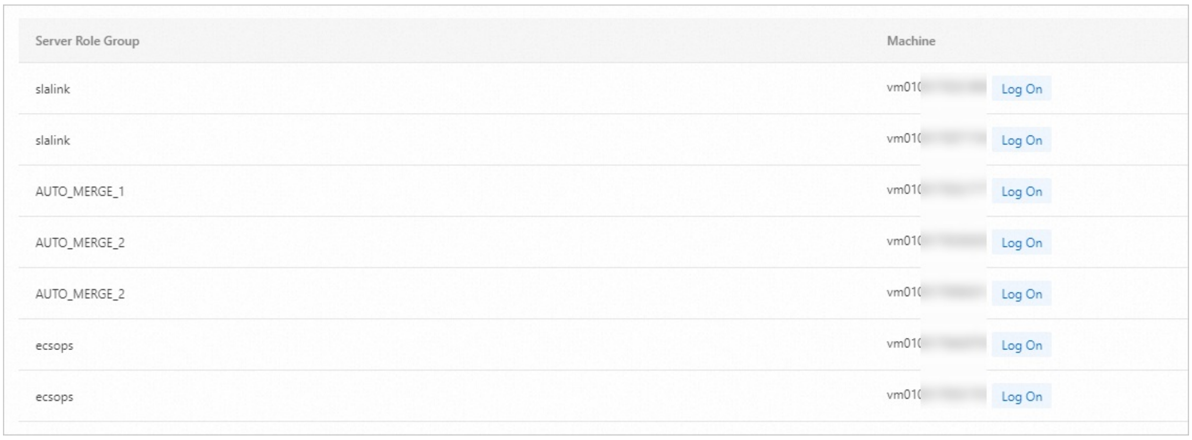
Server role group logon

You can log on to the VM where a server role in the server role group is deployed to perform related operations.

Procedure

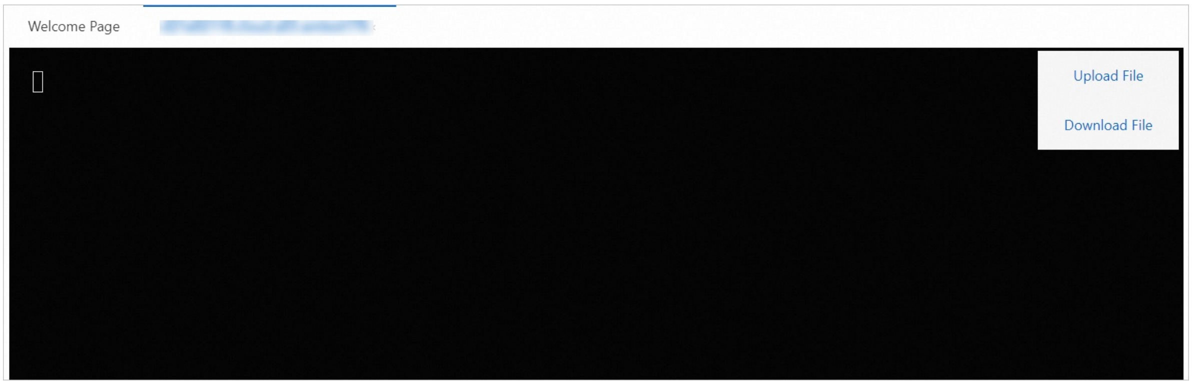
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Security O&M**.

   By default, the **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Click the **Server Role Group Login** tab.
4. Select a product and a server role group of the product from the **Cluster** drop-down list. Fuzzy search is supported. The server roles that are included in the group are displayed in the lower part of the page.
5. Find a server role and click **Log On** in the **Machine** column to log on to the VM on which the server role is deployed.



Server Role Group	Machine
slalink	vm010[redacted] Log On
slalink	vm010[redacted] Log On
AUTO_MERGE_1	vm010[redacted] Log On
AUTO_MERGE_2	vm010[redacted] Log On
AUTO_MERGE_2	vm010[redacted] Log On
ecsops	vm010[redacted] Log On
ecsops	vm010[redacted] Log On

6. After you log on to the VM, enter Linux commands in the CLI window to perform related operations.



   - Click **Upload** in the upper-right corner of the CLI window. You can use one of the following methods to upload a file:
     - 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**.
   - Click **Download File** in the upper-right corner of the CLI window. The **Download File** dialog box appears. Configure the **File Directory** and **File Name** parameters and then click **Download** to download the file to the default download folder used by your local browser.

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

Environment metadata query

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 **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Click the **Environment Metadata Query** tab.

4. Select a service name from the **Service** drop-down list. Fuzzy search is supported. The metadata of the service registered in Apsara Infrastructure Management is displayed in the lower part of the page.

   > **Note**
   >
   > You can also enter a keyword in the field above the displayed metadata to filter metadata.

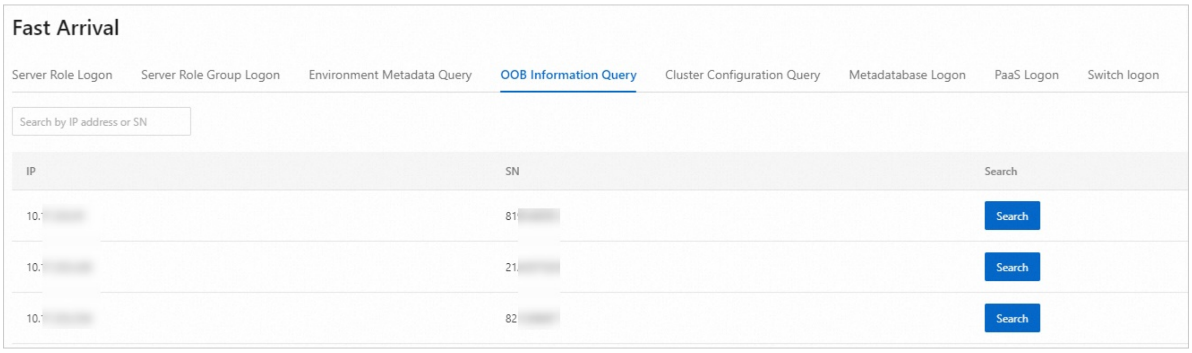
OOB information query

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 **General** > **Changes** > **Security O&M**.

   By default, the **Server Role Logon** tab of the **Fast Arrival** 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.



IP	SN	Search
10.[redacted]	81[redacted]	Search
10.[redacted]	21[redacted]	Search
10.[redacted]	82[redacted]	Search

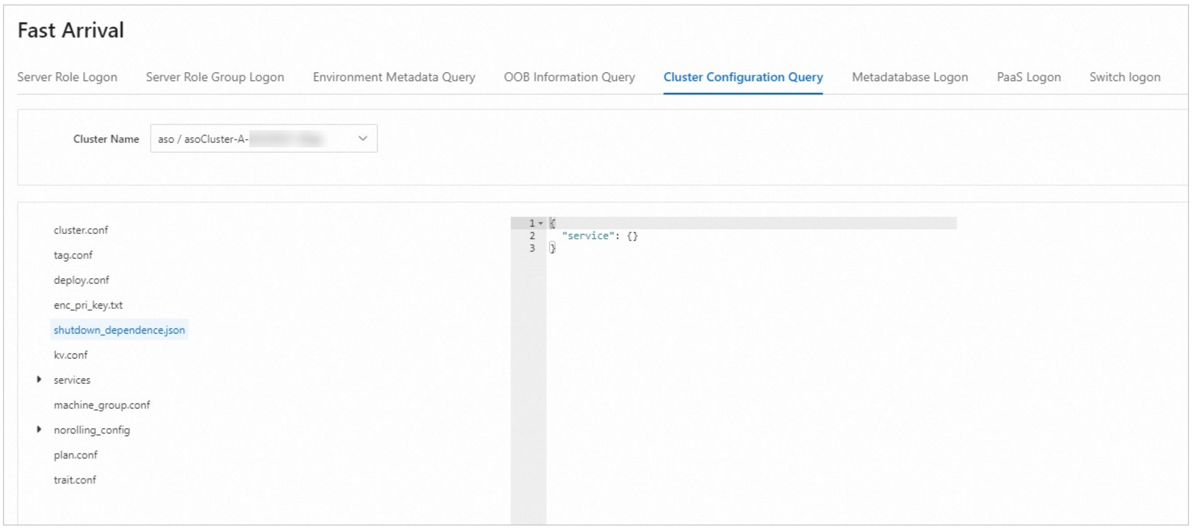
Cluster configuration query

You can query 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 **General** > **Changes** > **Security O&M**.

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



Fast Arrival

Cluster Name: aso / asoCluster-A-[redacted]

```
{
  "service": {}
}
```

5. Click a configuration file on the left to view its details on the right.

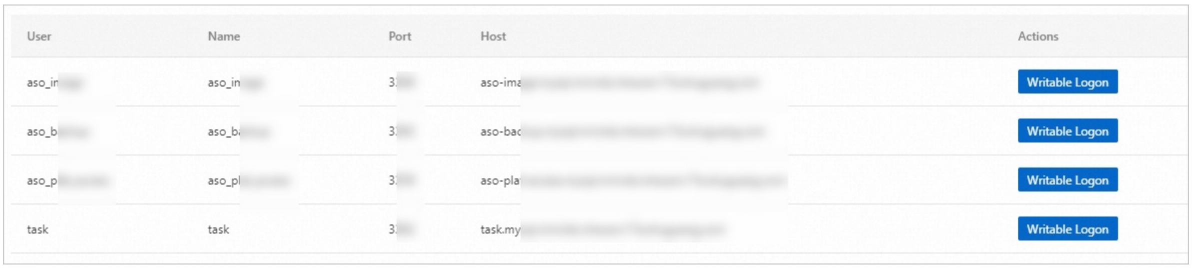
Metadatabase logon

You can log on to a metadatabase that is used by the server role of the service and perform related operations.

Procedure

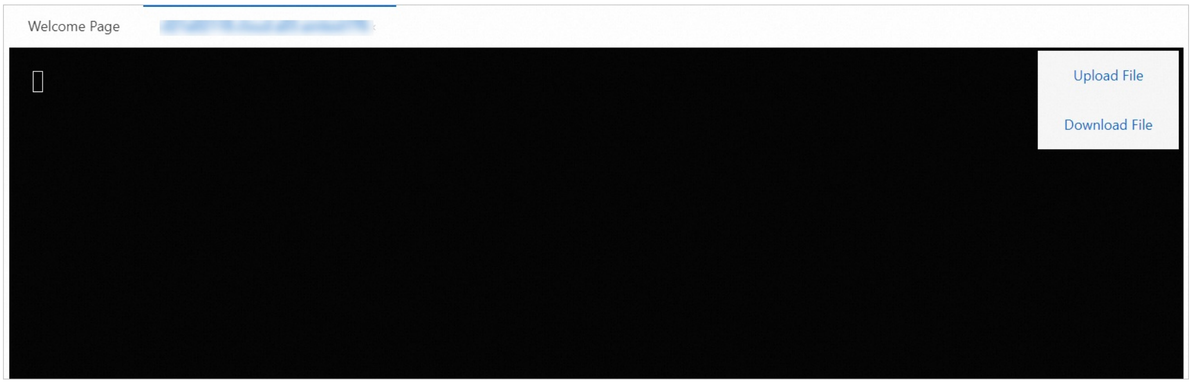
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Security O&M**.

   By default, the **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Click the **Metadatabase Logon** tab.
4. Select a service name from the **Service** drop-down list.
5. In the lower part of the page, Find the desired database in the metadatabases used by all server roles of the service and click **Writable Logon** in the **Actions** column.



User	Name	Port	Host	Actions
aso_in[redacted]	aso_in[redacted]	3[redacted]	aso-ima[redacted]	Writable Logon
aso_b[redacted]	aso_b[redacted]	3[redacted]	aso-bac[redacted]	Writable Logon
aso_p[redacted]	aso_pl[redacted]	3[redacted]	aso-pla[redacted]	Writable Logon
task	task	3[redacted]	task.my[redacted]	Writable Logon

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



- Click **Upload** in the upper-right corner of the CLI window. You can use one of the following methods to upload a file:
  - 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**.
- Click **Download File** in the upper-right corner of the CLI window. The **Download File** dialog box appears. Configure the **File Directory** and **File Name** parameters and then click **Download** to download the file to the default download folder used by your local browser.

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

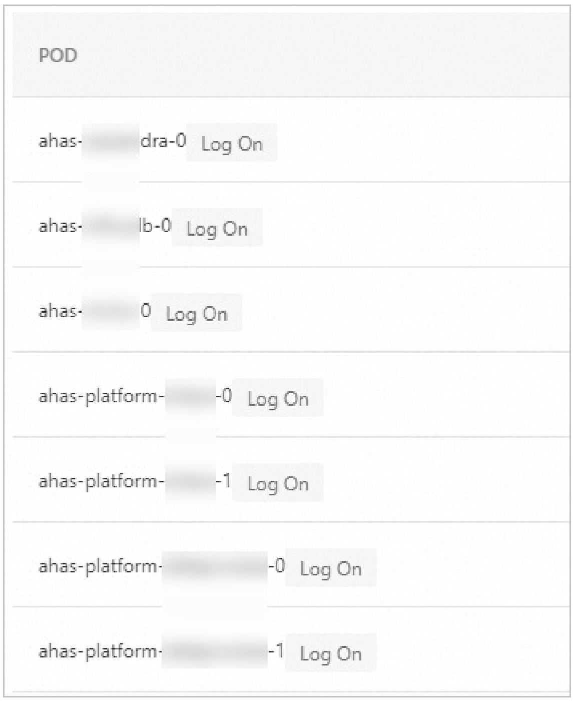
PaaS logon

You can log on to the VM where the pod resides to perform O&M operations.

Procedure

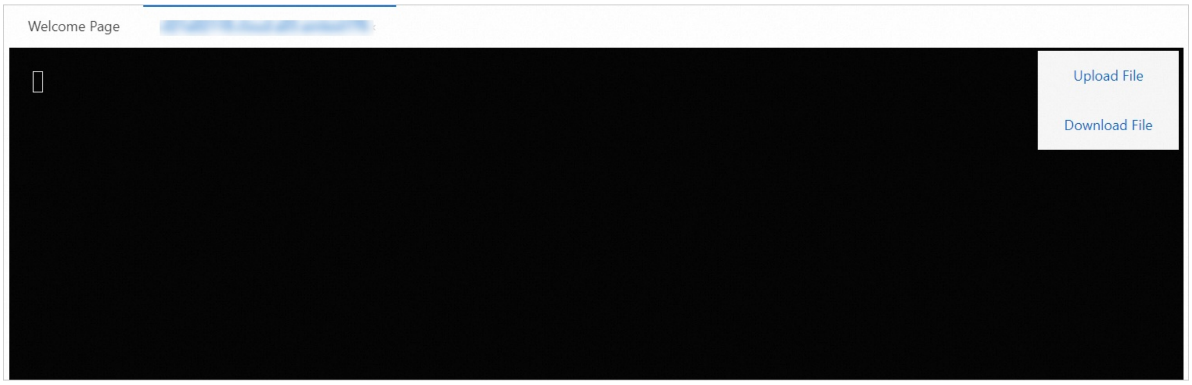
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Security O&M**.

   By default, the **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Click the **PaaS Logon** tab.
4. Select a namespace from the **namespace** drop-down list. Fuzzy search is supported.
5. Find the pod that you want to manage in the POD section and click **Log On**.



POD
ahas-[redacted]dra-0 Log On
ahas-[redacted]lb-0 Log On
ahas-[redacted]0 Log On
ahas-platform-[redacted]-0 Log On
ahas-platform-[redacted]-1 Log On
ahas-platform-[redacted]-0 Log On
ahas-platform-[redacted]-1 Log On

6. After you log on to the VM where the pod is deployed, enter Linux commands in the CLI window to perform related operations.



Welcome Page [redacted]

- Click **Upload** in the upper-right corner of the CLI window. You can use one of the following methods to upload a file:
  - 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**.
- Click **Download File** in the upper-right corner of the CLI window. The **Download File** dialog box appears. Configure the File Directory and File Name parameters and then click **Download** to download the file to the default download folder used by your local browser.

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

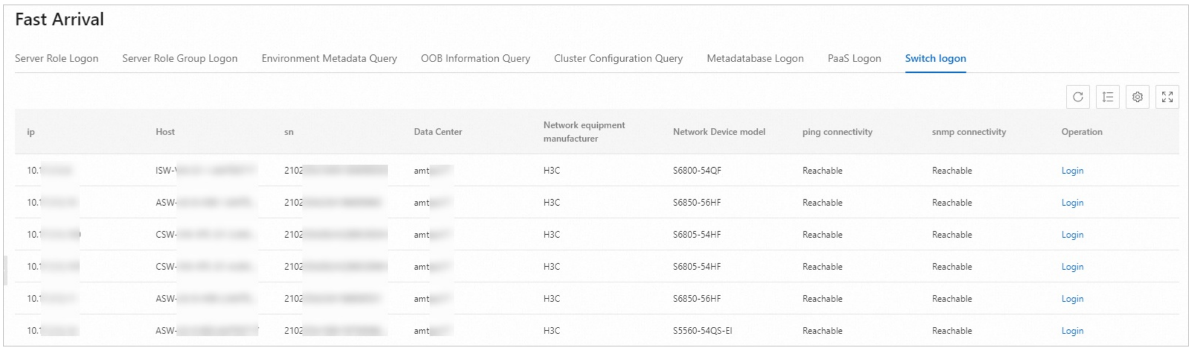
Switch logon

You can log on to a switch to perform related operations.

Procedure

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

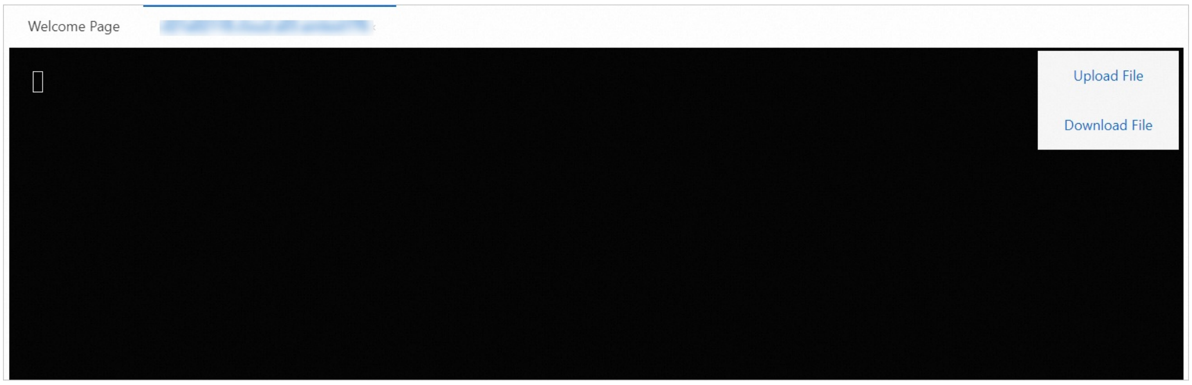
   By default, the **Server Role Logon** tab of the **Fast Arrival** page appears.
3. Click the **Log on to Switch** tab.
4. Find the switch to which you want to log on and click **Log On** in the **Actions** column.



Fast Arrival

ip	Host	sn	Data Center	Network equipment manufacturer	Network Device model	ping connectivity	snmp connectivity	Operation
10.1[redacted]	ISW-[redacted]	2102[redacted]	amt[redacted]	H3C	S6800-54QF	Reachable	Reachable	Login
10.1[redacted]	ASW-[redacted]	2102[redacted]	amt[redacted]	H3C	S6850-56HF	Reachable	Reachable	Login
10.1[redacted]	CSW-[redacted]	2102[redacted]	amt[redacted]	H3C	S6805-54HF	Reachable	Reachable	Login
10.1[redacted]	CSW-[redacted]	2102[redacted]	amt[redacted]	H3C	S6805-54HF	Reachable	Reachable	Login
10.1[redacted]	ASW-[redacted]	2102[redacted]	amt[redacted]	H3C	S6850-56HF	Reachable	Reachable	Login
10.1[redacted]	ASW-[redacted]	2102[redacted]	amt[redacted]	H3C	S5560-54QS-EI	Reachable	Reachable	Login

5. After you log on to the switch, enter Linux commands in the CLI window to perform related operations.



   - Click **Upload** in the upper-right corner of the CLI window. You can use one of the following methods to upload a file:
     - 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**.
   - Click **Download File** in the upper-right corner of the CLI window. The **Download File** dialog box appears. Configure the File Directory and File Name parameters and then click **Download** to download the file to the default download folder used by your local browser.

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

3.5.2.2. Audit

You can view the command operation records, file upload and download records, authorization information, and video playbacks on the fast arrival feature.

Command Records

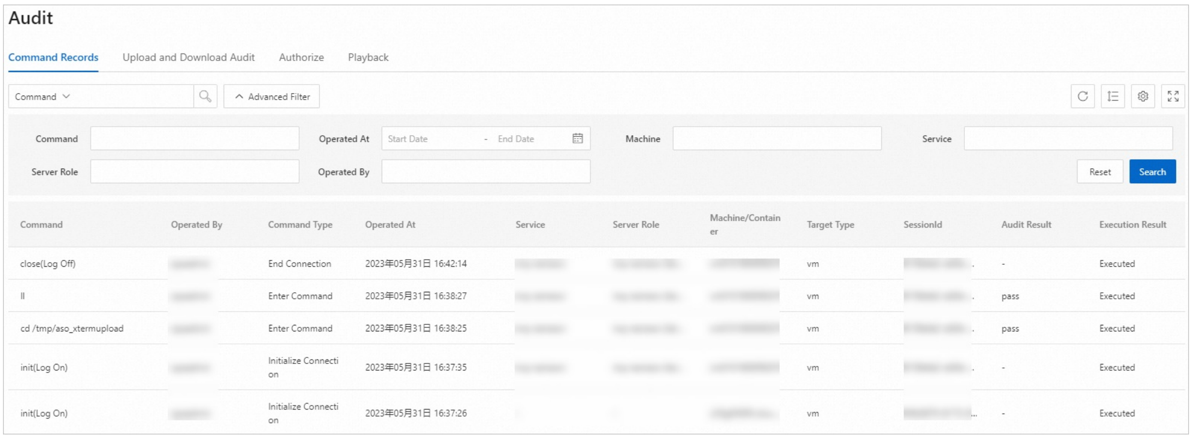
You can view the command operation records executed on the fast arrival feature.

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 **Audit**.

   By default, the **Command Records** tab appears.
4. Click **Advanced Filter** to filter command by **Command**, **Operated At**, **Machine**, **Service**, **Server Role**, and **Operated By** or their combinations.
5. In the command record list, you can view the following information: **Command**, **Operated By**, **Command Type**, **Operated At**, **Service**, **Server Role**, **Machine/Container**, **Target Type**, **SessionId**, **Audit Result**, and **Execution Result**.

> **Note**
>
> The system audits commands based on their risks. The following items list the possible audit results.
>
> - **pass**: The command passed the audit.
> - **fail**: The command failed the audit.
> - **multiVerify**: A further verification is required.
> - **codeVerify**: Authorization is required for use.



Command	Operated By	Command Type	Operated At	Service	Server Role	Machine/Container	Target Type	SessionId	Audit Result	Execution Result
close(Log Off)	[redacted]	End Connection	2023年05月31日 16:42:14	[redacted]	[redacted]	[redacted]	vm	[redacted]	-	Executed
ll	[redacted]	Enter Command	2023年05月31日 16:38:27	[redacted]	[redacted]	[redacted]	vm	[redacted]	pass	Executed
cd /tmp/aso_xtermupload	[redacted]	Enter Command	2023年05月31日 16:38:25	[redacted]	[redacted]	[redacted]	vm	[redacted]	pass	Executed
init(Log On)	[redacted]	Initialize Connection	2023年05月31日 16:37:35	[redacted]	[redacted]	[redacted]	vm	[redacted]	-	Executed
init(Log On)	[redacted]	Initialize Connection	2023年05月31日 16:37:26	[redacted]	[redacted]	[redacted]	vm	[redacted]	-	Executed

Upload and Download Audit

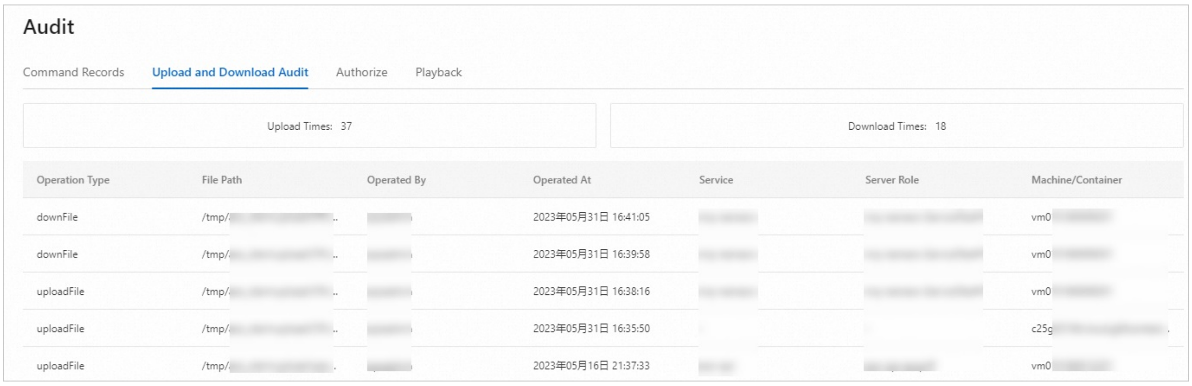
You can view information about file uploads and downloads performed on the fast arrival feature.

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 **Audit**.

   By default, the **Command Records** tab appears.
4. Click the **Upload and Download Audit** tab to view **Upload Times**, **Download Times**, and the list of uploads and downloads.

   The list contains the following information: **Operation Type**, **File Path**, **Operated By**, **Operated At**, **Service**, **Server Role**, and **Machine/Container**.



Upload Times: 37

Download Times: 18

Operation Type	File Path	Operated By	Operated At	Service	Server Role	Machine/Container
downFile	/tmp/[redacted]..	[redacted]	2023年05月31日 16:41:05	[redacted]	[redacted]	vm0[redacted]
downFile	/tmp/[redacted]..	[redacted]	2023年05月31日 16:39:58	[redacted]	[redacted]	vm0[redacted]
uploadFile	/tmp/[redacted]..	[redacted]	2023年05月31日 16:38:16	[redacted]	[redacted]	vm0[redacted]
uploadFile	/tmp/[redacted]..	[redacted]	2023年05月31日 16:35:50	[redacted]	[redacted]	c25g[redacted]
uploadFile	/tmp/[redacted].	[redacted]	2023年05月16日 21:37:33	[redacted]	[redacted]	vm0[redacted]

Authorize

You can view command authorization information.

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 **Audit**.

   By default, the **Command Records** tab appears.
4. Click the **Authorize** tab to view command authorization information.

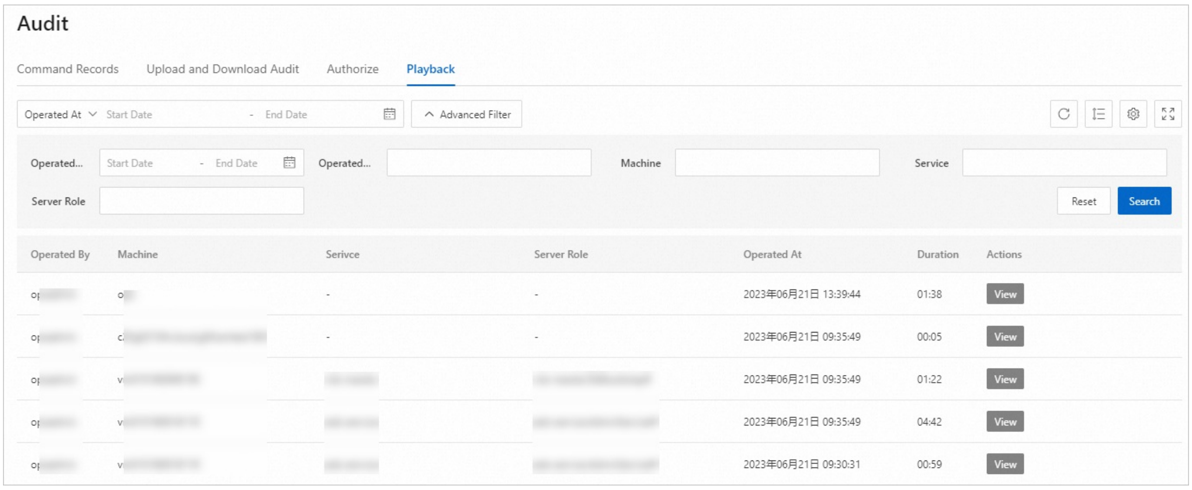
Playback

You can view the video playbacks of all commands that are executed on a machine.

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 **Audit**.

   By default, the **Command Records** tab appears.
4. Click the **Playback** tab.
5. Click **Advanced Filter** to filter video records by **Operated At**, **Operated By**, **Machine**, **Service**, and **Server Role** or their combinations.



Operated By	Machine	Serivce	Server Role	Operated At	Duration	Actions
op[redacted]	o[redacted]	-	-	2023年06月21日 13:39:44	01:38	View
op[redacted]	c[redacted]	-	-	2023年06月21日 09:35:49	00:05	View
op[redacted]	v[redacted]	[redacted]	[redacted]	2023年06月21日 09:35:49	01:22	View
op[redacted]	v[redacted]	[redacted]	[redacted]	2023年06月21日 09:35:49	04:42	View
op[redacted]	v[redacted]	[redacted]	[redacted]	2023年06月21日 09:30:31	00:59	View

6. Click **View** in the **Actions** column corresponding to an operation record.
7. In the video playback window, click the ▶ icon to play back the video.

3.5.2.3. Rules

This topic describes how to configure blocking rules for Linux commands.

Background information

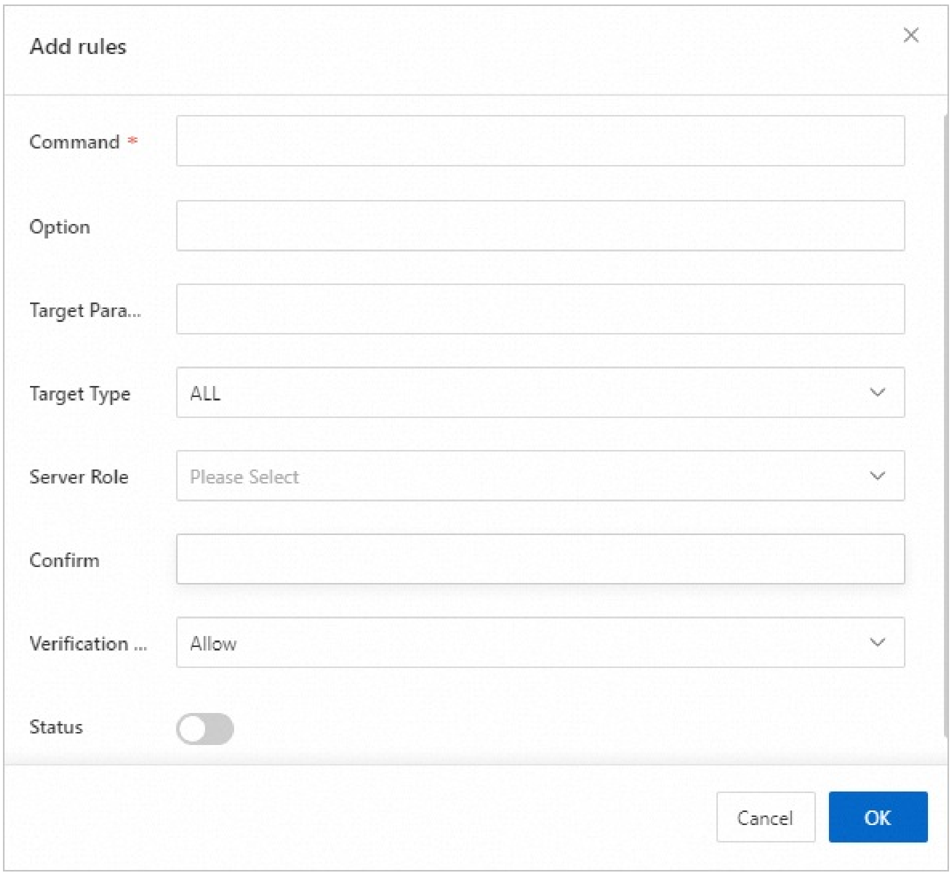
To control the risks that are caused by Linux commands, you can configure blocking rules for Linux commands.

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 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 no parameter is available for the command option, leave this parameter empty.	test
Target Type	The type of the command option. Valid values: ◦ ALL ◦ FILE ◦ DIR ◦ OPTION	OPTION
Server Role	The server roles of the machine on which the command is implemented. You can select one or more server roles.	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 that is used to block the command. Valid value: ◦ Allow: The command can be run. ◦ Block: The command is blocked. ◦ Confirm Again: You must confirm again before you run the command. ◦ Verification Code: The command can be run within a specific period of time after the authorization is approved. If you select this value, a verification code is requested from the system. The verification code is required before you run the command.	Allow
Status	The status of the rule.	On



Add rules

Command *

Option

Target Para...

Target Type: ALL

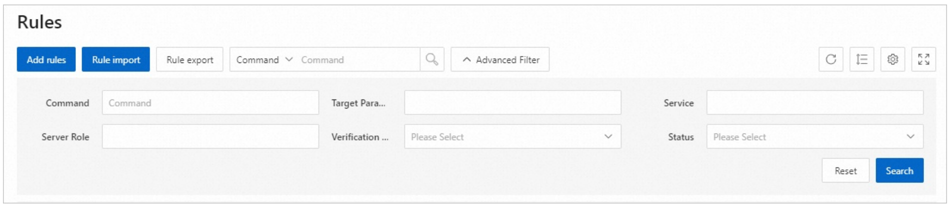
Server Role: Please Select

Confirm

Verification ...: Allow

Status

Related operations

Operation	Description
View blocking rules	You can view command blocking rules that you created or imported. Click **Advanced Filter**, and filter blocking rules by **Command**, **Target Parameter**, **Service**, **Server Role**, **Verification Rule**, and **Status**. Fuzzy search is supported in all fields.  Rules Add rules · Rule import · Rule export · Command · Advanced Filter Command · Target Para... · Service Server Role · Verification ...: Please Select · Status: Please Select Reset · Search

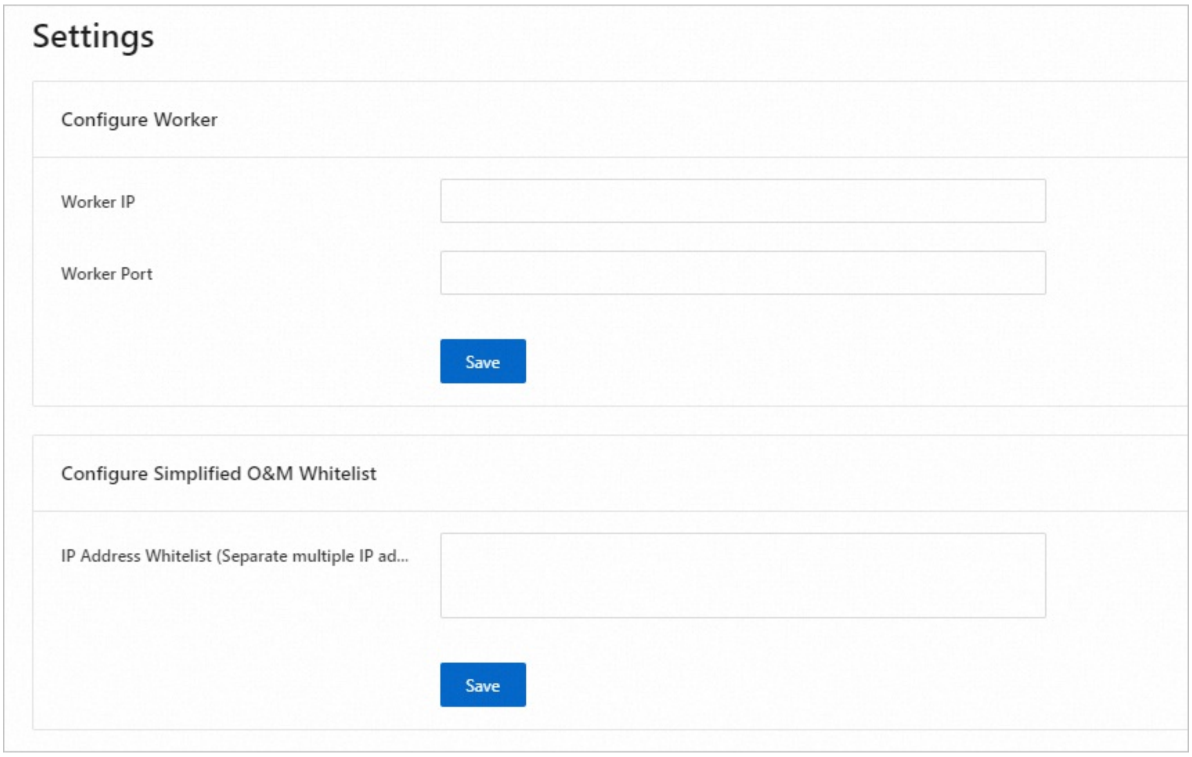
Import blocking rules	You can batch import command blocking rules. 1. In the upper-left corner of the Rules page, click**Rule import**. 2. Click **Click Here to Upload**, select the file that contains the command blocking rules that you want to import, and then click **Open** to import the rules. **Note** The file must be in the .xlsx format. You can export the template and then enter information in the template.
Export blocking rules	You can batch export command blocking rules that you created. In the upper-left corner of the Rules page, click**Rule export** to download the file that contains the command blocking rules that you want to export to your computer.
Modify a blocking rule	You can modify a command blocking rule that you created. 1. Find the command blocking rule that you want to modify and click**Modify** in the **Actions** column. 2. In the dialog box that appears, configure the parameters and click**OK**. **Note** In the **Status** column, turn on or off the switch to change the status of a rule.
Delete a blocking rule	You can delete a command blocking rule that you created. 1. Find the command blocking rule that you want to delete and click**Delete** in the **Actions** column. 2. In the message that appears, click **OK**.

3.5.2.4. 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**.


Settings
Configure Worker
Worker IP
Worker Port
Save
Configure Simplified O&M Whitelist
IP Address Whitelist (Separate multiple IP ad...
Save

4. In the **Configure Worker** section, enter the IP address and port number of the worker and 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.

