ALIBABA CLOUD

Alibaba Cloud

Apsara Stack

Apsara Uni-manager

Apsara Uni-manager Management Console User Guide

Product Version: V3.18.3

Document Version: 20250124

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.What is the Apsara Uni-manager Management Console?

The Apsara Uni-manager Management Console is provided by Apsara Stack to help organizations perform cloud deployment. The platform improves IT management and operations, aiming to provide large-scale, cost-efficient end-to-end cloud computing and big data services for customers in sectors like public service, education, healthcare, and financial services.

Overview

The Apsara Uni-manager Management Console simplifies the management and deployment of physical and virtual resources, facilitating application development, improving resource utilization, and reducing O&M costs. The console is an integral part of the ecosystem built around cloud computing.

Procedure

Operations in the Apsara Uni-manager Management Console are classified into the following parts:

- Basic configurations for system initialization, such as creating organizations, resource sets, and users, creating basic resources such as virtual private clouds (VPCs), and creating contacts and contact groups in CloudMonitor.
- Creation of cloud resources (performed by administrators).
- Resource management, such as starting, using, and releasing resources, and changing resource configurations and resource quotas.

Emergency mode

The Apsara Uni-manager Management Console is switched to the emergency mode when faults occur to Apsara Stack.

In this mode, only emergency features are available.

Apsara Stack faults

When faults occur to Apsara Stack and Apsara Uni-manager Management Console enters the emergency mode, the following features become unavailable.

Module	Feature	Description

Enterprise	• Organization management: manage AccessKeys; create users and user groups. • Resource set management: grant permissions to users. • Resource set details: grant permissions to users. • User management: create, modify, disable, delete, and grant permissions to users; add users to and remove users from user groups; configure logon policies; configure multi-factor authentication (MFA). • User group management: create, modify, delete, and grant permissions to user groups; add users to and remove users from user groups. • Role permissions: create, modify, disable, delete, replicate, and customize roles. • Data permissions: modify data permissions. • Access control: create, modify, disable, and delete access control policies. • Permission boundary: create, modify, disable, and delete service boundaries; create, modify, and delete API control policies.	The features become unavailable.
Products	• Create cloud resources. • Manage cloud resources. • Redirect to consoles of cloud products.	The features become unavailable.

Central region faults

If your Apsara Stack is deployed across regions, when a fault occurs to the central region, the following features become limited or unavailable in the general regions.

> **Important**
>
> Data inconsistency between the central and general regions may exist when the services are recovered, but will be resolved within five minutes.

Module	Feature	Description
Console	Logon status	• When the console enters the emergency mode, users on the general regions are logged out. • This also happens when the console goes back to normal. Users need to log on again.
Homepage	• Overview: view resources loads. • Platform operations: all features. • Platform resources: all features.	The features become unavailable.

Enterprise	• Organization management: create, modify, and delete organizations; manage AccessKeys; create resource sets, users, and user groups. • Resource set management: create and delete resource sets; modify the names of resource sets; grant permissions to members. • Resource set details: grant permissions to users. • Region management: update associations. • Change management: all change management features. • User management: create, modify, disable, delete, and grant permissions to users; add users to and remove users from user groups; configure logon policies; configure MFA. • User group management: create, modify, delete, and grant permissions to user groups; add users to and remove users from user groups. • Role permissions: create, modify, disable, delete, replicate, and customize roles; grant permissions to users and user groups. • Data permissions: modify data permissions. • Access control: create, modify, disable, and delete access control policies. • Permission boundary: create, modify, disable, and delete service boundaries; create, modify, and delete API control policies.	The features become unavailable.
Operations	• Service orders: all features. • Services: all features. • Quotas: manage quotas and quota alerts. • Statistical analysis: all features. • Metering management: all features. • Bills: all features. • Tags: all features. • Cloud resource optimization: all features. • Billing management: all features. • Global search: search for organizations, resource sets, and resources.	The features become unavailable.
	Product overview	The feature becomes unavailable.

Products	Instance creation	The feature becomes limited. - Service catalogs cannot be used when you create instances. - If instances of a specific cloud product have never been created in a level-1 organization, instances of that cloud product cannot be created within that organization and its sub-organizations.

2.Getting started

2.1. Log on to the Apsara Uni-manager Management Console

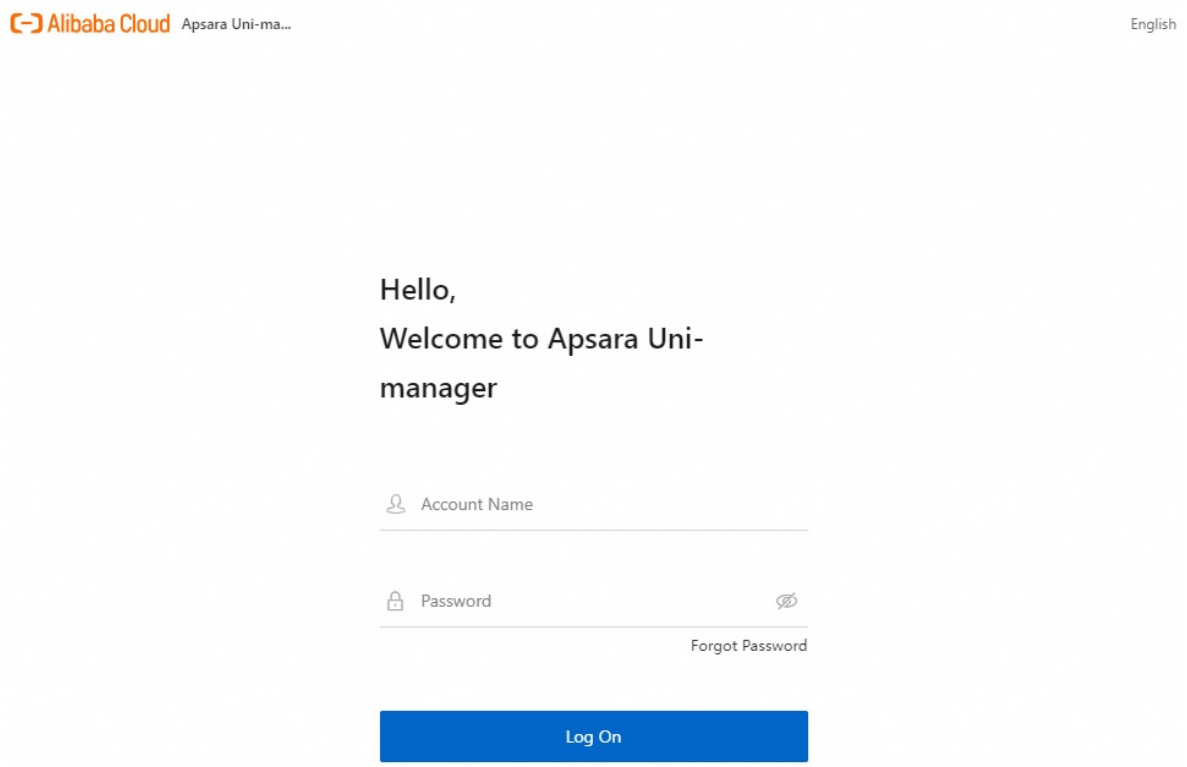
This topic describes how to log on to the Apsara Uni-manager Management Console.

Prerequisites

- The URL of the Apsara Uni-manager Management Console is obtained from the deployment personnel.
- A web browser is available. We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press the Enter key.



> **Note**
>
> - You can click the current language in the upper-right corner to switch to another language.

2. Enter your username and password.

> **Note**
>
> - Obtain the username and password from an operations administrator.
> - If this is the first time you log on to the Apsara Uni-manager Management Console, you must follow the on-screen instructions to change the password of your account. For security purposes, the password must be 10 to 32 characters in length. It must contain all of the following character types: uppercase letters, lowercase letters, digits, and special characters. The following special characters are supported: ! @ # $ %

3. Click **Log On**.
4. If multi-factor authentication (MFA) is enabled for your account, perform the corresponding operations in the following scenarios:
   - **This is the first time that you log on to the Apsara Uni-manager Management Console after MFA is forcefully enabled by the administrator.**
     a. On the Bind Virtual MFA Device page, follow the instructions to bind an MFA device.
     b. Enter the username and password again as in Step 2 and click **Log On**.
     c. Enter a 6-digit MFA verification code and click **Authenticate**.
   - **You have enabled MFA and bound an MFA device.**

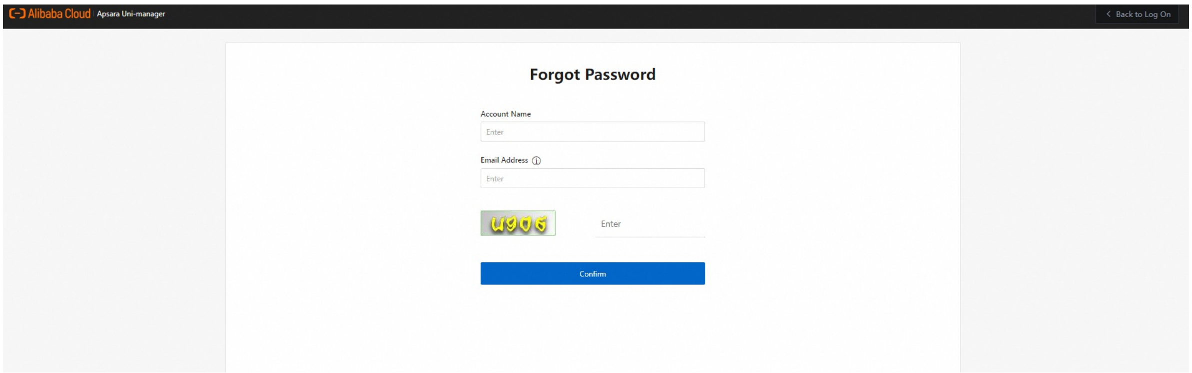
     Enter a six-digit MFA verification code and click **Authenticate**.

     > **Note**
     >
     > For information about how to enable MFA and bind an MFA device, see Manage MFA.

What to do next

Forget password

1. If you forget the logon password, click **Forgot Password** below the Password field.
2. On the Forgot Password page, configure the **Account Name** and **Email Address** parameters, specify the verification code, and then click **Confirm**.