3.5.3. Process approval

This topic describes the modules of the Process Approval module.

Modules

Module	Description
My Submission	You can view the list of O&M workflows that you submitted. You can also query or cancel these workflows.
Pending Approval	You can view the O&M workflows that are submitted for your approval. You can also query and approve these O&M workflows.

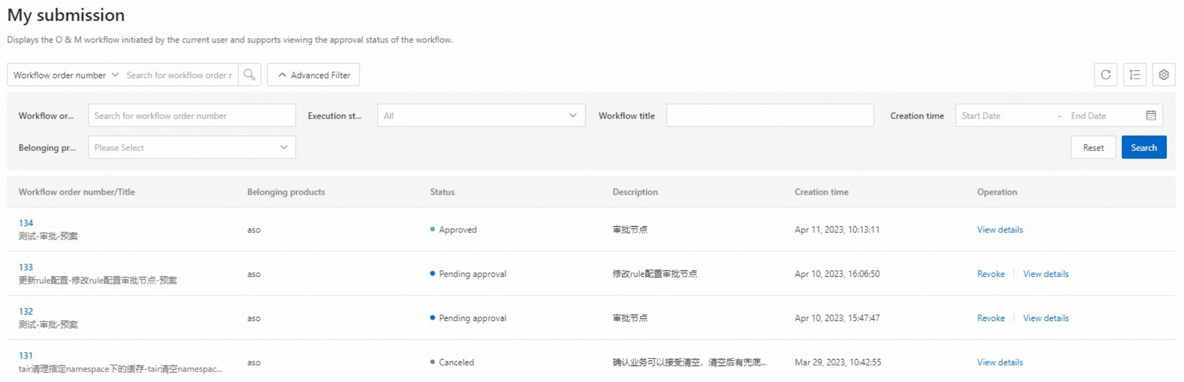
3.5.3.1. My submission

On the My submission page, you can view the details of O&M workflows that are submitted by the current user. You can also revoke submitted O&M workflows on this page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Process Approval**.
3. In the left-side navigation pane, click **My Submission**.
4. On the My submission page, view the list of O&M workflows that are submitted by the current user.

   You can also click **Advanced Filter** to filter workflows by **Workflow order number**, **Execution status**, **Workflow title**, **Creation time**, and **Belonging products**.



My submission

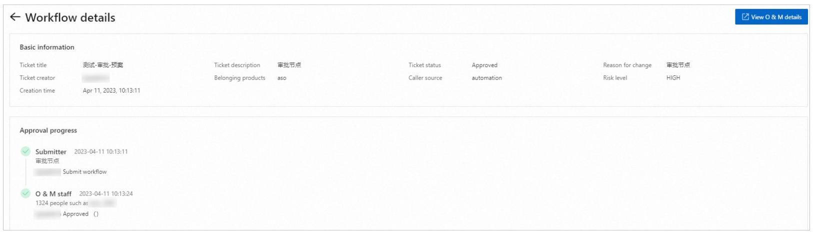
Displays the O & M workflow initiated by the current user and supports viewing the approval status of the workflow.

Workflow order number: Search for workflow order r

Workflow or...: Search for workflow order number
Execution st...: All
Workflow title:
Creation time: Start Date - End Date
Belonging pr...: Please Select

Workflow order number/Title	Belonging products	Status	Description	Creation time	Operation
134 测试-审批-预案	aso	● Approved	审批节点	Apr 11, 2023, 10:13:11	View details
133 更新rule配置-修改rule配置审批节点-预案	aso	● Pending approval	修改rule配置审批节点	Apr 10, 2023, 16:06:50	Revoke | View details
132 测试-审批-预案	aso	● Pending approval	审批节点	Apr 10, 2023, 15:47:47	Revoke | View details
131 tair清理指定namespace下的缓存-tair清空namespac...	aso	● Canceled	确认业务可以接受清空，清空后有兜底...	Mar 29, 2023, 10:42:55	View details

5. Perform the operations that are described in the following table.

Operation	Description
View the details of an O&M workflow	i. Find the O&M workflow that you want to manage and click the order number of the workflow or **View details** in the **Operation** column that corresponds to the workflow. ii. On the **Workflow details** page, view the basic information and approval progress of the workflow.  Workflow details Basic information Ticket title: 测试-审批-预案 · Ticket description: 审批节点 · Ticket status: Approved · Reason for change: 审批节点 Ticket creator: [redacted] · Belonging products: aso · Caller source: automation · Risk level: HIGH Creation time: Apr 11, 2023, 10:13:11 Approval progress Submitter 2023-04-11 10:13:11 审批节点 [redacted] Submit workflow O & M staff 2023-04-11 10:13:24 1324 people such as [redacted] [redacted] Approved () iii. Optional. In the upper-right corner of the Workflow details page, click **View O&M details**. You are redirected to the **Plan Task details** page. On the Plan Task details page, view the O&M details.

Revoke an O&M workflow	**Note** You can revoke an O&M workflow only when the workflow is in the **Pending Approval** state. i. Find the O&M workflow that you want to manage and click**Revoke** in the **Operation** column. ii. In the message that appears, click**OK**.

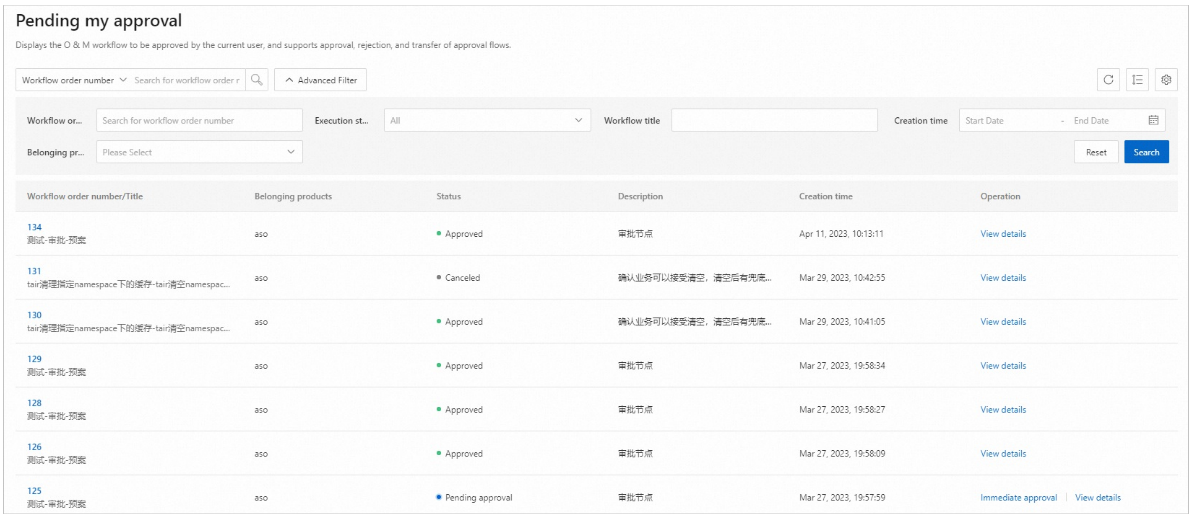
3.5.3.2. My approval

On the Pending my approval page, view the O&M workflows that require approval from the current user. You can also approve, reject, and transfer O&M workflows.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Changes** > **Process Approval**.
3. In the left-side navigation pane, click **My Approval**.
4. On the Pending my approval page, view the list of O&M workflows that require approval from by the current user.

   You can click **Advanced Filter** to filter workflows by **Workflow order number**, **Execution status**, **Workflow title**, **Creation time**, and **Belonging products**.



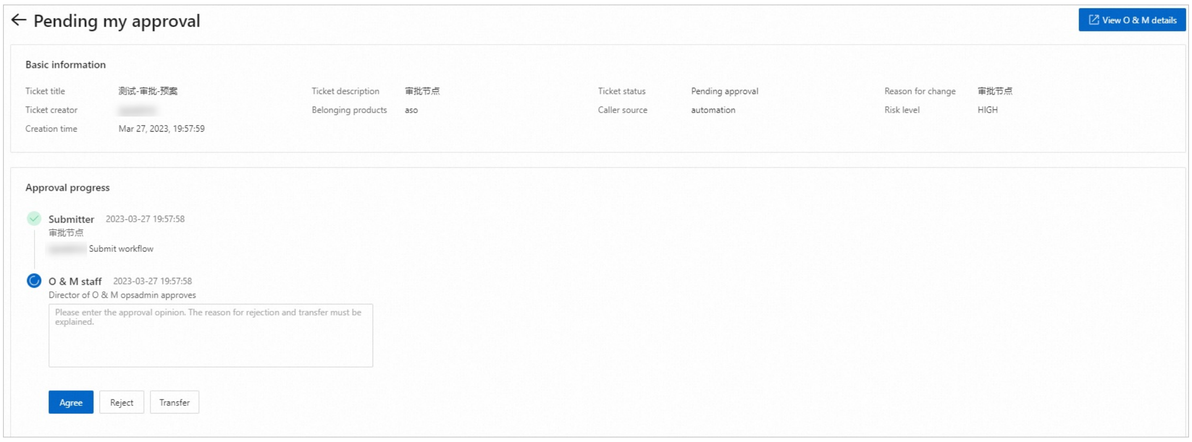
Pending my approval

Displays the O & M workflow to be approved by the current user, and supports approval, rejection, and transfer of approval flows.

Workflow order number/Title	Belonging products	Status	Description	Creation time	Operation
134 测试-审批-预案	aso	● Approved	审批节点	Apr 11, 2023, 10:13:11	View details
131 tair清理指定namespace下的缓存-tair清空namespac...	aso	● Canceled	确认业务可以接受清空，清空后有兜底...	Mar 29, 2023, 10:42:55	View details
130 tair清理指定namespace下的缓存-tair清空namespac...	aso	● Approved	确认业务可以接受清空，清空后有兜底...	Mar 29, 2023, 10:41:05	View details
129 测试-审批-预案	aso	● Approved	审批节点	Mar 27, 2023, 19:58:34	View details
128 测试-审批-预案	aso	● Approved	审批节点	Mar 27, 2023, 19:58:27	View details
126 测试-审批-预案	aso	● Approved	审批节点	Mar 27, 2023, 19:58:09	View details
125 测试-审批-预案	aso	● Pending approval	审批节点	Mar 27, 2023, 19:57:59	Immediate approval | View details

5. Find the O&M workflow that you want to manage and click the order number of the workflow or **View details** in the **Operation** column to view the basic information and approval progress of the workflow.

   > **Important**
   >
   > You can approve an O&M workflow only when the workflow is in the **Pending approval** status.



← Pending my approval

View O & M details

Basic information

Ticket title	测试-审批-预案	Ticket description	审批节点	Ticket status	Pending approval	Reason for change	审批节点
Ticket creator	[redacted]	Belonging products	aso	Caller source	automation	Risk level	HIGH
Creation time	Mar 27, 2023, 19:57:59						

Approval progress

Submitter 2023-03-27 19:57:58
审批节点
[redacted] Submit workflow

O & M staff 2023-03-27 19:57:58
Director of O & M opsadmin approves

Please enter the approval opinion. The reason for rejection and transfer must be explained.

6. In the **Approval progress** section, perform the following operations on the O&M workflow.
   - Approve: Click **Agree**. In the message that appears, click **OK**.
   - Reject: Click **Reject**. In the message that appears, click **OK**.
   - Transfer: Enter your comments and click **Transfer**. In the dialog box that appears, select the user to whom you want to transfer the workflow and click **OK**.
7. Optional. In the upper-right corner of the Workflow details page, click **View O&M details**. You are redirected to the **Plan Task details** page. On the Plan Task details page, view the O&M details.

3.6. Archives

This topic describes the modules related to archive management.

Modules

You can archive the key metadata of Apsara Stack. The archived metadata is used for quick recovery from Apsara Stack failures.

Prerequisites

- System administrator permissions on ASO are granted.
- Only the metadata of Apsara Distributed File System and OPS DNS can be archived.

Flowchart

Modules

Module	Description
Archive Settings	You can modify archive settings and trigger archive operations.
Archive Details	You can view archive details, including the archived product, archived item, file name, start time, and archive status.
Archive Products	You can configure products to archive and manage archived products.

Archiving Server Settings	You can configure the archive server for the storage of archive files.

3.6.1. Archive settings

This topic describes how to configure archived items.

Prerequisites

- The archive server is configured.
- Archive products are added. For more information, see Archive product management.

Procedure

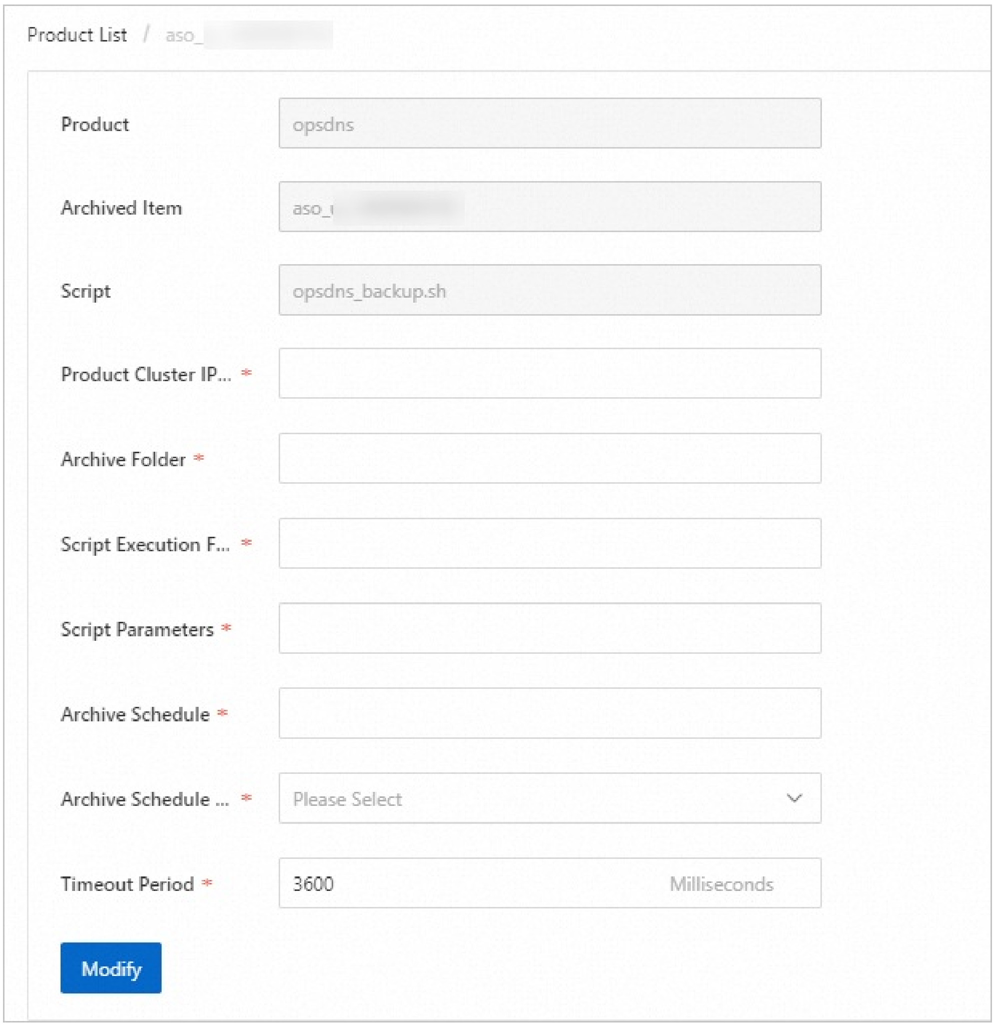
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Archive** > **Archive Settings**.

   On the left side of the page, the 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.

   > **Note**
   >
   > Only the metadata of Apsara Distributed File System and OPS DNS can be archived.

3. Click the item that you want to archive. In the right-side section, configure the following information and click **Modify** to trigger the archive operation.

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



Product List / aso_[redacted]

Product	opsdns
Archived Item	aso_[redacted]
Script	opsdns_backup.sh
Product Cluster IP... *	
Archive Folder *	
Script Execution F... *	
Script Parameters *	
Archive Schedule *	
Archive Schedule ... *	Please Select
Timeout Period *	3600 Milliseconds

Parameter	Description
Product Cluster IP Address	The IP address of the actual transfer server.
Archive Folder	A folder on the transfer server. You only need to enter a folder 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 only need to enter a folder in the field without manually creating a folder to store scripts to be executed. 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 IP address of the pangu master. ◦ opsdns: We recommend that you enter**--ip=127.0.0.1**.
Archive Schedule	The archive schedule. 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 archive schedule. 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. Unit: milliseconds. Default value: 3600.

4. Repeat Step 3 to configure all items.

What to do next

After you configure the items, you can view the archive details and status on the **Archive Details** page.

3.6.2. Archive details

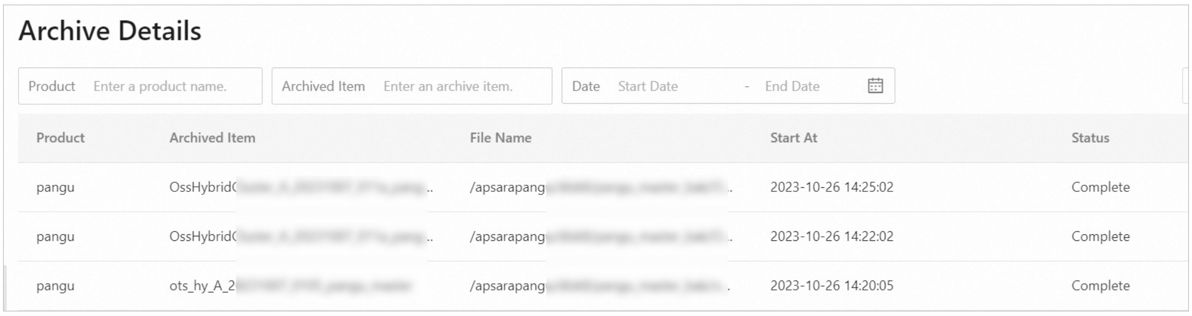
This topic describes how to view the archive details of each archived item.

Prerequisites

Archive settings are configured and an archive operation is triggered.

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, filter the details of the archive by **Product**, **Archive Item**, and **Date**.
4. View the archive details of an item, including the **Product**, **Archived Item**, **File Name**, **Start At**, and **Status**. The archive status includes **Not started**, **In progress**, **Complete**, **Timeout**, and **Failed**.



Archive Details

Product: Enter a product name.　Archived Item: Enter an archive item.　Date: Start Date - End Date

Product	Archived Item	File Name	Start At	Status
pangu	OssHybrid[redacted]..	/apsarapang[redacted].	2023-10-26 14:25:02	Complete
pangu	OssHybrid[redacted]..	/apsarapang[redacted].	2023-10-26 14:22:02	Complete
pangu	ots_hy_A_2[redacted]	/apsarapang[redacted].	2023-10-26 14:20:05	Complete

> **Note**
>
> If the status of an archived item is **Complete**, you must check whether the Message-Digest Algorithm 5 (MD5) values of the offline archive service and the archive server are consistent with each other. If the values are consistent with each other, the archive was successful.

3.6.3. Archive product management

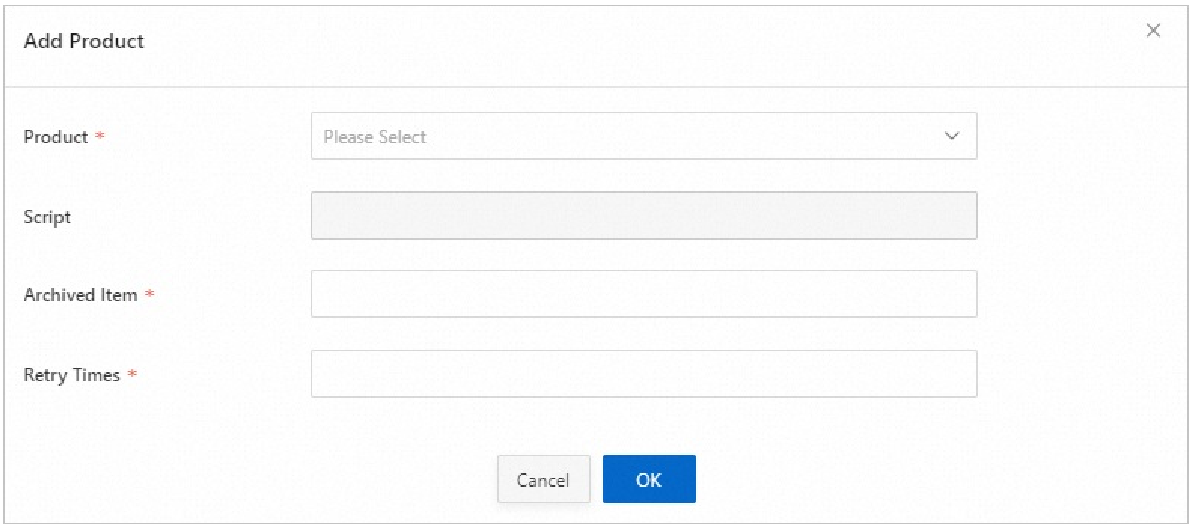
This topic describes how to add archive products.

Prerequisites

- Only the metadata of Apsara Distributed File System and OPS DNS can be archived.
- The archive server is configured.

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**.



Add Product

Product *: Please Select

Script

Archived Item *

Retry Times *

Parameter	Description	Example
Product	The name of the product. Select a product from the drop-down list. ◦ pangu ◦ opsdns	pangu
Script	The name of the archive script. The system automatically selects the script based on the product.	metadata_backup.py

Archived Item	The product information to be archived. Note 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.	ecs_pangu
Retry Times	The number of retries after an error occurs. Default value: 3.	3

5. Repeat Steps 3 and Step 4 to add all archived items. Typically, you need to add multiple archived items.

Related operations

Operation	Description
Modify archived items	1. Click **Modify** in the **Actions** column of the archived item. 2. In the dialog box that appears, modify the parameters and click**OK**. Note You can modify only **Retry Times**.
Delete archived items	1. Click **Delete** in the **Actions** column of the archived item. 2. In the message that appears, click **Delete**.

What to do next

After you add all new archived items of a product, the archived items are displayed on the **Archive Settings** page. You can configure archive settings for the archived items on the Archive Settings page.

3.6.4. Archive server settings

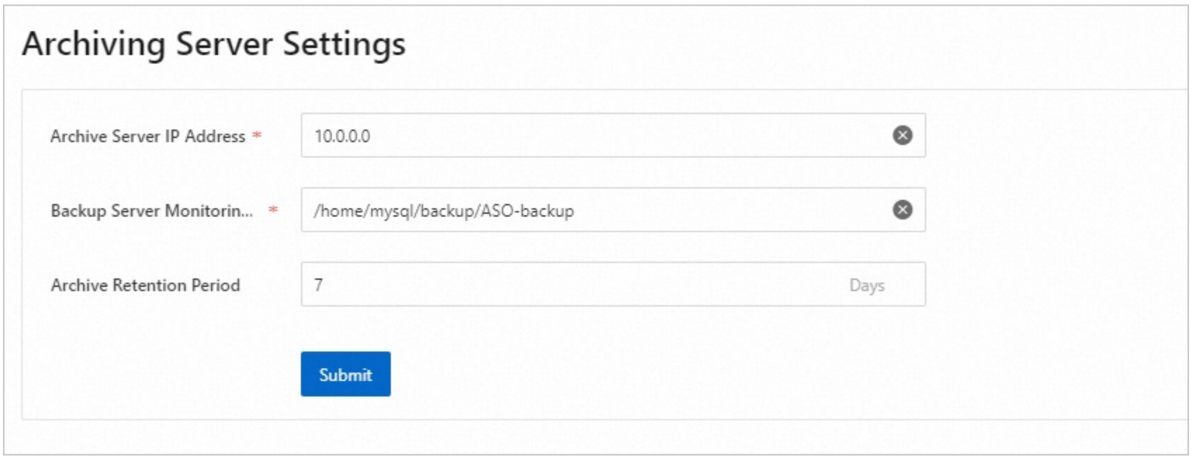
This topic describes how to configure the archive server that is used to store archive files.

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 parameters that are described in the following table and then click **Submit**.

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

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 managed 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.
Backup Server Monitoring Path	The storage path of archive files on the archive server. **Note** ◦ If the backup path does not start with /apsarapangu, /ASO-backup is added to the beginning of the path by default. ◦ 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.



Archiving Server Settings

Archive Server IP Address *: 10.0.0.0

Backup Server Monitorin... *: /home/mysql/backup/ASO-backup

Archive Retention Period: 7 Days

What to do next

After you configure the archive server, you need to add new archived items on the **Archive Products** page.

3.7. Event Center

This topic describes the modules related to the event center.

Modules

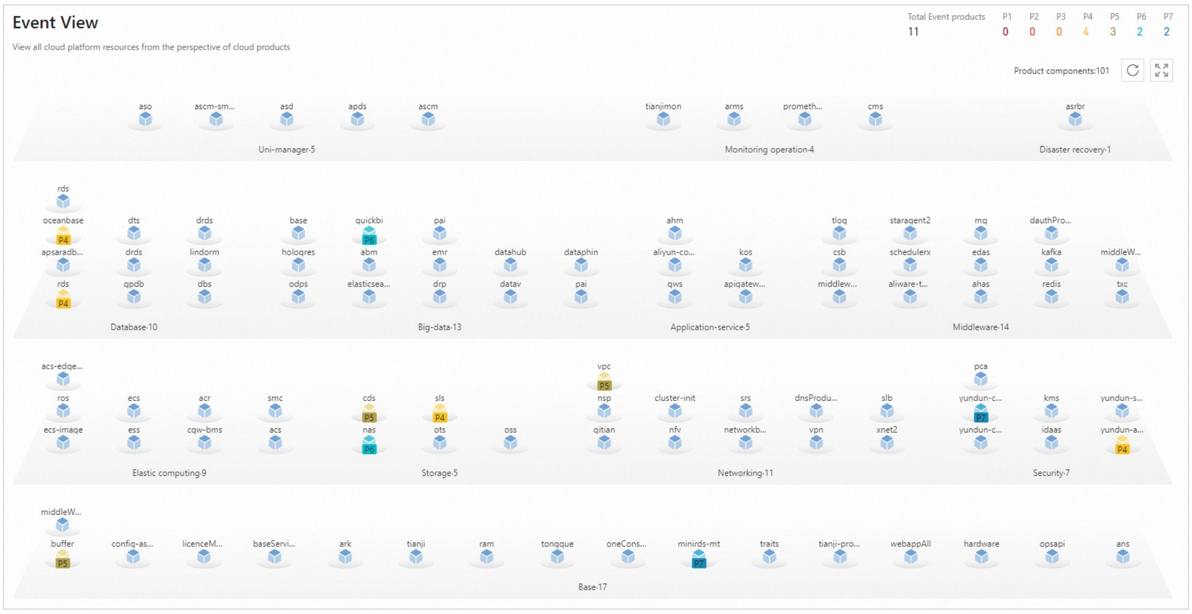
Module	Description
Event Chart	You can view the information about all cloud platform resources from the cloud product perspective, including the total number and status of product components, the total number of event products, and product event traces.

3.7.1. Event chart

You can view all events of the cloud platform from the perspective of cloud products.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **General** > **Event Center** > **Event Chart**.
3. View the events of the cloud platform from the perspective of cloud products.
    - In the upper-right corner of the page, view the total number of product components, the total number of products that trigger events, and the number of products that trigger events at each severity level.
    - View the status of each cloud product component: A blue icon indicates that the event of a product component is normal, whereas an icon with an event severity level indicates that the event of a product component is abnormal.
    - Move the pointer over the icon of a product component to view the associated product components.
    - Click the icon of a product to go to the Event trajectory page.



Event View

View all cloud platform resources from the perspective of cloud products

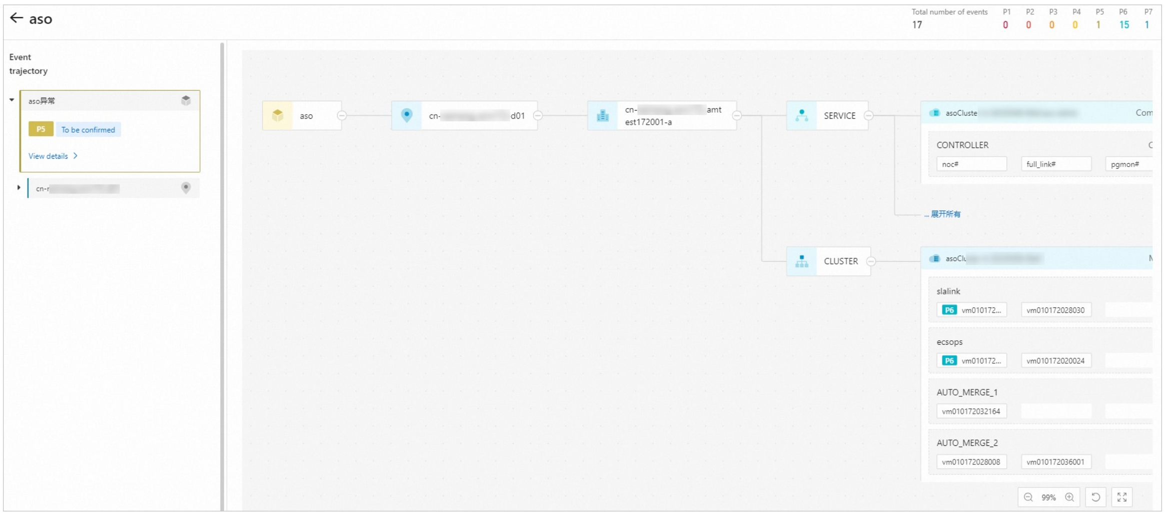
Total Event products	P1	P2	P3	P4	P5	P6	P7
11	0	0	0	4	3	2	2

Product components:101

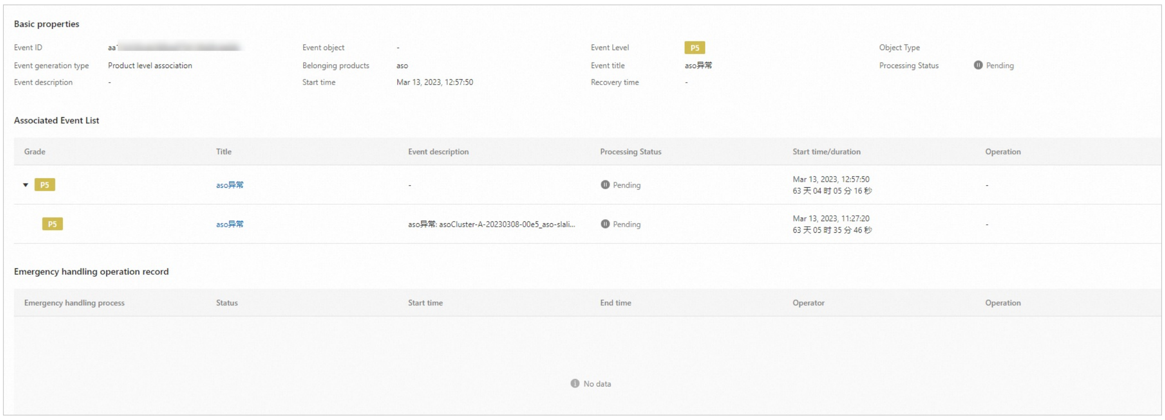
4. On the Event trajectory page, view the following information:
    - The number of events for the cloud product and the number of events at each severity level that are displayed in the upper-right corner of the page.
    - The catalog tree of the event trajectory that is displayed on the left side of the page.
    - The details of the event trajectory, including the information about the component architecture, name, quantity, and status, that are displayed on the right side of the page.

5. If a product reports abnormal events, you can perform the following operations. In this example, Apsara Uni-manager Operations Console is used.

    i. On the Event trajectory page, click **ASO Exceptions** in the catalog tree on the left, and then click **View details** to go to the event details page.

    ii. On the event details page, view the basic information about the event, associated events, and emergency responses for the event in the **Basic properties**, **Associated Event List**, and **Emergency handling operation record** sections.

    Basic properties

Event ID	aa[redacted]	Event object	-	Event Level	P5	Object Type	
Event generation type	Product level association	Belonging products	aso	Event title	aso异常	Processing Status	Pending
Event description	-	Start time	Mar 13, 2023, 12:57:50	Recovery time	-		

    Associated Event List

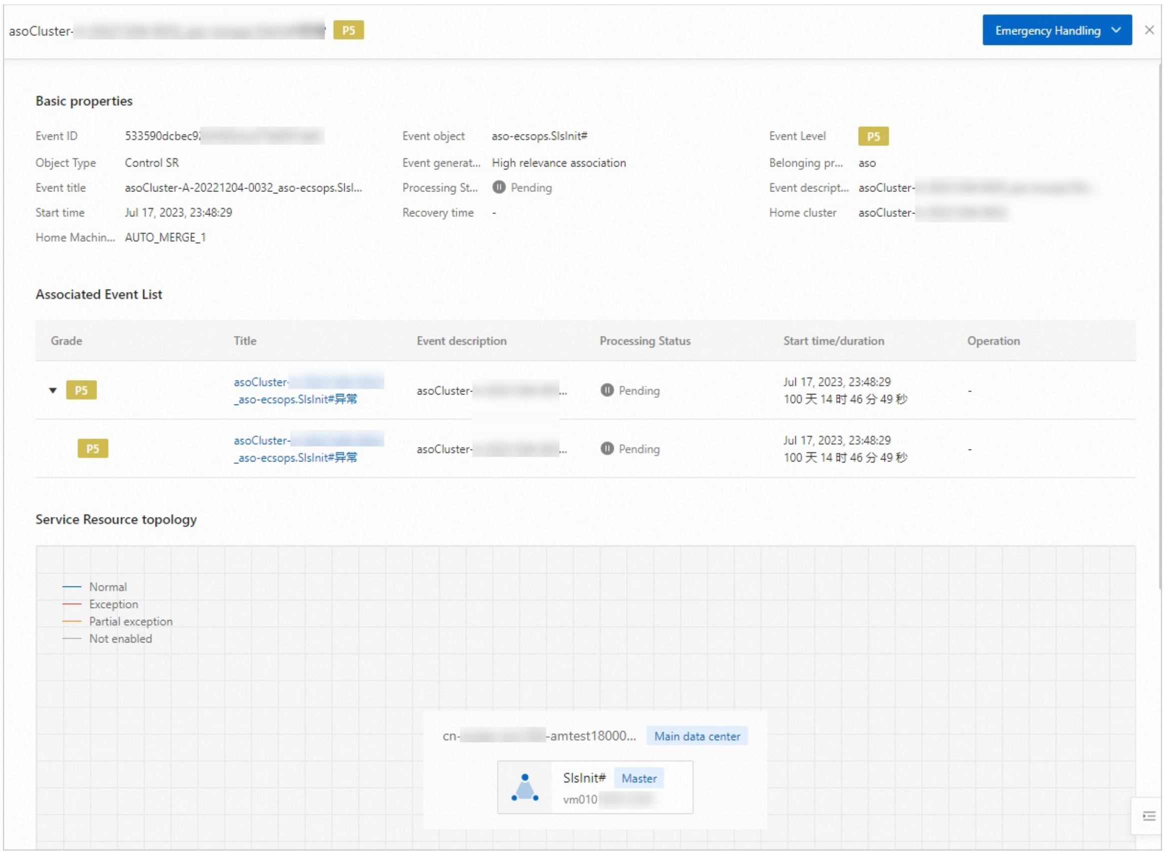
Grade	Title	Event description	Processing Status	Start time/duration	Operation
▾ P5	aso异常	-	Pending	Mar 13, 2023, 12:57:50 63 天 04 时 05 分 16 秒	-
P5	aso异常	aso异常: asoCluster-A-20230308-00e5_aso-slali...	Pending	Mar 13, 2023, 11:27:20 63 天 05 时 35 分 46 秒	-

    Emergency handling operation record

Emergency handling process	Status	Start time	End time	Operator	Operation

    No data

    The service resource topologies for only some abnormal events are provided on the page. You can obtain the relevant information based on specific cloud products on the event details page.



asoCluster-[redacted] P5

Basic properties

Event ID	533590dcbec9[redacted]	Event object	aso-ecsops.SlsInit#	Event Level	P5
Object Type	Control SR	Event generat...	High relevance association	Belonging pr...	aso
Event title	asoCluster-A-20221204-0032_aso-ecsops.Slsl...	Processing St...	Pending	Event descript...	asoCluster-[redacted]
Start time	Jul 17, 2023, 23:48:29	Recovery time	-	Home cluster	asoCluster-[redacted]
Home Machin...	AUTO_MERGE_1				

Associated Event List

Grade	Title	Event description	Processing Status	Start time/duration	Operation
▾ P5	asoCluster-[redacted] _aso-ecsops.SlsInit#异常	asoCluster-[redacted]...	Pending	Jul 17, 2023, 23:48:29 100 天 14 时 46 分 49 秒	-
P5	asoCluster-[redacted] _aso-ecsops.SlsInit#异常	asoCluster-[redacted]...	Pending	Jul 17, 2023, 23:48:29 100 天 14 时 46 分 49 秒	-

Service Resource topology

4.Product O&M

This topic lists the products for which you can perform O&M operations in the Apsara Uni-manager Operations Console. For more information about O&M operations, see Apsara Uni-manager Operations Console Operation Guide.

Category	Product
Computing	Compute Operations Console
	ECS Diagnosis
	BMS Operations Console
Network	Network Operations Console
	Apsara Network Intelligence
Storage	CDS
	Apsara Distributed File System
	EBS
	OSS Storage Operations and Maintenance System
	NAS Storage Operations and Maintenance System
	Tablestore Storage Operations and Maintenance System
Database	ApsaraDB Operations and Maintenance System
	DTS
	DRDS Manager
	Data Replication System
	ApsaraDB for OceanBase

	Database Backup
	ApsaraDB Operations and Maintenance System
Middleware	Tlog
	Global Transaction Service
	CSB
Big data	Apsara Bigdata Manager
	Elasticsearch
	Dataphin
Base or platform	Basic Service Control
	Tianjimon
	Configuration Management Database
	Apsara Infrastructure Management
	ApsaraDB Operations and Maintenance System (Lite)
	Apsara Stack Doctor
	Apsara Stack Inspection System
	PaaS Operations Console
	Base Container O&M Platform
	TianjiMon - Grafana
	Server Insight

	Cloud Product Anomaly Diagnosis Visualization · Diagnosis
	UniConsole
	ASR for Zone-disaster Recovery (Primary Zone)
	ASR for Geo-disaster Recovery
Security service	Apsara Stack Security

5.Security compliance

5.1. Security operations

5.1.1. Log management

You can view logs to check the resource usage and module status on the platform.