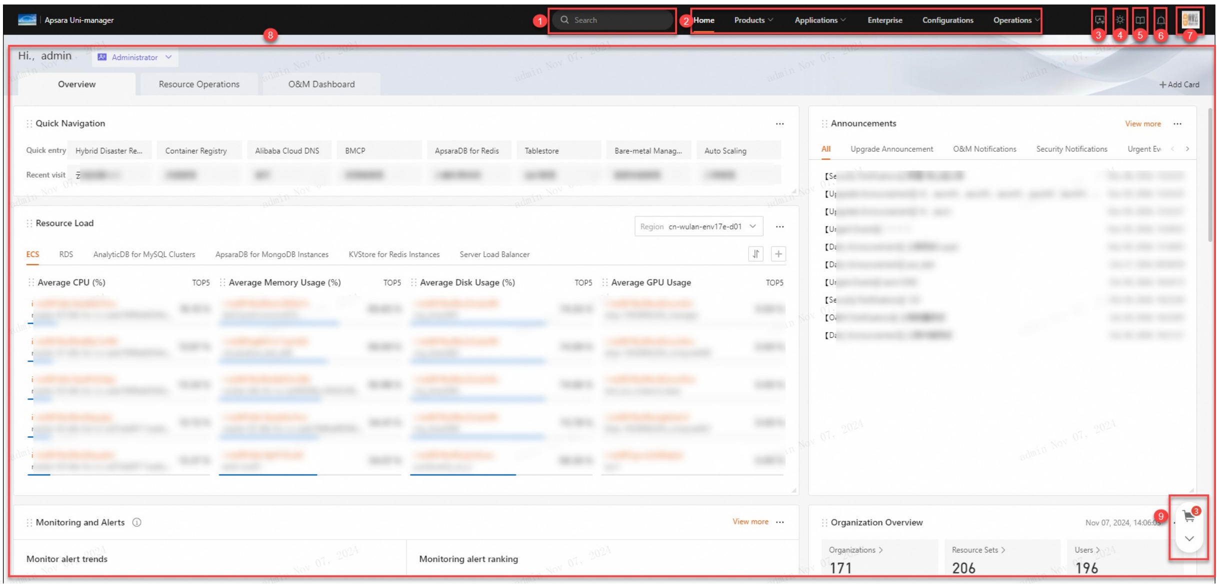


> **Note**
>
> - You can use the username of your account and the email address that was used to create the account.
> - The system sends a link for resetting the password to the email address that you specify.

2.2. Homepage

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

Homepage of the Apsara Uni-manager Management Console



No.	Section	Description
1	Search box	You can search for resources, features, services, users, and documents. After the search, the related search results are displayed by total, API, document, and console. On the Console tab, the cascading menu information is displayed. After you click the search box, recent searches and visits are displayed.
2	Top navigation bar	You can move the pointer over or click the required operation.
3	Multi-language switching	You can switch the language. **Simplified Chinese**, **Traditional Chinese**, and **English** are supported.
4	Color mode switching	You can switch between the dark mode and the light mode for the console.

5	Help information	You can view online documentation.
6	Notifications	You can click **More** to go to **Message Center** to view all messages.
7	User center	You can modify **user information**, view **version information**, or **log out**.
8	Information and operation section	Different information and related operations are displayed on different pages. **Note** Information is displayed in the list. - The ↻, ☰, ⚙, and ⛶ buttons are displayed above the list. You can adjust the list based on your business requirements. - ↻: refreshes the list. - ☰: displays information in the default or compact mode. - ⚙: shows or hides specific items in the list. Move the pointer over a display item and click the ↓ ↑ icon to the right of the display item to adjust the order of the items. - ⛶: displays information in full screen mode. - You can resize the width of columns based on your business requirements. The column width configuration is stored in the local storage of the browser. If you clear the local storage, the configuration becomes invalid.

9	Floating menu	You can expand the floating menu to switch roles, view the shopping cart, view documentation, and go to service consoles based on the permissions of the logon user. - 👤: allows you to switch to a specific Resource Access Management (RAM) role or the Apsara Stack tenant account to meet the requirements of various cloud services. - 🛒6: views the shopping cart. The number on the icon indicates the number of services added to the shopping cart. Whether this icon is displayed depends on the permissions of the current logon user. - 📖: views documentation. This icon is displayed on all pages of the cloud services that have documentation. - 🏠: navigates you to service consoles. This icon is displayed only after you go to a cloud service console. You can click the icon and click the cloud service that you want to manage in the dialog box that appears to go to the corresponding console.

2.3. Organization and permission models

The Apsara Uni-manager Management Console allows you to efficiently manage resources. The Apsara Uni-manager Management Console introduces organizations and resource sets for resource management. This allows enterprises to manage the resources of multi-level organizations and projects.

Organizational structure

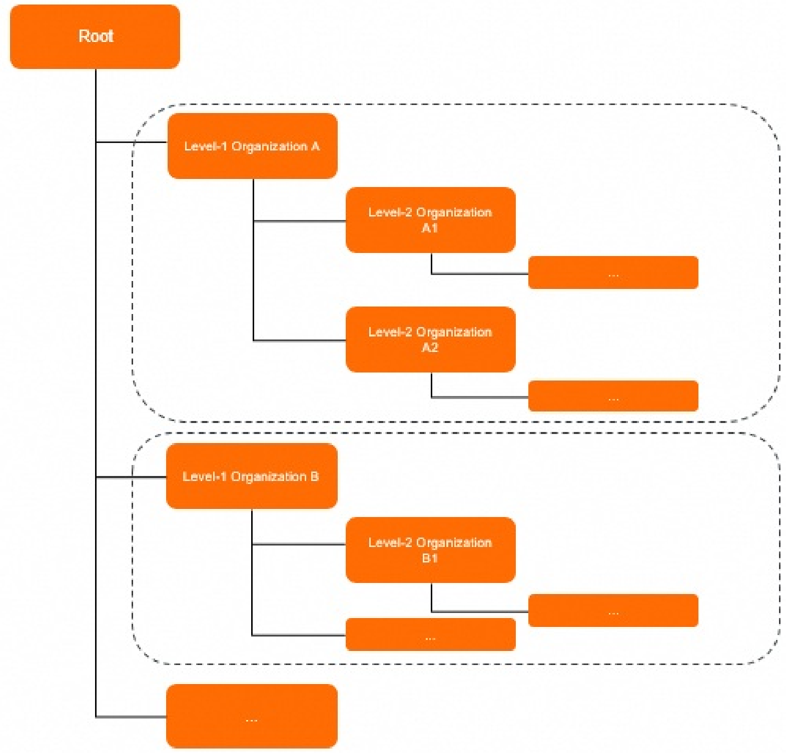
The Apsara Uni-manager Management Console provides the following features based on the multi-level organization structure of enterprises:

The organizational structure is a tree structure that consists of a root organization and multiple organizational units. The root organization is automatically generated by the system and is at the top of the tree structure. An organizational structure can have multiple organizational units, which indicate the subsidiaries or departments of an enterprise. Organizational units are parallel.

> **Note**
>
> An organization unit has only one level-1 organization. A level-1 organization can have multiple subordinate organizations. By default, an organization unit can have up to five levels of organizations.

In the Apsara Uni-manager Management Console, cloud resources and users belong to Apsara Stack tenant accounts and each level-1 organization corresponds to an Apsara Stack tenant account. The subordinate organizations of a level-1 organization and the related users belong to the Apsara Stack tenant account to which the level-1 organization belongs.

After a level-1 organization is created, the system automatically generates an AccessKey pair for the organization. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. AccessKey pairs are used to authenticate request senders. The AccessKey ID is used to identify a user. The AccessKey secret is used to encrypt a signature string.



Relationships between items

- **Organization**: Resources and accounts belong to organizations. An organization does not manage resources. Instead, the organization classifies resources into resource sets that belong to the organization. Organizations are similar to the subsidiaries or departments of enterprises.
- **User**: Users are user accounts associated with roles. When you create a user, you must associate the user with a role to grant the permissions of the role to the user. User accounts are used to log on to the Apsara Uni-manager Management Console.
- **User group**: A user group contains a group of users who have the same permissions. User groups can be associated with roles in the same way as users. This allows you to grant permissions to all users in a user group at a time.
- **Role**: A role specifies a set of access permissions. When you create users, you need to associate different roles with the users to grant various access permissions to the users based on your business requirements.
- **Resource set**: Similar to a project of an enterprise, a resource set allows you to manage resources in a centralized manner. All resources are added to resource sets. Users or user groups can manage resources in a resource set after they are added to the resource set.

Items	Relationship type	Description
Organization and resource set	One-to-many	An organization can have multiple resource sets, but a resource set can belong to only a single organization.

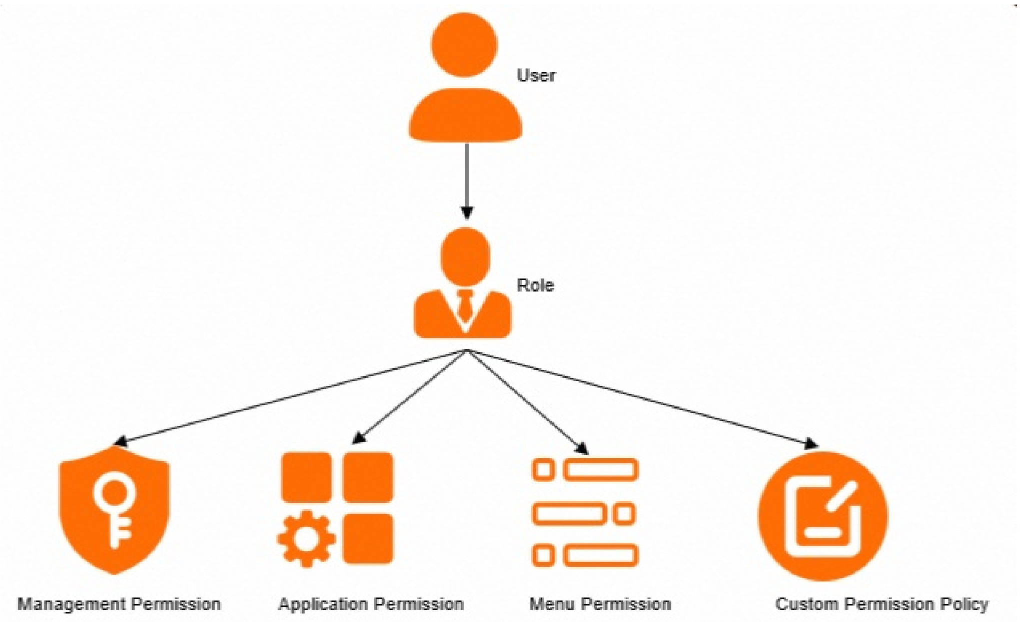
Organization and user	One-to-many	An organization can have multiple users, but a user can belong to only a single organization.
User and resource set	Many-to-many	A user can be added to multiple resource sets. A resource set can also be assigned to multiple users in the level-1 organization to which the resource set belongs.
User and role	Many-to-many	A user can have multiple roles. A role can be assigned to multiple users.
Resource set and resource	One-to-many	A resource set can have multiple resources, but a resource can belong to only a single resource set.

Role permissions

The Apsara Uni-manager Management Console supports fine-grained permission management. This allows you to grant write and read permissions on various cloud resources to different users.

A user can have multiple roles. However, you need to switch to one role to manage resources.

- **Management permissions**: allows a role to perform specific operations in the Apsara Uni-manager Management Console. For example, you can grant management permissions to a role to authorize the role to perform operations on organizations, users, or resource sets.
- **Application permissions**: allows a role to perform operations on cloud services. You can grant application permissions to a role to allow the role to perform specific operations on specific cloud services. For example, if you want to authorize the role to only view Elastic Compute Service (ECS) instances, you need to only select the ECS instance view permissions on the Application Permissions tab.
- **Menu permissions**: allows a role to view specific menus. This implements menu access control. If you grant management permissions on the Apsara Uni-manager Management Console and application permissions on cloud services to a role, you must grant menu permissions on the console to the role. This prevents the role from being unable to see corresponding menus.
- **Custom policy**: You can attach a custom Resource Access Management (RAM) policy to a role to allow or prohibit the role from performing specific operations on specific resources. When you configure a custom policy, you must specify the Allow and Deny parameters in the Set RAM Action for Application section. Enter the name of an action that you want to allow for the Allow parameter and enter the name of an action that you want to deny for the Deny parameter. If you specify both the Allow and Deny parameters, the deny authorization takes precedence over the allow authorization.

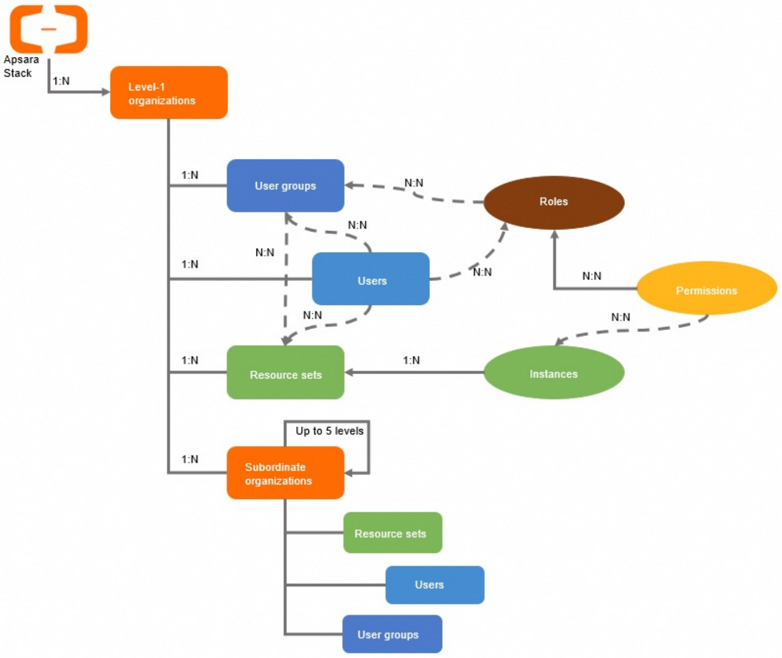


Account permission model

The Apsara Uni-manager Management Console provides a system that integrates accounts with permissions based on the permission and account system of Apsara Stack. In this system, accounts and roles are separately managed. You can flexibly control the permissions in Apsara Stack by associating accounts with roles.

In the Apsara Uni-manager Management Console, you can associate accounts with roles to grant or remove the permissions on corresponding resources.

The following figure shows the account permission model in the Apsara Uni-manager Management Console.

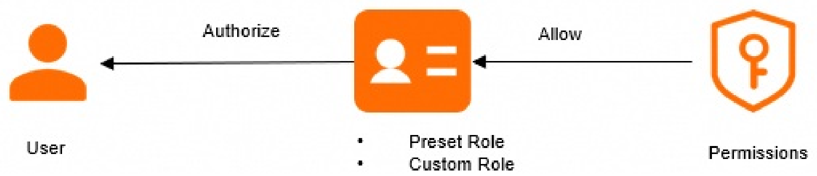


You can use one of the following three methods to grant permissions to users in the Apsara Uni-manager Management Console:

- **Associate a preset role or a custom role with a user**

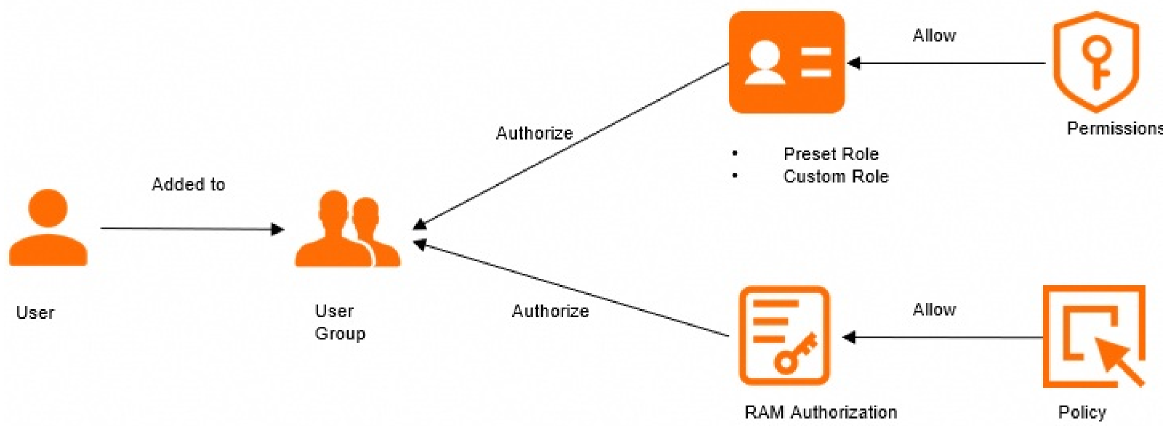
You can associate a preset role or a custom role with a user. This is a common authorization method.

- Preset roles are a set of roles that are preset by the system and have specific permissions. These roles have permissions for common operations and can be directly assigned to users. This simplifies the process of permissions configuration. For more information, see Preset roles and permissions.
- Administrators can configure custom permissions for custom roles based on their business requirements. This ensures that the user permissions match their responsibilities and prevents excessive or insufficient permissions. For more information, see Create a role.



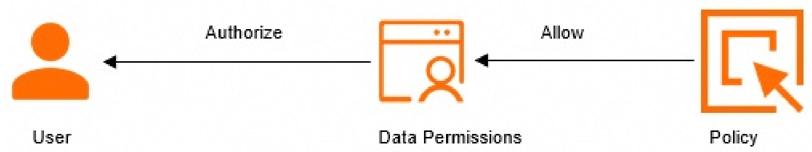
- **Grant permissions to multiple users by using a user group**

  To grant the same permissions to multiple users, you can add these users to a user group and associate the user group with a role that has the corresponding permissions. This way, users in the user group are granted the same permissions. For more information, see User groups.



- **Grant data permissions to users**

  You can grant data permissions to users, which is a critical permission management method. On the Data Permissions page, you can accurately grant access, operation, or management permissions to users on specific resources based on the business requirements of the users. This way, users can efficiently use the required data within their scope of responsibility. You can grant data permissions on resource instances to users. This enhances fine-grained management. For more information, see Data permissions.



Benefits

- Clear hierarchical relationships

  Hierarchical relationships between enterprise organizations are clearly displayed.

- Easy management

  Managers can clearly understand and easily manage various departments and teams.

- High flexibility

  Organization and permission models can be adjusted based on the business requirements of enterprises.

2.4. Initial configuration

2.4.1. Preset roles and permissions

To implement separation of privilege, the Apsara Uni-manager Management Console provides several preset roles based on common use cases on cloud platforms. Each role has a collection of permissions that fit their definition.

Before you use the Apsara Uni-manager Management Console, make sure that you are familiar with the preset roles and their permissions. This way, you can use the preset roles to properly manage the cloud platform.

- The Management scope column specifies the management scope of role permissions.
  - All Organizations: The role has permissions on all organizations.
  - Specified Organization and Subordinate Organizations: The role has permissions on an organization and its subordinate organizations.
  - Resource set: The role has permissions on the resource sets of the associated user.
- The permissions in the Permission list column include the permissions of roles to perform management operations and call API operations in the Apsara Uni-manager Management Console.

> **Note**
>
> - The preset roles and their permissions cannot be modified or deleted.
> - Basic permissions in the Permission list column refer to a set of encapsulated permissions to perform basic operations, such as viewing the homepage and managing user information.

Platform administrator (the username of the preset role is super)

Initializes the configurations of the Apsara Uni-manager Management Console, such as the technical component configurations, language configurations, and customization settings.

Management scope	Permission list

All organizations	**Enterprise**	• **User management** View, create, delete, enable, disable, and manage users. **Note** The platform administrators can view only preset users and custom operations administrators. ◦ Preset users: Platform administrators can only view preset users. ◦ Custom operations administrators: Platform administrators can manage custom operations administrators. • **AccessKey management** View, delete, enable, and disable the AccessKey pairs of users, view AccessKey logs, and create AccessKey pairs for users. • **Access policy** View, create, delete, and manage access policies. • **Service-linked role** View and create service-linked roles.
	Parameter	• **Menu management** Manage menus. • **Announcement** Manage announcements.
	Others	• **OpenAPI Explorer** View and modify page integration configurations, and modify custom settings. • **System configuration** Configure the system.
	Basic permissions	• **Basic permissions** Have basic management permissions.

Operations administrator (the username of the preset role is admin)

Creates and manages organizations and resource sets, adds and manages users, assigns and manages roles, and activates and manages resources in the Apsara Uni-manager Management Console.

Management scope	Permission list

		- **API control policy** View, create, delete, and manage API control policies.
	Enterprise	- **Role management** View, create, delete, manage, lock, and unlock roles, and grant permissions on cloud services to roles. - **Service boundary** View, create, manage, delete, enable, and disable service boundaries. - **User management** View, create, delete, enable, disable, lock, unlock, and manage users. - **Tag management** Manage tags. - **AccessKey management** View the AccessKey pairs of users and organizations, create AccessKey pairs for organizations and users, delete, enable, and disable the AccessKey pairs of organizations and users, and view AccessKey logs. - **Resource set management** View, create, delete, and manage resource sets. - **User group management** View, create, delete, and manage user groups. - **Organization management** View, create, delete, and manage organizations. - **Access policy** View, create, delete, and manage access policies. - **Change management** Change organizations, resource sets, users, or resources. - **Service-linked role** View and create service-linked roles.

All organizations	**Operations**	- **Quota management** View quotas and manage quotas and specification quotas. - **Idle resource and bottleneck analysis** View the idle resource and bottleneck analysis. - **Document management** View, create, modify, copy, delete, publish, and unpublish documents, add, modify, move, and delete document categories, and manage document versions. - **Discount management** View, delete, create, and modify discount configurations. - **Billing configuration** View, manage, create, and delete prices. - **Health analysis** View health status, and view and modify resource optimization configurations. - **Operation log** View and set the storage mode of operation logs. - **Service catalog** View, create, modify, delete, publish, and unpublish service catalogs, and manage service catalogs by category. - **Carbon footprint report** View the carbon footprint reports of organizations and resource sets, and export carbon footprint reports. - **Process management** View, create, modify, publish, disable, and delete processes, and view organization applications. - **Report download** View, create, and delete tasks, download reports, and view and create report pushing rules. - **Bill reconciliation** Manage bills. - **Portal management** View, create, modify, publish, unpublish, and delete sites, view, create, modify, copy, build, publish, and delete pages, and view, upload, modify, and delete materials. - **Usage statistics** View and export usage statistics. - **Bill management** View the bills of organizations and resource sets, and export and regenerate bills. - **Order management** View organization orders.