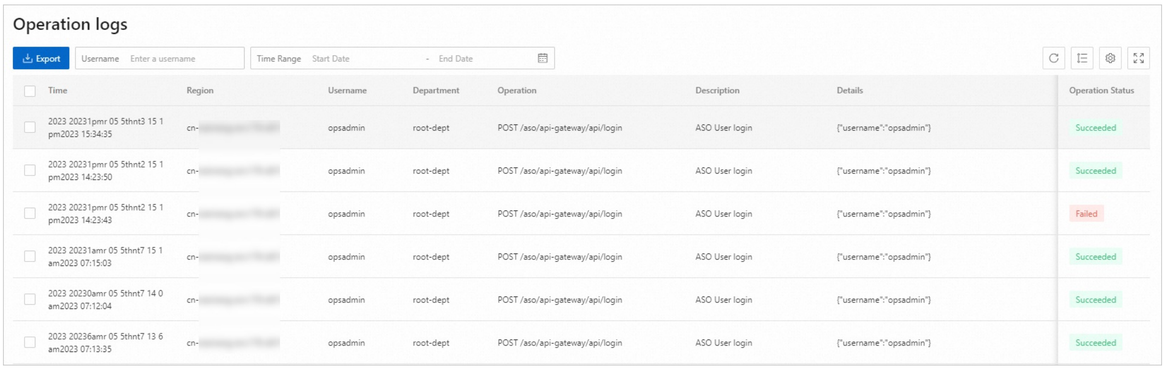
Background information

On the Operation logs page, you can view all the records of backend API calls, including audit operations. An auditor can filter logs by username and time range and 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, choose **Security & Compliance** > **Security Operations** > **Log Management**.
3. On the **Operation Logs** page, perform the following operations:
   - Query logs

     Filter operation logs by **username** and **time range**. The logs that you want to query are displayed in the log list.



Operation logs

□	Time	Region	Username	Department	Operation	Description	Details	Operation Status
□	2023 20231pmr 05 5thnt3 15 1 pm2023 15:34:35	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Succeeded
□	2023 20231pmr 05 5thnt2 15 1 pm2023 14:23:50	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Succeeded
□	2023 20231pmr 05 5thnt2 15 1 pm2023 14:23:43	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Failed
□	2023 20231amr 05 5thnt7 15 1 am2023 07:15:03	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Succeeded
□	2023 20230amr 05 5thnt7 14 0 am2023 07:12:04	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Succeeded
□	2023 20236amr 05 5thnt7 13 6 am2023 07:13:35	cn-[redacted]	opsadmin	root-dept	POST /aso/api-gateway/api/login	ASO User login	{"username":"opsadmin"}	Succeeded

   - Export logs

     Select logs that you want to export. Click **Export** in the upper part of the page to export the selected logs. If you do not select logs, 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. Host security

5.2.1. 文档标题缺失，请补全后重新导出

5.2.1.1. Physical server security

5.2.1.1.1. Create and grant permissions to a security administrator account

The physical server security feature is used to ensure the security of physical servers on the platform side. This feature requires you to use a dedicated security administrator account for the platform. This topic describes how to create and grant permissions to a security administrator account.

Procedure

1. Log on to the Apsara Uni-manager Management Console as a system administrator.
   For more information, see the **"Log on to the Apsara Uni-manager Management Console"** topic of **Apsara Uni-manager Management Console User Guide**.
2. Create a dedicated organization that is used to manage the security of physical servers, and obtain the primary key of the organization.

   > ⓘ **Important** Make sure that the organization is used only to manage the security of physical servers. Do not add Elastic Compute Service (ECS) instances to the organization.

   i. Create the dedicated organization.
   For more information, see **Enterprise Center > Organization Management > Create Organization** in **Apsara Uni-manager Management Console User Guide**.

   ii. Obtain the **primary key** of the newly created organization.
   For more information, see **Enterprise Center > Organization Management > Obtain the AccessKey pair of an organization** in **Apsara Uni-manager Management Console User Guide**.
3. Create a dedicated account to manage the security of physical servers.

   For more information, see **Enterprise Center > User Management > System User Management > Create User** in **Apsara Uni-manager Management Console User Guide**.

   > ⓘ **Note** When you create the account, take note of the following points for the **organization** and **role**:
   >
   > - In the **Organization** section, select the organization that is created in the previous step.
   > - In the **Role** section, select **Platform Security Configuration Administrator** and **Security System Configuration Administrator**.
4. Log on to Apsara Stack Security Center by using the newly created account.
   For more information, see Log on to Apsara Stack Security Center.
5. Add the **primary key** of the newly created organization to the protection configuration of physical servers.

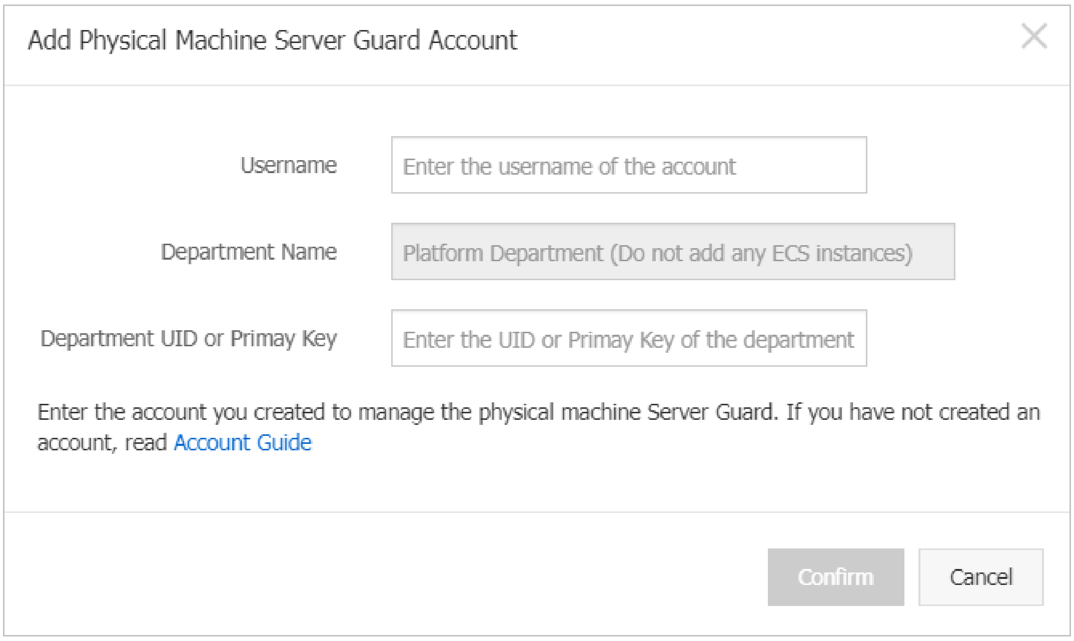
   i. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.

   ii. In the left-side navigation pane, click **Global Settings**

   iii. On the **Global Settings** page, click the **Physical Machine Protection Configurations** tab.

iv. Click **Add Account**.

v. In the **Add Physical Machine Server Guard Account** dialog box, configure the **Username** and **Department UID or Primay Key** parameters.



Add Physical Machine Server Guard Account

Username: Enter the username of the account

Department Name: Platform Department (Do not add any ECS instances)

Department UID or Primay Key: Enter the UID or Primay Key of the department

Enter the account you created to manage the physical machine Server Guard. If you have not created an account, read Account Guide

- **Username**: Enter the account that you created in Step 3.
- **Primary Key**: Enter the primary key that you obtained in Step 2.

vi. Click **Confirm**.

Result

After the settings are complete, you can use the dedicated security administrator account that is created in this section to ensure the security of physical servers on the platform side.

5.2.1.1.2. Physical servers

5.2.1.1.2.1. Manage physical server groups

This topic describes how to manage physical server groups. To facilitate the security management of physical servers, you can add the physical servers to groups and view their security events by group.

Background information

By default, physical servers do not belong to a server group. You must add your physical servers to a server group. If you delete a group, all the physical servers in the group are retained but no longer belong to a server group.

Procedure

1. Log on to Apsara Stack Security Center.

   > **Note** For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.

3. In the left-side navigation pane, choose **Physical Server Security** > **Servers**.
4. In the left-side group pane, manage sever groups.
   - Create a group.

     Click the Add Subgroup icon next to **All Servers** or a specific group, enter a group name, and click **OK**.

     > ⓘ **Note** The system supports a maximum of three levels of groups.

   - Modify a group.

     Click the Modify Group Name icon next to the target group, enter a new name, and click **OK**.

   - Delete a group.

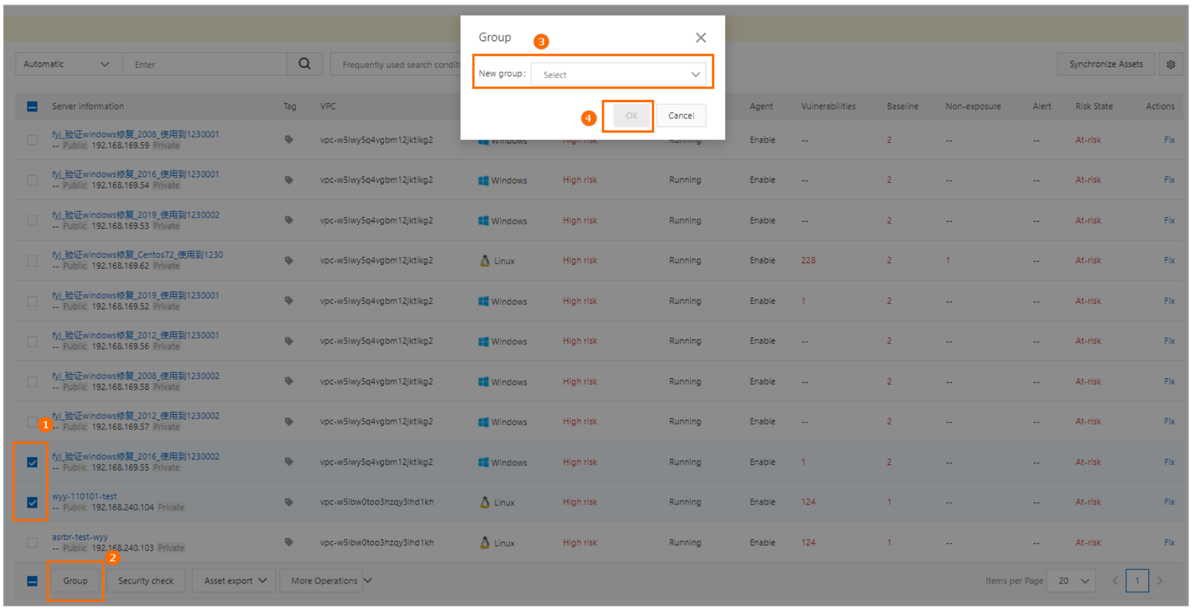
     Click the Delete icon next to the target group. In the message that appears, click **OK**.

     > ⓘ **Note** After you delete a group, all servers in the group are automatically moved to the **default** group.

   - Sort groups.

     Click **Manage Groups** to sort groups in descending order by priority.

5. Change the server group of specific physical servers.



Group

New group: Select

OK Cancel

☐ Server information	Tag	VPC				Agent	Vulnerabilities	Baseline	Non-exposure	Alert	Risk State	Actions
☐ fyj_验证windows修复_2008_使用到1230001 -- Public 192.168.169.59 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_2016_使用到1230001 -- Public 192.168.169.54 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_2019_使用到1230002 -- Public 192.168.169.53 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_Centos72_使用到1230 -- Public 192.168.169.62 Private		vpc-w5lwy5q4vgbm12jktikg2	Linux	High risk	Running	Enable	228	2	1	--	At-risk	Fix
☐ fyj_验证windows修复_2019_使用到1230001 -- Public 192.168.169.52 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	1	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_2012_使用到1230001 -- Public 192.168.169.56 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_2008_使用到1230002 -- Public 192.168.169.58 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☐ fyj_验证windows修复_2012_使用到1230002 -- Public 192.168.169.57 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	--	2	--	--	At-risk	Fix
☑ fyj_验证windows修复_2016_使用到1230002 -- Public 192.168.169.55 Private		vpc-w5lwy5q4vgbm12jktikg2	Windows	High risk	Running	Enable	1	2	--	--	At-risk	Fix
☑ wyy-110101-test -- Public 192.168.240.104 Private		vpc-w5lbw0too3hzqy3lhd1kh	Linux	High risk	Running	Enable	124	1	--	--	At-risk	Fix
☐ asrbr-test-wyy -- Public 192.168.240.103 Private		vpc-w5lbw0too3hzqy3lhd1kh	Linux	High risk	Running	Enable	124	1	--	--	At-risk	Fix

   i. Select servers from the list on the right.
   ii. Click **Change Group**.
   iii. In the Change Group dialog box that appears, select a group from the drop-down list.
   iv. Click **OK**.

5.2.1.1.2.2. Manage physical servers

This topic describes how to manage servers. On the Servers page, you can view the status of servers protected by Server Guard.

Procedure

1. Log on to Apsara Stack Security Center.

   > **Note** For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Servers**.
4. **Optional:**Search for a server.
   To view the agent status of a server, enter the server IP address in the search bar, and click **Search**. Detailed server information, such as security information, is displayed.
5. View the agent status and detailed security information of the server.
   Click ⚙ in the upper-right corner of the page to select the information columns you want to display. The following table lists the information categories.

Category	Information
Basic information	◦ Server IP/Name ◦ Tag ◦ OS ◦ Region
Agent status	Agent Status
Threat prevention	◦ Vulnerability ◦ Baseline Risk
Intrusion detection	◦ Unusual Logons ◦ Webshells ◦ Suspicious Servers
Server fingerprints	◦ Processes ◦ Ports ◦ Root Accounts/Total Accounts

6. Manage servers.

Action	Description
Change Group	Select servers and click **Change Group** to add the selected servers to a new group.
Modify Tag	Select servers and click **Modify Tag** to modify tags for the servers.
Security Inspection	Select servers and click **Security Inspection** to select the items to be checked.
Delete External Servers	Select **external** servers, and choose **More > Delete External Servers**.

Disable Protection	Select the servers whose agent status is **Online**, and choose **More > Disable Protection**. This temporarily disables protection for these servers to reduce server resource consumption.
Enable Protection	Select the servers whose agent status is **Disable Protection**, and choose **More > Enable Protection**. This enables protection for these servers.

5.2.1.1.3. Server fingerprints

5.2.1.1.3.1. Manage listening ports

This topic describes how to view information about the listening port of a server. The information helps you identify suspicious listening behavior.

Background information

This topic is suitable for the following scenarios:

- Check for servers that listen on a specific port.
- Check for ports that a specific server listens.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Port** tab to view **listening ports**, **network protocols**, and server information.
   You can search for a port by using the port number, server process name, server name, or server IP address.

   In the server information list, you can view the **process**, **IP address**, and **latest scan time** of a server.

5.2.1.1.3.2. Manage software versions

This topic describes how to regularly view and collect the software version information about a server. This helps you check your software assets.

Background information

This topic covers the following scenarios:

- Check for software assets that are installed without authorization.
- Check for outdated software assets.
- Locate affected assets if vulnerabilities are detected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Server Security > Sever Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Software** tab. On the tab, view all the **software**

assets that are in use and the **number of the servers** that use the software assets. You can search for specific software by using its name, version, installation directory, server name, or IP address.

5. Click software to view the details, such as the software versions and the servers that use the software.

   You can click the ⤓ icon in the upper-right corner to download a software version table to your computer for subsequent asset check.

5.2.1.1.3.3. Manage processes

This topic describes how to regularly collect the process information on a server and record changes. This way, you can view process information and historical process changes.

Background information

This task is suitable for the following scenarios:

- Check for servers on which a specific process runs.
- Check for processes that run on a specific server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Process** tab. On the tab, view all running processes and the number of servers that run these processes.
   You can search for a process by using the **process name**, **running user**, **startup parameter**, or **server name or IP address**.
5. Click the name of a process to view the details of the process, such as the servers, paths, and startup parameters.

5.2.1.1.3.4. Manage account information

This topic describes how to regularly collect the account information on a server and record the changes to the accounts. This way, you can check your accounts and view historical changes to your accounts.

Background information

You can use the information collected in this topic for the following scenarios:

- Check for servers on which a specific account is created.
- Check for accounts that are created on a server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Account** tab.
5. View all the logged-on accounts and the numbers of servers on which the accounts are created.

You can search for an account by using the account name, root permissions, server name, or server IP address.

6. Click an account name to view the details, such as the server information, root permissions, and user group.

5.2.1.1.3.5. Manage scheduled tasks

This topic describes how to view scheduled tasks on servers.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Scheduled Tasks** tab.
5. View the paths of all tasks and the number of servers that run these tasks.
   You can search for a task by using the task path, server name, or IP address.
6. Click a task path to view the details, such as the servers, executed commands, and task cycles.

5.2.1.1.3.6. Set the fingerprint collection frequency

You can set the frequency at which the data of running processes, system accounts, listening ports, and software versions is collected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. In the upper-right corner of the **Asset Fingerprints** page, click **Settings**.
5. Select the collection frequency from each drop-down list.
6. Click **OK** to complete the configuration.

5.2.1.1.4. Intrusion events

5.2.1.1.4.1. Intrusion event types

If Server Guard detects sensitive file tampering, suspicious processes, webshells, unusual logons, or malicious processes, it generates alerts. Based on these alerts, you can monitor the security status of your assets and handle potential threats at the earliest opportunity.

Apsara Stack Security provides statistics on enabled alerts and defense items. These statistics help you monitor the overall security of your assets. You can view the statistics on the **Intrusions** page.

Alerts

The following table describes the alerts.

Alert	Description
Threat intelligence	Identify potential threats to your assets based on the threat intelligence of Apsara Stack Security. Threat intelligence can correlate threat information to analyze and process the information. If threats are detected, threat intelligence can generate alerts. This helps improve the detection efficiency and response speed. Threat intelligence can detect the following items: • Malicious domain names • Malicious IP addresses • IP addresses of dark web services • IP addresses of command and control (C&C) servers • IP addresses of mining pools • Malicious URLs • Malicious download sources
Unusual Logon	Detect unusual logons to your servers. You can specify approved logon IP addresses, time periods, and accounts. Logons from unapproved IP addresses,time periods, or accounts trigger alerts. You can manually add approved logon locations or configure the system to automatically update approved logon locations. You can also specify assets on which alerts are triggered when unapproved logon locations are detected. Server Guard can detect the following events: • Logons to Elastic Compute Service (ECS) instances from unapproved IP addresses • Logons to ECS instances from unapproved locations • Execution of unusual commands after SSH-based logons to ECS instances • Brute-force attacks on SSH passwords of ECS instances
Webshell	Use engines developed by Alibaba Cloud to scan common webshell files. Server Guard supports scheduled scan tasks, provides real-time protection, and quarantines webshell files. • Server Guard scans the entire web directory early in the morning on a daily basis. A change made to files in the web directory triggers dynamic detection. • You can specify the assets on which Server Guard scans for webshells. • You can quarantine or ignore detected trojan files. You can also restore the quarantined trojan files.
Precision defense	The **antivirus** feature provides precise protection from common ransomware, DDoS trojans, mining programs, trojans, malicious programs, webshells, and computer worms.
Suspicious Account	Detect logons to your assets from unapproved accounts.
Cloud threat detection	Detect threats in other cloud services.
Persistence	Detect suspicious scheduled tasks on servers and generate alerts when advanced persistent threats (APTs) to the servers are detected.
Unusual Network Connection	Detect disconnections or unusual network connections.
Suspicious Process	Detect whether suspicious processes exist.

Malicious Process	Scan your servers in real time. An agent is used to collect process information, and the information is uploaded to the cloud for detection. If viruses are detected, alerts are generated. You can handle detected viruses in Apsara Stack Security Center. Server Guard can detect the following malicious activities and processes: • Access to malicious IP addresses • Mining programs • Self-mutating trojans • Malicious programs • Trojans
Sensitive File Tampering	Check whether sensitive files on your servers are maliciously modified. The sensitive files include preloaded configuration files in Linux shared libraries.
Other	Detect other types of attacks, such as DDoS attacks.
Web Application Threat Detection	Detect intrusions that use web applications.
Application intrusion event	Detect intrusions that use system application components.

5.2.1.1.4.2. View and handle alert events

This topic describes how to view and handle detected alert events on the Intrusions page.

Background information

After alert events are detected, the alerts events are displayed on the **Intrusions** page in Apsara Stack Security Center. If the detected alert events are not handled, they are displayed in the **Unhandled Alerts** list on the **Intrusions** page. After the alert events are handled, the status of the alert events changes from **Unhandled Alerts** to **Handled**.

> **Note** Apsara Stack Security Center retains the records of **Unhandled Alerts** and **Handled** on the **Intrusions** page. By default, the records of **Unhandled Alerts** are displayed.

View alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the page that appears, search for or view all alert events. You can also view the details about the alert events.

Handle alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.

3. In the left-side navigation pane, click **Intrusions**.
4. On the **Intrusions** page, find the alert event that you want to handle and click **Handle** in the **Actions** column. In the dialog box that appears, configure Process Method and click **Process Now**.

   > **Note** If the alert event is related to multiple exceptions, the panel that shows alert event details appears after you click **Handle**. You can handle the exceptions in the panel.

   - **Ignore**: If you ignore the alert event, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event.
   - **Add To Whitelist**: If the alert event is a false positive, you can add the alert event to the whitelist. Then, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event. In the **Handled** list, you can click **Cancel whitelist** to remove the alert event from the whitelist.

     > **Note** When Server Guard generates a false alert on a normal process, this alert is considered a false positive. A common false positive is a **suspicious process that sends TCP packets**. The false positive notifies you that suspicious scans on other devices are detected on your servers.

   - **Batch unhandled**: This method allows you to batch handle multiple alert events. Before you batch handle multiple alert events, we recommend that you view the details about the alert events.
5. **Optional:**If you confirm that one or more alert events are false positives or need to be ignored, go to the **Intrusions** page. Then, select the alert events and click **Ignore Once** or **Whitelist**.

Export alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-left corner above the alert event list on the **Intrusions** page, click the ⭳ icon to export the list.
   After the list is exported, the **Done** message appears in the upper-right corner of the Intrusions page.
5. In the **Done** notification of the **Alerts** page, click **Download**.
   The alert list is downloaded to your computer.

5.2.1.1.4.3. View exceptions related to an alert

Server Guard supports automatic analysis of exceptions related to an alert. You can click an alert name in the alert list to view and handle all exceptions that are related to the alert. You can also view the results of automatic attack tracing to analyze the exceptions.

Background information

- Security Center automatically associates alerts with exceptions in real time to detect potential threats.
- Exceptions related to an alert are listed in chronological order. This allows you to analyze and handle the exceptions to improve the emergency response mechanism of your system.

- An automatically correlated alert is identified by the 📌 icon.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the Intrusions page, click the **name of the alert** that you want to handle. The alert details panel appears.
5. In the alert details panel, view the details and related exceptions of the alert. Then, handle the exceptions.
   - View alert details

     You can view the assets that are affected by the alert, the first and latest time when the alert was triggered, and the details about the related exceptions.
   - View affected assets

     You can move the pointer over the name of an **affected asset** to view the details about the asset. The details include information about all the alerts, vulnerabilities, baseline risks, and asset fingerprints on the asset.
   - View and handle **related exceptions**

     In the **Related Exceptions** section, you can view the details about all the exceptions that are related to the alert. You can also view suggestions on how to handle the exceptions.
     - Click **Note** to the right of an exception to add a note for the exception.
     - Click the × icon to the right of a note to delete the note.

5.2.1.1.4.4. Use the file quarantine feature

Sever Guard can quarantine malicious files. Quarantined files are listed in the Quarantine panel of the Intrusions page. You can restore a quarantined file with a few clicks. However, 30 days after a file is quarantined, the system automatically deletes the file. This topic describes how to view and restore quarantined files.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the **Intrusions** page, click **Quarantine**.
   In the **Quarantine** panel, you can perform the following operations:
   - View information about quarantined files. The information includes server IP addresses, directories in which the files are stored, file status, and modification time.
   - Click **Restore** in the **Actions** column to restore a quarantined file. The restored file appears in the alert list.

5.2.1.1.4.5. Configure alerts

This topic describes how to configure alerts. You can specify approved logon locations and customize web directories to scan.

Background information

Server Guard supports advanced logon settings. You can configure more fine-grained logon detection rules. For example, you can specify approved logon IP addresses, logon time ranges, and logon accounts to block unauthorized requests that are sent to your assets.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the page that appears, click **Settings**.
   Configure the parameters on different tabs.
   - **Add an approved logon location**
     a. In the **Login Location** section, click **Management** on the right.
     b. Select the logon location that you want to specify as the approved logon location and select the servers that allow logons from the specified location.
     c. Click **Ok**.

     Server Guard allows you to **edit** or **delete** approved logon locations that you have specified.

     - To change the servers that allow logons from an approved location, find the approved location and click **Edit** on the right.
     - To delete an approved logon location, find the logon location and click **Delete** on the right.
   - **Configure advanced logon settings**

     > ⓘ **Note** When you configure advanced logon settings, you can specify the IP addresses, accounts, and time ranges that are allowed for logons to your assets. After the advanced logon settings are configured, Server Guard generates alerts if your assets receive unauthorized logon requests. The procedure of configuring advanced logon settings is similar to the procedure of configuring **Login Location**. You can **add**, **edit**, or **delete** advanced logon settings in a similar manner.

     - Turn on or turn off Uncommon IP Alert to the right of **Common Login IPs**. If you turn on Uncommon IP Alert and your assets receive logon requests from unapproved IP addresses, alerts are triggered.
     - Turn on or turn off Uncommon Time Alert to the right of **Common Login Time**. If you turn on Uncommon Time Alert and your assets receive logon requests during unapproved time ranges, alerts are triggered.
     - Turn on or turn off Uncommon Account Alert to the right of **Common Login Accounts**. If you turn on Uncommon Account Alert and your assets receive logon requests from unapproved accounts, alerts are triggered.
   - **Add web directories to scan**

     Server Guard automatically scans web directories of data assets in your servers and runs dynamic and static scan tasks. You can also manually add other web directories.

     a. In the **Add Scan Targets** section, click **Management** on the right.

b. Specify a valid web directory and select the servers on which the specified web directory is scanned.

> **Note** To ensure the scan performance and efficiency, we recommend that you do not specify a root directory.

c. Click **Ok**.

5.2.1.1.5. Log retrieval

5.2.1.1.5.1. Supported log sources and fields

This topic describes the log sources and fields that are supported by the log retrieval feature.

The log retrieval feature allows you to query the following types of log sources. You can click a log source link to view the fields that can be retrieved.

Log source	Description
Logon history	Log entries about successful system logons
Logs of brute-force attacks	Log entries about failed system logons during brute-force attacks
Process snapshot logs	Log entries about processes on a server at a specific point in time
Logs of listening port snapshots	Log entries about listening ports on a server at a specific point in time
Account snapshot logs	Log entries about account-based logons on a server at a specific point in time
Process startup logs	Log entries about process startups on a server
Network connection logs	Log entries about active connections from a server to the Internet.

Logon history

The following table describes the fields that you can use to query the logon history.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address used for the logon.
warn_port	string	The logon port.
warn_user	string	The username used for the logon.
warn_type	string	The logon type.

warn_count	string	The number of logon attempts.

Logs of brute-force attacks

The following table describes the fields that you can use to query logs of brute-force attacks.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address of the attack.
warn_port	string	The target port of the attack.
warn_user	string	The target username of the attack.
warn_type	string	The attack type.
warn_count	string	The number of brute-force attack attempts.

Process startup logs

The following table describes the fields that you can use to query process startup logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
pid	string	The ID of the process.
groupname	string	The user group.
ppid	string	The ID of the parent process.
uid	string	The ID of the user.
username	string	The username.
filename	string	The file name.
pfilename	string	The name of the parent process file.
cmdline	string	The command line.
filepath	string	The path of the process file.
pfilepath	string	The path of the parent process file.

Logs of listening port snapshots

The following table describes the fields that you can use to query logs about listening port snapshots.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_port	string	The listening port.
src_ip	string	The listening IP address.
proc_path	string	The path of the process file.
pid	string	The ID of the process.
proc_name	string	The name of the process.
proto	string	The protocol.

Account snapshot logs

The following table describes the fields you can use to query account snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
perm	string	Indicates whether the user has root permissions.
home_dir	string	The home directory.
warn_time	string	The time when a password expiration notification is sent.
groups	string	The group to which the user belongs.
login_ip	string	The IP address of the last logon.
last_chg	string	The time when the password was last changed.
shell	string	The Linux shell command.
domain	string	The Windows domain.
tty	string	The logon terminal.
account_expire	string	The time when the account expires.
passwd_expire	string	The time when the password expires.

last_logon	string	The last logon time.
user	string	The username.
status	string	The account status. Valid values: • 0: disabled • 1: normal

Process snapshot logs

The following table describes the fields that you can use to query process snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
path	string	The path of the process file.
start_time	string	The time when the process was started.
uid	string	The ID of the user.
cmdline	string	The command line.
pname	string	The name of the parent process.
name	string	The name of the process.
pid	string	The ID of the process.
user	string	The username.
md5	string	The MD5 hash value of the process file. If the size of the process file exceeds 1 MB, the system does not calculate the MD5 hash value of the process file.

Network connection logs

The following table describes the fields that you can use to query network connection logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_ip	string	The source IP address.
src_port	string	The source port.

proc_path	string	The path of the process file.
dst_port	string	The destination port.
proc_name	string	The name of the process.
dst_ip	string	The destination IP address.
status	string	The status.

5.2.1.1.5.2. Logical operators

The log retrieval feature supports multiple search conditions. You can add multiple logical operators to one search condition for one log source, or combine multiple search conditions for several log sources by using different logical operators. This topic describes the logical operators that are supported in log retrieval. Examples are provided to help you understand these operators.

The following table describes the logical operators that are supported in log retrieval. Table 1. Logical operators

Logical operator	Description
and	Binary operator. This operator is in the format of `query 1 and query 2`, which indicates the intersection of the query results of `query 1` and `query 2`. **Note** If no logical operators are used for multiple keywords, the default operator is AND.
or	Binary operator. This operator is in the format of `query 1 or query 2`, which indicates the union of the query results of `query 1` and `query 2`.
not	Binary operator. This operator is in the format of `query 1 not query 2`, which indicates the results that match `query 1` but do not match `query 2`. This format is equivalent to `query 1 - query 2`. **Note** If you use only `not query 1`, the log data that does not contain the query results of `query 1` is returned.

5.2.1.1.5.3. Query logs

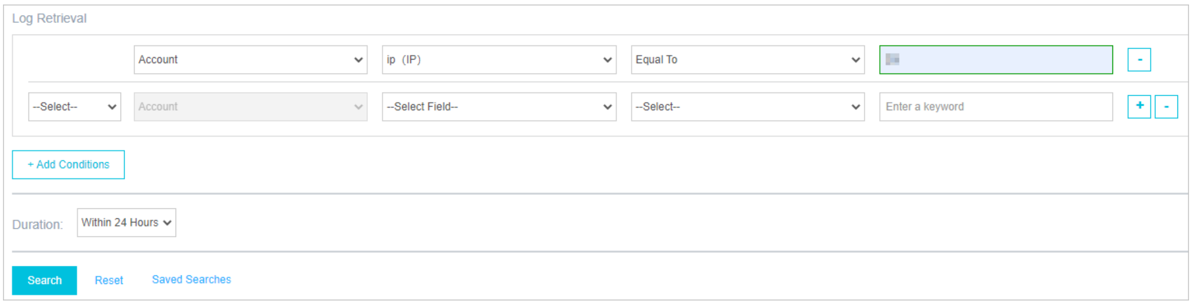
This topic describes how to search for and view physical server logs.

Procedure

1. Log on to Apsara Stack Security Center.

> Note For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Log Retrieval**.
4. Specify search conditions.



> Note For more information about log sources, log fields, and logical operators, see Supported log sources and fields and Inference rules and logical operators.

5. Click **Search** and view the search result.
   - **Reset**: Click **Reset** to clear the search condition configurations.
   - **Save Search**: Click **Save Search** to save the search condition configurations which you can use to search for logs in the future.
   - **Saved Searches**: Click **Saved Searches** to select and use a search condition that you saved.

5.2.1.1.6. Configure security settings for physical servers

This topic describes how to configure security settings for physical servers. You can enable or disable periodic trojan scans. You can also specify the working mode of the Server Guard agent.

Procedure

1. Log on to Apsara Stack Security Center.

> Note For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the left-side navigation pane, choose **Physical Server Security > Settings**.
3. Enable periodic trojan scans for physical servers.
   i. In the Trojan Scan section, click **Manage**.
   ii. In the All Servers section, select the physical servers on which you want to perform periodic trojan scans. Then, click the rightwards arrow.
   iii. Click **OK**.
4. On the **Protection First Mode** page, click **Manage** next to Protection Mode. Configure protection modes for servers.

- **Business First Mode**: In this mode, the peak CPU utilization is less than 10%, and the peak memory usage is less than 50 MB.
- **Protection First Mode**: In this mode, the peak CPU utilization is less than 20%, and the peak memory usage is less than 80 MB.

5.3. Network security

5.3.1. Network Security Management Center

5.3.1.1. East-west security management

5.3.1.1.1. Policy center

5.3.1.1.1.1. Policy content management

You can view and manage the CIDR block whitelist and virtual private cloud (VPC) whitelist on the Policy Content Management page.

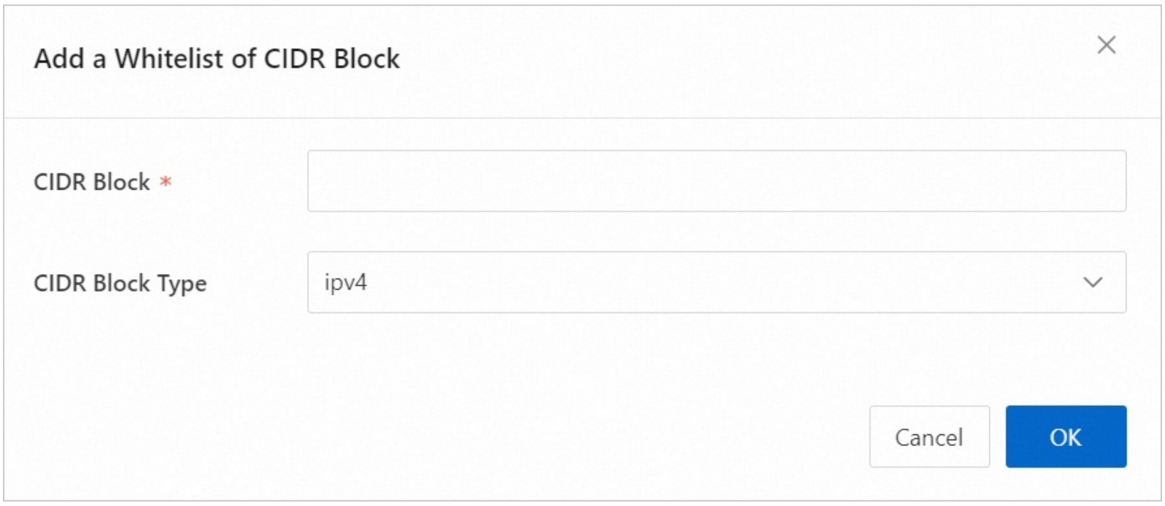
Background information

- The CIDR block whitelist is used to manage access to virtual IP addresses (VIPs) of classic networks by using AccessKey pairs of Alibaba Cloud accounts. Only users that use CIDR blocks in the whitelist can access VIPs of classic networks and call API operations by using Alibaba Cloud accounts.
- The VPC whitelist is used to manage access to AnyTunnel VIPs. Only VPCs in the whitelist can access specific AnyTunnel VIPs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Network Security** > **Network Security Management Center**.
3. In the left-side navigation pane, choose **Security Management** > **Policy Center** > **Policy Content Management**.
4. On the **CIDR Block Whitelist** tab, perform the following operations:
    - Add a CIDR block whitelist: click **Add a Whitelist of CIDR Block**, configure the parameters, and then click **OK**. The following table describes the parameters.

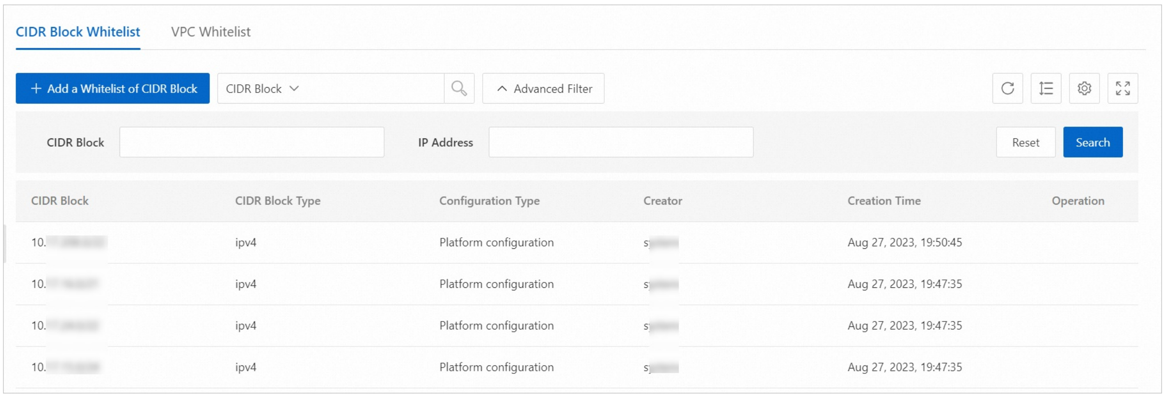
Parameter	Description
CIDR Block	Enter a CIDR block that you want to add to the whitelist.
CIDR Block Type	The type of the CIDR block. Only**ipv4** is supported.



CIDR Block *

CIDR Block Type: ipv4

- View the CIDR block whitelist: click **Advanced Filter** and filter CIDR blocks by **CIDR Block** and **IP Address**.