	Configuration	- **Multi-cloud management** Manage multi-cloud organizations, multi-cloud resource sets, and multi-cloud roles. - **Announcement management** Manage announcements. - **Billing switch** Modify billing switch settings. - **Multi-cloud management platform hosting** Configure multi-cloud management platform hosting.
	Others	- **OpenAPI Explorer** View call statistics, view and modify page integration configurations, and modify custom settings.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Organization administrator

Manages the specified organization, creates and manages subordinate organizations, creates and manages resource sets, adds and manages users, assigns and manages roles, activates and manages resources, assigns administrators and quotas to subordinate organizations and resource sets, and approves resource applications based on service process settings.

Management scope	Permission list

Specified organization and its subordinate organizations	**Enterprise**	• **Role management** View, create, delete, and manage roles, and grant permissions on cloud services to roles. • **User management** View, create, delete, enable, disable, and manage users. • **Tag management** Manage tags. • **AccessKey management** View the AccessKey pairs of users and organizations, create AccessKey pairs for organizations and users, delete, enable, and disable the AccessKey pairs of organizations and users, and view AccessKey logs. • **Resource set management** View, create, delete, and manage resource sets. • **User group management** View, create, delete, and manage user groups. • **Organization management** View, create, delete, and manage organizations. • **Access policy** View, create, delete, and manage access policies. • **Change management** Change organizations, resource sets, users, or resources. • **Service-linked role** View and create service-linked roles.

	Operations	- **Quota management** View and manage quotas. - **Idle resource and bottleneck analysis** View the idle resource and bottleneck analysis. - **Health analysis** View health status and resource optimization configurations. - **Service catalog** View, create, modify, delete, publish, and unpublish service catalogs. - **Carbon footprint report** View the carbon footprint reports of organizations and resource sets, and export carbon footprint reports. - **Process management** View processes and organization applications. - **Report download** View, create, and delete tasks, download reports, and view and create report pushing rules. - **Usage statistics** View and export usage statistics. - **Bill management** View the bills of organizations and resource sets, and export bills. - **Order management** View organization orders.
	Others	- **OpenAPI Explorer** View call statistics and page integration configurations.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Resource set administrator

Manages the specified resource set, adds and manages users, activates and manages resources, and approves resource applications based on service process settings.

Management scope	Permission list

Resource set	**Enterprise**	- **User management** View users. - **Tag management** Manage tags. - **AccessKey management** View AccessKey logs. - **Resource set management** View and manage resource sets. - **User group management** View user groups. - **Organization management** View organizations.
	Operations	- **Quota management** View quotas. - **Idle resource and bottleneck analysis** View the idle resource and bottleneck analysis. - **Health analysis** View health status. - **Carbon footprint report** View the carbon footprint reports of organizations and resource sets, and export carbon footprint reports. - **Report download** View, create, and delete tasks, download reports, and view and create report pushing rules. - **Usage statistics** View and export usage statistics.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Resource user

Uses the cloud resources created and allocated by the operations administrator.

Management scope	Permission list

Resource set	**Enterprise**	• **Tag management** Manage tags. • **Resource set management** View resource sets. • **Organization management** View organizations. • **Service-linked role** View service-linked roles.
	Operations	• **Quota management** View quotas. • **Report download** View, create, and delete tasks, download reports, and view and create report pushing rules.
	Basic permissions	• **Basic permissions** Have basic management permissions.

Resource auditor (the username of the preset role is auditor)

This role has the read-only permission on all resources in Apsara Stack.

Management scope	Permission list	
	Enterprise	• **Role management** View roles. • **User management** View users. • **AccessKey management** View the AccessKey pairs of users and AccessKey logs. • **Resource set management** View resource sets. • **User group management** View user groups. • **Organization management** View organizations. • **Access policy** View access policies.

All organizations	**Operations**	- **Quota management** View quotas. - **Idle resource and bottleneck analysis** View the idle resource and bottleneck analysis. - **The configuration of the billing method.** View prices. - **Health analysis** View health status. - **Operation log** View and download operation logs, and view the storage mode of operation logs. - **Service catalog** View service catalogs. - **Process management** View organization applications. - **Report download** View tasks, download reports, and view and create report pushing rules. - **Usage statistics** View and export usage statistics. - **Bill management** View the bills of organizations and resource sets, and export bills. - **Order management** View organization orders.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Organization resource auditor

Has read-only permissions on all resources in the organization to which it belongs.

Management scope	Permission list

Specified organization and its subordinate organizations	**Enterprise**	- **Role management** View roles. - **User management** View users. - **AccessKey management** View the AccessKey pairs of users and AccessKey logs. - **Resource set management** View resource sets. - **User group management** View user groups. - **Organization management** View organizations. - **Access policy** View access policies.
	Operations	- **Quota management** View quotas. - **Idle resource and bottleneck analysis** View the idle resource and bottleneck analysis. - **Health analysis** View health status. - **Operation log** View and download operation logs. - **Service catalog** View service catalogs. - **Process management** View organization applications. - **Report download** View tasks, download reports, and view and create report pushing rules. - **Usage statistics** View and export usage statistics. - **Bill management** View the bills of organizations and resource sets, and export bills. - **Order management** View organization orders.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Security auditor

Audits the security of Apsara Stack.

Management scope	Permission list	
All organizations	Operations	- **Operation log** View and download operation logs.
	Other	- **OpenAPI Explorer** View call statistics and page integration configurations.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Platform security administrator

This role has the permissions to use SOC to manage the security of Apsara Stack.

Management scope	Permission list	
All organizations	Operations	- **Operation log** View and download operation logs.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Global organization security administrator (the username of the preset role is yundunadmin)

Uses SOC to conduct security management for Apsara Stack and all tenants, and manages security products related to Elastic Compute Service (ECS).

Management scope	Permission list

All organizations	**Enterprise**	- **Role management** View, create, delete, and manage roles. - **User management** View, enable, disable, and manage users. - **AccessKey management** View AccessKey logs. - **Resource set management** View resource sets. - **Organization management** View organizations. - **Service-linked role** View and create service-linked roles.
	Operations	- **Operation log** View and download operation logs.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Organization security administrator

Uses SOC to manage the security of hosts, applications, and networks for an organization. This role also manages security products related to Elastic Compute Service (ECS).

Management scope	Permission list	
Specified organization and its subordinate organizations	**Enterprise**	- **Resource set management** View resource sets. - **Organization management** View organizations. - **Service-linked role** View and create service-linked roles.
	Operations	- **Operation log** View and download operation logs.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Security system configuration administrator

Configures system security features such as the upgrade center and global configurations.

Management scope	Permission list	
All organizations	Operations	• **Operation log** View and download operation logs.
	Basic permissions	• **Basic permissions** Have basic management permissions.

Platform security auditor

This role has the permissions to use SOC to check the security conditions of Apsara Stack.

Management scope	Permission list	
All organizations	Enterprise	• **Resource set management** View resource sets. • **Organization management** View organizations.
	Operations	• **Operation log** View and download operation logs.
	Basic permissions	• **Basic permissions** Have basic management permissions.

Global organization security auditor

This role has the permissions to use SOC to check the security conditions of all organizations.

Management scope	Permission list	
	Enterprise	• **Resource set management** View resource sets. • **Organization management** View organizations.

All organizations	**Operations**	- **Operation log** View and download operation logs.
	Basic permissions	- **Basic permissions** Have basic management permissions.

Platform security configuration administrator

This role has the permissions to configure security services in Apsara Stack, such as Server Guard and Web Application Firewall (WAF).

Management scope	Permission list	
All organizations	**Operations**	- **Operation log** View and download operation logs.
	Basic permissions	- **Basic permissions** Have basic management permissions.

2.4.2. Configuration description

Before you use the Apsara Uni-manager Management Console, you must complete a series of basic configuration operations as an administrator, such as creating organizations, resource sets, users, and roles and initializing resources. This is the initial system configuration.

The Apsara Uni-manager Management Console manages the organizations, resource sets, users, and roles of cloud data centers in a centralized and service-oriented manner to grant different resource access permissions to different users.

- Organization

  After the Apsara Uni-manager Management Console is deployed, a root organization is automatically generated. You can create other organizations under the root organization.

  Organizations are displayed in a hierarchical structure. You can create subordinate organizations under each organization level.

- Resource Set

  A resource set is a container used to store resources. Each resource must belong to a resource set.

- User

  A user is a resource manager and user.

- Role

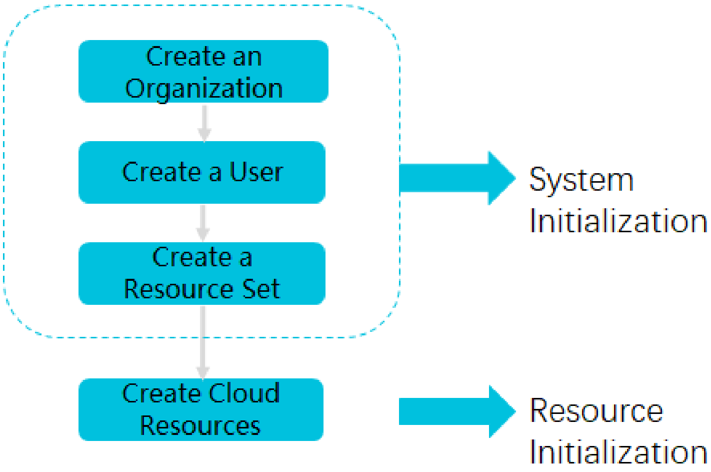
  A role is a set of access permissions. You can assign different roles to different users to implement system access control to meet a variety of different requirements.

The following table describes the relationships among organizations, resource sets, users, roles, and cloud resources.

Relationship between two items	Relationship type	Description
Organization and resource set	One-to-many	An organization can have multiple resource sets, but each resource set can belong to only a single organization.
Organization and user	One-to-many	An organization can have multiple users, but each user can belong to only a single organization.
Resource set and user	Many-to-many	A user can have multiple resource sets, and a resource set can be assigned to multiple users under the same level-1 organization.
User and role	Many-to-many	A user can have multiple roles, and a role can be assigned to multiple users.
Resource set and resource	One-to-many	A resource set can have multiple resources, but each cloud resource can belong to only a single resource set.

2.4.3. Configuration process

Before users can the Apsara Uni-manager Management Console, administrators must complete the initial system configuration based on the process shown in the following figure.



1. Create an organization

   Create an organization to store resource sets and their resources.

2. Create a user

   Create users and assign the users different roles to meet different requirements for system access control.

3. Create a resource set

   Create a resource set before you apply for resources.

   Users that have the permissions on a resource set can use the resources in the resource set. For information about how to authorize a user to use a resource set, see the Grant users the permissions on a resource set section of the "Manage resource sets" topic.

4. Create cloud resources

Create instances in the consoles of cloud services based on project requirements. For more information about how to create cloud service instances, see the user guide of each cloud service.

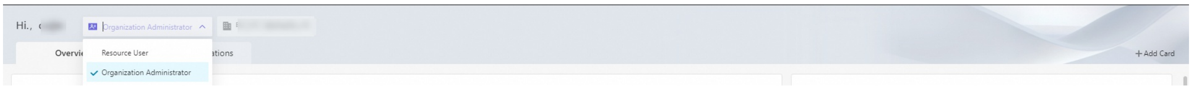
3.Home

The Home page displays the usage and monitoring status of system resources in different regions from different dimensions by using a card-based layout. This helps you understand the overall resource status and provides supporting data for refined operations and statistical analysis.

Procedure

By default, the card-based layout of the Home page varies based on roles. You can add or remove cards to change the layout based on your business requirements.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Home**.
3. If you have multiple roles, you can change roles in the upper-left corner.

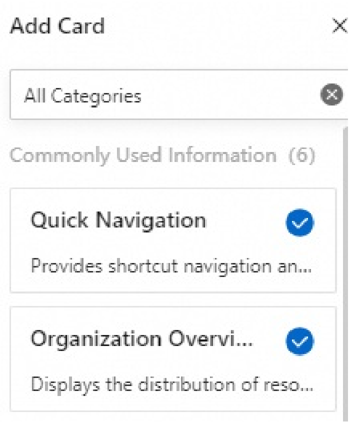


4. In the upper-right corner of the page, click **Add Card**.

> **Note**
>
> If multiple tabs are displayed on the Home page, you can click a specific tab, and then add cards on the tab.

5. In the **Add Card** panel, select or deselect a card to specify the information that you want to display on the Home page.

> **Note**
>
> - You can select or deselect cards to add cards to or remove the cards from the Home page. After you add a card, you can click the ... icon in the upper-right corner of the card and then click **Remove from Workbench** to remove the card from the Home page.
> - You can click and drag the ◢ icon in the lower-right corner of a card to resize the card. You can click and drag the ⠿ icon in the upper-left corner of a card to change the position at which the card is displayed.
> - You can click **Restore to Default Layout** at the bottom of the **Add Card** panel to restore the default layout of the Home page.



Add Card

All Categories

Commonly Used Information (6)

Quick Navigation ✓

Provides shortcut navigation an...

Organization Overvi... ✓

Displays the distribution of reso...

Card categories

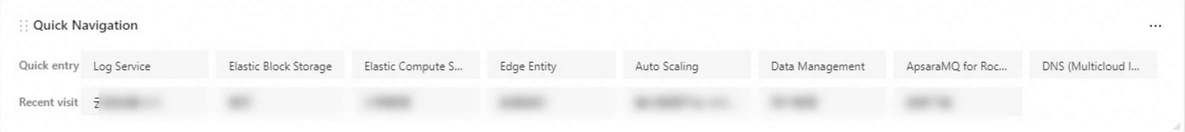
The cards are classified into the following categories: commonly used information, resource alerts, resource health analysis, resource statistics and analysis, and resource bills. Different roles have different permissions. The cards associated with a role are displayed.

Commonly used information

The commonly used information category includes the following cards: **Quick Navigation**, **Organization Overview**, **Announcements**, **To Do Center**, **Services and Support**, **Physical Resource Overview**, **Virtual Resource Overview**, **Resource Overview**, and **Resource Search**.

- **Quick Navigation**: provides multiple shortcuts for quick navigation to the corresponding pages. In the **Quick Entry** and **Recent Visit** sections, you can click the displayed shortcuts to go to the corresponding pages.

> **Note**
>
> In the Quick Entry section, you can add the shortcuts based on your business requirements. You can add up to 12 shortcuts of services and modules. To add a shortcut, you can perform the following steps: Click **Add Entry** in the Quick Entry section. In the drop-down menu that appears, click a service category in the left-side navigation pane, move the pointer over the name of the service whose shortcut you want to add, and then click the ☆ icon. After you add a shortcut, the ★ icon is displayed to the right of the service name.

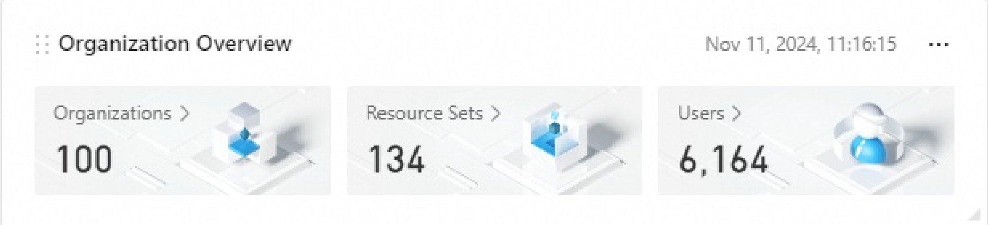


Quick Navigation

Quick entry: Log Service | Elastic Block Storage | Elastic Compute S... | Edge Entity | Auto Scaling | Data Management | ApsaraMQ for Roc... | DNS (Multicloud I...

Recent visit

- **Organization Overview**: displays the resource distribution of organizations. You can click the sections in the card to go to the corresponding pages.



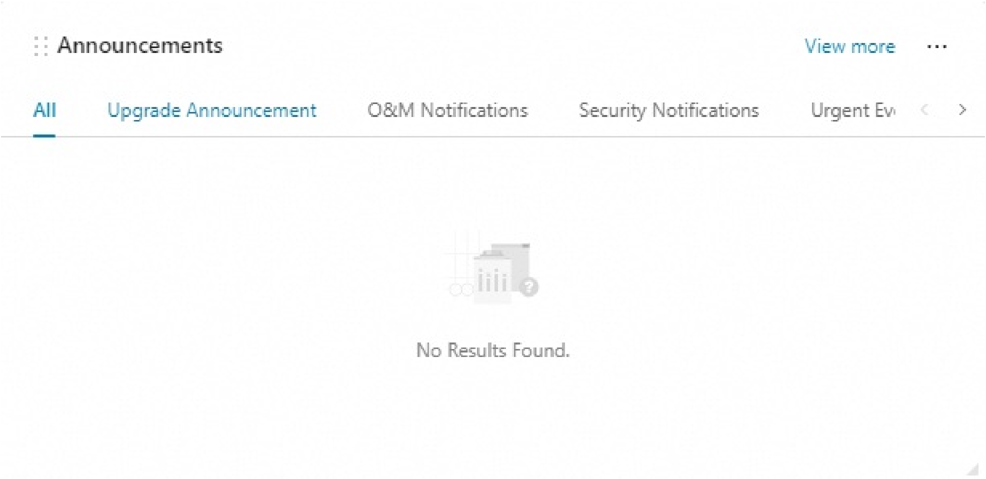
Organization Overview Nov 11, 2024, 11:16:15

Organizations 100

Resource Sets 134

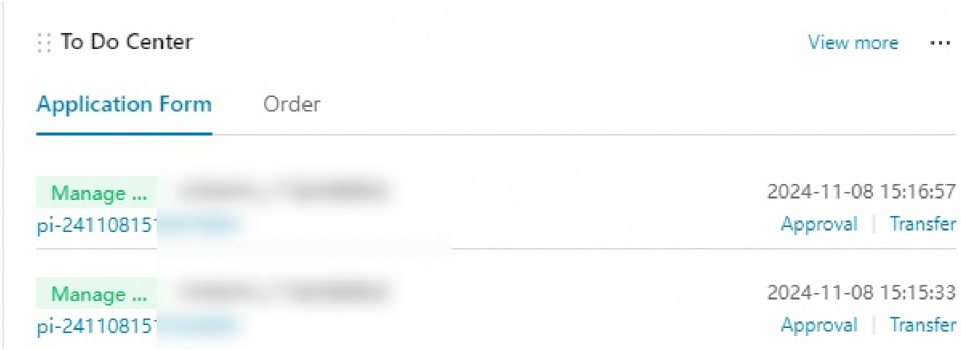
Users 6,164

- **Announcements**: displays announcements and details. You can click **View More** to view more announcements in the **Announcement** panel.



No Results Found.

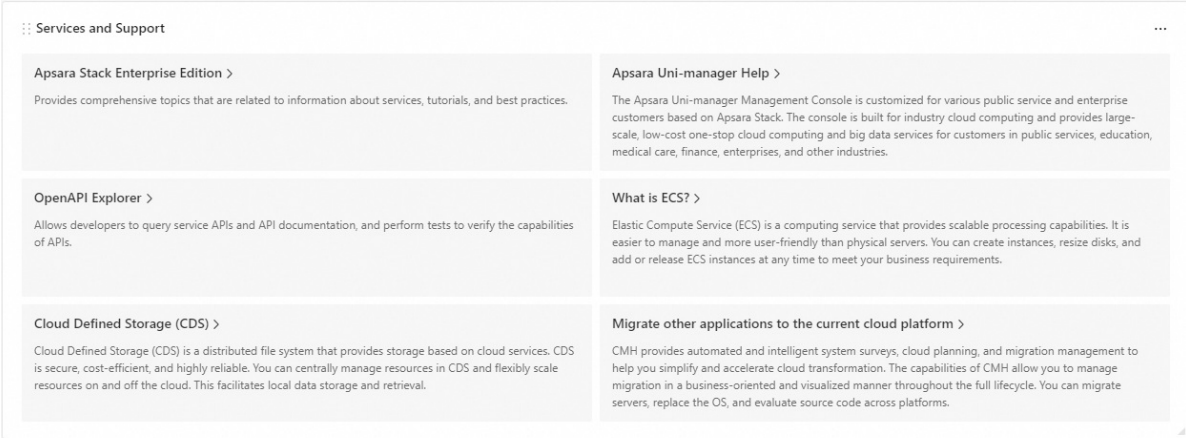
- **To Do Center**: displays the to-do list of the current role. You can click **View More** to view more to-do items in the **To-do Center** panel.



Manage ... [redacted] 2024-11-08 15:16:57
pi-24110815[redacted] Approval | Transfer

Manage ... [redacted] 2024-11-08 15:15:33
pi-24110815[redacted] Approval | Transfer

- **Services and Support**: provides links to technical support and documentation. You can click the links to go to the corresponding pages.



Apsara Stack Enterprise Edition >

Provides comprehensive topics that are related to information about services, tutorials, and best practices.

Apsara Uni-manager Help >

The Apsara Uni-manager Management Console is customized for various public service and enterprise customers based on Apsara Stack. The console is built for industry cloud computing and provides large-scale, low-cost one-stop cloud computing and big data services for customers in public services, education, medical care, finance, enterprises, and other industries.

OpenAPI Explorer >

Allows developers to query service APIs and API documentation, and perform tests to verify the capabilities of APIs.