CIDR Block

IP Address

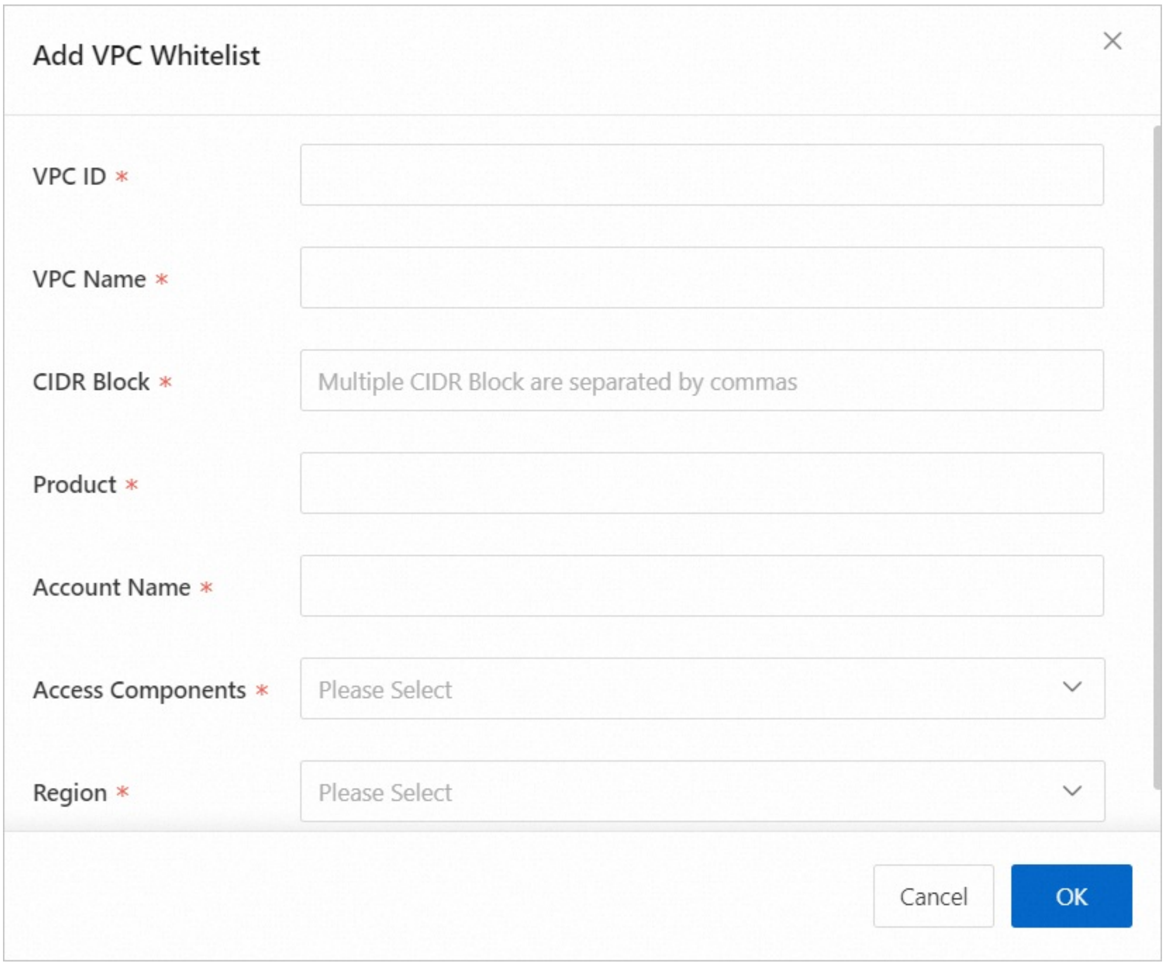
CIDR Block	CIDR Block Type	Configuration Type	Creator	Creation Time	Operation
10.[redacted]	ipv4	Platform configuration	s[redacted]	Aug 27, 2023, 19:50:45	
10.[redacted]	ipv4	Platform configuration	s[redacted]	Aug 27, 2023, 19:47:35	
10.[redacted]	ipv4	Platform configuration	s[redacted]	Aug 27, 2023, 19:47:35	
10.[redacted]	ipv4	Platform configuration	s[redacted]	Aug 27, 2023, 19:47:35	

5. On the **VPC Whitelist** tab, perform the following operations:

   - Add a VPC whitelist: click **Add VPC Whitelist**, configure the parameters, and then click **OK**. The following table describes the parameters.

Parameter	Description
VPC ID	Enter the ID of the VPC that you want to add to the VPC whitelist.
VPC Name	Enter the name of the VPC that you want to add to the VPC whitelist.
CIDR Block	Enter CIDR blocks of the VPC that you want to add to the whitelist. Separate multiple CIDR blocks with commas (,).
Product	Enter the product to which the VPC belongs.
Account Name	Enter the ID of the account to which the VPC belongs.

Access Components	Select components that can be accessed by the VPC. You can specify multiple components. ▪ pop-inner ▪ asapi-inner ▪ sls-inner ▪ docker-registry
Region	Select the region where the VPC takes effect.



Add VPC Whitelist

VPC ID *

VPC Name *

CIDR Block * Multiple CIDR Block are separated by commas

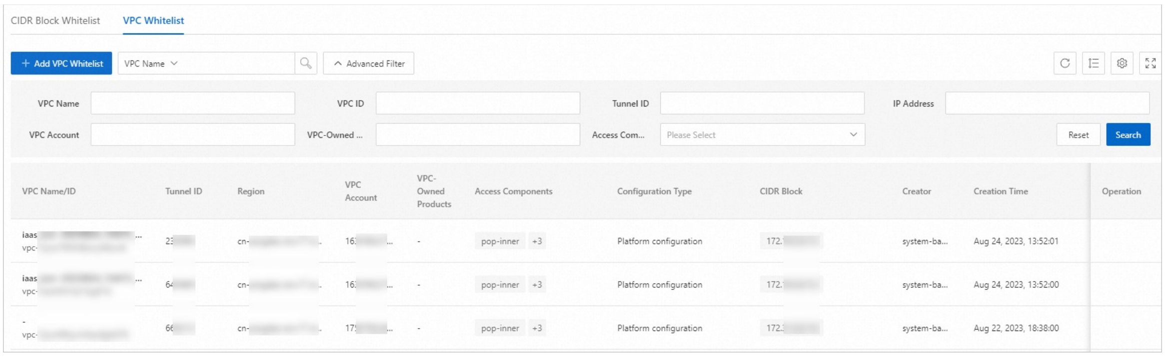
Product *

Account Name *

Access Components * Please Select

Region * Please Select

- View the VPC whitelist: click **Advanced Filter** and filter VPCs by **VPC Name**, **VPC ID**, **Tunnel ID**, **IP Address**, **VPC Account**, **VPC-Owned Products**, and **Access Components**.



VPC Name/ID	Tunnel ID	Region	VPC Account	VPC-Owned Products	Access Components	Configuration Type	CIDR Block	Creator	Creation Time	Operation
iaas[redacted]... vpc-[redacted]	23[redacted]	cn-[redacted]	16[redacted]...	-	pop-inner +3	Platform configuration	172.[redacted]	system-ba...	Aug 24, 2023, 13:52:01	
iaas[redacted]... vpc-[redacted]	64[redacted]	cn-[redacted]	16[redacted]...	-	pop-inner +3	Platform configuration	172.[redacted]	system-ba...	Aug 24, 2023, 13:52:00	
- vpc-[redacted]	66[redacted]	cn-[redacted]	17[redacted]...	-	pop-inner +3	Platform configuration	172.[redacted]	system-ba...	Aug 22, 2023, 18:38:00	

5.3.1.1.1.2. VIP protection

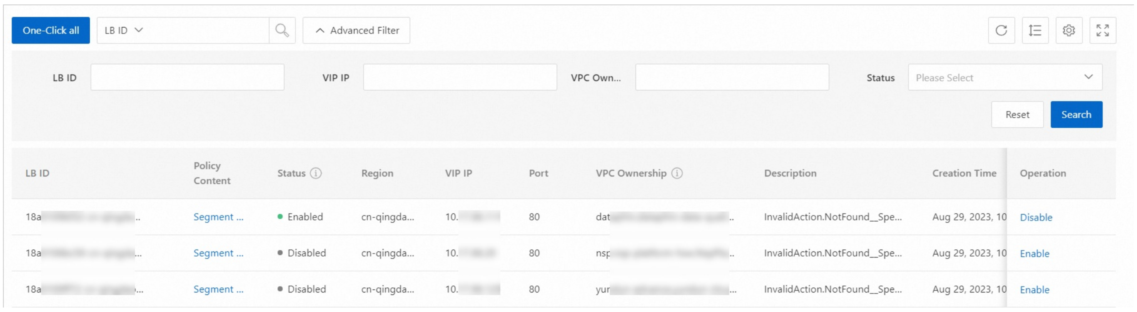
Platform VIP security protection includes classic network VIP and AnyTunnel VIP security protection policies. This feature is used to limit the access scope of classic network VIP and AnyTunnel VIP to avoid security risks caused by excessive open access scope.

Background information

- Classic network VIP protection: By using the ACL capability of SLB, the classic network VIP can only be accessed by the base classic network.
- AnyTunnel VIP protection: For AnyTunnel VIPs provided by the platform, you can configure a VPC whitelist by using the ACL capability of SLB to allow access only from trusted VPCs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Network Security** > **Network Security Management Center**.
3. In the left-side navigation pane, choose **East-west Security Management** > **Policy Center** > **VIP Security**.
4. On the **Classic network VIP** tab, you can perform the following operations:
    - Enable or disable the **Add the default whitelist policy for classic network VIP** .
        - Enable: If you add a classic network VIP, a whitelist policy is applied by default. This policy allows the VIP to be used only within the CIDR block whitelist.
        - Disable: By default, the whitelist policy is no longer issued for new classic network VIPs.
    - View the content of the whitelist policy for classic network VIP
        a. Click **Advanced Filter** to obtain the whitelist policy information of the classic network VIP by **LB ID**, **VIP IP**, **VPC Ownership**, and **Status**.



LB ID	Policy Content	Status	Region	VIP IP	Port	VPC Ownership	Description	Creation Time	Operation
18a[redacted]...	Segment ...	● Enabled	cn-qingda...	10.[redacted]	80	dat[redacted]...	InvalidAction.NotFound_Spe...	Aug 29, 2023, 10	Disable
18a[redacted]...	Segment ...	● Disabled	cn-qingda...	10.[redacted]	80	nsp[redacted]...	InvalidAction.NotFound_Spe...	Aug 29, 2023, 10	Enable
18a[redacted]...	Segment ...	● Disabled	cn-qingda...	10.[redacted]	80	yur[redacted]...	InvalidAction.NotFound_Spe...	Aug 29, 2023, 10	Enable

        b. Click **CIDR block whitelist** in the **Policy Content** column corresponding to the target classic network VIP. You are redirected to the **CIDR block whitelist** tab on the **Policy Content Management** page.

- Enable or disable the Classic network VIP whitelist policy
  - Enable: Click **Enable** in the **Actions** column corresponding to the target classic network VIP. In the dialog box that appears, confirm the information and click **OK**.

    > **Note**
    >
    > When the **Status** of the whitelist policy of the classic network VIP is **Disabled**, and the content in the **Description** column is not **The current VIP has been bound to another ACL policy, and the whitelist policy cannot be issued.** You can enable the whitelist policy of the classic network VIP.

  - Disable: Click **Disable** in the **Actions** column corresponding to the target classic network VIP. In the dialog box that appears, confirm the information and click **OK**.

    > **Note**
    >
    > - If the **Status** of the whitelist policy of the classic network VIP is **Enabled**, you can disable the whitelist policy of the classic network VIP.
    > - If you disable this operation, the classic network VIP does not have security control policies. This poses security risks.

- Disable all whitelist policies for classic network VIPs

  a. In the upper part of the page, click **One-click All**.

  b. In the message that appears, click **Delete**.

  > **Important**
  >
  > If you release all of them with one click, the whitelist policies of all classic network VIPs that have been issued will be disabled, and the security prevention and control capabilities of the source IP address will not be available, which will cause a certain degree of security risks. After performing one-click all, if you want to restart the VIP security feature, you need to manually enable it for each LB, so please confirm it before executing it.

5. On the **AnyTunnel VIP** tab, you can perform the following operations:

- View the whitelist policy information of AnyTunnel VIP

  > **Note**
  >
  > - If the AnyTunnel VIP is enabled, the whitelist can access the VPC and Tiangong. If the AnyTunnel VIP is disabled, the whitelist can access the VPC and Tiangong.
  > - If classToAnyTunnel types of VIPs are enabled, they can be accessed from VPCs and Tiangong in the whitelist. If they are disabled, they can be accessed from all VPCs without a whitelist policy.

  Click **VPC Whitelist** in the **Policy Content** column corresponding to the AnyTunnel VIP. You are redirected to the **VPC Whitelist** tab on the **Policy Content Management** page.

- Enable or disable the whitelist policy for AnyTunnel VIP

- Enable: **Enable** in the Actions column corresponding to the AnyTunnel VIP. In the dialog box that appears, confirm the information and click **OK**.

  > **Note**
  >
  > - If the **Status** of the whitelist policy for an AnyTunnel VIP is **Disabled**, you can enable the whitelist policy for an AnyTunnel VIP.
  > - The Enable action allows VPC networks in the VPC whitelist to access this AnyTunnel VIP.

- Disable the AnyTunnel VIP: **Disable** in the Actions column. In the dialog box that appears, confirm the information and click **OK**.

  > **Note**
  >
  > - If the **Status** of the whitelist policy for an AnyTunnel VIP is **Enabled**, you can disable the whitelist policy for an AnyTunnel VIP.
  > - You cannot manually disable the anyTunnelVIP of ASAPI and POP.
  > - If you disable this operation, the AnyTunnel VIP does not have security control policies. This poses security risks.

5.4. Account security

5.4.1. Linux account management

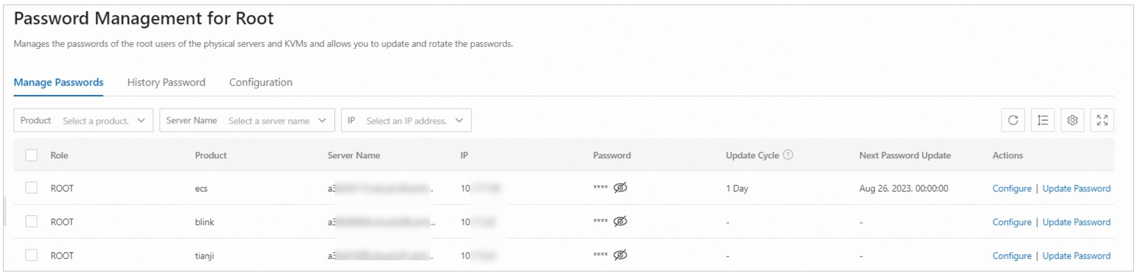
5.4.1.1. Password management for root

The Password Management for Root module allows you to obtain and manage the passwords of all root users in physical servers and KVMs in the Apsara Stack environment. You can use this module to update and rotate the passwords.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Linux Account Management**.
3. In the left-side navigation pane, click **Password Management for Root**.
4. On the **Manage Passwords** tab, you can view the information about all physical servers and KVMs in the Apsara Stack environment. You can also perform the following operations:
   - Query the information about a physical server or KVM.

a. To query a physical server or KVM, you can select the **product**, **hostname**, and **IP address** of the physical server or KVM from the corresponding filters. The following figure shows the information about physical servers and KVMs that you can view on the Manage Passwords tab.



Password Management for Root

Manages the passwords of the root users of the physical servers and KVMs and allows you to update and rotate the passwords.

□	Role	Product	Server Name	IP	Password	Update Cycle	Next Password Update	Actions
□	ROOT	ecs	a[redacted]	10[redacted]	**** 👁	1 Day	Aug 26, 2023, 00:00:00	Configure | Update Password
□	ROOT	blink	a[redacted]	10[redacted]	**** 👁	-	-	Configure | Update Password
□	ROOT	tianji	a[redacted]	10[redacted]	**** 👁	-	-	Configure | Update Password

b. If you click the 👁 icon next to a password in the **Password** column, the password is displayed in plaintext for 10 seconds.

- Update a password
  - To update the password of a physical server or KVM, perform the following operations: Find the physical server or KVM for which you want to update the password and click **Update Password** in the **Actions** column. In the Update Password dialog box, specify the new password that you want to use for the physical server twice and click **OK**.
  - To update the passwords of multiple physical servers or KVMs at a time, perform the following operations: Select multiple physical servers or KVMs for which you want to update the passwords and click **Batch Update** in the lower part of the page. In the Update Password dialog box, specify the new password that you want to use for the physical servers twice and click **OK**.

  > **Note**
  >
  > - The password must be 12 to 30 characters in length and contain at least three of the following data types: lowercase letters, uppercase letters, digits, and special characters.
  > - Make sure that the same password is entered twice.

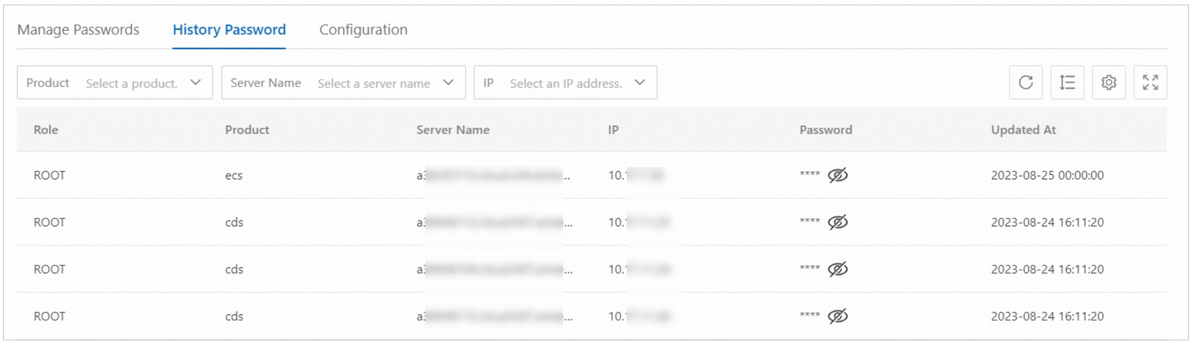
- Configure a password expiration period
  - To configure the password expiration period for a physical server or KVM, perform the following operations: Find the physical server or KVM for which you want to configure the password expiration period and click **Configure** in the **Actions** column. In the Configuration Items dialog box, specify a password expiration period and click **OK**.
  - To configure the password expiration periods for multiple physical servers or KVMs at a time, perform the following operations: Select multiple physical servers or KVMs for which you want to configure the password expiration periods and click **Set Passwords** in the lower part of the page. In the Configuration Items dialog box, specify a password expiration period and click **OK**.

  > **Note**
  >
  > The valid password expiration period ranges from 1 day to 180 days.

5. On the **History Password** tab, you can view the password update records of all physical servers and KVMs in the Apsara Stack environment.

To query the password update records of a physical server or a KVM, you can select the **product**, **hostname**, and **IP address** of the physical server from the corresponding filters.

If you click the 👁 icon next to a password in the **Password** column, the password is displayed in plaintext for 10 seconds.



Manage Passwords | History Password | Configuration

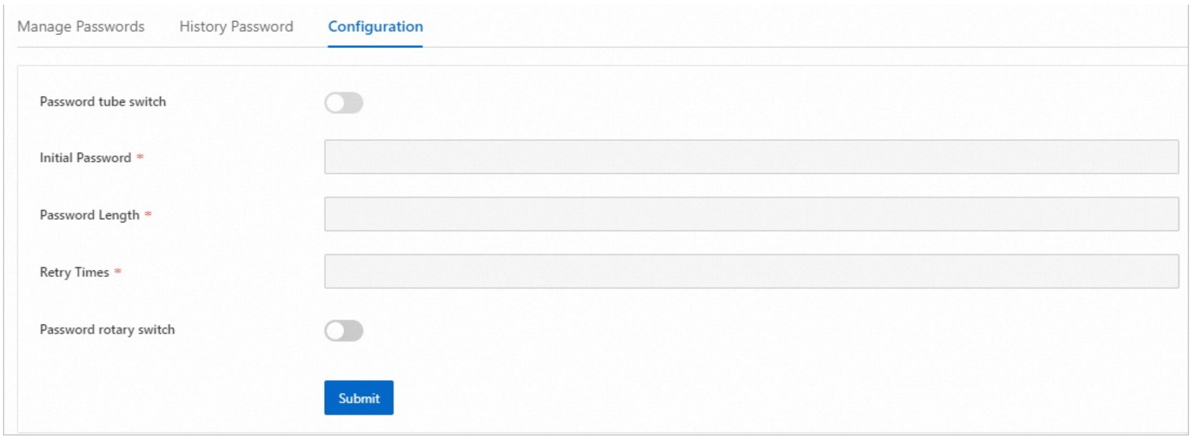
Product: Select a product. | Server Name: Select a server name | IP: Select an IP address.

Role	Product	Server Name	IP	Password	Updated At
ROOT	ecs	a[redacted]...	10.[redacted]	**** 👁	2023-08-25 00:00:00
ROOT	cds	a[redacted]...	10.[redacted]	**** 👁	2023-08-24 16:11:20
ROOT	cds	a[redacted]...	10.[redacted]	**** 👁	2023-08-24 16:11:20
ROOT	cds	a[redacted]...	10.[redacted]	**** 👁	2023-08-24 16:11:20

6. On the **Configuration** tab, you can view and modify the configuration policy of the passwords. Then, click **Submit** to update the configuration policy.

   The following table describes the parameters that you can configure.

Parameter	Description
Password tube switch	Specifies whether to enable password policy configuration. ◦ If you turn on this switch, you can modify the configuration policy of server or KVM passwords, such as password updates and automatic rotation. ◦ If you turn off this switch, you cannot modify the configuration policy of server or KVM passwords, such as password updates and automatic rotation.
Initial Password	The password that is assigned to a physical server or a KVM when the server or KVM is deployed in the Apsara Stack environment.
Password Length	The maximum length of an automatically updated password.
Retry Times	The number of retries after the password fails to be updated.
Password rotary switch	Specifies whether to enable automatic password rotation. ◦ If you turn on this switch, automatic password rotation is enabled. ◦ If you turn off this switch, automatic password rotation is disabled.



Manage Passwords | History Password | Configuration

Password tube switch	○
Initial Password *	
Password Length *	
Retry Times *	
Password rotary switch	○

Submit

5.4.1.2. SSH key management

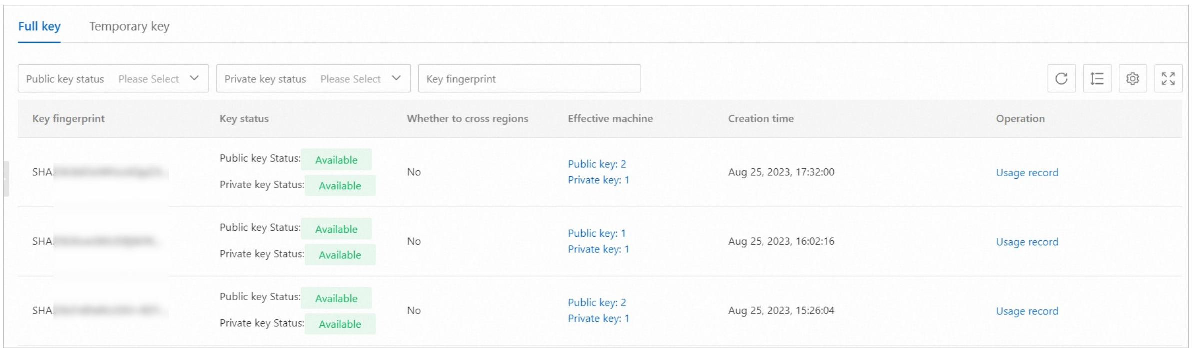
This feature allows you to view and manage SSH keys on physical machines, KVMs, and containers in Apsara Stack. This feature allows you to view full keys, query key validation records and usage records, and manage temporary keys.

Prerequisites

- You have obtained the permissions to manage SSH keys on the host.
- The Tianji-sshtunnel service is in desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Linux Account Management**.
3. In the left-side navigation pane, click **SSH Key Management**.
4. On the **Full Key** tab, you can filter key fingerprints by **Public Key Status**, **Private Key Status**, and **Key Fingerprint**. The **Key Fingerprint** field supports fuzzy search.



Full key | Temporary key

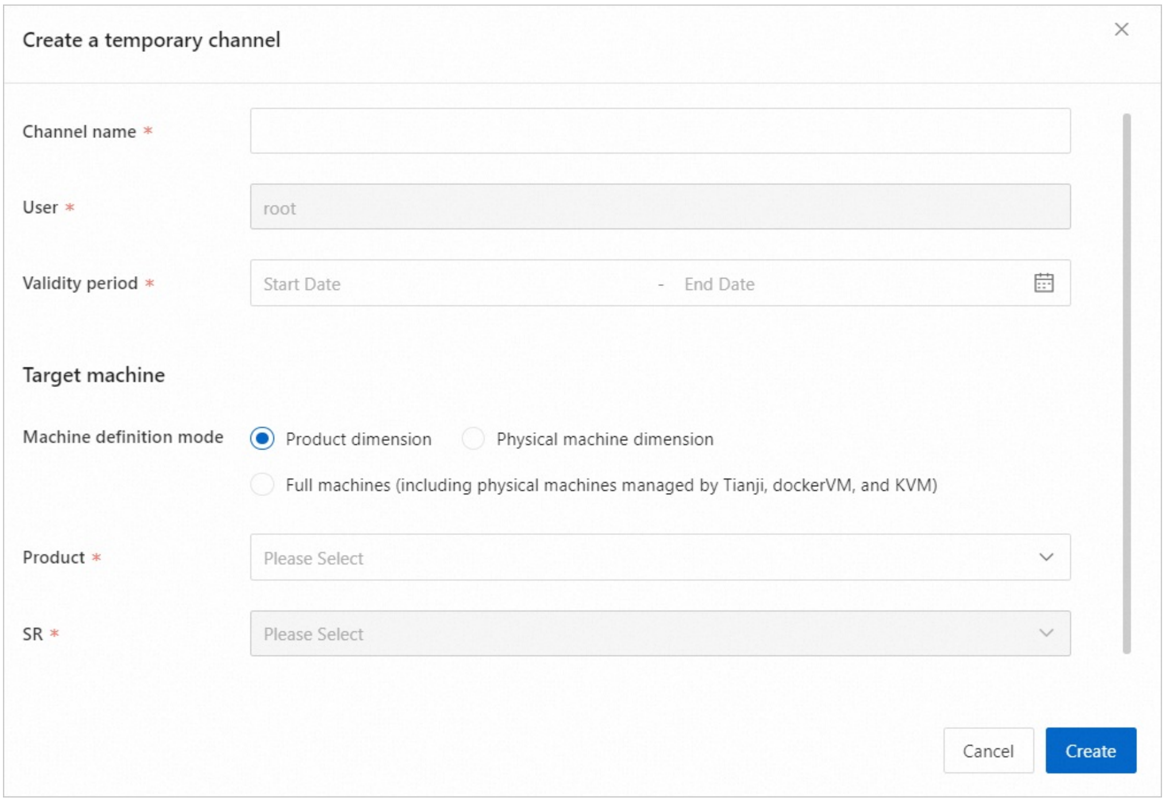
Public key status: Please Select | Private key status: Please Select | Key fingerprint

Key fingerprint	Key status	Whether to cross regions	Effective machine	Creation time	Operation
SHA[redacted]	Public key Status: Available Private key Status: Available	No	Public key: 2 Private key: 1	Aug 25, 2023, 17:32:00	Usage record
SHA[redacted]	Public key Status: Available Private key Status: Available	No	Public key: 1 Private key: 1	Aug 25, 2023, 16:02:16	Usage record
SHA[redacted]	Public key Status: Available Private key Status: Available	No	Public key: 2 Private key: 1	Aug 25, 2023, 15:26:04	Usage record

   - In the **Machine** column of the target key fingerprint, click any blue icon. In the panel that appears, you can view the **public key** information, including the public key, machine name, container ID, user, key path, status, and creation time. You can also view the **private key** information, including the machine name, user, key path, container ID, status, and creation time.
   - Click **Usage Records** in the **Actions** column of the target key fingerprint. In the panel that appears, you can view the **source**, **target**, and **Usage Time** of the key.
5. On the **Temporary Key** tab, you can create a temporary channel to obtain temporary keys.

i. Click **Create Temporary Channel**. In the dialog box that appears, configure the following parameters and click **Create**.

Parameter	Description
Channel name	The name of the temporary channel.
Validity period	The dates when the temporary channel starts and stops taking effect.
Machine definition mode	Select the delineation method of the target machine. ▪ Product dimension ▪ Physical Machine Dimension ▪ All machines, including Apsara Infrastructure Management Framework-managed physical machines, dockerVMs, and KVMs
The product that triggered the alert.	This field takes effect only when you set **Machine Dimensions** to **Product Dimension**. Fuzzy match is supported.
SR	This field takes effect only when you set **Machine Dimensions** to **Product Dimension**. You can select multiple server roles from the drop-down list.
Machine name	This property takes effect only when you set **Machine Deposition Method** to **Physical Machine Dimension**. The name of the server. Fuzzy match is supported.



Create a temporary channel

Channel name *

User * root

Validity period * Start Date - End Date

Target machine

Machine definition mode ● Product dimension ○ Physical machine dimension

○ Full machines (including physical machines managed by Tianji, dockerVM, and KVM)

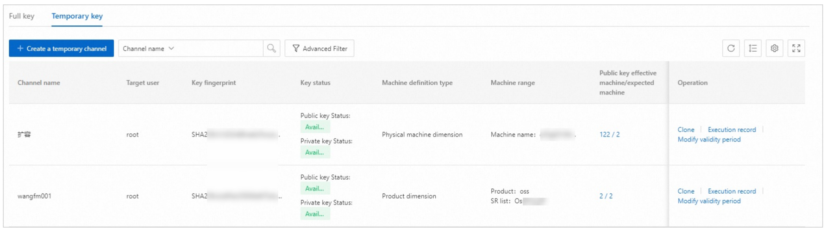
Product * Please Select

SR * Please Select

ii. The following table describes other operations that you can perform on the Temporary key tab.

<table>
<tr><th>Operation</th><th>Description</th></tr>
<tr><td>View temporary channels</td><td>

a. Click **Advanced Filter** to obtain the information of the target channel by **Channel Name**, **Key Fingerprint**, **Public Key Status**, and **Private Key Status**.



Full key | Temporary key

+ Create a temporary channel | Channel name | Advanced Filter

<table>
<tr><th>Channel name</th><th>Target user</th><th>Key fingerprint</th><th>Key status</th><th>Machine definition type</th><th>Machine range</th><th>Public key effective machine/expected machine</th><th>Operation</th></tr>
<tr><td>扩容</td><td>root</td><td>SHA2[redacted]</td><td>Public key Status: Avail...
Private key Status: Avail...</td><td>Physical machine dimension</td><td>Machine name: [redacted]</td><td>122 / 2</td><td>Clone | Execution record | Modify validity period</td></tr>
<tr><td>wangfm001</td><td>root</td><td>SHA2[redacted]</td><td>Public key Status: Avail...
Private key Status: Avail...</td><td>Product dimension</td><td>Product: oss
SR list: Os[redacted]</td><td>2 / 2</td><td>Clone | Execution record | Modify validity period</td></tr>
</table>

b. Click the number in the **Public Key Effective Machine /Expected Machine** column corresponding to the target temporary channel. In the panel that appears, you can view the list of machines whose public keys are effective, including **Machine Name**, **Container ID**, **User**, **Key Path**, and **Status**.

</td></tr>
<tr><td>Clone a temporary channel</td><td>

a. Click **Clone** in the **Actions** column corresponding to the temporary channel. In the dialog box that appears, you can view a temporary channel with the same configurations.

b. Modify the parameters as required and click **Create Create**.

</td></tr>
<tr><td>View execution records</td><td>

a. Click **Execution Records** in the **Actions** column corresponding to the temporary channel.

b. On the **Linux Account Management Tasks** page, click the **Task Execution Records** tab to obtain the execution record details.

</td></tr>
<tr><td>Modify the validity period</td><td>

a. Click **Modify Validity Period** in the **Actions** column corresponding to the temporary channel.

b. In the Modify validity period dialog box, specify a new validity period for the temporary channel and click **OK**. The maximum duration of a validity period is 90 days.

> **Note**
>
> When the validity period of a temporary channel expires, you cannot modify the validity period.

</td></tr>
</table>

5.4.1.3. System user management

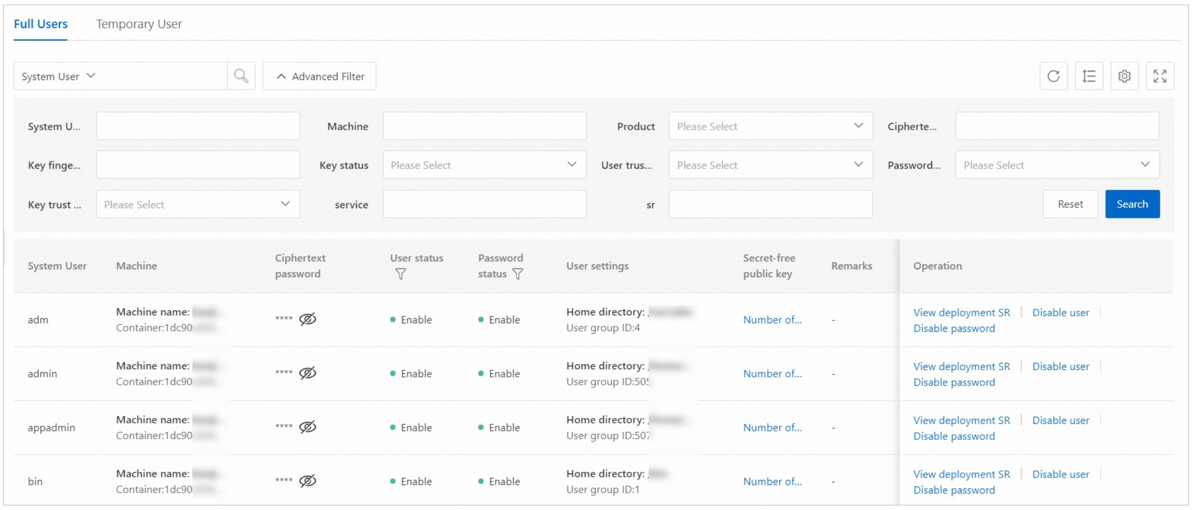
You can manage Linux users, passwords, and SSH keys on physical servers and containers, including granting /canceling, disabling /enabling, and creating temporary system users.

Procedure

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

2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Linux Account Management**.
3. In the left-side navigation pane, choose **System User Management**.
4. On the **Full Users** tab, click **Advanced Filter** to filter system users by **System User**, **Machine**, **Product**, **Ciphertext Password**, **Key Fingerprint**, **Key Status**, **User Information Status**, **Password Trust Status**, **Key Trust Status**, **service**, and **sr**.

> **Note**
>
> - In the **User Status** and **Password Status** columns, you can filter users who are **disabled** or **enabled**.
> - Click the icon in the **Ciphertext Password** column. The password of the system user is displayed in plaintext. The ciphertext is automatically restored after an interval of 10 seconds.

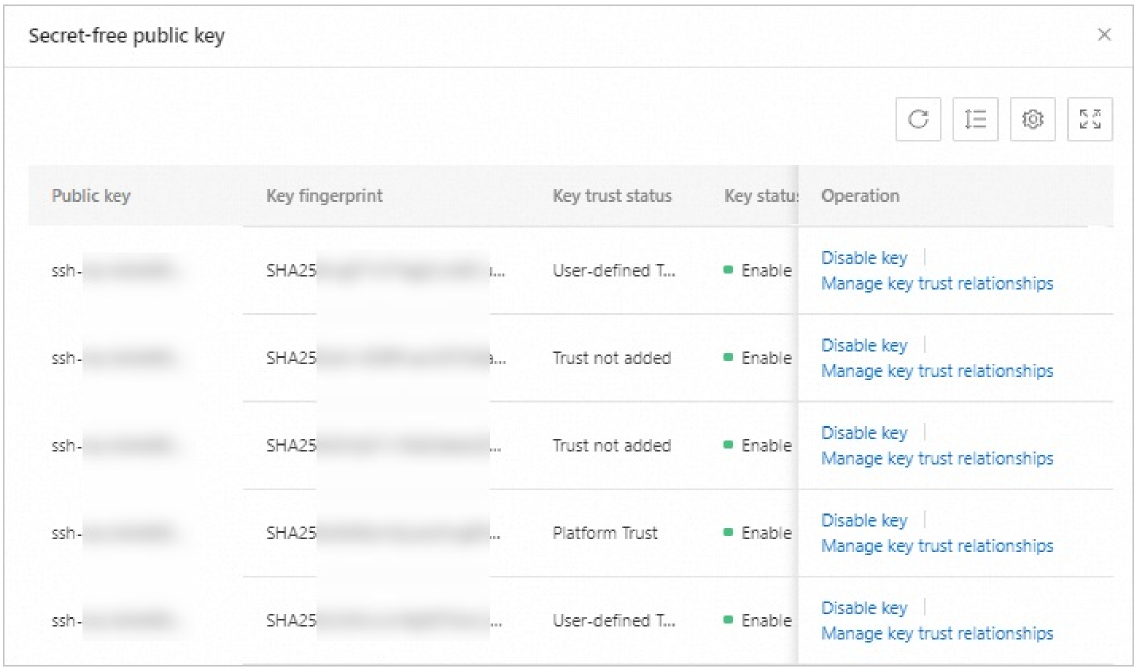


System U...		Machine		Product	Please Select	Cipherte...	
Key finge...		Key status	Please Select	User trus...	Please Select	Password...	Please Select
Key trust ...	Please Select	service		sr		Reset	Search

System User	Machine	Ciphertext password	User status	Password status	User settings	Secret-free public key	Remarks	Operation
adm	Machine name: [redacted] Container:1dc90[redacted]	****	● Enable	● Enable	Home directory: [redacted] User group ID:4	Number of...	-	View deployment SR | Disable user | Disable password
admin	Machine name: [redacted] Container:1dc90[redacted]	****	● Enable	● Enable	Home directory: [redacted] User group ID:50[redacted]	Number of...	-	View deployment SR | Disable user | Disable password
appadmin	Machine name: [redacted] Container:1dc90[redacted]	****	● Enable	● Enable	Home directory: [redacted] User group ID:50[redacted]	Number of...	-	View deployment SR | Disable user | Disable password
bin	Machine name: [redacted] Container:1dc90[redacted]	****	● Enable	● Enable	Home directory: [redacted] User group ID:1	Number of...	-	View deployment SR | Disable user | Disable password

5. You can also perform the following operations on the added physical tables:
   - View the information about secret-free public keys
     a. Find the system user that you want to view and click Number of public keys in the **Secret-free public key** column.

b. In the panel that appears, view the information about the secret-free public key, including **Public Key**, **Key Fingerprint**, **Key Trust Status**, **Key Status**, and **Obtain Time**.



Secret-free public key

Public key	Key fingerprint	Key trust status	Key statu:	Operation
ssh-[redacted]	SHA25[redacted]...	User-defined T...	● Enable	Disable key | Manage key trust relationships
ssh-[redacted]	SHA25[redacted]...	Trust not added	● Enable	Disable key | Manage key trust relationships
ssh-[redacted]	SHA25[redacted]...	Trust not added	● Enable	Disable key | Manage key trust relationships
ssh-[redacted]	SHA25[redacted]...	Platform Trust	● Enable	Disable key | Manage key trust relationships
ssh-[redacted]	SHA25[redacted]...	User-defined T...	● Enable	Disable key | Manage key trust relationships

c. In the **Actions** column, click **Disable Key** if **Status** is **Enabled**. In the message that appears, click **OK** to disable the CMK. In the message that appears, click **Enable Key** if **Status** is **Disabled**. In the message that appears, click **OK** to enable the CMK.

> **Note**
>
> Untrusted keys are automatically removed on a regular basis.

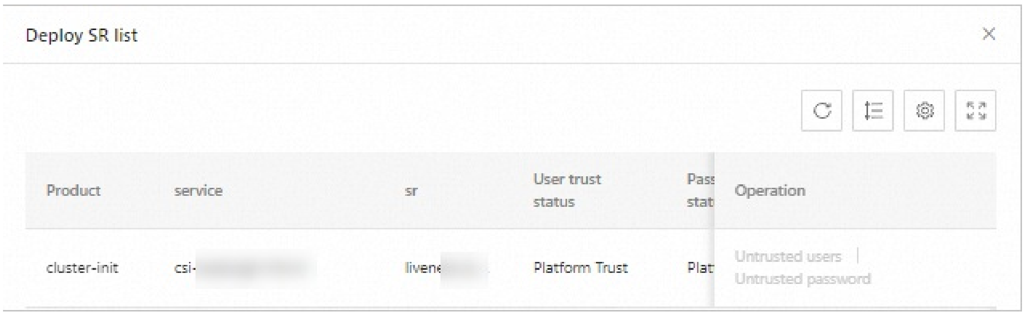
d. In the **Actions** column, click **Manage Key Trust Relationships**. In the dialog box that appears, specify which sRs are allowed to trust the key or cancel the trust of the key. Then, click **OK**.

> **Note**
>
> If **Key Trust Status** is set to **Platform Trust**, you cannot manage key trust relationships.

- View the server role information for the deployment

a. Find the system user that you want to view and click **View deployment SR** in the **Operation** column.

b. In the panel that appears, view the server role information for the deployment, including the **product**, **service**, **server role**, **user trust status**, and **password trust status**.



Deploy SR list

Product	service	sr	User trust status	Pass stat	Operation
cluster-init	csi-[redacted]	livene[redacted]	Platform Trust	Plat	Untrusted users | Untrusted password

c. In the Actions column, click **Trust User** or **Trust Password** to add a user to the trust status. Click **Untrust User** or **Untrust Password** to cancel the trust.

> **Note**
>
> - If **User Trust Status** or **Password Trust Status** is set to **Platform Trust**, you cannot cancel the trust.
> - When performing the trust password operation, we will scan the system users existing on the machine and verify whether the password meets your expectation, so as to prevent potential risks such as password tampering caused by other reasons.

- Disable or enable a system user

a. In the **Actions** column, click **Disable User** or **Enable User**.

> **Note**
>
> If the **User Status** field is set to **Enabled**, the **Disable** operation is supported. If the **User Status** field is set to **Disabled**, the **Enable** operation is supported.

b. In the message that appears, confirm the information about the **system user**, **physical server**, and **container**, and click **OK**.

- Disable or enable the password of a system user

a. In the **Actions** column, click **Disable Password** or **Enable Password**.

> **Note**
>
> The **Disable Password** operation is supported when **Password Status** is **Enabled**. The **Enable Password** operation is supported when **Password Status** is **Disabled**.

b. In the dialog box that appears, confirm the system user information and click **OK**.

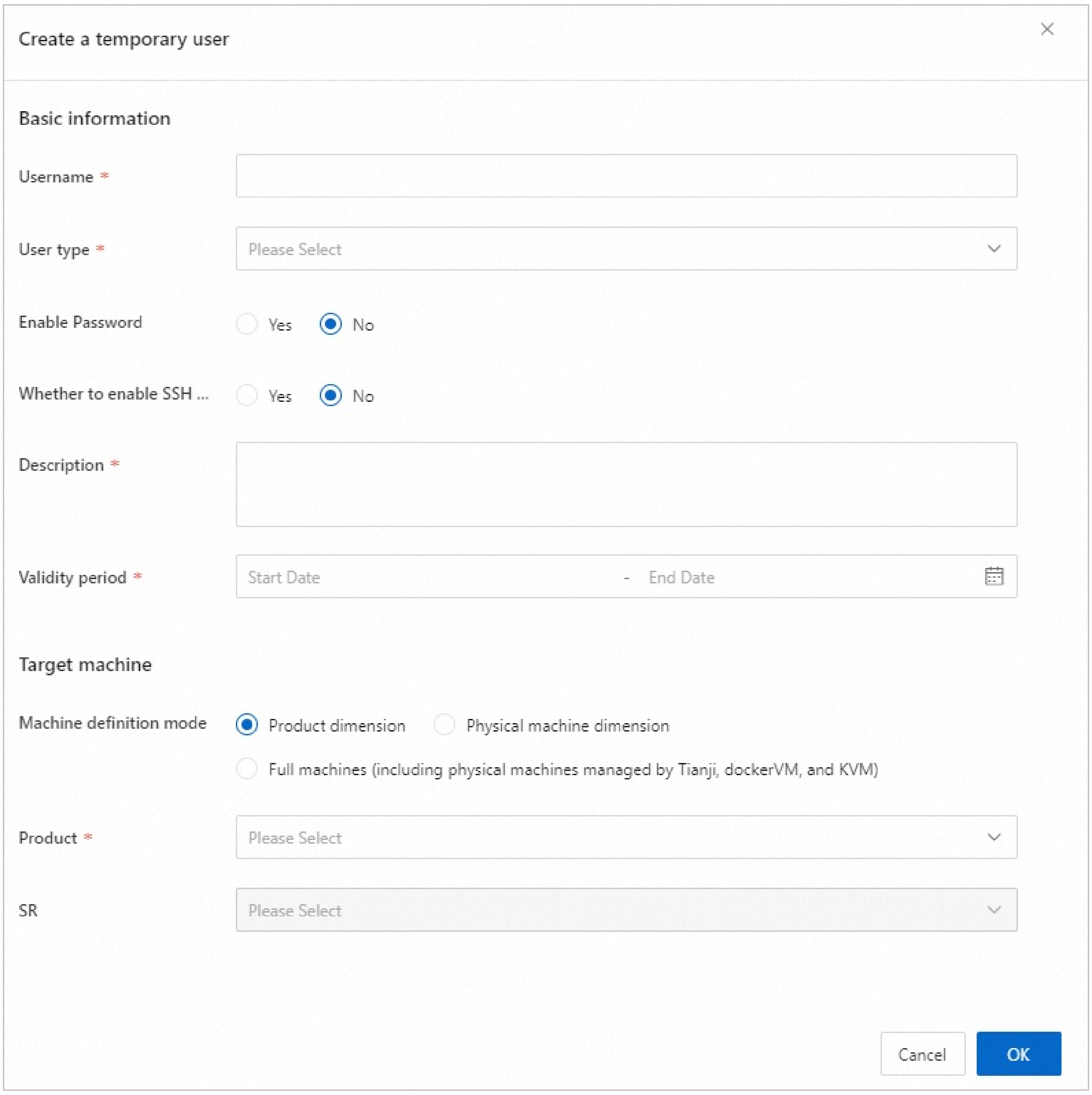
6. On the **Temporary Users** tab, you can create temporary users.

i. Click **Create Temporary User**. In the dialog box that appears, configure the following parameters and click **OK**.

Parameter	Description

Username	Enter the name of the temporary user.
User type	Select a user type. ▪ regular user ▪ sudo user
Enable Password	Select whether to enable the password. ▪ Yes ▪ No
Enter Password	This field takes effect only when you set **Enable Password** to **Yes**. The password of the temporary user. The password must be 12 to 30 characters in length and must contain at least three types of digits, lowercase letters, uppercase letters, and special characters.
Confirm Password	This field takes effect only when you set **Enable Password** to **Yes**. Enter the password of the temporary user again. Make sure that the two passwords are the same.
Whether to enable SSH key	Select whether to enable the SSH key. ▪ Yes ▪ No
Description	Enter the description of the temporary user.
Validity Period	Select the start and end dates for the temporary user.
Machine definition mode	Select the delineation method of the target machine. ▪ Product Dimension ▪ Physical machine dimension ▪ All machines, including Apsara Infrastructure Management Framework-managed physical machines, dockerVMs, and KVMs
Product	This field takes effect only when you set **Machine Dimensions** to **Product Dimension**. Fuzzy match is supported.
SR	This field takes effect only when you set **Machine Dimensions** to **Product Dimension**. You can select multiple server roles from the drop-down list.

Machine Name	This property takes effect only when you set **Machine Deposition Method** to **Physical Machine Dimension**. The name of the server. Fuzzy match is supported.



Create a temporary user

Basic information

Username *

User type * Please Select

Enable Password ○ Yes ● No

Whether to enable SSH ... ○ Yes ● No

Description *

Validity period * Start Date - End Date

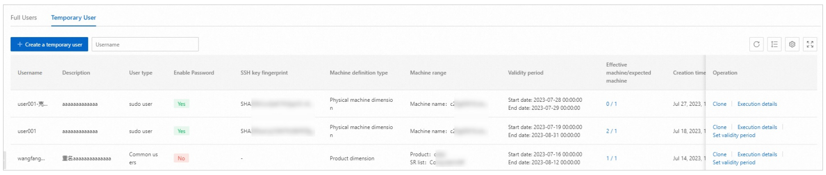
Target machine

Machine definition mode ● Product dimension ○ Physical machine dimension ○ Full machines (including physical machines managed by Tianji, dockerVM, and KVM)

Product * Please Select

SR Please Select

ii. The following table describes other operations that you can perform on the Temporary key tab.

<table>
<tr><th>Operation</th><th>Description</th></tr>
<tr><td>View temporary user information</td><td>a. Enter a keyword in the <b>Username</b> field to obtain the user information.

Full Users | Temporary User
+ Create a temporary user | Username
<table>
<tr><th>Username</th><th>Description</th><th>User type</th><th>Enable Password</th><th>SSH key fingerprint</th><th>Machine definition type</th><th>Machine range</th><th>Validity period</th><th>Effective machine/expected machine</th><th>Creation time</th><th>Operation</th></tr>
<tr><td>user001-亮...</td><td>aaaaaaaaaaaa</td><td>sudo user</td><td>Yes</td><td>SHA[redacted]</td><td>Physical machine dimension</td><td>Machine name：c[redacted]</td><td>Start date: 2023-07-28 00:00:00
End date: 2023-07-29 00:00:00</td><td>0 / 1</td><td>Jul 27, 2023, 1</td><td>Clone | Execution details</td></tr>
<tr><td>user001</td><td>aaaaaaaaaaaa</td><td>sudo user</td><td>Yes</td><td>SHA[redacted]</td><td>Physical machine dimension</td><td>Machine name：c[redacted]</td><td>Start date: 2023-07-19 00:00:00
End date: 2023-08-31 00:00:00</td><td>2 / 1</td><td>Jul 18, 2023, 1</td><td>Clone | Execution details |
Set validity period</td></tr>
<tr><td>wangfang...</td><td>重名aaaaaaaaaaaaa</td><td>Common users</td><td>No</td><td>-</td><td>Product dimension</td><td>Product：c[redacted]
SR list：Co[redacted]</td><td>Start date: 2023-07-16 00:00:00
End date: 2023-08-12 00:00:00</td><td>1 / 1</td><td>Jul 14, 2023, 1</td><td>Clone | Execution details |
Set validity period</td></tr>
</table>
b. Click the number in the <b>Effective Machine /Expected Machine</b> column corresponding to the target temporary user. In the panel that appears, you can view the list of effective machines, including <b>Machine Name</b>, <b>Container ID</b>, <b>Home Directory</b>, and <b>Creation At</b>.</td></tr>
<tr><td>Clone a temporary user</td><td>a. Click <b>Clone</b> in the <b>Actions</b> column corresponding to the temporary user. In the dialog box that appears, you can view a temporary user with the same configurations.
b. Modify the parameters as required and click <b>OK</b>.</td></tr>
<tr><td>View the details of a task</td><td>a. Find the temporary user that you want to view and click <b>Execution Details</b> in the <b>Actions</b> column.
b. On the <b>Linux Account Management Tasks</b> page, click the <b>Task Execution Records</b> tab to obtain the execution record details.</td></tr>
<tr><td>Configure the validity period pf a temporary user</td><td>a. Click <b>Set Validity Period</b> in the <b>Actions</b> column corresponding to the temporary user.
b. In the dialog box that appears, modify the validity period of the temporary user. The validity period can be up to 90 days, and then click <b>OK</b>.
<b>Note</b>
When the validity period of a temporary user expires, you cannot modify the validity period.</td></tr>
</table>

5.4.1.4. Linux account management task

5.4.1.4.1. Task template management

A host task template specifies an automatic rotation period for a specified key. The task automatically rotates the key on a regular basis to improve the security of sensitive information such as keys. You can also create a custom rotation task template in advance and trigger the task when key rotation is required. The following types of tasks are supported: global password-free removal across regions, SSH key rotation, OPS emergency O&M channel creation, temporary channel creation, and temporary user creation.

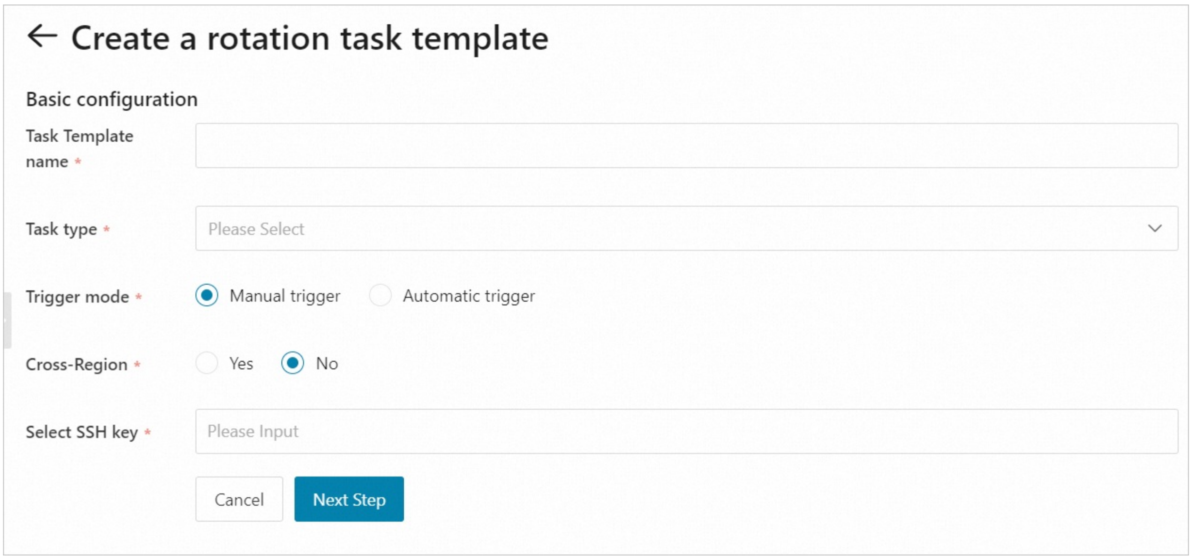
Prerequisites

- You have obtained the permissions to manage host task templates.
- The Tianji-sshtunnel service has reached the desired state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Linux Account Management**.
3. In the left-side navigation pane, choose **Linux Account Management Task** > **Task Template Management**.
4. On the page that appears, click **Create a task template**, configure the parameters described in the following table, and then click **Next Step**.

Parameter	Description
Task Template name	The name of the custom task template.
Task type	The rotation task type. Only **SSH key rotation** is supported.
Trigger mode	The trigger mode of the rotation task. You can select**Manual trigger** or **Automatic trigger**.
Trigger cycle	This field is displayed only when you set**Trigger mode** to **Automatic trigger**. Specify the trigger cycle and execution time of the next rotation task. **Note** Valid values: 7 to 365 days.
Cross-Region	Specifies whether to support cross-region rotation tasks.
Select SSH key	The SSH key.



← Create a rotation task template

Basic configuration

Task Template name *

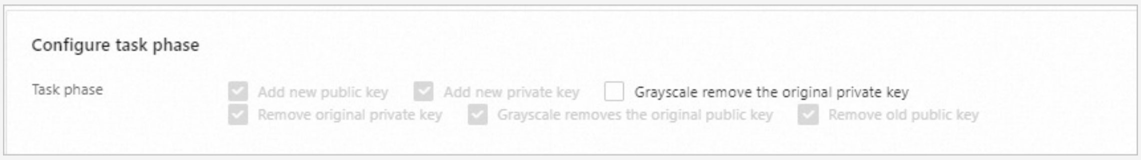
Task type * Please Select

Trigger mode * ● Manual trigger ○ Automatic trigger

Cross-Region * ○ Yes ● No

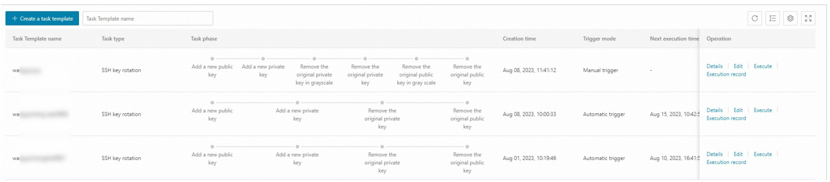
Select SSH key * Please Input

5. In the **Configure task phase** section, select a task phase.

> **Note**
>
> If you set **Trigger mode** to **Manual trigger**, you can specify whether to select the **Grayscale remove the original private key** phase.
>
> 
>
> Configure task phase
>
> Task phase ☑ Add new public key ☑ Add new private key □ Grayscale remove the original private key ☑ Remove original private key ☑ Grayscale removes the original public key ☑ Remove old public key

6. In the **Task template preview** section, check the template information and click **Create**.

Related operations

<table>
<tr><th>Operation</th><th>Procedure</th></tr>
<tr><td>View a rotation task template</td><td>
1. On the Task Templates for Dedicated Hosts page, enter a keyword in the <b>Task Template name</b> field to query the desired task template. You can query task templates based on <b>Task Template name</b>, <b>Task type</b>, <b>Task phase</b>, <b>Creation time</b>, <b>Trigger method</b>, and <b>Next execution time</b>.

+ Create a task template | Task Template name
<table>
<tr><th>Task Template name</th><th>Task type</th><th>Task phase</th><th>Creation time</th><th>Trigger mode</th><th>Next execution time</th><th>Operation</th></tr>
<tr><td>wa[redacted]</td><td>SSH key rotation</td><td>Add a new public key → Add a new private key → Remove the original private key in grayscale → Remove the original private key → Remove the original public key in gray scale → Remove the original public key</td><td>Aug 08, 2023, 11:41:12</td><td>Manual trigger</td><td>-</td><td>Details | Edit | Execute | Execution record</td></tr>
<tr><td>wa[redacted]</td><td>SSH key rotation</td><td>Add a new public key → Add a new private key → Remove the original private key → Remove the original public key</td><td>Aug 08, 2023, 10:00:33</td><td>Automatic trigger</td><td>Aug 15, 2023, 10:42:5</td><td>Details | Edit | Execute | Execution record</td></tr>
<tr><td>wa[redacted]</td><td>SSH key rotation</td><td>Add a new public key → Add a new private key → Remove the original private key → Remove the original public key</td><td>Aug 01, 2023, 10:19:46</td><td>Automatic trigger</td><td>Aug 10, 2023, 16:41:5</td><td>Details | Edit | Execute | Execution record</td></tr>
</table>
2. Find the task template that you want to view and click<b>Details</b> in the <b>Operation</b> column.
</td></tr>
</table>

Modify a rotation task template	1. On the Task Templates for Dedicated Hosts page, find the desired task template and click **Edit** in the **Operation** column. 2. Modify the parameters in the **Basic configuration** section and click **Next Step**. 3. Modify the parameters in the **Edit rotation task template** section and click Next Step. In the **Task template preview** section, confirm the template information and click **Update**. **Note** You cannot modify the preset rotation task template.
Execute a rotation task	1. On the Task Templates for Dedicated Hosts page, find the desired task template and click **Execute** in the **Operation** column. 2. In the dialog box that appears, click **OK**.
View the execution records of a rotation task	1. On the Task Templates for Dedicated Hosts page, find the desired task template and click **Execution record** in the **Operation** column. 2. View all the execution records of the task template on the **Host task execution record** page.

5.4.1.4.2. Task execution records

You can view the records of all historical rotation tasks, including global password-free removal tasks, OPS emergency O&M channel creation tasks, temporary channel creation tasks, and rotation tasks for updating the SSH keys. You can view all historical key pairs, update operations, and points in time of the updates in the current region. You can view all historical key pairs, update operations, and points in time of the updates.

Prerequisites

- You have obtained the permission to operate the task execution records of the host.
- The Tianji-sshtunnel service has reached the desired state.

Background information

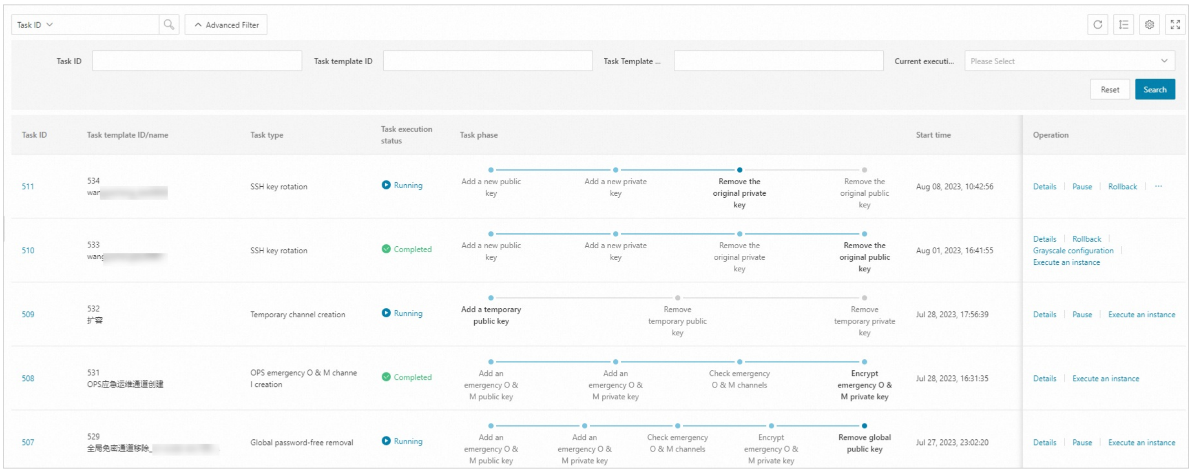
- You may need to manage SSH key pairs across multiple regions. In this case, a rotation task have subtasks. The name of a subtask is suffixed with the region where the SSH key pair is used. You can distinguish subtasks by the suffix. You can also use the subtask name to identify the parent rotation task to which the subtask belongs.
- A subtask is always synchronized with its parent task in status. The subtask status cannot be manually modified. All execution stages of a parent task are displayed after the task is created. The execution stages of a subtask are fully displayed only after all stages of the parent task are complete. When the parent task is running, you can view only the completed stages and the ongoing stage of the subtask.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Linux Account Management**.

3. In the left-side navigation pane, choose **Linux Account Management Task** > **Task Records**.

4. Click **Advanced Filter** to filter execution records by **Task ID**, **Task Template ID**, **Task Template**, and **Current execution status**.



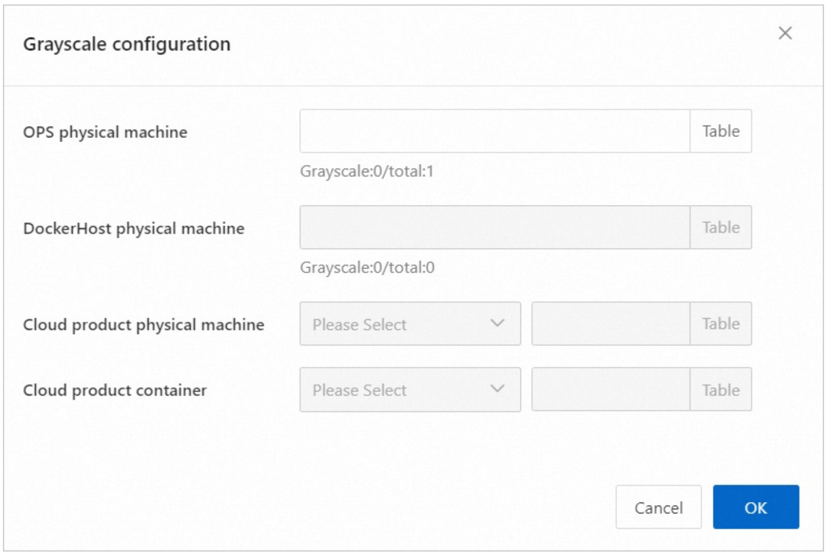
Task ID	Task template ID/name	Task type	Task execution status	Task phase	Start time	Operation
511	534 war[redacted]	SSH key rotation	Running	Add a new public key Add a new private key Remove the original private key Remove the original public key	Aug 08, 2023, 10:42:56	Details | Pause | Rollback | ···
510	533 wang[redacted]	SSH key rotation	Completed	Add a new public key Add a new private key Remove the original private key Remove the original public key	Aug 01, 2023, 16:41:55	Details | Rollback | Grayscale configuration | Execute an instance
509	532 扩容	Temporary channel creation	Running	Add a temporary public key Remove temporary public key Remove temporary private key	Jul 28, 2023, 17:56:39	Details | Pause | Execute an instance
508	531 OPS应急运维通道创建	OPS emergency O & M channel creation	Completed	Add an emergency O & M public key Add an emergency O & M private key Check emergency O & M channels Encrypt emergency O & M private key	Jul 28, 2023, 16:31:35	Details | Execute an instance
507	529 全局免密通道移除_[redacted]	Global password-free removal	Running	Add an emergency O & M public key Add an emergency O & M private key Check emergency O & M channels Encrypt emergency O & M private key Remove global public key	Jul 27, 2023, 23:02:20	Details | Pause | Execute an instance

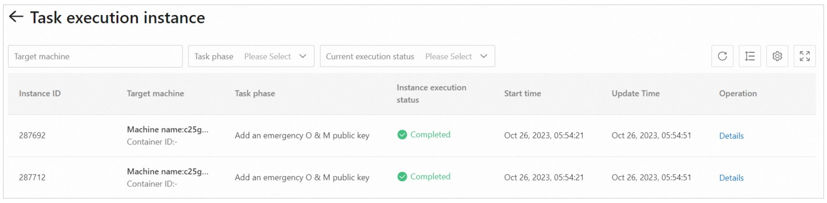
5. Find the task execution record that you want to view and click **Details** in the **Actions** column. In the panel that appears, you can view the details of the task execution record.

Operations

Operation	Description
Pause a rotation task	**Note** You can pause a rotation task when its **Status** is **Running**. 1. Find the rotation task that you want to manage and click **Pause** in the **Operation** column. 2. In the message that appears, click **OK**.
Continue a rotation task	**Note** If **Status** is set to **Paused**, you can continue to rotate the task. 1. In the **Operation** column corresponding to the rotation task, click **Continue**. 2. In the message that appears, click **OK**.

Rollback a rotation task	**Note** When the task type is set to**SSH key rotation** (including cross-region tasks) or **Global password-free removal** (including cross-region tasks), you can roll back the rotation task. 1. Click **Rollback** in the **Operation** column corresponding to the rotation task. 2. In the dialog box that appears, select a **Rollback type** and click **OK**. A new task is generated to roll back the key to the target key pair. **Note** ◦ You can set the **Rollback type** parameter to **This rollback** or **Initialize Rollback**. ◦ After the rollback, the cloud will add the global access root account key, which may cause the cloud platform to be in an insecure state. Please recycle the root account key timely.

Grayscale configuration	**Note** If you set Task type to **SSH key rotation** and configure a **Grayscale removes the original private key** task, you can configure phased-out tasks. For more information, see Manage task templates. 1. In the **Actions** column corresponding to the rotation task, click **Grayscale Configuration**. 2. In the dialog box that appears, configure the following parameters. Then, click **OK**. **Important** ◦ The parameters take effect in sequence from top to bottom. ◦ The current parameters are configured only when the number of machines that have been phased out is the same as the total number.  Grayscale configuration OPS physical machine: Table — Grayscale:0/total:1 DockerHost physical machine: Table — Grayscale:0/total:0 Cloud product physical machine: Please Select — Table Cloud product container: Please Select — Table Cancel OK

Obtain an execution instance	1. Click **Execute an instance** in the **Operation** column corresponding to the rotation task. Alternatively, click the ID in the **Task ID** column corresponding to the rotation task. 2. On the **Task execution instance** page, view the information about the instance based on the **Target machine**, **Task phase**, and **Instance execution status**.  ← Task execution instance Target machine Task phase Please Select Current execution status Please Select Instance ID Target machine Task phase Instance execution status Start time Update Time Operation 287692 Machine name:c25g... Container ID:- Add an emergency O & M public key Completed Oct 26, 2023, 05:54:21 Oct 26, 2023, 05:54:51 Details 287712 Machine name:c25g... Container ID:- Add an emergency O & M public key Completed Oct 26, 2023, 05:54:21 Oct 26, 2023, 05:54:51 Details 3. Find the instance that you want to view and click**Details** in the **Operation** column. In the panel that appears, you can view the details of the instance. **Note** If the **Instance execution status** is **Failed** or **Timeout Failed**, you can perform the following operations: ◦ Click **Retry** in the **Actions** column. In the dialog box that appears, click **OK** to retry the selected task instance. ◦ Click **Skip** in the **Actions** column. In the dialog box that appears, click **OK**.

5.4.2. Account management for cloud services

5.4.2.1. Manage account ACLs

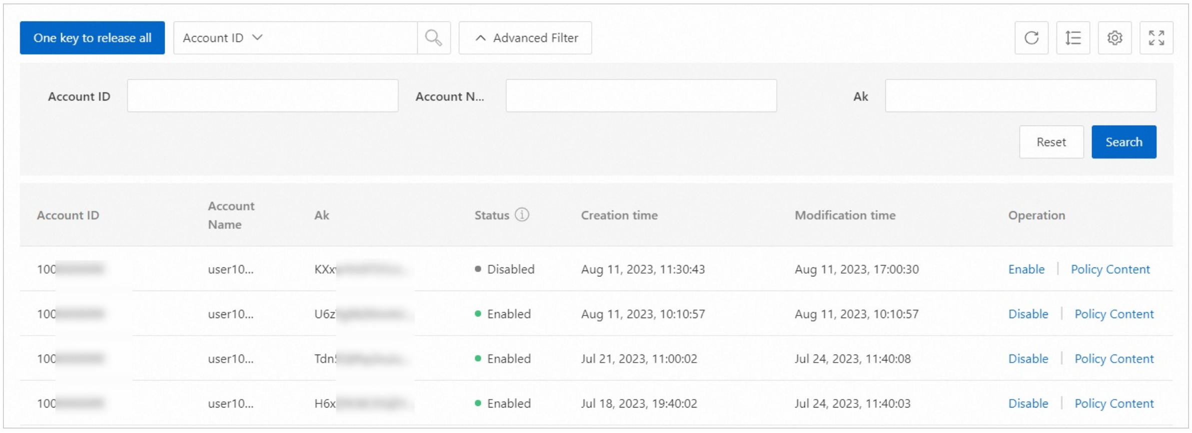
You can use the account to limit the permissions of the account to avoid security risks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Security & Compliance** > **Account Security** > **Cloud Product Account Management**.
3. In the left-side navigation pane, click **Account ACL**.
4. At the top of the page, you can enable or disable the default whitelist policy for the AccessKey pair of the new platform account.
   - Enable: A whitelist policy is issued to the AccessKey pair of the new platform account. Only the AccessKey pair is allowed to be used within the network whitelist.

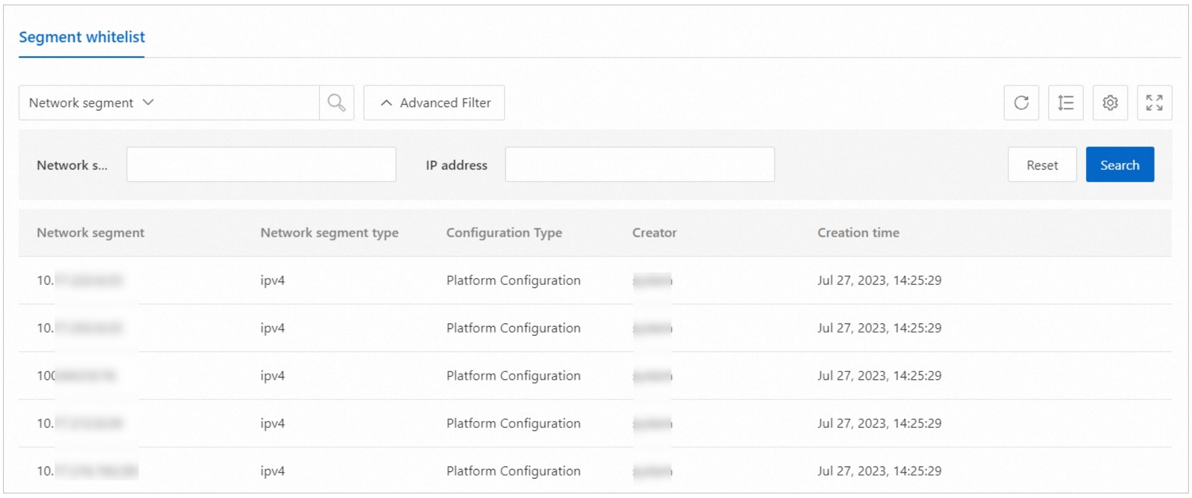
- Disable: By default, the AccessKey pair of a new platform account no longer issues whitelist policies. This poses security risks.

5. Click **Advanced Filter** to obtain the policy information of the target account by **Account ID**, **Account Name**, and **Ak** combination.



Account ID	Account Name	Ak	Status	Creation time	Modification time	Operation
100[redacted]	user10...	KXx[redacted]	Disabled	Aug 11, 2023, 11:30:43	Aug 11, 2023, 17:00:30	Enable | Policy Content
100[redacted]	user10...	U6z[redacted]	Enabled	Aug 11, 2023, 10:10:57	Aug 11, 2023, 10:10:57	Disable | Policy Content
100[redacted]	user10...	Tdn[redacted]	Enabled	Jul 21, 2023, 11:00:02	Jul 24, 2023, 11:40:08	Disable | Policy Content
100[redacted]	user10...	H6x[redacted]	Enabled	Jul 18, 2023, 19:40:02	Jul 24, 2023, 11:40:03	Disable | Policy Content

6. Click **Policy Content** in the **Actions** column corresponding to the account to obtain the CIDR block whitelist. You can search for **Network segment** and **IP address**.



Network segment	Network segment type	Configuration Type	Creator	Creation time
10.[redacted]	ipv4	Platform Configuration	[redacted]	Jul 27, 2023, 14:25:29
10.[redacted]	ipv4	Platform Configuration	[redacted]	Jul 27, 2023, 14:25:29
100[redacted]	ipv4	Platform Configuration	[redacted]	Jul 27, 2023, 14:25:29
10.[redacted]	ipv4	Platform Configuration	[redacted]	Jul 27, 2023, 14:25:29
10.[redacted]	ipv4	Platform Configuration	[redacted]	Jul 27, 2023, 14:25:29

Operations

Operation	Procedure

Disable the whitelist policy for the AccessKey pair of an Alibaba Cloud account	ⓘ **Note** • If the **Status** of the whitelist policy of the AccessKey pair is **Enabled**, you can disable the whitelist policy of the AccessKey pair. • If you disable this operation, the AccessKey pair of the Alibaba Cloud account does not have security control policies. You cannot use the AccessKey pair of the Alibaba Cloud account based on the request source. This poses security risks. 1. Click **Disable** in the **Operation** column corresponding to the account that you want to disable. 2. In the dialog box that appears, confirm the**Account Name** and **Ak** and click **OK**.
Enable the whitelist policy for the AccessKey pair of the Alibaba Cloud account	ⓘ **Note** • If the **Status** of the whitelist policy of the AccessKey pair is **Disabled**, you can enable the Whitelist policy of the AccessKey pair. • The enable operation issues a whitelist policy to the platform account and allows it to be used only within the network whitelist. 1. Click **Enable** in the **Operation** column corresponding to the target account. 2. In the dialog box that appears, confirm the**Account Name** and **Ak** and click **OK**.
Disable all whitelist policies of a platform account AccessKey pair	ⓘ **Important** If you allow all access with one click, the whitelist policy of the platform account AccessKey pair that has been issued will be disabled, and the security control capability of the request source of the platform account will not be available, which imposes security risks. If you want to re-enable the account ACL control, you need to manually enable it for each AccessKey pair. Therefore, exersice caution before you perform this operation. 1. Click **One Key to Release All**. 2. In the message that appears, click**OK**.