What is ECS? >

Elastic Compute Service (ECS) is a computing service that provides scalable processing capabilities. It is easier to manage and more user-friendly than physical servers. You can create instances, resize disks, and add or release ECS instances at any time to meet your business requirements.

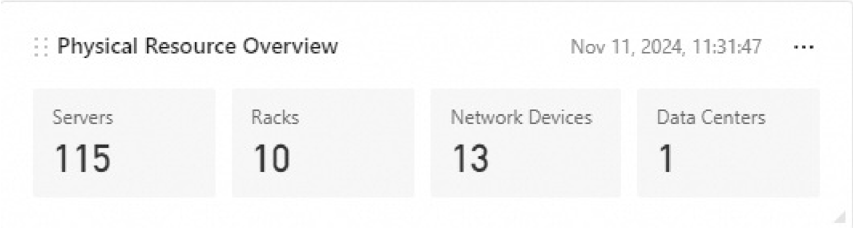
Cloud Defined Storage (CDS) >

Cloud Defined Storage (CDS) is a distributed file system that provides storage based on cloud services. CDS is secure, cost-efficient, and highly reliable. You can centrally manage resources in CDS and flexibly scale resources on and off the cloud. This facilitates local data storage and retrieval.

Migrate other applications to the current cloud platform >

CMH provides automated and intelligent system surveys, cloud planning, and migration management to help you simplify and accelerate cloud transformation. The capabilities of CMH allow you to manage migration in a business-oriented and visualized manner throughout the full lifecycle. You can migrate servers, replace the OS, and evaluate source code across platforms.

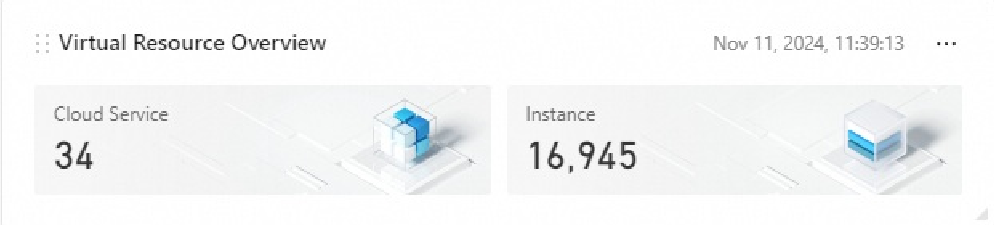
- **Physical Resource Overview**: displays statistics on the number of physical resources on the current platform.



Nov 11, 2024, 11:31:47

Servers	Racks	Network Devices	Data Centers
115	10	13	1

- **Virtual Resource Overview**: displays statistics on the number of cloud resources on the current platform.



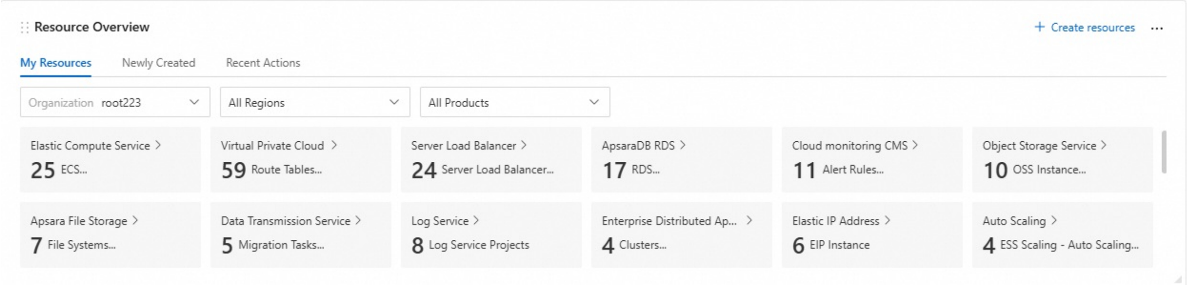
Virtual Resource Overview

Nov 11, 2024, 11:39:13

Cloud Service
34

Instance
16,945

- **Resource Overview**: displays global resources. Click **Create resources**. In the dialog box that appears, find the service that you want to manage and activate the service.



Resource Overview

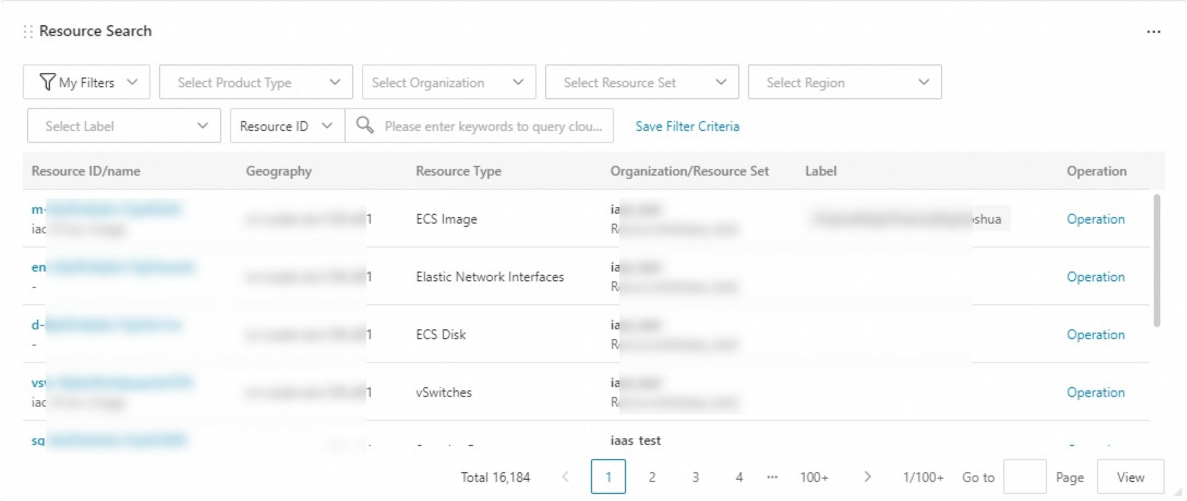
+ Create resources

My Resources | Newly Created | Recent Actions

Organization root223 | All Regions | All Products

Elastic Compute Service > 25 ECS...	Virtual Private Cloud > 59 Route Tables...	Server Load Balancer > 24 Server Load Balancer...	ApsaraDB RDS > 17 RDS...	Cloud monitoring CMS > 11 Alert Rules...	Object Storage Service > 10 OSS Instance...
Apsara File Storage > 7 File Systems...	Data Transmission Service > 5 Migration Tasks...	Log Service > 8 Log Service Projects	Enterprise Distributed Ap... > 4 Clusters...	Elastic IP Address > 6 EIP Instance	Auto Scaling > 4 ESS Scaling - Auto Scaling...

- **Resource Search**: allows you to search for cloud resources globally. You can search for resources by service type, organization, resource set, region, label, resource ID, and keyword.



Resource Search

My Filters | Select Product Type | Select Organization | Select Resource Set | Select Region

Select Label | Resource ID | Please enter keywords to query clou... | Save Filter Criteria

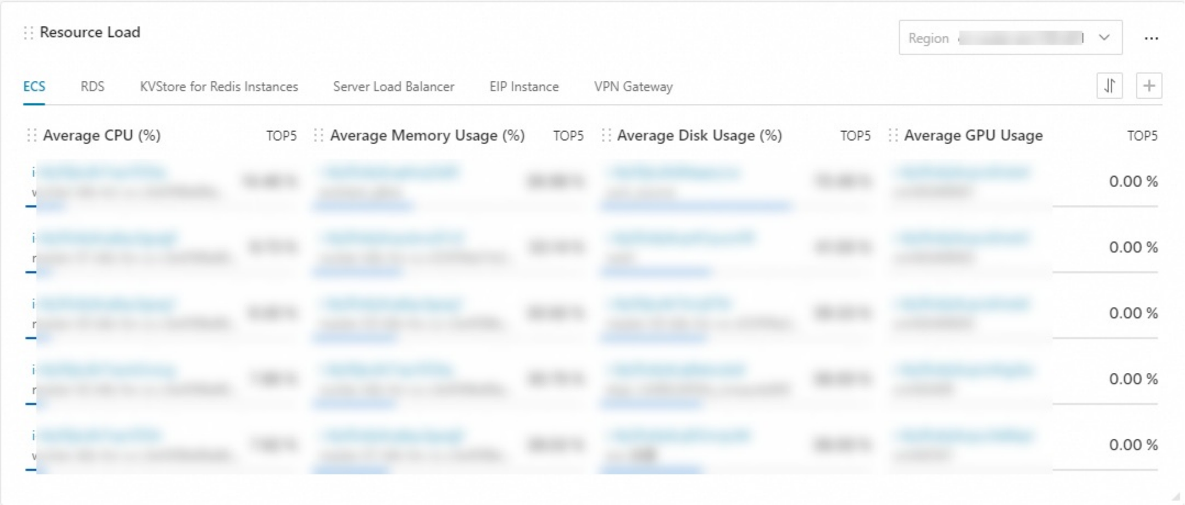
Resource ID/name	Geography	Resource Type	Organization/Resource Set	Label	Operation
m-[redacted] iac[redacted]	[redacted]1	ECS Image	ia[redacted] R[redacted]	[redacted]shua	Operation
en[redacted] -	[redacted]1	Elastic Network Interfaces	ia[redacted] R[redacted]		Operation
d-[redacted] -	[redacted]1	ECS Disk	ia[redacted] R[redacted]		Operation
vs[redacted] iac[redacted]	[redacted]1	vSwitches	ia[redacted] R[redacted]		Operation
sq[redacted]			iaas test		

Total 16,184 < 1 2 3 4 ··· 100+ > 1/100+ Go to Page View

Resource alerts

The resource alerts category includes the following cards: **Resource Load**, **Monitoring and Alerts**, and **Alerts**.

- **Resource Load**: displays the resource load of the current account. You can click the Region drop-down list above the resource list to change regions.

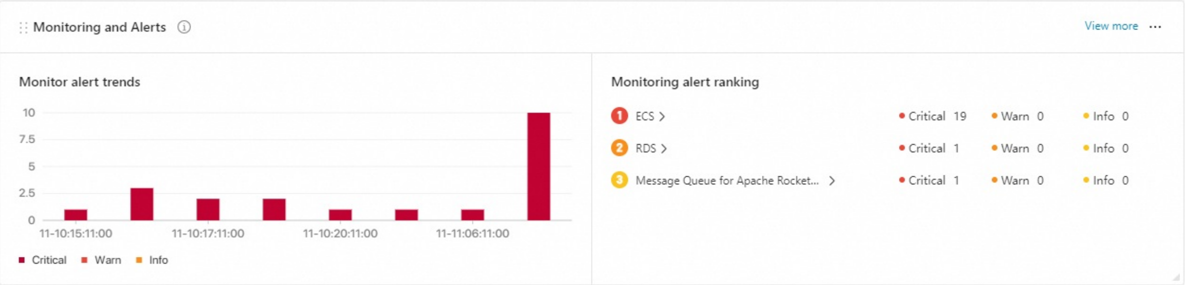


Resource Load

Region [redacted]

Average CPU (%)	TOP5	Average Memory Usage (%)	TOP5	Average Disk Usage (%)	TOP5	Average GPU Usage	TOP5
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0.00 %
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0.00 %
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0.00 %
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0.00 %
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0.00 %

- **Monitoring and Alerts**: displays the information about resource monitoring and alert analysis from the CloudMonitor console. You can click **View More** to go to the **Alert History** page of the CloudMonitor console.