6.System settings

6.1. User permissions

6.1.1. User management

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

Prerequisites

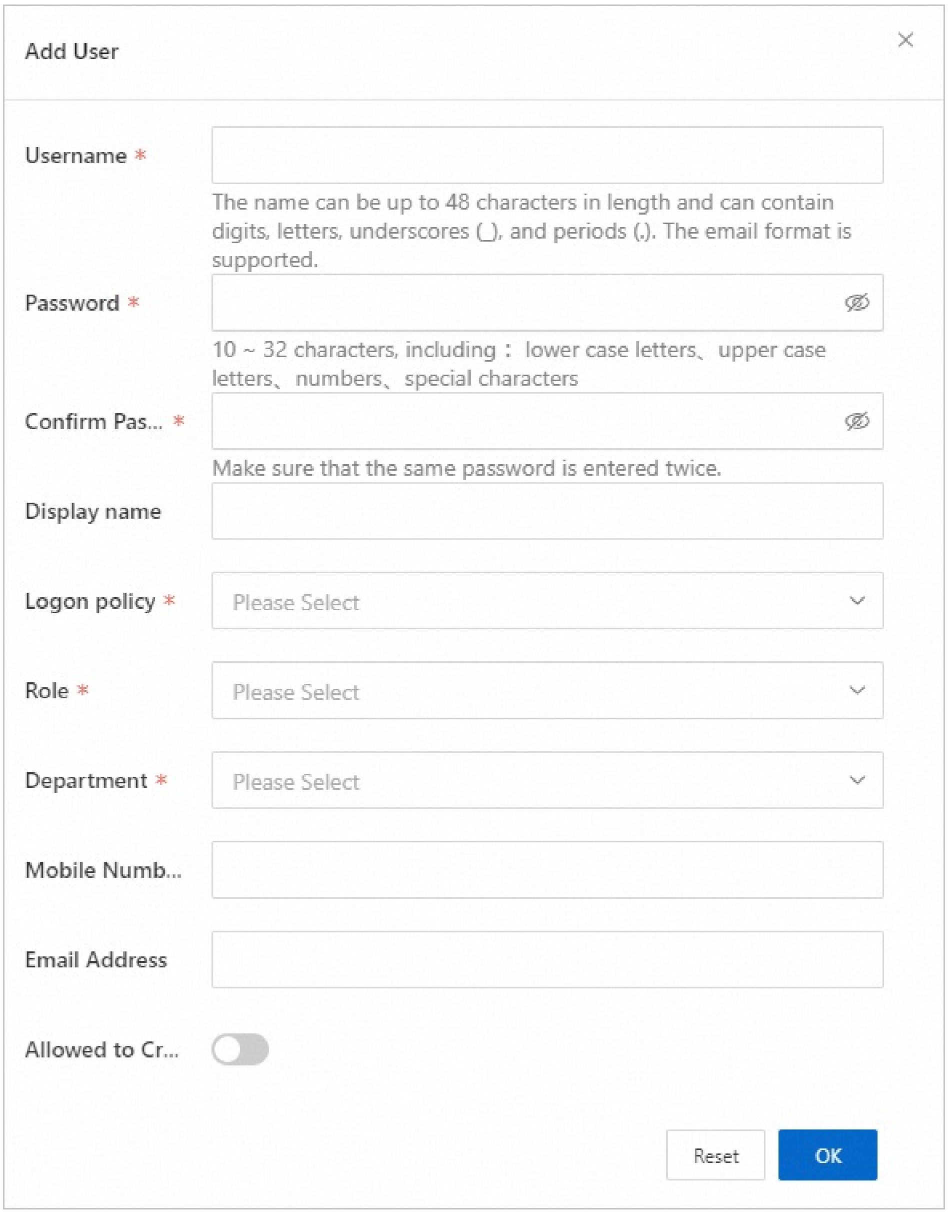
- You are a role administrator.
- A department is created.
- A logon policy is created.
- If you want to assign a user a custom role, you need to first create the custom role.

Procedure

1. Go 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** > **Users**.
4. On the **Users** tab, click **Add**. In the dialog box that appears, configure the following parameters and click **OK**.

Parameter	Parameters
Username	The Apsara Stack account of the user. The account can be up to 48 characters in length and can contain digits, letters, underscores (_), hyphens (-), and periods (.). The email address format is supported.
Password	The password of the account. The password can be 8 to 32 characters in length and must contain lowercase letters, digits, and special characters.
Confirm Password	The password that you enter in the Password field. Make sure that the two passwords that you enter are the same.
Display Name	Enter a display name for the user.
Logon policy	The logon policy of the user. If you want to create a new logon policy, choose **User Permissions** > **Logon Policies** in the left-side navigation pane.

Role	The role that is assigned to the user. If you want to create a new role, choose **User Permissions** > **Roles** in the left-side navigation pane. **Note** You can add multiple roles to a user.
Department	The department to which the user belongs. If you want to create a new department, choose **User Permissions** > **Departments** in the left-side navigation pane.
Mobile phones	Enter the user's mobile phone number.
Email address	Enter the user's email address.
Allowed to Create AccessKey ID	Specifies whether to enable the creation of an AccessKey ID.



Add User

Username *

The name can be up to 48 characters in length and can contain digits, letters, underscores (_), and periods (.). The email format is supported.

Password *

10 ~ 32 characters, including： lower case letters、 upper case letters、 numbers、 special characters

Confirm Pas... *

Make sure that the same password is entered twice.

Display name

Logon policy * Please Select

Role * Please Select

Department * Please Select

Mobile Numb...

Email Address

Allowed to Cr...

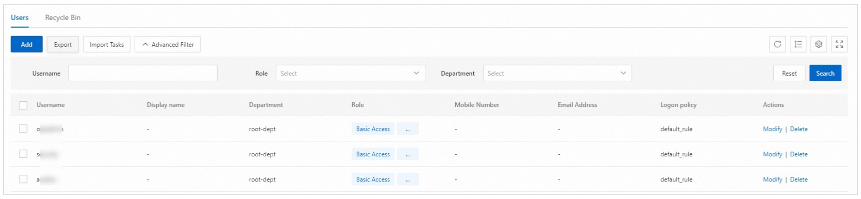
5. After a user is added, you can view the information of the added user on the **User Management** page.
6. On the **Recycle Bin** tab, you can view the information of deleted users.

References

Operation	Procedure

<table>
<tr><td>Query a user</td><td>

1. Click **Advanced Filter**.
2. You can filter users by **username**, **role**, and **department** to query the information of specific users.



<table>
<tr><th>Username</th><th>Display name</th><th>Department</th><th>Role</th><th>Mobile Number</th><th>Email Address</th><th>Logon policy</th><th>Actions</th></tr>
<tr><td>o[redacted]</td><td>-</td><td>root-dept</td><td>Basic Access ...</td><td>-</td><td>-</td><td>default_rule</td><td>Modify | Delete</td></tr>
<tr><td>s[redacted]</td><td>-</td><td>root-dept</td><td>Basic Access ...</td><td>-</td><td>-</td><td>default_rule</td><td>Modify | Delete</td></tr>
<tr><td>a[redacted]</td><td>-</td><td>root-dept</td><td>Basic Access ...</td><td>-</td><td>-</td><td>default_rule</td><td>Modify | Delete</td></tr>
</table>

</td></tr>
<tr><td>Export convenience users</td><td>

Select the users to be exported and click**Export List** to export the information of the users to your computer.

> **Note**
>
> If you do not select a user, the information of all the users is exported by default.

</td></tr>
<tr><td>Import a user List</td><td>

1. Click **Import Tasks**.
2. Click **Click here to upload the file** and select the user list file that you want to upload.

</td></tr>
<tr><td>Modify a user</td><td>

1. Find the user that you want to modify. Click**Modify** in the **Actions** column.
2. In the **Modify User** dialog box, modify the parameters and click**OK**.

</td></tr>
<tr><td>Delete a RAM user</td><td>

1. Find the user that you want to delete. Click**Delete** in the **Actions** column.
2. In the message that appears, click**OK**.

> **Note**
>
> - After you delete an account, the AccessKey pairs for RAM users of the account are disabled. In this case, services or applications that use the AccessKey pairs may fail to run.
> - Deleted users are displayed on the**Recycle Bin** tab. To restore a user, go to the **Recycle Bin** tab, find the user that you want to restore, and click **Restore** in the **Actions** column. In the message that appears, click **OK**.

</td></tr>
<tr><td>Activate a user account</td><td>

If the account of a user is frozen because the user does not log on to the Apsara Uni-manager Operations Console within the time period specified by the account freeze policy, the administrator can activate the account.

1. Find the account that you want to activate. Click**Activate** in the **Actions** column.
2. In the message that appears, click**OK**.

</td></tr>
</table>

Modify multiple user logon policies at a time	1. Select the users for which you want to modify the logon policies. Click **Modify Logon Policy** in the lower part of the page. 2. In the dialog box that appears, select the **logon policy** that you want to attach to the users and click **OK**. ⓘ **Note** The logon policies of the opsadmin user cannot be modified.

6.1.2. User group management

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

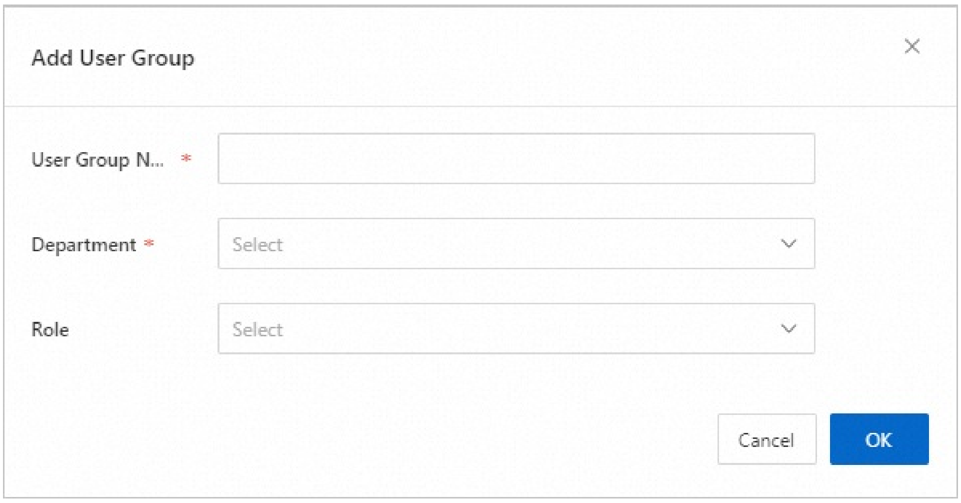
Prerequisites

- You have the administrator permissions.
- A department has been created.

Procedure

1. Go 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 Group Management**.
4. In the upper part of the page, click **Add**.
5. In the **Add User Group** dialog box, set the following parameters and click **OK**.

Parameter	Parameters
User Group Name	Enter the name of the user group.
Department	Select the department to which the user group belongs. If you want to create a new department, choose **User Permissions** > **Departments** in the left-side navigation pane.
Role	Select the role that you want to add to the user group. If you want to create a new role, choose **User Permissions** > **Roles** in the left-side navigation pane. ⓘ **Note** You can add multiple roles to a user group.



Add User Group

User Group N... *

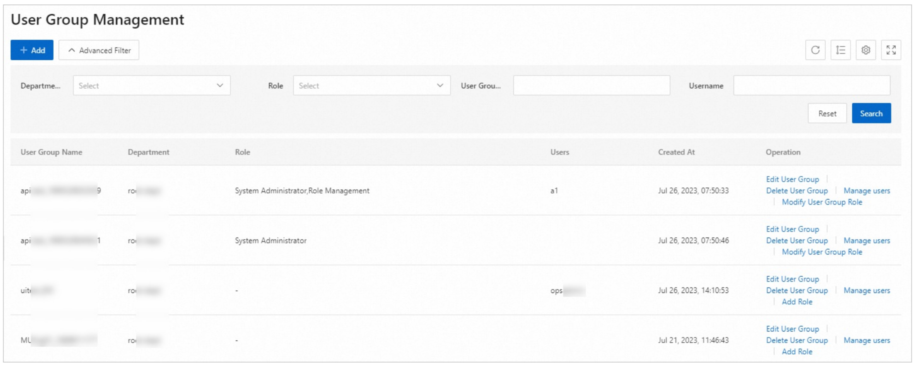
Department * Select

Role Select

Cancel OK

References

<table>
<tr><th>Operation</th><th>Procedure</th></tr>
<tr><td>View a user group</td><td>Click <b>Advanced Filter</b> to filter user groups by <b>Department Name</b>, <b>Role</b>, <b>User Group Name</b>, and <b>User Name</b>.



User Group Management

+ Add | Advanced Filter

Departme... Select | Role Select | User Grou... | Username

Reset | Search

<table>
<tr><th>User Group Name</th><th>Department</th><th>Role</th><th>Users</th><th>Created At</th><th>Operation</th></tr>
<tr><td>api[redacted]9</td><td>ro[redacted]</td><td>System Administrator,Role Management</td><td>a1</td><td>Jul 26, 2023, 07:50:33</td><td>Edit User Group | Delete User Group | Manage users | Modify User Group Role</td></tr>
<tr><td>api[redacted]1</td><td>ro[redacted]</td><td>System Administrator</td><td></td><td>Jul 26, 2023, 07:50:46</td><td>Edit User Group | Delete User Group | Manage users | Modify User Group Role</td></tr>
<tr><td>uit[redacted]</td><td>ro[redacted]</td><td>-</td><td>ops[redacted]</td><td>Jul 26, 2023, 14:10:53</td><td>Edit User Group | Delete User Group | Manage users | Add Role</td></tr>
<tr><td>ML[redacted]</td><td>ro[redacted]</td><td>-</td><td></td><td>Jul 21, 2023, 11:46:43</td><td>Edit User Group | Delete User Group | Manage users | Add Role</td></tr>
</table>
</td></tr>
<tr><td>Modify a user group</td><td>1. In the user group list, find the user group whose name you want to modify and click <b>Edit User Group</b> in the <b>Actions</b> column.
2. In the dialog box that appears, modify the <b>User Group Name</b> and click <b>OK</b>.</td></tr>
<tr><td>Delete a group</td><td>1. In the user group list, find the user group that you want to delete and click <b>Delete User Group</b> in the <b>Actions</b> column.
2. In the message that appears, click <b>Delete</b>.</td></tr>
<tr><td>Manage users</td><td>1. In the user group list, find the user group for which you want to manage users and click <b>Manage Users</b> in the <b>Actions</b> column.
2. In the dialog box that appears, you can add or delete users in the user group.
◦ Add: Click <b>Add</b>. In the dialog box that appears, select one or more usernames and click <b>OK</b>.
◦ Delete: Click <b>Delete</b> in the <b>Actions</b> column to delete the username.
3. Click <b>Determine</b>.</td></tr>
</table>

Add a role for the user group	If the user group has no roles, you can add roles to the group. 1. In the list of user groups, find the user group whose role you want to modify and click **Add Role** in the **Actions** column. 2. In the dialog box that appears, add the**role** and click **OK**. **Note** You can add multiple roles to a user group.
Modify the roles of a user group	If a user group has roles, you can modify the roles of the user group. 1. Find the user group that you want to modify and click**Modify User Group Role** in the **Actions** column. 2. In the dialog box that appears, modify the**Role** information and click **OK**.

6.1.3. Role management

A role is a collection of access permissions. You can assign different roles to different users to meet your requirements for system access control. You can set custom roles in the Apsara Uni-manager Operations Console to implement more flexible and efficient permission control.

Prerequisites

You are a role administrator.

Background information

Roles are classified into basic roles and custom roles. Basic roles are preset by the Open Application Model (OAM) system. You cannot modify or delete these roles. Custom roles can be modified or deleted.

The following table describes the preset basic roles and their permissions on menus.

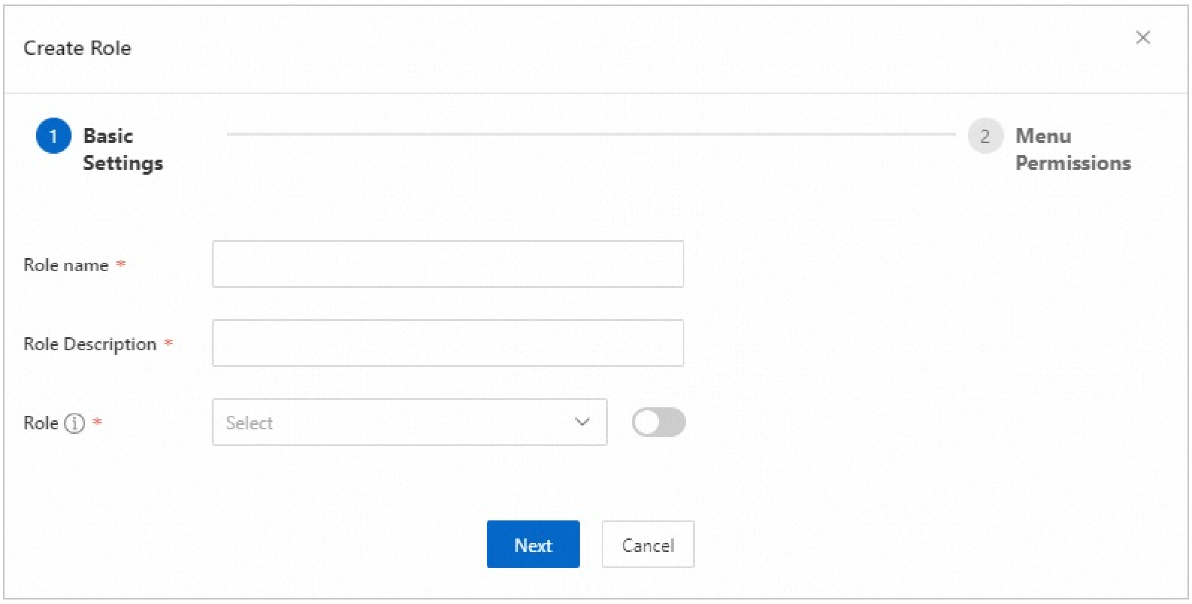
Role	Duty	Menu permission
Security auditor	Audits, tracks, and analyzes operations of the system administrator and the security officer.	• Security & Compliance ◦ Security Operations
Security officer	Manages the data security and account security, and maintains the security policies and logon policies.	• Security & Compliance ◦ Data Security ◦ Account Security • System Settings ◦ User Permissions - Security Policies ◦ User Permissions - Logon Policies ◦ User Permissions - Two-factor Authentication

Role administrator	Manages the permissions of the users on the platform.	• System Settings ◦ User Permissions - Users ◦ User Permissions - User Groups ◦ User Permissions - Roles ◦ User Permissions - Departments ◦ User Permissions - Region Authorization
System administrator	Manages the O&M of the platform.	A system administrator can access all the menus except the menus that are displayed for the security officer, security auditor, and role administrator.
Product DevOps	Manages the O&M of the products on the platform.	A product DevOps can access all the menus except the menus that are displayed for the security officer, security auditor, and role 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 **User Permissions** > **Roles**.
4. In the upper part of the page, click **Create Role**.
5. In the **Basic Settings** step, configure the following parameters and click **Next**.

Parameter	Description
Role name	The name of the role.
Role Description	The description of the role.
Role	Specifies the basic role. If you turn on the switch, all roles are displayed.



Create Role

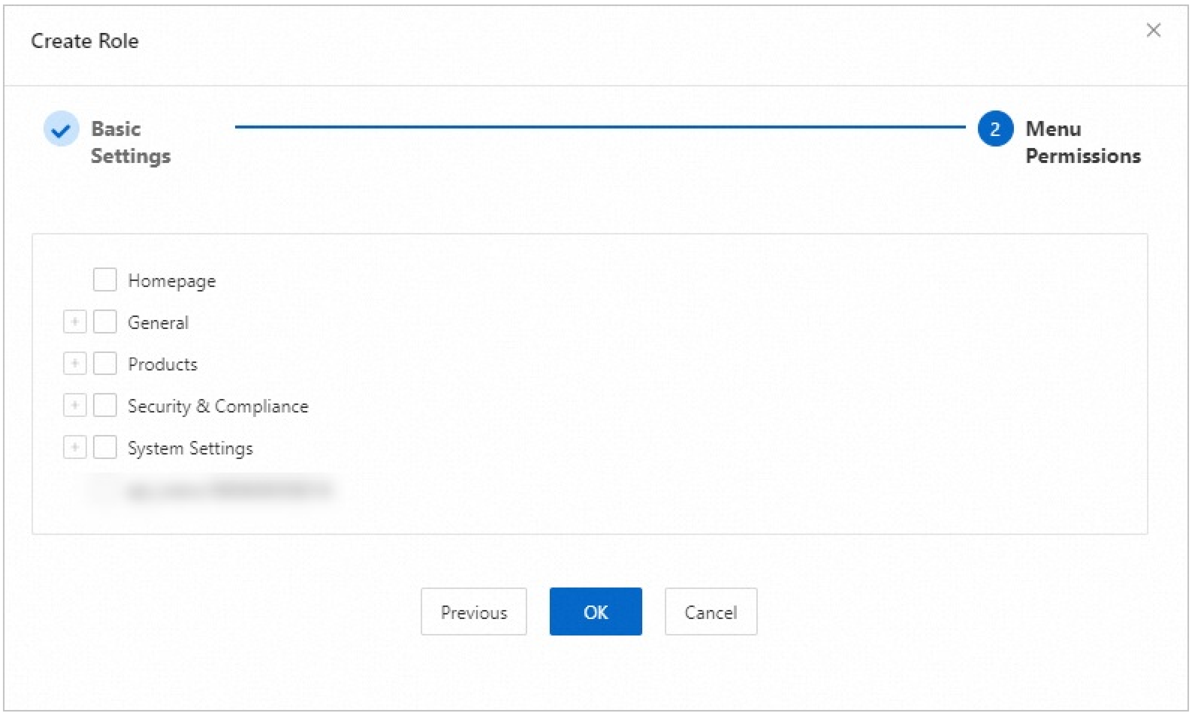
1 Basic Settings — 2 Menu Permissions

Role name *

Role Description *

Role ⓘ * Select

6. In the **Menu Permissions** step, select the menus that the role can access and click **OK**.



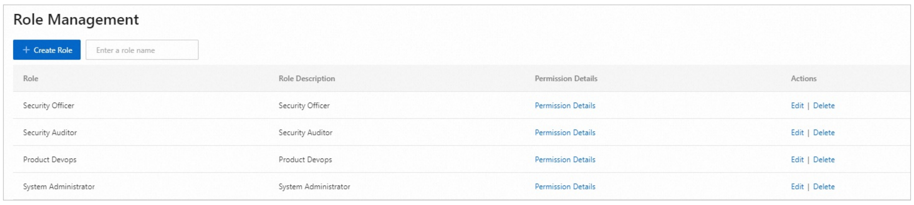
Create Role

✓ Basic Settings — 2 Menu Permissions

- □ Homepage
- + □ General
- + □ Products
- + □ Security & Compliance
- + □ System Settings

Related operations

Operation	Procedure

<table>
<tr><td>Query a role</td><td>You can filter roles by role name. Move the pointer over the<b>Permission Details</b> in the Permission Details column. The basic information of the role is displayed.

Role Management
+ Create Role   Enter a role name
<table><tr><th>Role</th><th>Role Description</th><th>Permission Details</th><th>Actions</th></tr><tr><td>Security Officer</td><td>Security Officer</td><td>Permission Details</td><td>Edit | Delete</td></tr><tr><td>Security Auditor</td><td>Security Auditor</td><td>Permission Details</td><td>Edit | Delete</td></tr><tr><td>Product Devops</td><td>Product Devops</td><td>Permission Details</td><td>Edit | Delete</td></tr><tr><td>System Administrator</td><td>System Administrator</td><td>Permission Details</td><td>Edit | Delete</td></tr></table></td></tr>
<tr><td>Modify a role</td><td>1. Find the role that you want to modify and click<b>Edit</b> in the <b>Actions</b> column.
2. In the <b>Basic Settings</b> step, modify the <b>Role Description</b> and <b>Role</b> parameters. Then, click <b>Next</b>.
3. In the <b>Menu Permissions</b> step, modify the menus that the role can access and click <b>OK</b>.</td></tr>
<tr><td>Delete a role</td><td><b>Note</b>
Before you delete a role, make sure that the role is not bound to a user. Otherwise, the role cannot be deleted.
1. Find the role that you want to delete. Click<b>Delete</b> in the <b>Actions</b> column.
2. In the dialog box that appears, click<b>OK</b>.</td></tr>
</table>

6.1.4. Departments

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

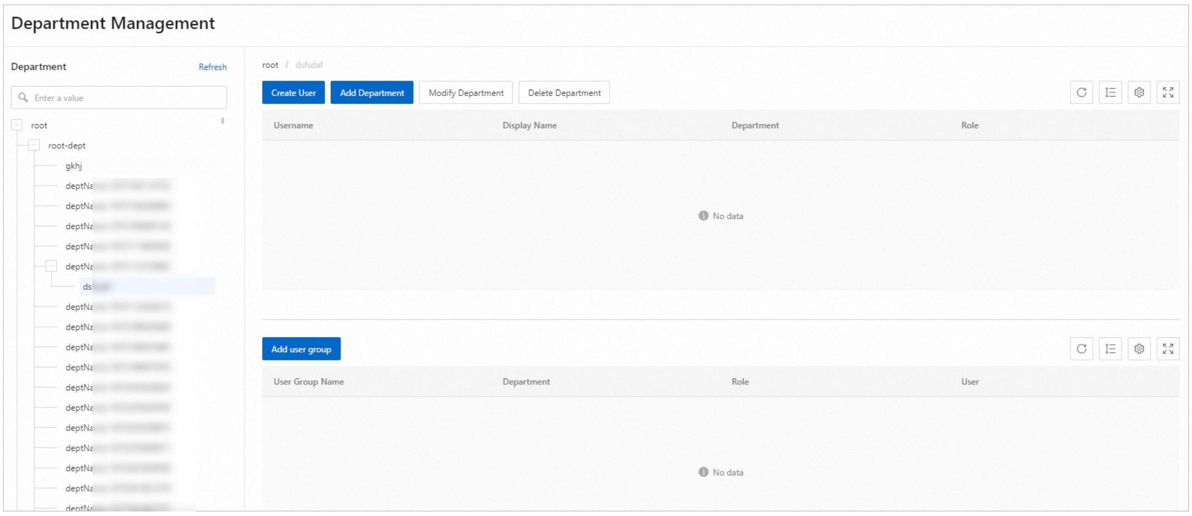
Prerequisites

- You have the administrator permissions.
- You can create up to five levels of 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** > **Departments**.
4. On the left side of the Department Management page, you can view the tree structure of all created departments. You can also view the information about all users and user groups in each department by clicking the department name.
5. 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 right section. In the Add Department dialog box, enter a value in the **Department Name** field, and click **OK**.

   Then, you can view the created department in the catalog tree.



Related operations

Operation	Description
Modify a department	1. In the catalog tree on the left, select the department that you want to modify and click **Modify Department** in the right section. 2. In the dialog box that appears, enter a new department name and click**OK**.
Delete a department	**Note** Before you delete a department, make sure that no users exist in the department. Otherwise, the department cannot be deleted. 1. In the catalog tree on the left, select the department that you want to delete and click **Delete Department** in the right section. 2. In the message that appears, click**OK**. The department is then deleted.
Add a user to a department	1. In the catalog tree on the left, select the department to which you want to add a user, click **Add User** in the right section. 2. In the dialog box that appears, configure the parameters and click**OK**. For more information about the parameters, see the Manage users. After a user is added, choose **User Permissions** > **Users** in the left-side navigation pane to view the information about the user.
Add a user group to a department	1. 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 right section. 2. In the dialog box that appears, enter a user group name and select a role. Click **OK**. After a user group is added, choose **User Permissions** > **User Groups** to view the information about the user group.

6.1.5. Region authorization

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

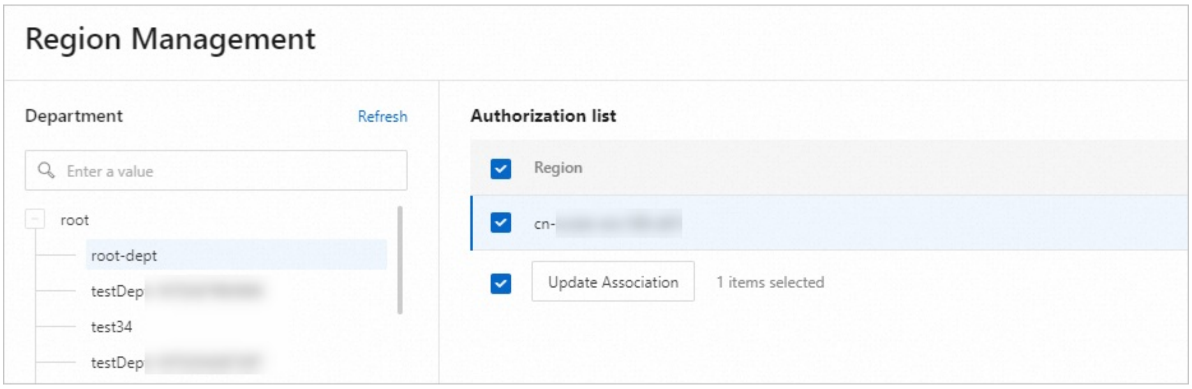
In multi-region scenarios, a region is managed by its own administrator. After administrators log on to the Apsara Uni-manager Operations Console, each administrator can manage only resources in the region that they are authorized to manage.

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. In the left-side catalog tree, click a department and select one or more regions in the **Authorizations list** section on the right.



Region Management

Department   Refresh

Enter a value

- root
  - root-dept
  - testDep[redacted]
  - test34
  - testDep[redacted]

Authorization list

☑ Region

☑ cn-[redacted]

☑ Update Association   1 items selected

5. Click **Update Association**.

6.1.6. Security policies

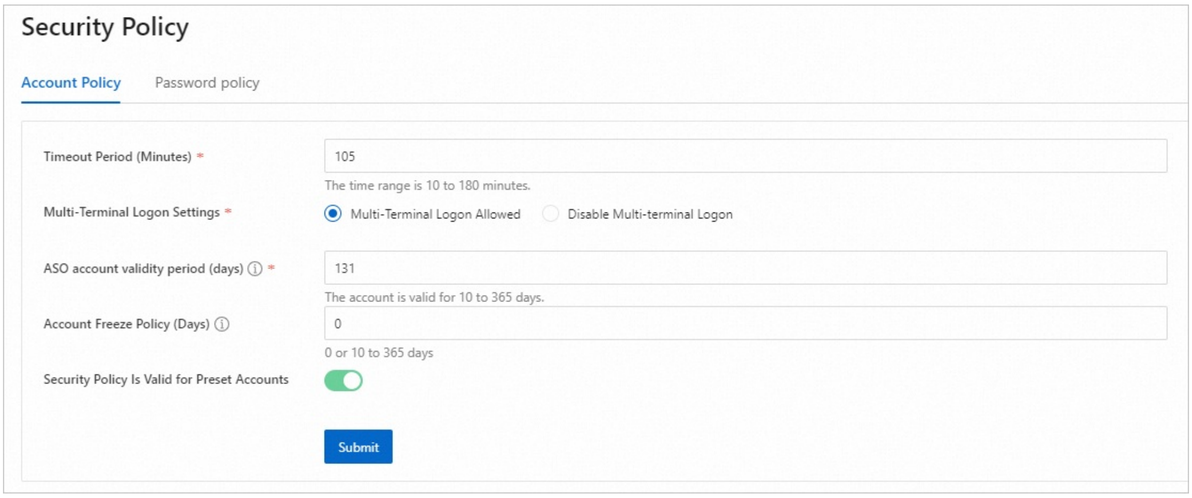
You can modify the account policies and password policies of the current account in the Security Policies module.

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** > **Security Policy**.
4. On the **Account Policy** tab, configure the parameters and click **Submit**. The following table describes the parameters.

Parameter	Description

Timeout Period (Minutes)	Specify a logon timeout period for 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 the current account is allowed to log on to the Apsara Uni-manager Operations Console from multiple terminals at the same time. ◦ On: The current account is allowed to log on to the Apsara Uni-manager Operations Console from multiple terminals at the same time. ◦ Off: The current account is not allowed to log on to the Apsara Uni-manager Operations Console from multiple terminals at the same time.
ASO account validity period (days)	Specify the validity period of the current account. If the account is expired, the system locks this account and only the security administrator can unlock the account. Valid values: 10 to 365.
Account Freeze Policy (Days)	Specify the period during which the current account remains available. If the specified period elapses, the system freezes this account. Valid values: ◦ 0: indicates that the account freezing policy is disabled. ◦ 10-365
Security Policy Is Valid for Preset Accounts	Specify whether the security policy is valid for preset accounts. ◦ On: If a security policy expires (for example, the account or password expires), preset accounts cannot log on to the system. We recommend that you set a long validity period. ◦ Off: If a security policy expires, preset accounts can still log on to the system. Preset accounts never expire. By default, the Security Policy Is Valid for Preset Accounts switch is turned off.



Security Policy

Timeout Period (Minutes) * 105
The time range is 10 to 180 minutes.

Multi-Terminal Logon Settings * ● Multi-Terminal Logon Allowed ○ Disable Multi-terminal Logon

ASO account validity period (days) ⓘ * 131
The account is valid for 10 to 365 days.

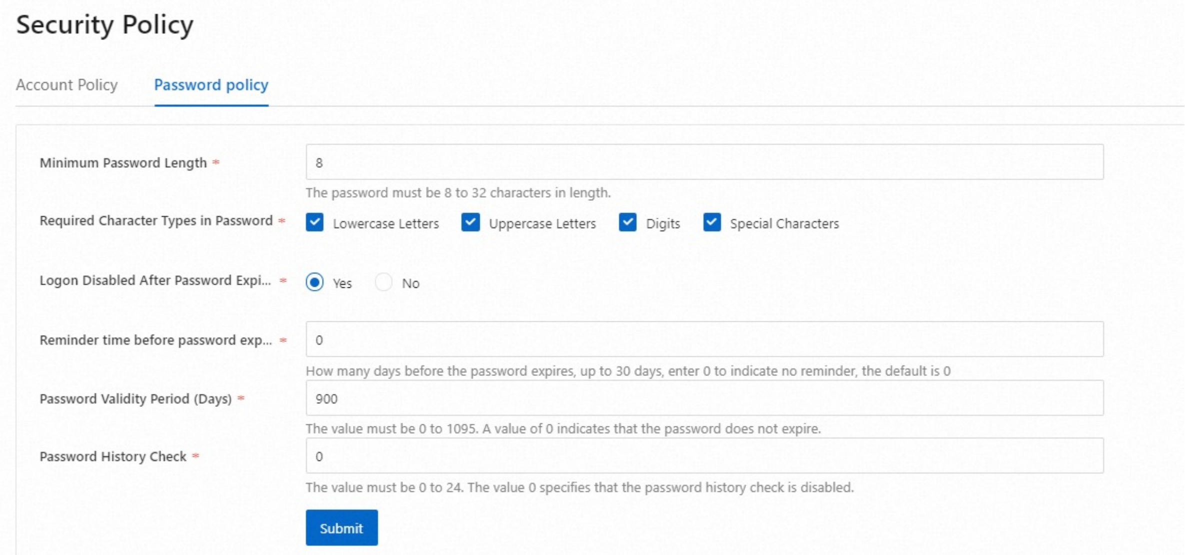
Account Freeze Policy (Days) ⓘ 0
0 or 10 to 365 days

Security Policy Is Valid for Preset Accounts ●

5. Click the **Password policy** tab, configure the parameters, and click **Submit**. The following table describes the parameters.

Parameter	**Description**
Minimum Password Length	Specify the minimum number of characters in the password. Valid values: 8 to 32.
Required Character Types in Password	Select one or more character types that must be contained in the password. ◦ Lowercase Letters ◦ Uppercase Letters ◦ Number ◦ Special Characters
Logon Disabled After Password Expires	Specify whether to prohibit the current account from logging on to the system after the password expires. ◦ Yes ◦ No
Reminder time before password expiration (days)	Set the time to send a reminder before the password of an account expires. For example, a value of 10 indicates that the expiration reminder is sent 10 days before the password expires when the user logs on. A value of 0 indicates that no reminder is sent. Valid values: 0 to 30.
Password Validity Period (Days)	Specify the validity period for the password. If the password expires, the system sends a notification to the user. 0 indicates that the password does not expire. Valid values: 0 to 1095.

Password History Check	Specify the number of historical passwords that you cannot reuse. For example, if you set this parameter to 3, the most recent three historical passwords cannot be reused. 0 indicates that all historical passwords can be reused. Valid values: 0 to 24.



Security Policy

Account Policy   Password policy

Minimum Password Length * 8

The password must be 8 to 32 characters in length.

Required Character Types in Password * ☑ Lowercase Letters ☑ Uppercase Letters ☑ Digits ☑ Special Characters

Logon Disabled After Password Expi... * ● Yes ○ No

Reminder time before password exp... * 0

How many days before the password expires, up to 30 days, enter 0 to indicate no reminder, the default is 0

Password Validity Period (Days) * 900

The value must be 0 to 1095. A value of 0 indicates that the password does not expire.

Password History Check * 0

The value must be 0 to 24. The value 0 specifies that the password history check is disabled.

6.1.7. Logon policies

As an administrator, you can configure logon policies to manage the logon time and logon IP addresses of users.

Background information

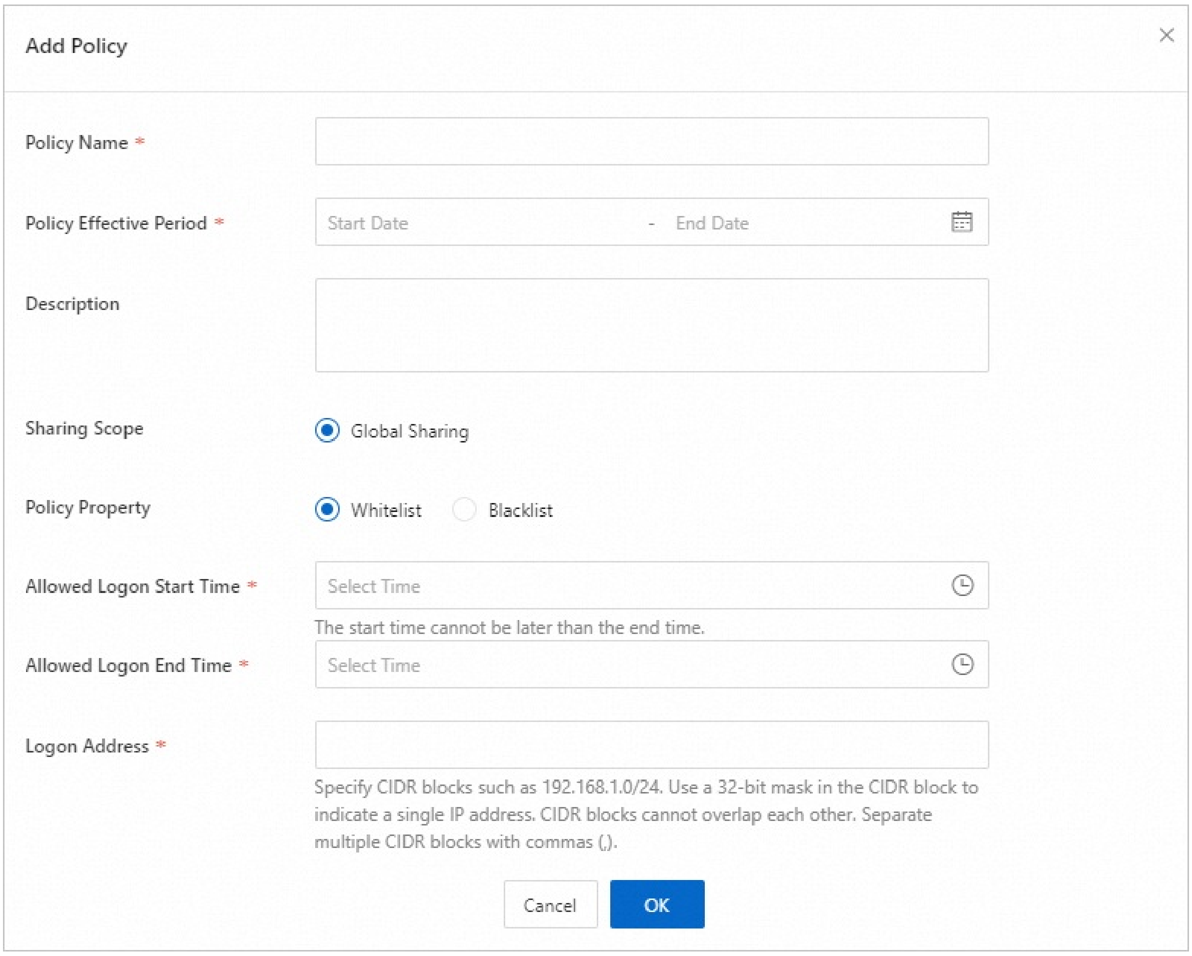
The system provides a default policy. You can configure custom logon policies based on your business requirements to better control the read and write permissions of users and enhance system security.

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 Policy page, click **Add Policy**. In the Add Policy dialog box, configure the parameters and click **OK**. The following table describes the parameters.

Parameter	Description
Policy Name	The name of the logon policy.
Policy Effective Period	The dates when the logon policy starts and stops taking effect.
Description	The description of the logon policy.

Sharing Scope	The scope in which you want to share the logon policy. Set this parameter to **Global Sharing**.
Policy Property	◦ Whitelist ◦ Blacklist
Allowed Logon Start Time	The point in time from which users are allowed for logon. The start time for logon cannot be later than the end time for logon.
Allowed Logon End Time	The point in time from which users are not allowed for logon.
Logon Address	The CIDR blocks of the logon policy. If you set the Policy Property parameter to Whitelist, you need to specify the CIDR blocks that are allowed for logon in the Logon Address field. If you set the Policy Property parameter to Blacklist, you need to specify the CIDR blocks that are prohibited from logon in the Logon Address field. Specify CIDR blocks such as 192.168.1.0/24. Use a 32-bit mask in the CIDR block to indicate a single IP address. CIDR blocks cannot overlap each other. Separate multiple CIDR blocks with commas (,).



Add Policy

Policy Name *

Policy Effective Period * Start Date - End Date

Description

Sharing Scope ● Global Sharing

Policy Property ● Whitelist ○ Blacklist

Allowed Logon Start Time * Select Time

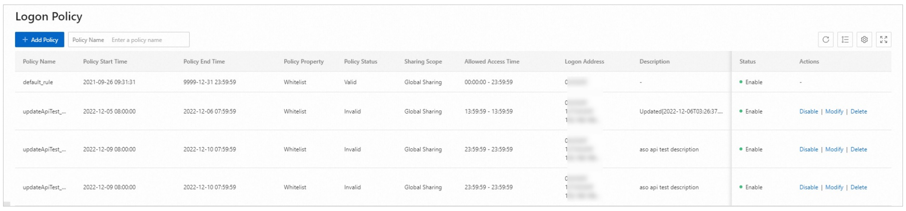
The start time cannot be later than the end time.

Allowed Logon End Time * Select Time

Logon Address *

Specify CIDR blocks such as 192.168.1.0/24. Use a 32-bit mask in the CIDR block to indicate a single IP address. CIDR blocks cannot overlap each other. Separate multiple CIDR blocks with commas (,).

Related operations

<table>
<tr><th>Operation</th><th>Description</th></tr>
<tr><td>Query a logon policy</td><td>To obtain information about a logon policy, you can enter the policy name in the **Policy Name** search box.

Logon Policy
+ Add Policy | Policy Name: Enter a policy name
<table>
<tr><th>Policy Name</th><th>Policy Start Time</th><th>Policy End Time</th><th>Policy Property</th><th>Policy Status</th><th>Sharing Scope</th><th>Allowed Access Time</th><th>Logon Address</th><th>Description</th><th>Status</th><th>Actions</th></tr>
<tr><td>default_rule</td><td>2021-09-26 09:31:31</td><td>9999-12-31 23:59:59</td><td>Whitelist</td><td>Valid</td><td>Global Sharing</td><td>00:00:00 - 23:59:59</td><td>[redacted]</td><td>-</td><td>● Enable</td><td>-</td></tr>
<tr><td>updateApiTest_...</td><td>2022-12-05 08:00:00</td><td>2022-12-06 07:59:59</td><td>Whitelist</td><td>Invalid</td><td>Global Sharing</td><td>13:59:59 - 13:59:59</td><td>[redacted]</td><td>Updated[2022-12-06T03:26:37....</td><td>● Enable</td><td>Disable &#124; Modify &#124; Delete</td></tr>
<tr><td>updateApiTest_...</td><td>2022-12-09 08:00:00</td><td>2022-12-10 07:59:59</td><td>Whitelist</td><td>Invalid</td><td>Global Sharing</td><td>23:59:59 - 23:59:59</td><td>[redacted]</td><td>aso api test description</td><td>● Enable</td><td>Disable &#124; Modify &#124; Delete</td></tr>
<tr><td>updateApiTest_...</td><td>2022-12-09 08:00:00</td><td>2022-12-10 07:59:59</td><td>Whitelist</td><td>Invalid</td><td>Global Sharing</td><td>23:59:59 - 23:59:59</td><td>[redacted]</td><td>aso api test description</td><td>● Enable</td><td>Disable &#124; Modify &#124; Delete</td></tr>
</table></td></tr>
<tr><td>Modify a logon policy</td><td>1. Find the logon policy that you want to modify and click**Modify** in the **Actions** column.
2. In the Modify Policy dialog box, modify the configurations and click**OK**.</td></tr>
<tr><td>Delete a logon policy</td><td>1. Find the logon policy that you want to delete and click**Delete** in the **Actions** column.
2. In the dialog box that appears, click **OK**.
Note
A logon policy that is bound to a user cannot be deleted. You must unbind the policy before you delete it.</td></tr>
<tr><td>Disable a logon policy</td><td>1. Find the logon policy that you want to disable and click**Disable** in the **Actions** column.
2. In the message that appears, click **OK**.
Note
• After you disable a logon policy, users that are bound to the policy are not allowed for logon.
• You can disable a logon policy only when **Enable** is displayed in the **Status** column corresponding to the policy.</td></tr>
<tr><td>Enable a policy</td><td>1. Find the logon policy that you want to enable and click**Enable** in the **Actions** column.
2. In the message that appears, click **OK**.
Note
You can enable a logon policy only when **Disable** is displayed in the **Status** column corresponding to the policy.</td></tr>
</table>

6.1.8. Two-factor authentication

To protect user logon in a more secure manner, you can configure two-factor authentication for users.

Background information

The Apsara Uni-manager Operations Console supports only **Google two-factor authentication**. After you enable two-factor authentication and add a key to a user, the user can use a random verification code generated by the authentication app for logon. This ensures the security of user accounts.

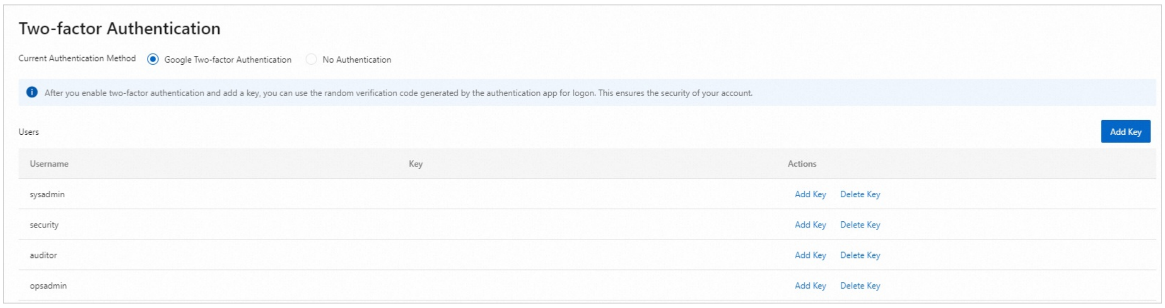
Procedure

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. In the upper part of the Two-factor Authentication page, specify an authentication method. The following authentication methods are provided:
    - **Google two-factor authentication**
        - Add a key
            a. In the upper-right corner of the Two-factor Authentication page, click **Add Key**. In the dialog box that appears, specify a username and click **OK**. The specified user is displayed in the user list.

            b. Click **Add Key** in the **Actions** column. If the **The operation is successful** message occurs, a key is added to the user and **Show Key** is displayed in the **Actions** column.

            c. If you click **Show Key**, the key is displayed in plaintext. If you click **Hide Key**, the key is displayed in ciphertext.
        - Delete a key
            a. Find the user for whom you want to delete the key and click **Delete Key** in the **Actions** column.

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



Two-factor Authentication

Current Authentication Method ● Google Two-factor Authentication ○ No Authentication

After you enable two-factor authentication and add a key, you can use the random verification code generated by the authentication app for logon. This ensures the security of your account.

Users

Username	Key	Actions
sysadmin		Add Key Delete Key
security		Add Key Delete Key
auditor		Add Key Delete Key
opsadmin		Add Key Delete Key

    - **No authentication**

        If you set the Current Authentication Method parameter to **No Authentication**, two-factor authentication is disabled and all two-factor authentication methods become invalid.

6.2. Platform settings

6.2.1. Menu settings

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

Usage notes

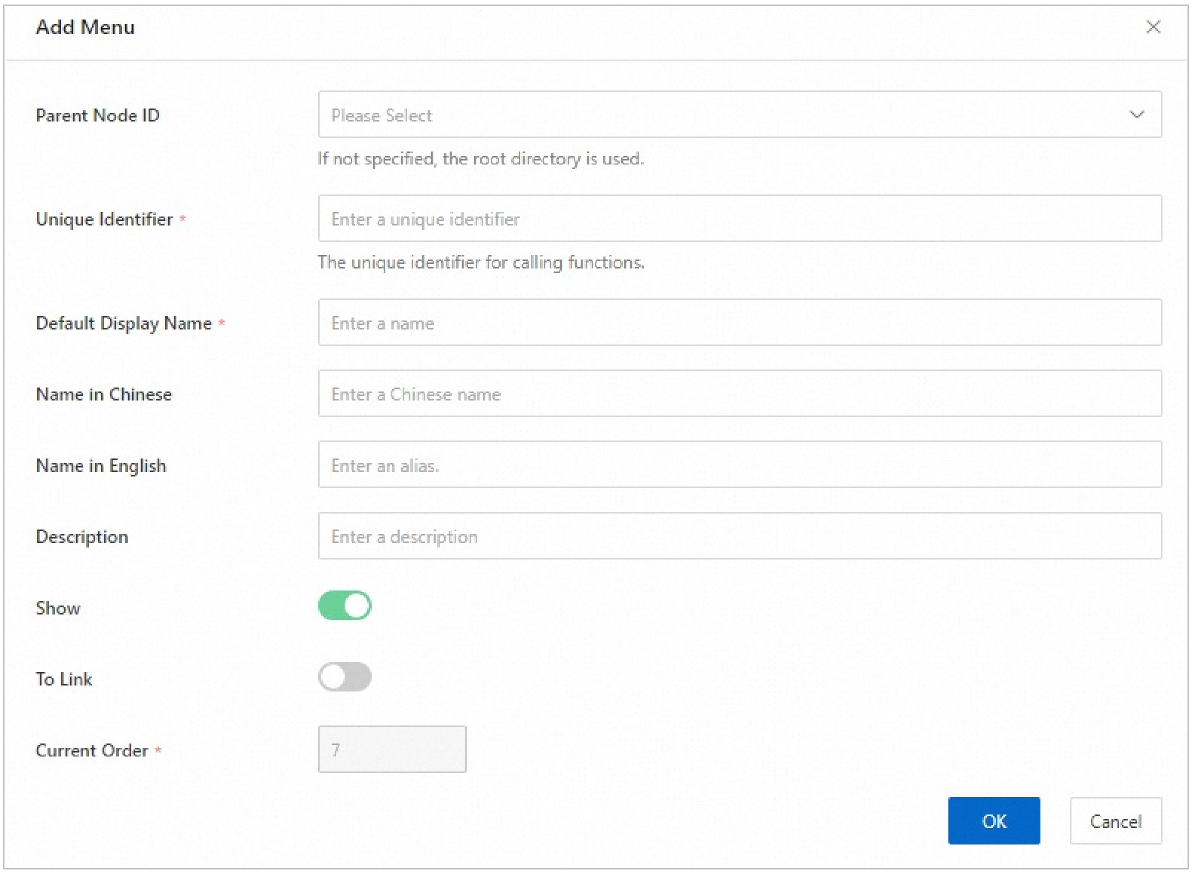
A menu supports up to five menu levels.

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 Menu Settings page, click **Add Menu Data**. In the Add Menu panel, configure the parameters and click **OK**. The following table describes the parameters.

Parameter	Description
Parent Node ID	The parent menu. You do not need to specify this parameter when you add a level-1 menu.
Unique Identifier	The unique identifier that is used to invoke functions. We recommend that you specify a unique identifier that contains 5 to 20 characters.
Default Display Name	The default display name of the menu.
Name in Chinese	The menu name in Chinese. If you set the language of the Apsara Uni-manager Operations Console to Chinese and specify a Chinese name for the menu, the Chinese name is displayed as the menu name by default.
Name in English	The menu name in English. If you set the language of the Apsara Uni-manager Operations Console to English and specify an English name for the menu, the English name is displayed as the menu name by default.
Description	The description of the menu.
Show	Specifies whether to display the menu after it is added. By default, this feature is enabled.
To Link	Specifies whether to navigate users to another page when they click the menu. By default, this feature is disabled.

URL	This parameter appears if you turn on **To Link**. The URL to which users are navigated when they click the menu. ◦ To navigate users to a page of the system, specify the absolute or relative path of the page. ◦ To navigate users to a page of a third-party system, specify the absolute path of the page.
Open Linked Page	This parameter appears if you turn on **To Link**. Specifies whether to open the URL on a new page after users click the menu. By default, this feature is disabled.
Current Order	The order of the menu among all menus in the same parent menu. You cannot specify this parameter in the Add Menu panel. To change the order of the menu, you can first add the menu, find it on the Menu Settings page, and then click Move Up or Move Down in the Actions column.



Add Menu

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

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

Default Display Name *: Enter a name

Name in Chinese: Enter a Chinese name

Name in English: Enter an alias.

Description: Enter a description

Show: ●

To Link: ○

Current Order *: 7

5. After the menu is added, you can view it in the menu list.

Related operations

Operation	Description

Modify a menu	1. In the menu list, find the menu that you want to modify and click **Modify** in the **Actions** column. 2. In the Modify Menu panel, modify the configurations and click **OK**. 3. In the **Actions** column, click **Move Up** or **Move Down** to change the order of the menu.
Delete a menu	1. In the menu list, find the menu that you want to delete and click **Delete** in the **Actions** column. 2. In the message that appears, click **OK**. **Note** Built-in menus of the system cannot be deleted.

6.2.2. Authorization information

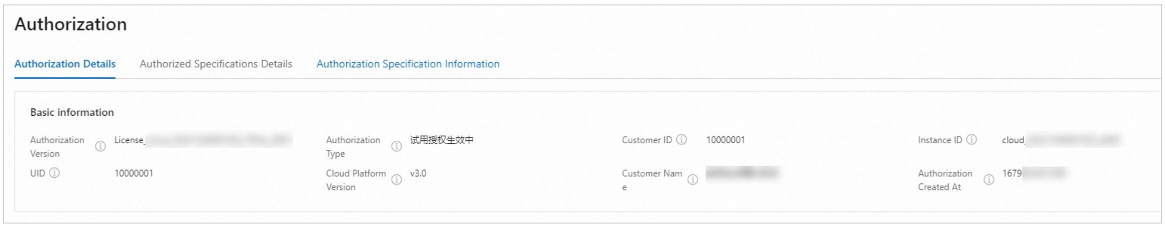
Users, field engineers, and O&M engineers can query services that failed authorization and troubleshoot the issues in the Authorization Information module of the Apsara Uni-manager Operations Console. You can also configure thresholds, usage monitoring tasks, and alert notifications in this module.

Prerequisites

- You have the administrator permissions.
- 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 customer business manager (CBM) of your project.

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**.
4. 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. The following table describes the parameters in the authorization information.



Authorization

Authorization Details
Authorized Specifications Details
Authorization Specification Information

Basic information

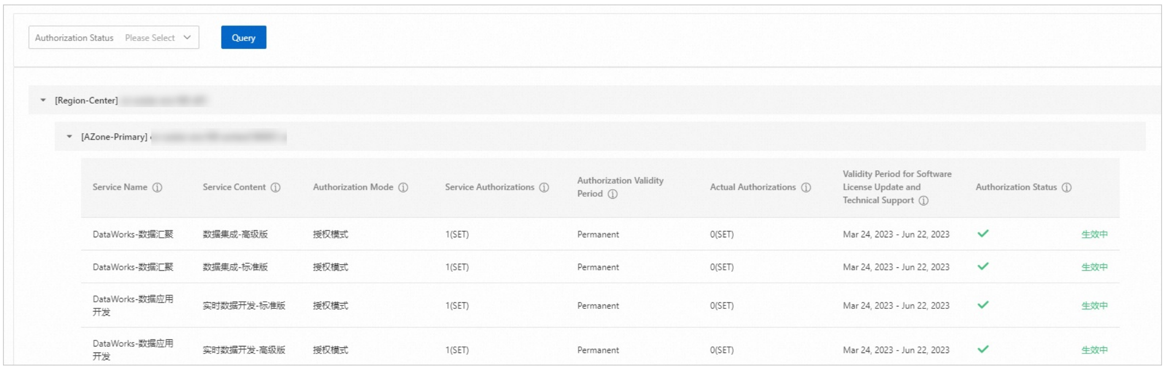
Authorization Version: License_[redacted]
Authorization Type: 试用授权生效中
Customer ID: 10000001
Instance ID: cloud_[redacted]
UID: 10000001
Cloud Platform Version: v3.0
Customer Name: [redacted]
Authorization Created At: 1679[redacted]

Parameter	Description

Authorization Version	The BP number in the version. You can use this number to associate a project or contract. Fields in the BP number: ■ **TRIAL** in the version indicates that the trial authorization is used. The trial authorization is valid within 90 days from the date of deployment. ■ **FORMAL** in the version indicates that the formal authorization is used. The authorization information of the service comes from the signed contract.
Authorization Type	The current authorization type and authorization status. ■ The following authorization types are available: ■ **Trial Authorization** ■ **Formal Authorization** ■ The following authorization states are available: ■ **Not Activated** ■ **About to expire** ■ **Taking effect** ■ **Expired** ■ **Expired/Excess**
Customer ID	The unique ID of the customer.
Instance ID	The ECS instance ID in the deployment planner of the field environment.
UID	The unique ID of the user.
Cloud Platform Version	The Apsara Stack version of the current cloud platform.
Customer Name	The name of the customer who purchased the Apsara Stack service.
Authorization Created At	The start time of the authorization.

- You can select an authorization state from the **Authorization Status** drop-down list and click **Query** to view the authorization details.

  You can also view the detailed authorization information of cloud services across regions. The authorization information includes the following parameters: **Service Name**, **Service Content**, **Authorization Mode**, **Service Authorizations**, **Authorization Validity Period**, **Actual Authorizations**, **Validity Period for Software License Update and Technical Support**, and **Authorization Status**.



[Region-Center] [redacted]

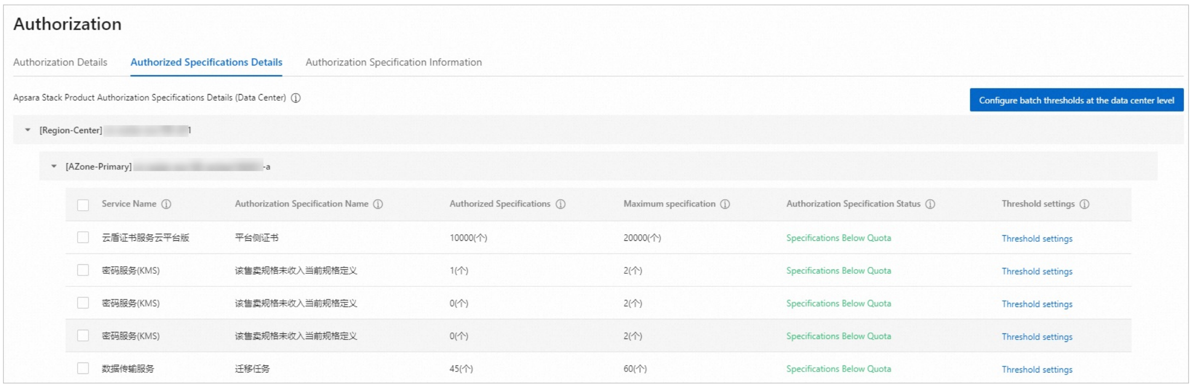
[AZone-Primary] [redacted]

Service Name	Service Content	Authorization Mode	Service Authorizations	Authorization Validity Period	Actual Authorizations	Validity Period for Software License Update and Technical Support	Authorization Status
DataWorks-数据汇聚	数据集成-高级版	授权模式	1(SET)	Permanent	0(SET)	Mar 24, 2023 - Jun 22, 2023	✓ 生效中
DataWorks-数据汇聚	数据集成-标准版	授权模式	1(SET)	Permanent	0(SET)	Mar 24, 2023 - Jun 22, 2023	✓ 生效中
DataWorks-数据应用开发	实时数据开发-标准版	授权模式	1(SET)	Permanent	0(SET)	Mar 24, 2023 - Jun 22, 2023	✓ 生效中
DataWorks-数据应用开发	实时数据开发-高级版	授权模式	1(SET)	Permanent	0(SET)	Mar 24, 2023 - Jun 22, 2023	✓ 生效中

Take note of the following values in the **Authorization Status** column of a service:

- **RENEW Service Expired**: indicates that the customer must renew the subscription as soon as possible. Otherwise, field operations services (including ticket processing) are terminated.
- **Specification Quota Exceeded**: indicates that the specifications deployed for a service have exceeded the contract quota, and the customer must scale up the service as soon as possible.

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



Authorization

Authorization Details
Authorized Specifications Details
Authorization Specification Information
Configure batch thresholds at the data center level

Apsara Stack Product Authorization Specifications Details (Data Center)

[Region-Center] [redacted]1

[AZone-Primary] [redacted]-a

□	Service Name	Authorization Specification Name	Authorized Specifications	Maximum specification	Authorization Specification Status	Threshold settings
□	云盾证书服务云平台版	平台侧证书	10000(个)	20000(个)	Specifications Below Quota	Threshold settings
□	密码服务(KMS)	该售卖规格未收入当前规格定义	1(个)	2(个)	Specifications Below Quota	Threshold settings
□	密码服务(KMS)	该售卖规格未收入当前规格定义	0(个)	2(个)	Specifications Below Quota	Threshold settings
□	密码服务(KMS)	该售卖规格未收入当前规格定义	0(个)	2(个)	Specifications Below Quota	Threshold settings
□	数据传输服务	迁移任务	45(个)	60(个)	Specifications Below Quota	Threshold settings

The following table describes the parameters in the authorization specification information.

Parameter	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 existing authorizations of a specification for a service.
Maximum specification	The maximum number of authorizations of a specification for a service.

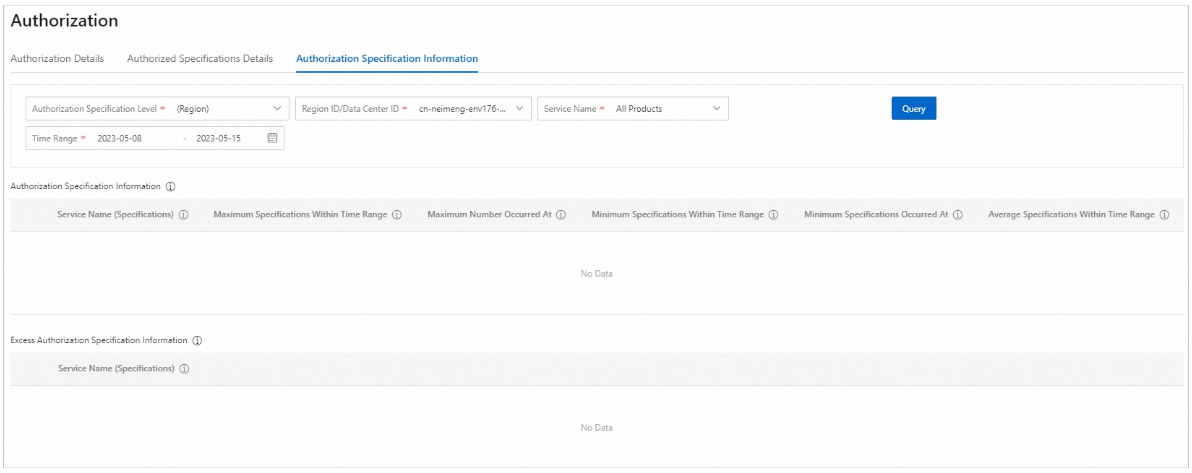
Authorization Specification Status	The current authorization status of a specification for a service.
Threshold settings	The threshold for alerts on the authorization usage of a specification for a service. You can configure thresholds to trigger alerts. When a threshold is exceeded, an alert is triggered. You can view the alert in the Alerts module. i. To configure the threshold for a single product, find the product and click **Threshold settings** in the **Threshold settings** column. ii. To configure the threshold for multiple products at the same time, select the check boxes of the products. In the upper-right corner of the authorized specification details section, click **Configure batch thresholds at the data center level** or **Region-level bulk threshold configuration**. iii. In the Threshold configuration dialog box, turn on**Threshold Level switch**. Enter a value in the**Threshold Level (%)** field. iv. Click **OK**.

6. Click the **Authorization Specification Information** tab to view the statistics on the authorized specifications of services and the information about services whose actual authorized specifications exceed the quota of authorized specifications.

   - You can specify the **Authorization Specification Level**, **Region ID/Data Center ID**, **Service Name**, and **Time Range** parameters, and then click **Query**. This way, you can obtain the statistics on the authorized specifications of a service in the current environment. The statistics include the following parameters: **Maximum Specifications Within Time Range**, **Maximum Number Occurred At**, **Minimum Specifications Within Time Range**, **Minimum Specifications Occurred At**, and Average Specifications Within Time Range.

   - In the **Authorization Specification Information** section, click the + icon on the left of a service to view the number of authorized specifications, quotas of authorized specifications, and the recorded time of the specification authorization on the previous day. Click **View More** to view the authorization specification information of the services within the specified time range by date.

   - In the **Excess Authorization Specification Information** section, you can view the information about the excess authorized specifications of each service.



Authorization

Authorization Details
Authorized Specifications Details
Authorization Specification Information

Authorization Specification Level * (Region)

Region ID/Data Center ID * cn-neimeng-env176-...

Service Name * All Products

Time Range * 2023-05-08 - 2023-05-15

Authorization Specification Information ⓘ

Service Name (Specifications) ⓘ	Maximum Specifications Within Time Range ⓘ	Maximum Number Occurred At ⓘ	Minimum Specifications Within Time Range ⓘ	Minimum Specifications Occurred At ⓘ	Average Specifications Within Time Range ⓘ
		No Data			

Excess Authorization Specification Information ⓘ

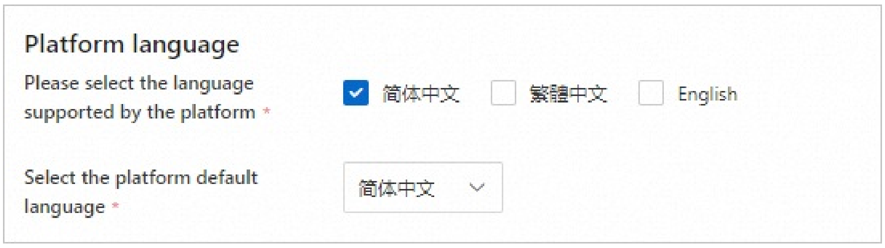
Service Name (Specifications) ⓘ
No Data

6.2.3. Custom settings

The Custom Settings module allows you to customize platform settings such as the logon page and the logo.

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** > **Custom Settings**.
4. You can customize settings in the following sections:
   - Platform language: You can select the languages supported by the platform and the default language. Simplified Chinese, traditional Chinese, and English are available.

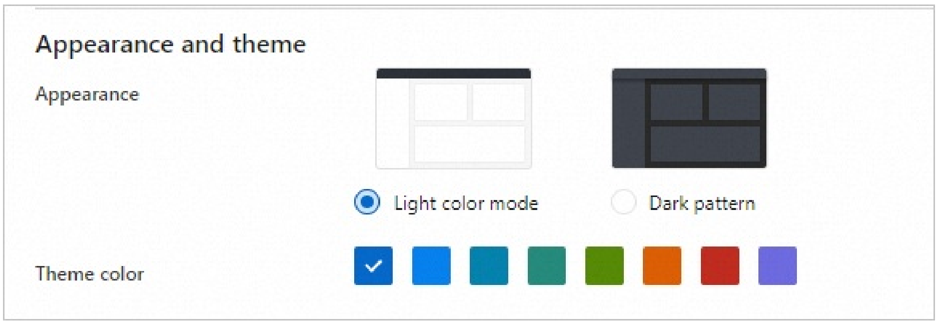


Platform language

Please select the language supported by the platform * ☑ 简体中文 □ 繁體中文 □ English

Select the platform default language * 简体中文

   - Appearance and theme: You can select the light or dark color mode and the theme color for the platform.

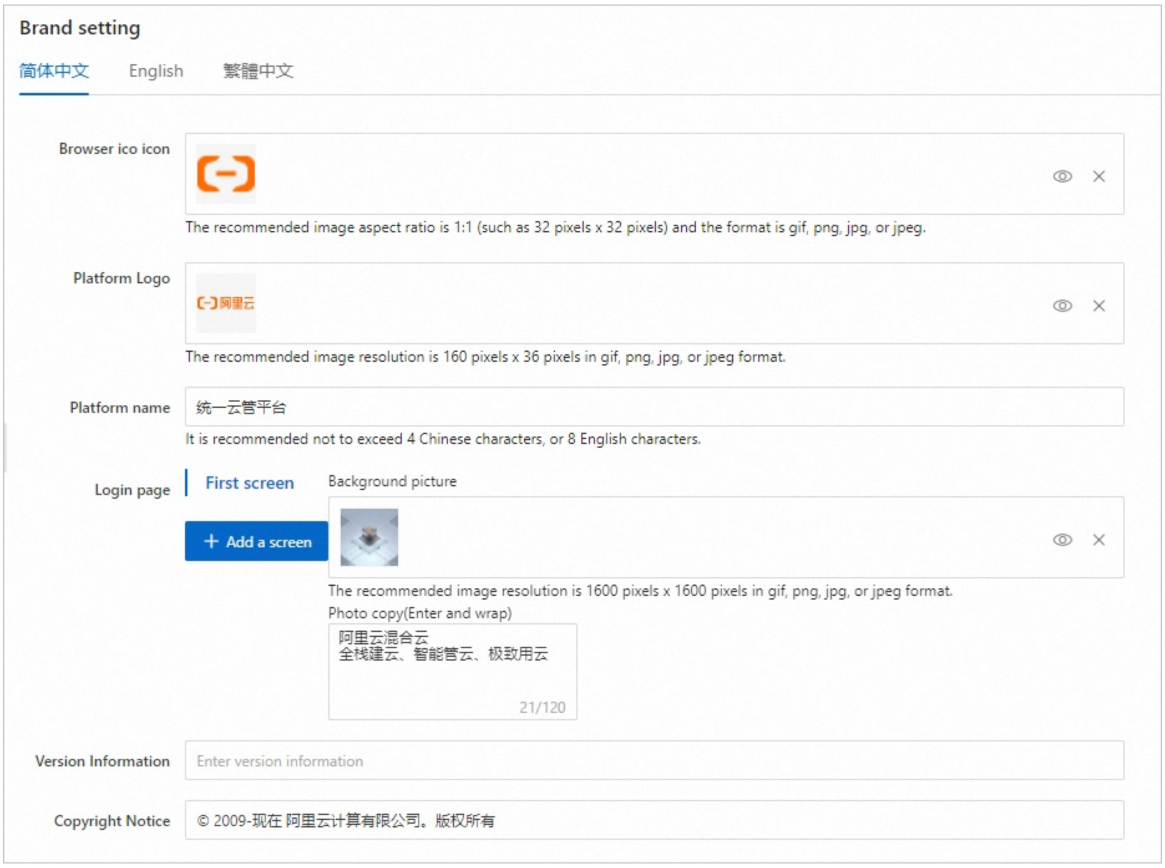


Appearance and theme

Appearance ● Light color mode ○ Dark pattern

Theme color

   - Page watermark: You can select whether to add a watermark to platform pages.
   - You can configure the **browser icon**, **platform logo**, **platform name**, **logon page**, **version information**, and **copyright notice** on the tabs of the preceding three languages.



Brand setting

简体中文 English 繁體中文

Browser ico icon

The recommended image aspect ratio is 1:1 (such as 32 pixels x 32 pixels) and the format is gif, png, jpg, or jpeg.

Platform Logo

The recommended image resolution is 160 pixels x 36 pixels in gif, png, jpg, or jpeg format.

Platform name: 统一云管平台

It is recommended not to exceed 4 Chinese characters, or 8 English characters.

Login page: First screen

+ Add a screen

Background picture

The recommended image resolution is 1600 pixels x 1600 pixels in gif, png, jpg, or jpeg format.

Photo copy(Enter and wrap)

阿里云混合云
全栈建云、智能管云、极致用云

21/120

Version Information: Enter version information

Copyright Notice: © 2009-现在 阿里云计算有限公司。版权所有

5. After the settings are complete, click **Determine**.

6.2.4. Notification management

6.2.4.1. Channel management

You can configure channels to send notifications.

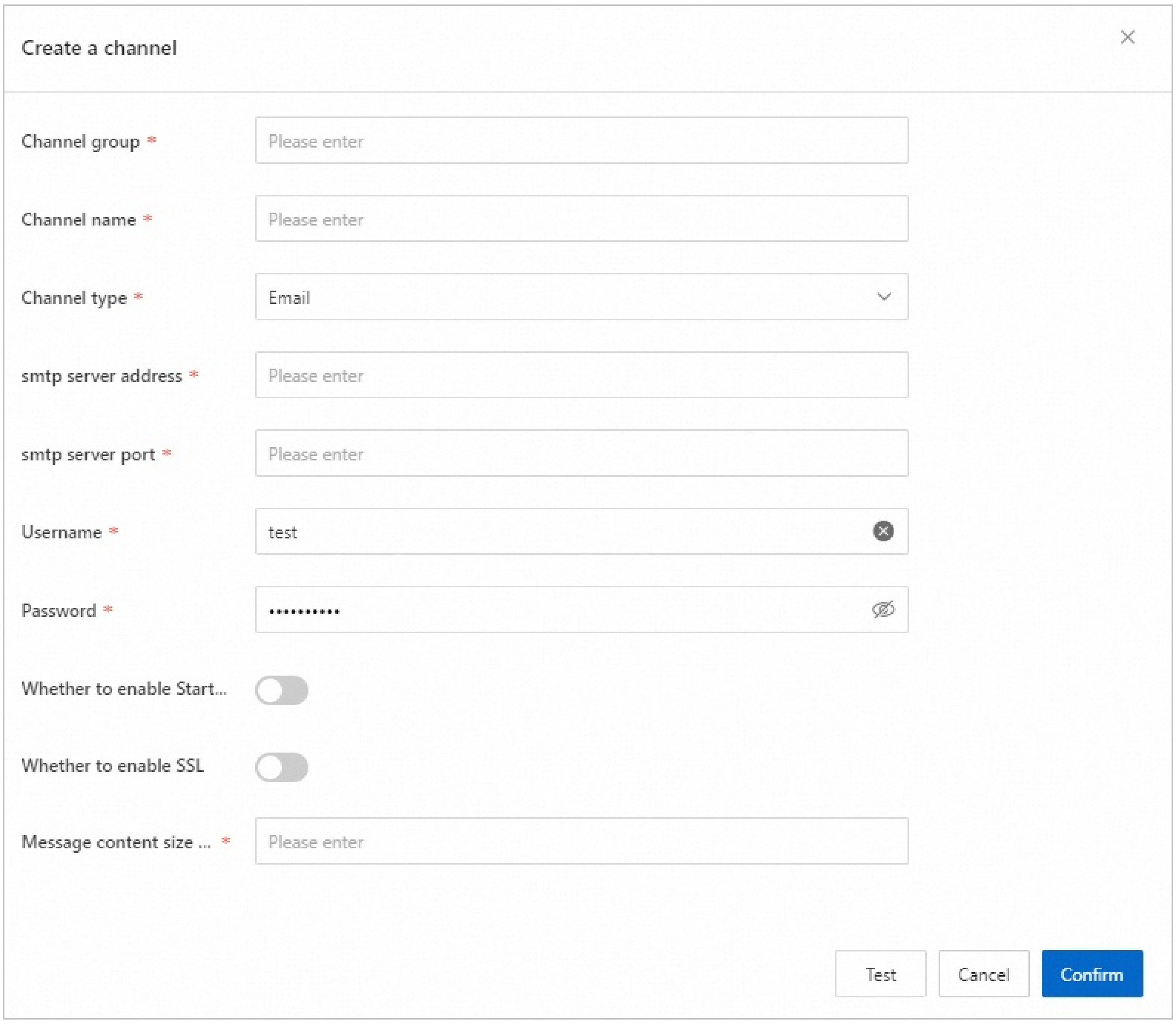
Procedure

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** > **Notification Management** > **Channel Management**.
4. Click **Create a channel** and configure the parameters. The following table describes the parameters.