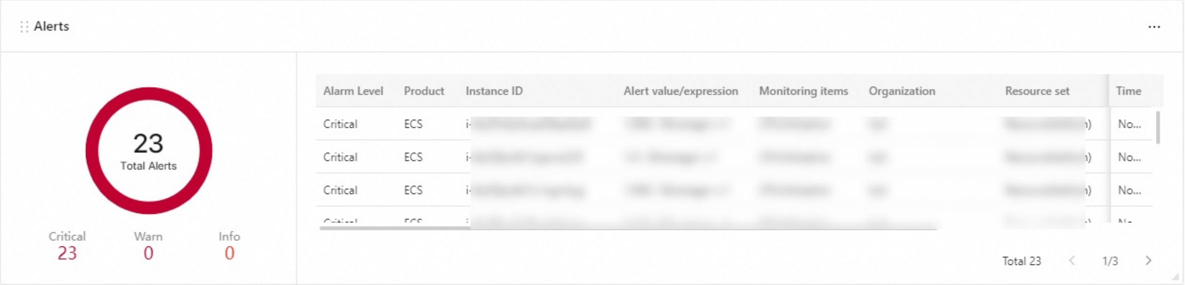


Monitoring and Alerts

Monitoring alert ranking

1	ECS >	● Critical 19	● Warn 0	● Info 0
2	RDS >	● Critical 1	● Warn 0	● Info 0
3	Message Queue for Apache Rocket... >	● Critical 1	● Warn 0	● Info 0

- **Alerts**: display the alerts of the current account.



Alerts

23 Total Alerts

Critical 23 | Warn 0 | Info 0

Alarm Level	Product	Instance ID	Alert value/expression	Monitoring items	Organization	Resource set	Time
Critical	ECS	i-[redacted]	[redacted]	[redacted]	[redacted]	[redacted])	No...
Critical	ECS	i-[redacted]	[redacted]	[redacted]	[redacted]	[redacted])	No...
Critical	ECS	i-[redacted]	[redacted]	[redacted]	[redacted]	[redacted])	No...

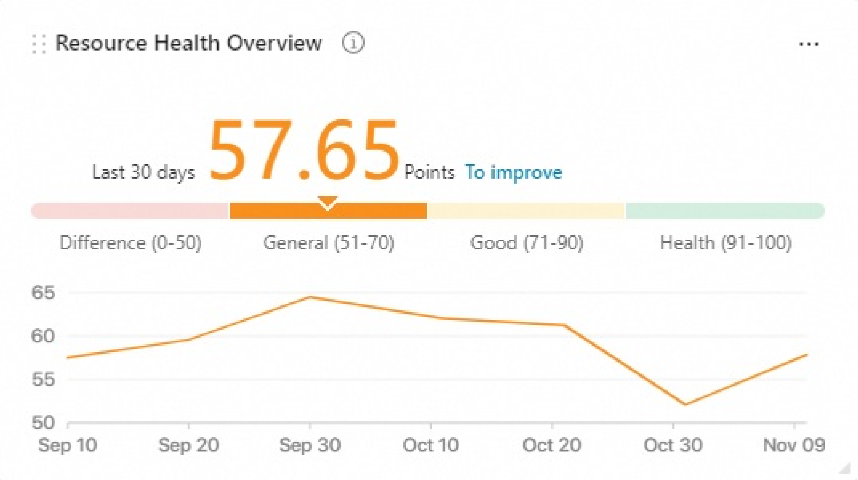
Total 23 < 1/3 >

Resource health analytics

The resource health analytics category includes the following cards: **Resource Health Overview**, **Resource Health Analytics**, **Idle Resource Ranking**, and **Resource Bottleneck Rankings**.

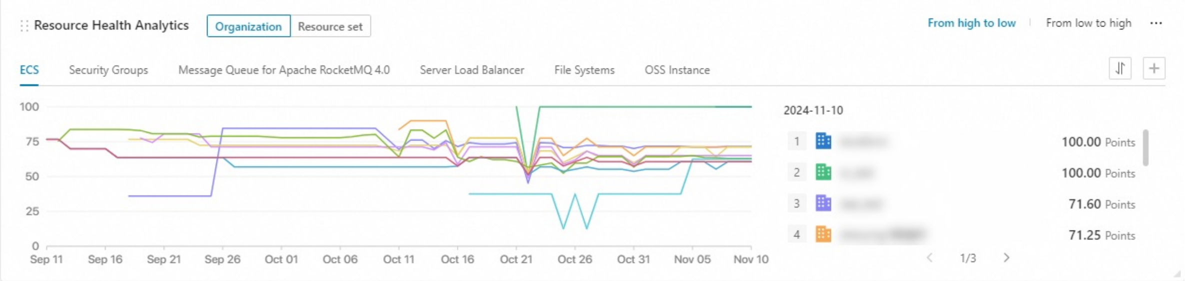
- **Resource Health Overview**: displays the health status of the current organization resources. You can click **To improve** to go to the Overall Health Score page under the Operations menu to view details.

> **Note**
>
> - The overall health score is calculated based on resource usage, idle resource analytics, and resource compliance analytics.
> - The following items describe the health score classification:
>   - 0 to 50 points: poor
>   - 51 to 70 points: average
>   - 71 to 90 points: good
>   - 91 to 100 points: healthy



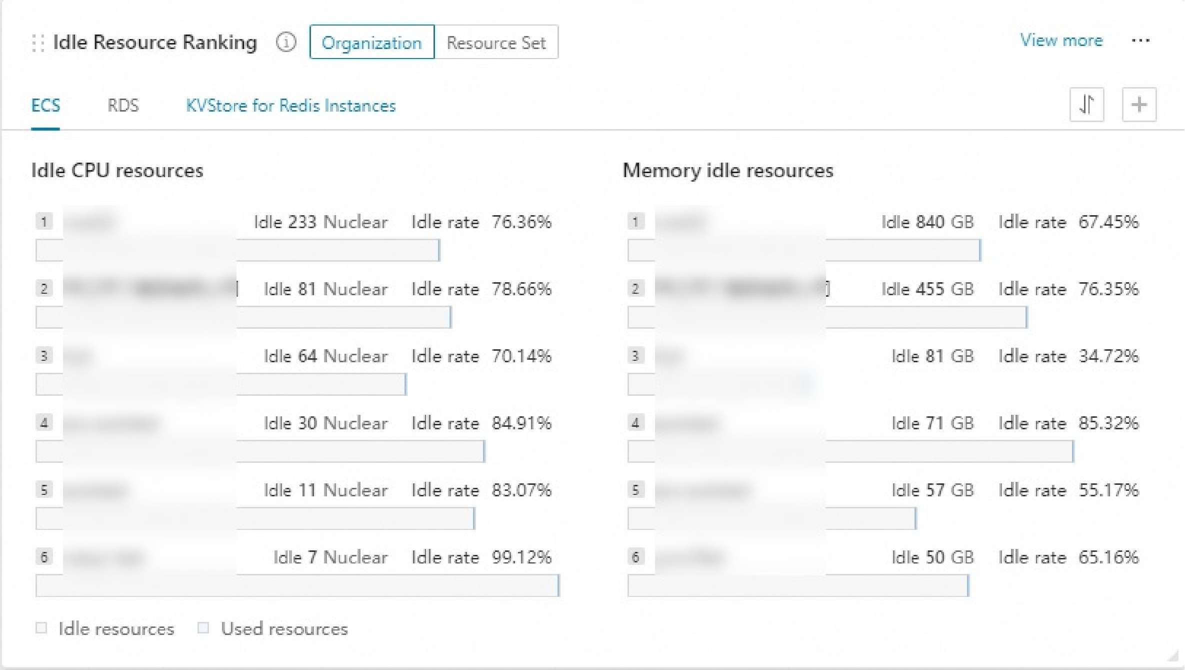
- **Resource Health Analytics**: displays the health status of the resources and resource sets of the current account. You can click **From high to low** or **From low to high** to sort the health status based on health cores.

> **Note**
>
> - You can click the ⇅ icon to change the display order of resources based on your business requirements.
> - You can click the + icon to add the resources that you want to display.



- **Idle Resource Ranking**: displays idle resources by organization or resource set and provides idle resource analysis and detailed data. You can click **View More** to go to the Idle Resource Analysis page under the Operations menu to view details.

> **Note**
>
> - You can click the ⇅ icon to change the display order of resources based on your business requirements.
> - You can click the + icon to add the resources that you want to display.



Idle Resource Ranking ⓘ Organization | Resource Set   View more ···

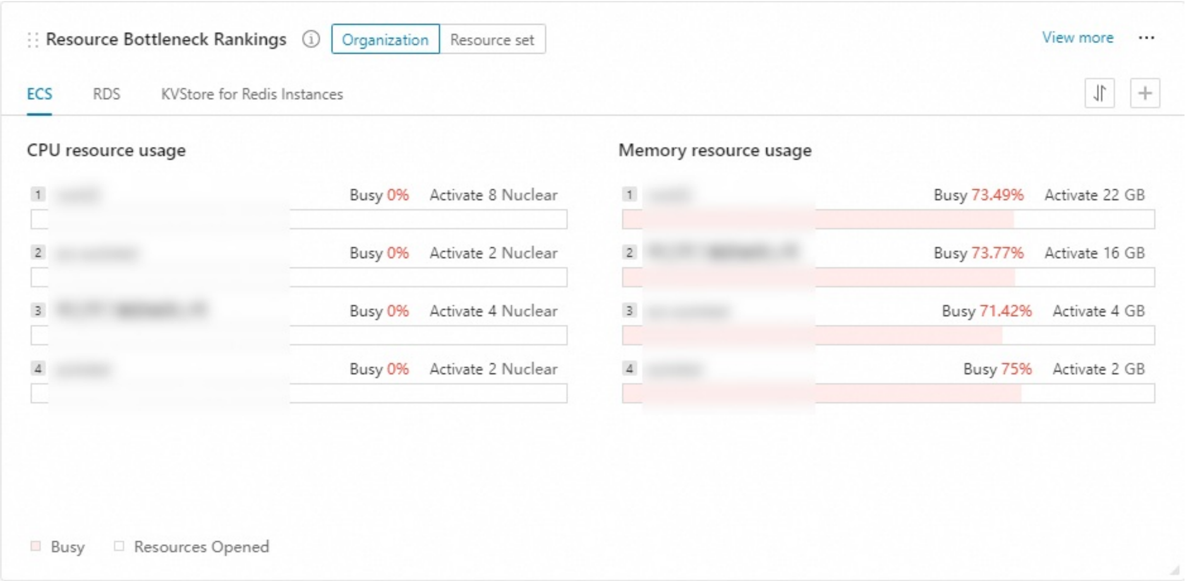
ECS   RDS   KVStore for Redis Instances   ⇅ +

Idle CPU resources			Memory idle resources		
1 [redacted]	Idle 233 Nuclear	Idle rate 76.36%	1 [redacted]	Idle 840 GB	Idle rate 67.45%
2 [redacted]	Idle 81 Nuclear	Idle rate 78.66%	2 [redacted]	Idle 455 GB	Idle rate 76.35%
3 [redacted]	Idle 64 Nuclear	Idle rate 70.14%	3 [redacted]	Idle 81 GB	Idle rate 34.72%
4 [redacted]	Idle 30 Nuclear	Idle rate 84.91%	4 [redacted]	Idle 71 GB	Idle rate 85.32%
5 [redacted]	Idle 11 Nuclear	Idle rate 83.07%	5 [redacted]	Idle 57 GB	Idle rate 55.17%
6 [redacted]	Idle 7 Nuclear	Idle rate 99.12%	6 [redacted]	Idle 50 GB	Idle rate 65.16%

□ Idle resources □ Used resources

- **Resource Bottleneck Rankings**: displays resource bottlenecks by organization or resource set and provides resource bottlenecks analysis and detailed data. You can click **View More** to go to the Bottleneck Analysis page under the Operations menu to view details.