Parameter	Description
Channel group	Specify a name for the channel group.
Channel name	Specify a name for the channel.

Channel type	Select the channel type. Valid values: ◦ DingTalk ◦ Email ◦ Webhook
DingTalk message push URL	This parameter is available only when you set the**Channel type** parameter to **DingTalk**. The URL that a DingTalk robot uses to push notifications. Default value: https://oapi.dingtalk.com/robot/send.
Robot AccessToken	This parameter is available only when you set the**Channel type** parameter to **DingTalk**. Enter the access token of the DingTalk robot.
Robot SecretKey	This parameter is available only when you set the**Channel type** parameter to **DingTalk**. Enter the secret key of the DingTalk robot.
smtp server address	This parameter is available only when you set the**Channel type** parameter to **Email**. Specify the address of the Simple Mail Transfer Protocol (SMTP) server.
smtp server port	This parameter is available only when you set the**Channel type** parameter to **Email**. Specify the port of the SMTP server.
Username	This parameter is available only when you set the**Channel type** parameter to **Email**. Specify a username that is used to log on to the SMTP server and send notifications.
Password	This parameter is available only when you set the**Channel type** parameter to **Email**. Specify the password of the username that is used to log on to the SMTP server and send notifications.
Whether to enable StartTLS	This parameter is available only when you set the**Channel type** parameter to **Email**. Specify whether to enable StartTLS as the protocol extension for mutual negotiations regarding encryption.

Whether to enable SSL	This parameter is available only when you set the **Channel type** parameter to **Email**. Specify whether to use the Secure Sockets Layer (SSL) protocol to encrypt data transmission.
Push URL	This parameter is available only when you set the **Channel type** parameter to **Webhook**. Enter the push URL.
Custom URL parameters	This parameter is available only when you set the **Channel type** parameter to **Webhook**. Specify the URL parameters in a POST request. The following preset parameter mappings are supported: ◦ ${contact_list}: the list of contacts. ◦ ${content_title}: the content title. ◦ ${content_body}: the content body.
Custom header	This parameter is available only when you set the **Channel type** parameter to **Webhook**. Specify the headers in a POST request. Preset parameter mappings are supported.
Request body template (JSON string)	This parameter is available only when you set the **Channel type** parameter to **Webhook**. The request body in the POST request. Preset parameter mappings are supported.
Message content size (byte)	Specify the maximum number of bytes allowed in a message.



Create a channel

Channel group * Please enter

Channel name * Please enter

Channel type * Email

smtp server address * Please enter

smtp server port * Please enter

Username * test

Password * ••••••••••

Whether to enable Start...

Whether to enable SSL

Message content size ... * Please enter

5. Click **Test** to check the connectivity of the channel.
6. Click **Confirm** to complete the channel configuration.

Related operations

Operation	Description
View the information about a channel	1. In the upper-left corner of the Channel Management page, select **Channel group**, **Channel name**, **Token**, **Channel type**, or **Channel Status** from the drop-down list, and then specify a keyword to filter the channel whose information you want to view. 2. Click **Details** in the **Operation** column of the channel. 3. On the channel details page, click **Test** to check the connectivity of the channel.
Modify the information about a channel	1. Find the channel whose information you want to modify and click **Edit** in the **Operation** column of the channel. 2. In the dialog box that appears, modify the parameters and click **Test** to check the connectivity of the channel. 3. Click **OK** to complete the modification.

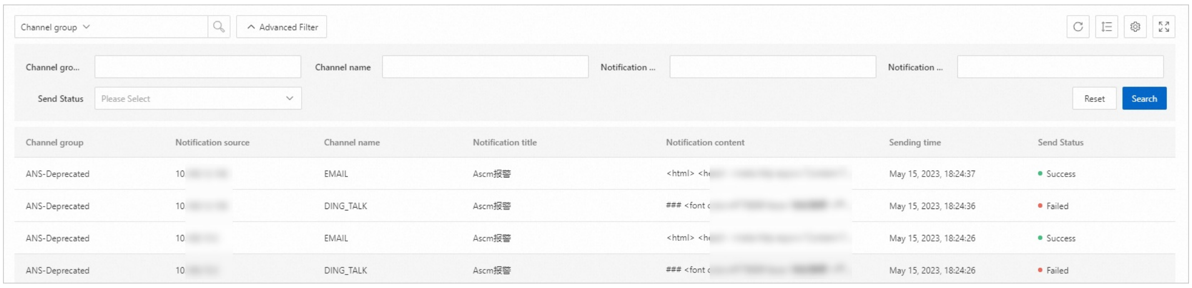
Delete a channel	1. Find the channel that you want to delete and click**Delete** in the **Operation** column of the channel. 2. In the message that appears, click **Delete**.

6.2.4.2. Push history

You can view the message push records of the platform.

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** > **Notification Management** > **Push History**.
4. In the upper part of the page, select **Channel group**, **Channel name**, **Notification source**, **Notification title**, or **Send Status** from the drop-down list. Then, specify the keyword to search for the push records that you want to view.
5. Alternatively, click **Advanced Filter**, specify the **Channel group**, **Channel name**, **Notification source**, **Notification title**, and **Send Status** parameters to filter push records that you want to view.



Channel group	Notification source	Channel name	Notification title	Notification content	Sending time	Send Status
ANS-Deprecated	10[redacted]	EMAIL	Ascm报警	<html> <h[redacted]	May 15, 2023, 18:24:37	● Success
ANS-Deprecated	10[redacted]	DING_TALK	Ascm报警	### <font c[redacted]	May 15, 2023, 18:24:36	● Failed
ANS-Deprecated	10[redacted]	EMAIL	Ascm报警	<html> <h[redacted]	May 15, 2023, 18:24:26	● Success
ANS-Deprecated	10[redacted]	DING_TALK	Ascm报警	### <font c[redacted]	May 15, 2023, 18:24:26	● Failed

6.2.5. Regions

If multiple regions exist in the current environment, 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

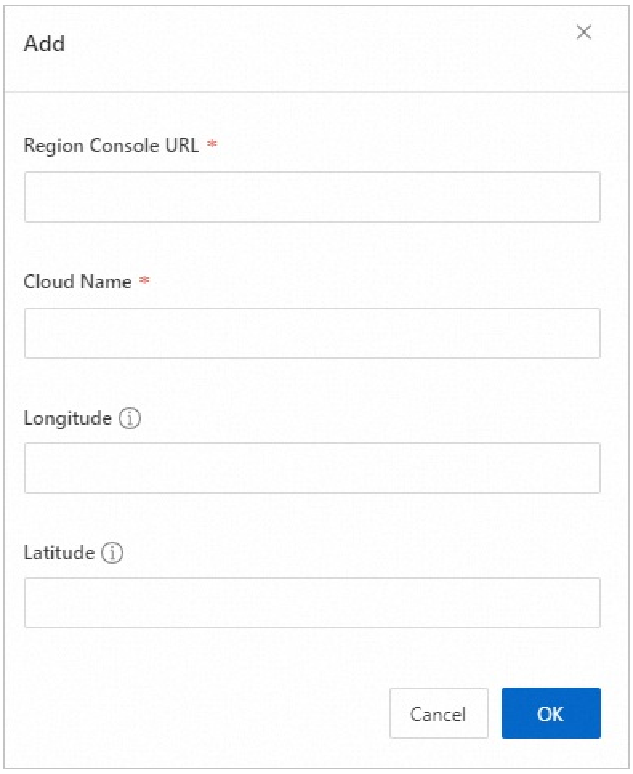
Before you add regions, make sure that the following conditions are met:

- 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 **Platform Settings** > **Regions**.
4. In the upper-left corner of the Regions page, click **Add**, configure the parameters, and then click **OK**. The following table describes the parameters.

Parameter	Description
Region Console URL	The console URL of the region. Make sure that the console URL is valid. Otherwise, an error message is returned.
Cloud Name	The name of the new data center.
Longitude	The geographic longitude of the region. Valid values: 73 to 134.
Latitude	The geographic latitude of the region. Valid values: 18 to 53.



5. 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.

Related operations

You can modify the settings of the regions that you added.

1. Find the region that you want to modify and click **Edit** in the **Actions** column.
2. In the dialog box that appears, modify the parameters and click **OK**.

6.3. API management

The API Management module is used to view and manage product information and API information registered on OpsAPI Gateway.

6.3.1. Namespace management

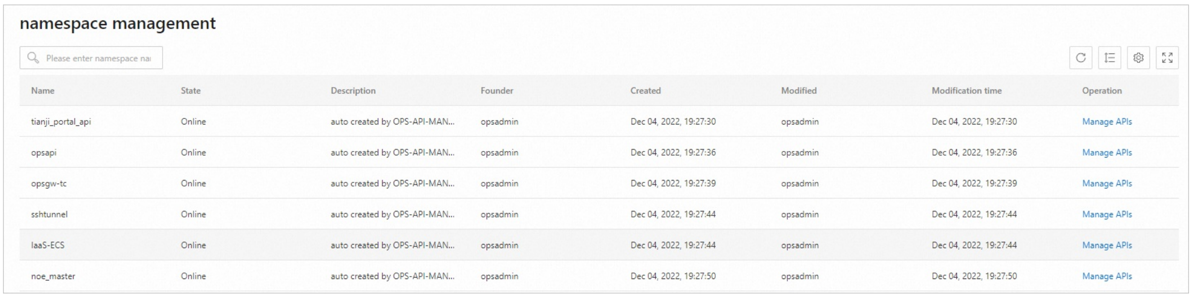
This topic describes how to delete a namespace that is currently registered on the OpsAPI Gateway.

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. View the information of services that are currently registered on the OpsAPI Gateway. You can also filter services by namespace to query the information of specific services.



namespace management

Name	State	Description	Founder	Created	Modified	Modification time	Operation
tianji_portal_api	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:30	opsadmin	Dec 04, 2022, 19:27:30	Manage APIs
opsapi	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:36	opsadmin	Dec 04, 2022, 19:27:36	Manage APIs
opsgw-tc	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:39	opsadmin	Dec 04, 2022, 19:27:39	Manage APIs
sshtunnel	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:44	opsadmin	Dec 04, 2022, 19:27:44	Manage APIs
IaaS-ECS	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:44	opsadmin	Dec 04, 2022, 19:27:44	Manage APIs
noe_master	Online	auto created by OPS-API-MAN...	opsadmin	Dec 04, 2022, 19:27:50	opsadmin	Dec 04, 2022, 19:27:50	Manage APIs

5. Find the service for which you want to query the API information. Click **Manage APIs** in the **Operation** column. On the **API management** page, you can view the API information of the service.

6.3.2. Manage APIs

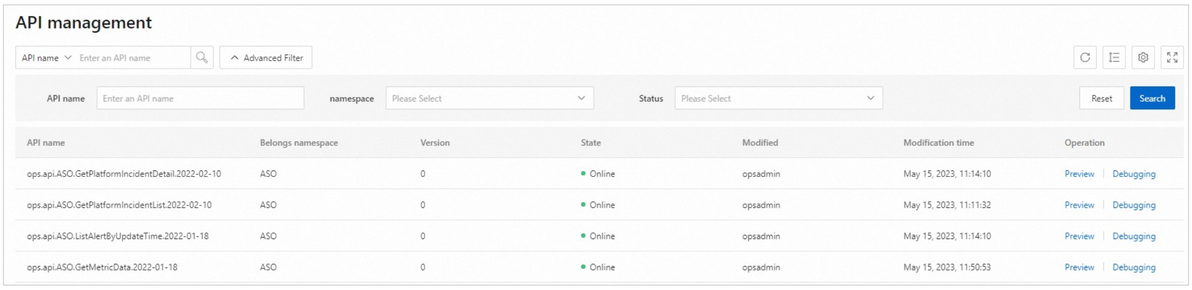
This topic describes how to view the API information of a product that is registered with OpsAPI Gateway.

Prerequisites

OpsAPI is in desired state.

Procedure

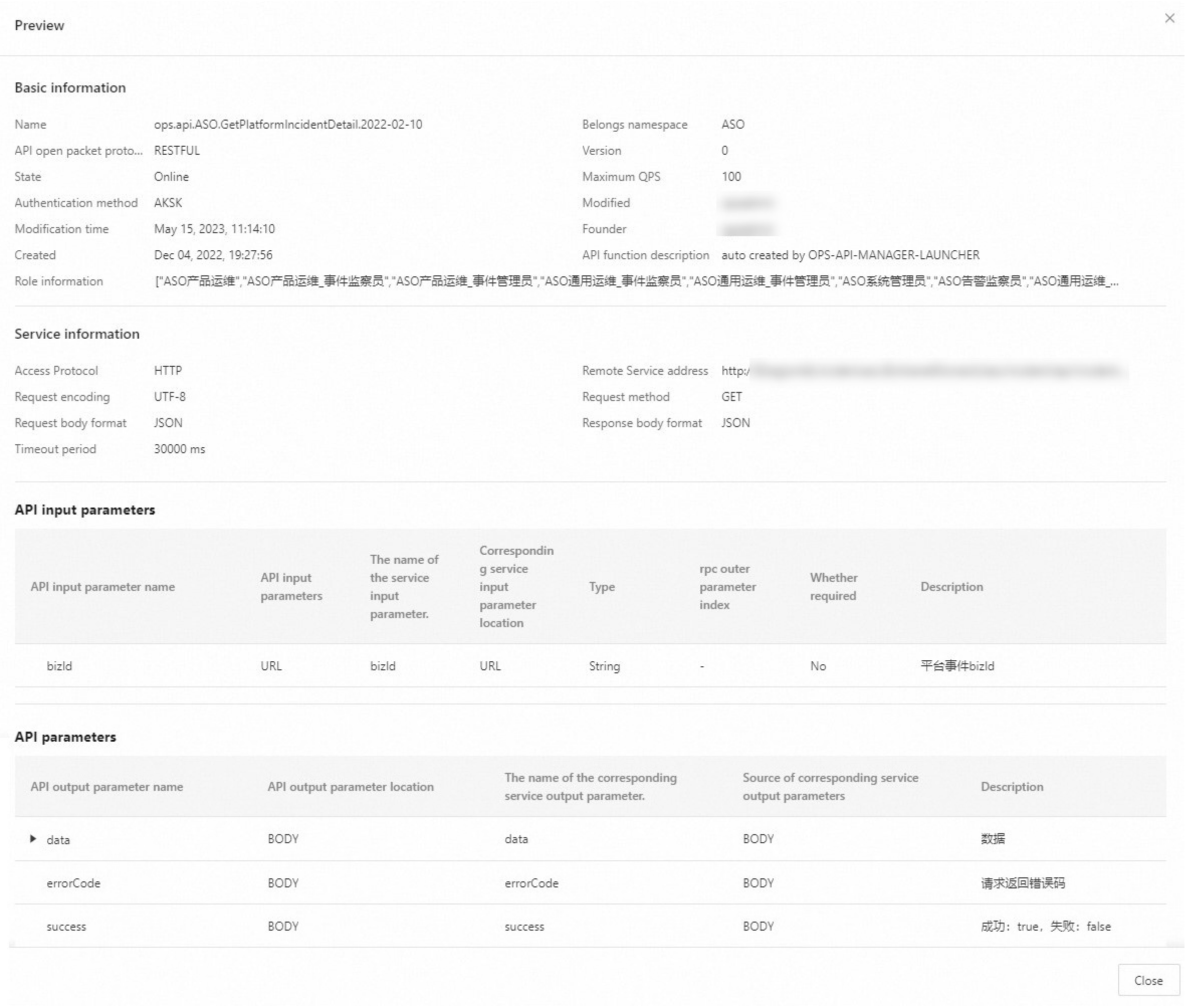
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs** > **API Management**.
4. Click **Advanced Filter** and search for an API by specifying the following filter conditions: **API name**, **namespace**, and **status**.



API management

API name	Belongs namespace	Version	State	Modified	Modification time	Operation
ops.api.ASO.GetPlatformIncidentDetail.2022-02-10	ASO	0	● Online	opsadmin	May 15, 2023, 11:14:10	Preview | Debugging
ops.api.ASO.GetPlatformIncidentList.2022-02-10	ASO	0	● Online	opsadmin	May 15, 2023, 11:11:32	Preview | Debugging
ops.api.ASO.ListAlertByUpdateTime.2022-01-18	ASO	0	● Online	opsadmin	May 15, 2023, 11:14:10	Preview | Debugging
ops.api.ASO.GetMetricData.2022-01-18	ASO	0	● Online	opsadmin	May 15, 2023, 11:50:53	Preview | Debugging

5. Find the API that you want to manage and click **Preview** in the **Operation** column. In the Preview dialog box, you can view the details of the API, including the **basic information**, **service information**, **API request parameters**, and **API response parameters**.



Preview

Basic information

Name	ops.api.ASO.GetPlatformIncidentDetail.2022-02-10	Belongs namespace	ASO
API open packet proto...	RESTFUL	Version	0
State	Online	Maximum QPS	100
Authentication method	AKSK	Modified	[redacted]
Modification time	May 15, 2023, 11:14:10	Founder	[redacted]
Created	Dec 04, 2022, 19:27:56	API function description	auto created by OPS-API-MANAGER-LAUNCHER
Role information	["ASO产品运维","ASO产品运维_事件监察员","ASO产品运维_事件管理员","ASO通用运维_事件监察员","ASO通用运维_事件管理员","ASO系统管理员","ASO告警监察员","ASO通用运维_...		

Service information

Access Protocol	HTTP	Remote Service address	http:/[redacted]
Request encoding	UTF-8	Request method	GET
Request body format	JSON	Response body format	JSON
Timeout period	30000 ms		

API input parameters

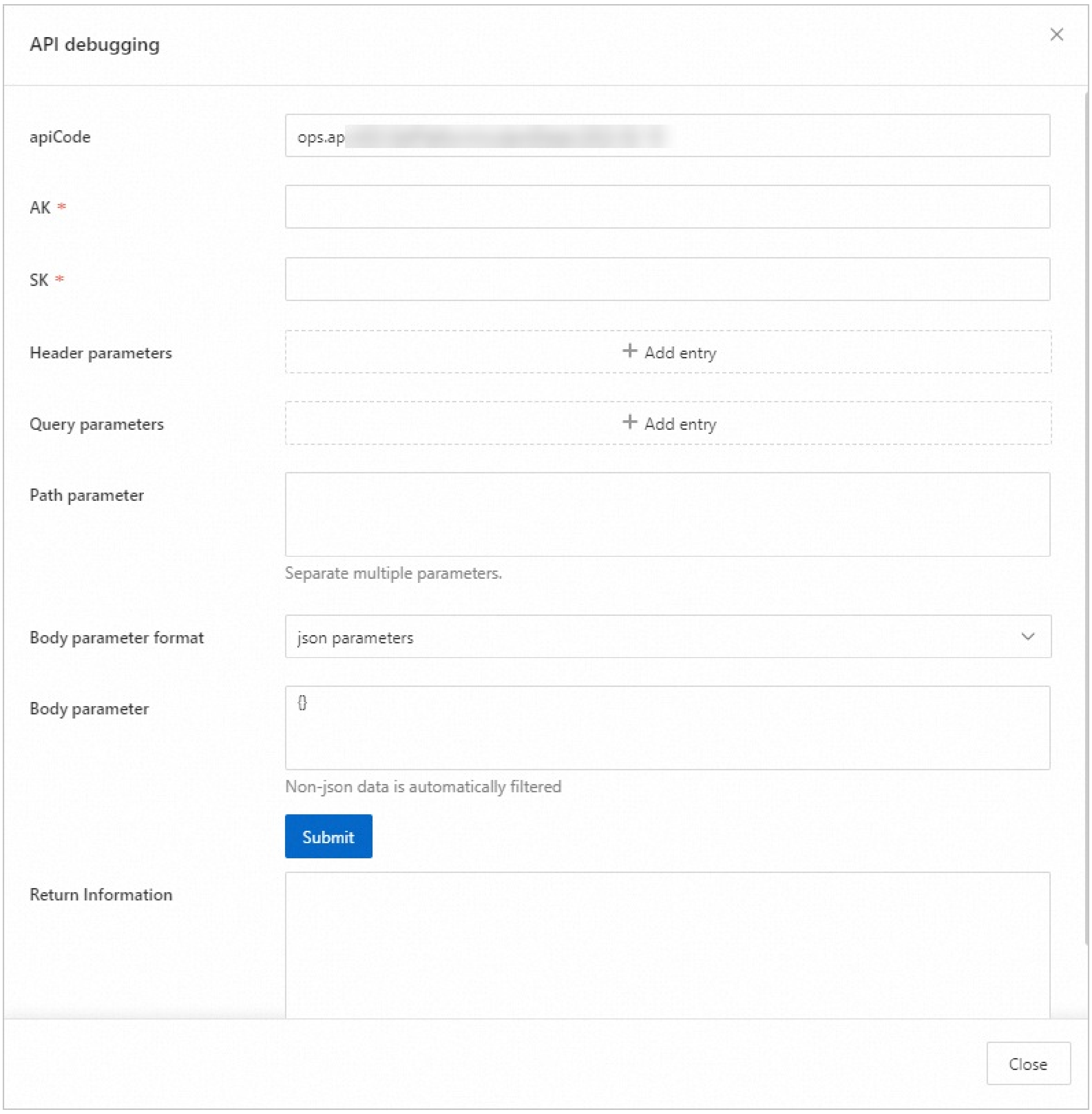
API input parameter name	API input parameters	The name of the service input parameter.	Corresponding service input parameter location	Type	rpc outer parameter index	Whether required	Description
bizId	URL	bizId	URL	String	-	No	平台事件bizId

API parameters

API output parameter name	API output parameter location	The name of the corresponding service output parameter.	Source of corresponding service output parameters	Description
▸ data	BODY	data	BODY	数据
errorCode	BODY	errorCode	BODY	请求返回错误码
success	BODY	success	BODY	成功：true，失败：false

6. Find the API that you want to manage and click **Debugging** in the **Operation** column to test whether the API that is registered with OpsAPI Gateway is available.

   In the API debugging dialog box, configure parameters and click **Submit** to initiate the request. Then, the response data is displayed in the **Return Information** text box.



API debugging

apiCode: ops.ap[redacted]

AK *

SK *

Header parameters: + Add entry

Query parameters: + Add entry

Path parameter

Separate multiple parameters.

Body parameter format: json parameters

Body parameter: {}

Non-json data is automatically filtered

Submit

Return Information

Close

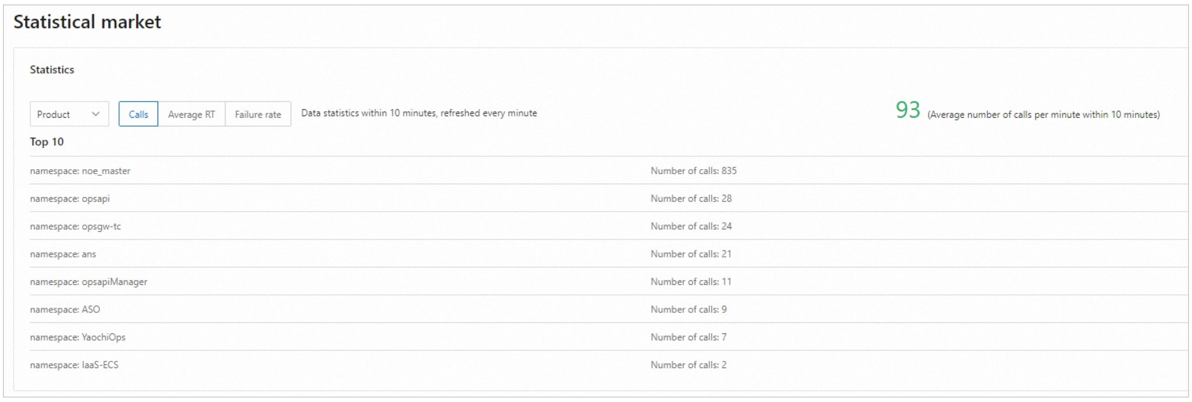
6.3.3. API statistics

6.3.3.1. API overview

This topic describes how to view the calls, average response time, and failure rate of APIs in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs** > **API Statistics** > **Overview**.
4. In the **Statistics** section, select **Product** or **API** from the drop-down list. You can view the **calls**, **average response time**, and **failure rate** of APIs. You can also view the average number of calls per minute within 10 minutes in the right part of this section.



Statistical market

Statistics

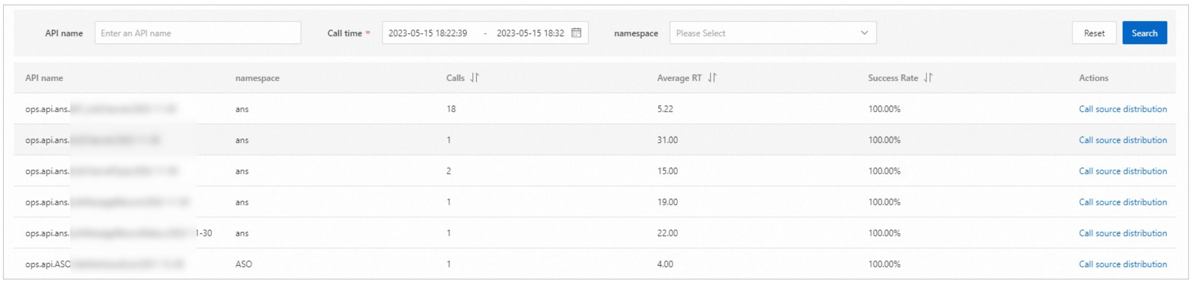
Product | Calls | Average RT | Failure rate | Data statistics within 10 minutes, refreshed every minute

93 (Average number of calls per minute within 10 minutes)

Top 10

namespace: noe_master	Number of calls: 835
namespace: opsapi	Number of calls: 28
namespace: opsgw-tc	Number of calls: 24
namespace: ans	Number of calls: 21
namespace: opsapiManager	Number of calls: 11
namespace: ASO	Number of calls: 9
namespace: YaochiOps	Number of calls: 7
namespace: IaaS-ECS	Number of calls: 2

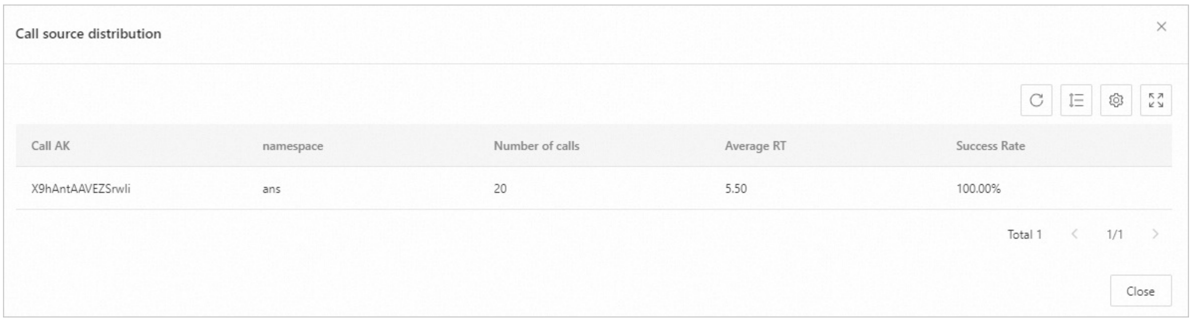
5. In the lower part of the page, you can search for an API by specifying the following filter conditions: **API name**, **call time**, and **namespace**.



API name: Enter an API name | Call time *: 2023-05-15 18:22:39 - 2023-05-15 18:32 | namespace: Please Select | Reset | Search

API name	namespace	Calls	Average RT	Success Rate	Actions
ops.api.ans.[redacted]	ans	18	5.22	100.00%	Call source distribution
ops.api.ans.[redacted]	ans	1	31.00	100.00%	Call source distribution
ops.api.ans.[redacted]	ans	2	15.00	100.00%	Call source distribution
ops.api.ans.[redacted]	ans	1	19.00	100.00%	Call source distribution
ops.api.ans.[redacted]	ans	1	22.00	100.00%	Call source distribution
ops.api.ASO[redacted]	ASO	1	4.00	100.00%	Call source distribution

6. To view the source distribution of an API call, find the API that you want to view and click **Call source distribution** in the **Operation** column.



Call source distribution

Call AK	namespace	Number of calls	Average RT	Success Rate
X9hAntAAVEZSrwli	ans	20	5.50	100.00%

Total 1 < 1/1 >

Close

6.3.3.2. Statistical tasks

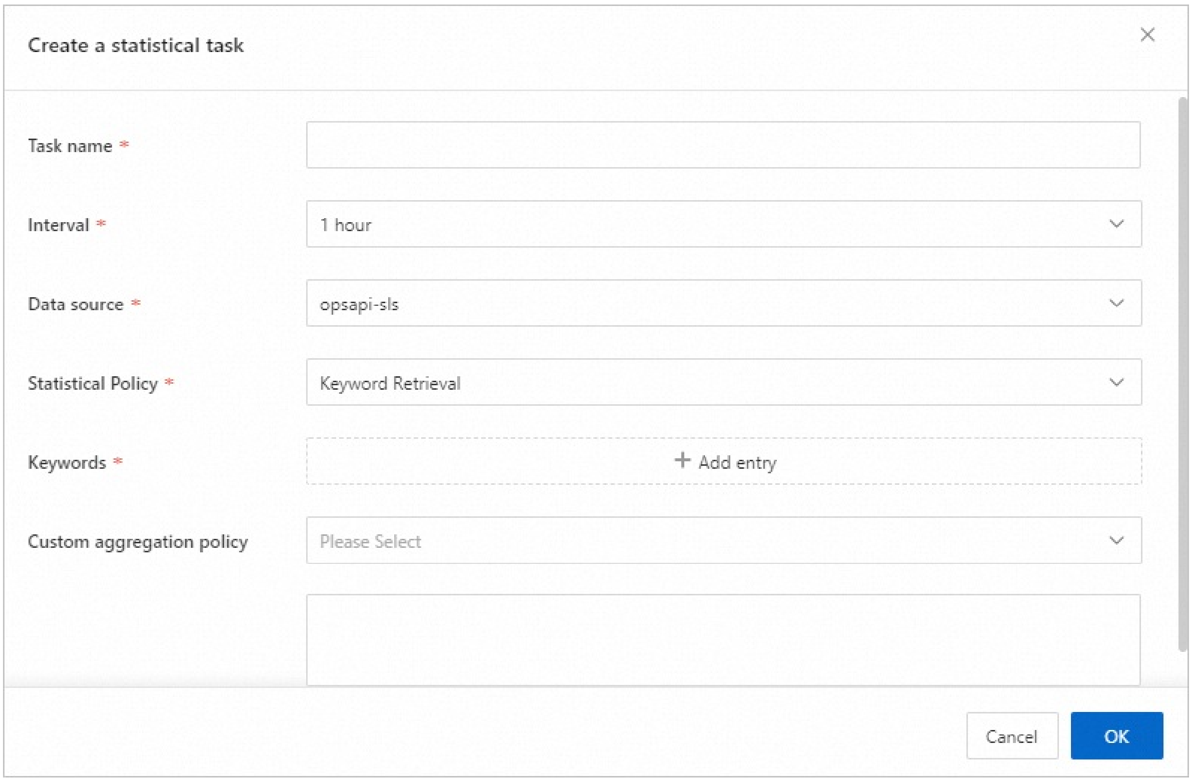
The Apsara Uni-manager Operations Console allows you to create a scheduled statistical task to retrieve the audit logs of each gateway on a regular basis based on the specified statistical policy. This way, the system generates statistical reports by aggregating the audit logs. This topic describes how to create a scheduled statistical task in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **System Settings**.
3. In the left-side navigation pane, choose **APIs** > **API Statistics** > **Tasks**.
4. Click **Create a task**. In the Create a statistical task dialog box, configure the parameters that are described in the following table, and click **OK**.

Parameter	Description

Task name	The name of the statistical task. ⓘ **Important** The task name must be globally unique. Otherwise, the task fails to be created.
Interval	The interval at which the statistical task recurs. Valid values: ◦ 1 hour ◦ 6 hours ◦ 12 hours ◦ 24 hours
Data source	The following data sources are supported: ◦ opsapi-sls ◦ pop-sls
Statistical Policy	Only **Keyword Retrieval** is supported.
Keywords	Click **Add entry**, set the **key** parameter to **ALL_KEY**, and then specify the **value**.
Custom aggregation policy	Select an aggregation policy from the drop-down list.



Create a statistical task

Task name *

Interval * 1 hour

Data source * opsapi-sls

Statistical Policy * Keyword Retrieval

Keywords * + Add entry

Custom aggregation policy Please Select

Related operations

Operation	Description
Start a statistical task	1. Find the statistical task that you want to start and click**Start** in the **Operation** column. 2. If **RUNNING** is displayed in the **Status** column of the task, the task is started.
Stop a statistical task	1. Find the statistical task that you want to stop and click**Stop** in the **Operation** column. 2. If **STOP** is displayed in the **Status** column of the task, the task is stopped.
View the details of a statistical task	1. In the search box next to Create a task, enter a**task name** to search for a statistical task. 2. Find the statistical task that you want to view and click**Task details** in the **Operation** column. 3. In the Task details dialog box, view the details of the statistical task.
View task reports	1. Find the statistical task that you want to view and click**View reports** in the **Operation** column. 2. On the **Statistical report** page, you can view the statistical reports of the statistical task.

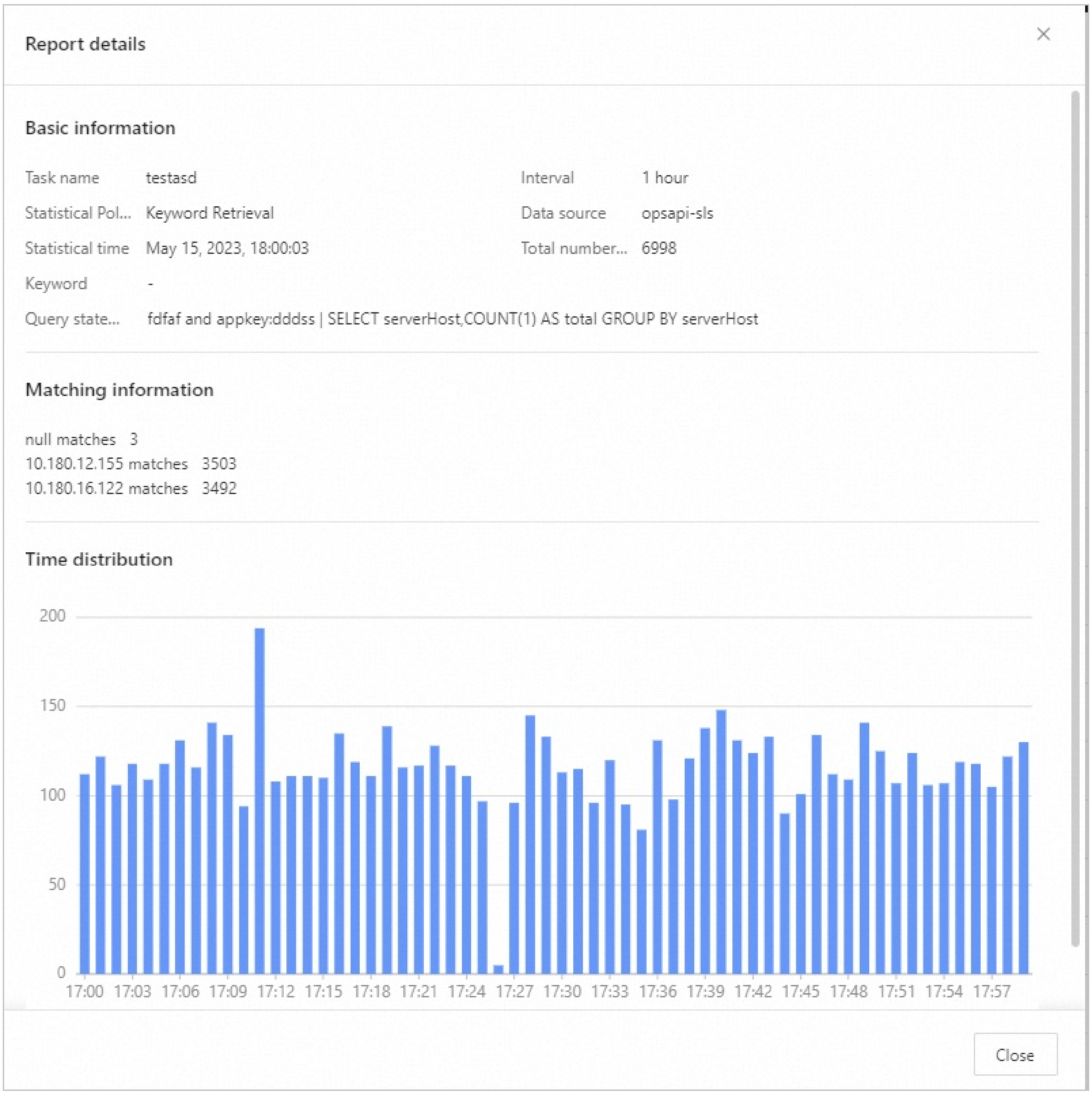
Delete a statistical task	1. Find the statistical task that you want to delete and click **Delete** in the **Operation** column. 2. In the message that appears, click **OK**.

6.3.3.3. Statistical reports

This topic describes how to view the statistical reports that are generated for a statistical task in the Apsara Uni-manager Operations Console. The statistical reports are generated at the interval that you specified when you created the statistical task.

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 Statistics** > **Reports**.
4. In the upper part of the Statistical report page, search for a statistical task by entering a **task name** in the search box.
5. Find the task that you want to view and click **View details** in the **Operation** column.
6. In the dialog box that appears, you can view the report details, including the **basic information**, **matching information**, and **time distribution**.
   - Drag the sliders in the lower part of the Time distribution section to view the task triggering details within a time range.
   - Move the pointer over the graph to view the times that the task is triggered within a time range.



Report details

Basic information

Task name	testasd	Interval	1 hour
Statistical Pol...	Keyword Retrieval	Data source	opsapi-sls
Statistical time	May 15, 2023, 18:00:03	Total number...	6998
Keyword	-		
Query state...	fdfaf and appkey:dddss | SELECT serverHost,COUNT(1) AS total GROUP BY serverHost		

Matching information

null matches 3
10.180.12.155 matches 3503
10.180.16.122 matches 3492

Time distribution