> **Note**
>
> - You can click the ⇅ icon to change the display order of resources based on your business requirements.
> - You can click the + icon to add the resources that you want to display.



Resource Bottleneck Rankings ⓘ Organization | Resource set View more ···

ECS RDS KVStore for Redis Instances

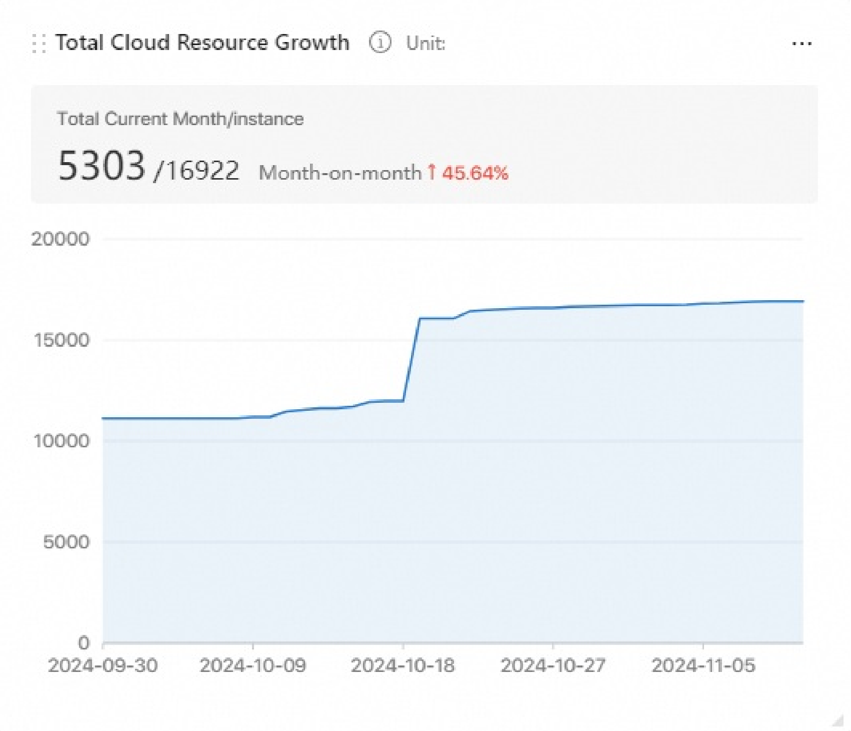
CPU resource usage				Memory resource usage			
1	[redacted]	Busy 0%	Activate 8 Nuclear	1	[redacted]	Busy 73.49%	Activate 22 GB
2	[redacted]	Busy 0%	Activate 2 Nuclear	2	[redacted]	Busy 73.77%	Activate 16 GB
3	[redacted]	Busy 0%	Activate 4 Nuclear	3	[redacted]	Busy 71.42%	Activate 4 GB
4	[redacted]	Busy 0%	Activate 2 Nuclear	4	[redacted]	Busy 75%	Activate 2 GB

🟥 Busy □ Resources Opened

Resource statistics and analysis

The resource statistics and analysis category includes the following cards: **Total Cloud Resource Growth**, **Instance Distribution**, **Total Instance Distribution**, **Organization Resources**, **Resources**, **Regions**, **Server Distribution**, **Quota Overview**, and **Resource Set Resource Statistics**.

- **Total Cloud Resource Growth**: displays the total amount of cloud resources and the monthly growth rate of cloud resources. The cloud resources include only instances that belong to the organizations of users.

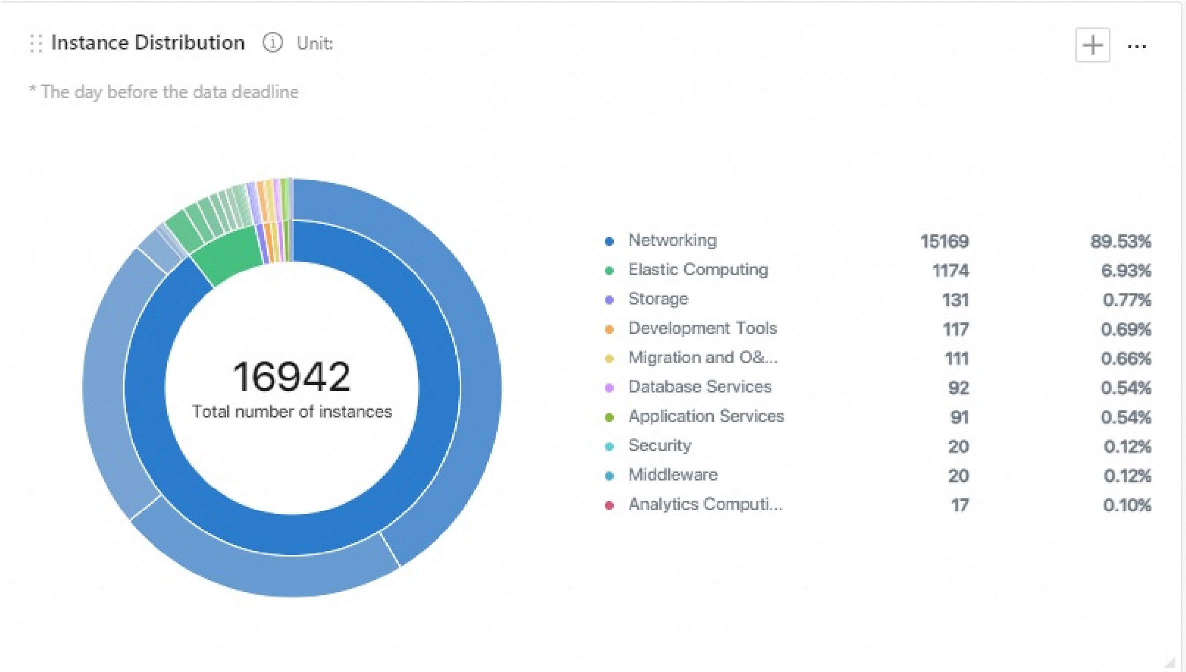


Total Cloud Resource Growth ⓘ Unit: ···

Total Current Month/instance

5303 /16922 Month-on-month ↑ 45.64%

- **Instance Distribution**: displays the distribution of the total number of cloud service instances. You can view the cloud service types and the corresponding number of instances.

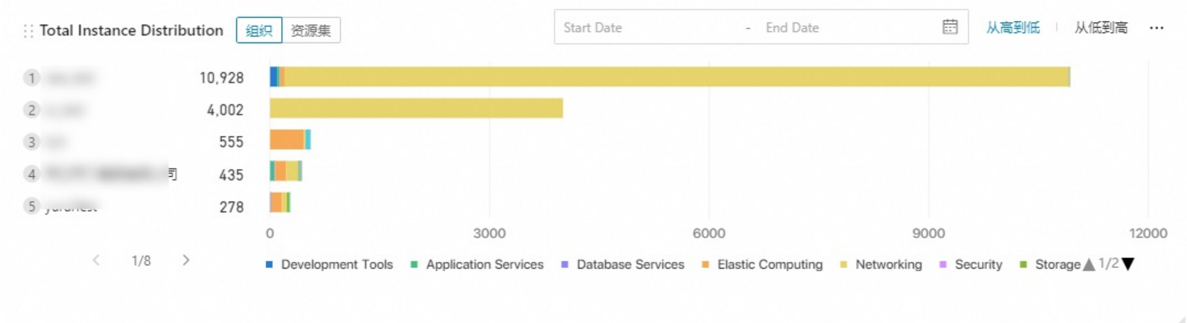


Instance Distribution ⓘ Unit:

* The day before the data deadline

● Networking	15169	89.53%
● Elastic Computing	1174	6.93%
● Storage	131	0.77%
● Development Tools	117	0.69%
● Migration and O&...	111	0.66%
● Database Services	92	0.54%
● Application Services	91	0.54%
● Security	20	0.12%
● Middleware	20	0.12%
● Analytics Computi...	17	0.10%

- **Total Instance Distribution**: displays the distribution of the total number of instances that are created on the current platform.

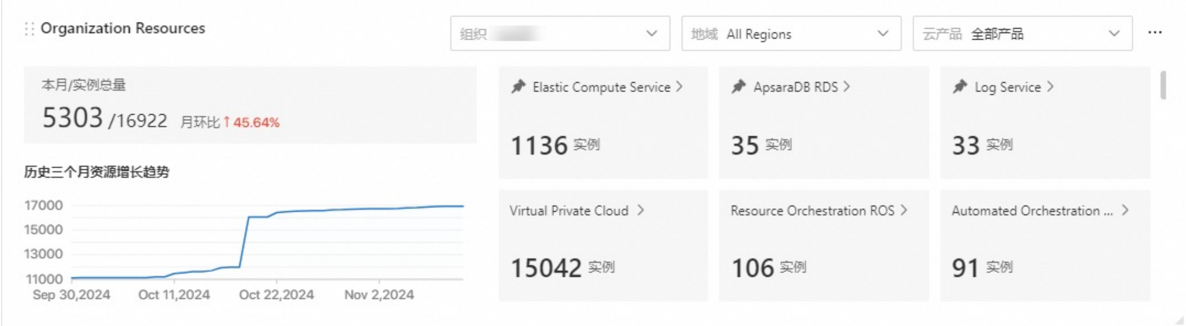


Total Instance Distribution 组织 资源集

Start Date - End Date 从高到低 | 从低到高 ···

1	[redacted]	10,928
2	[redacted]	4,002
3	[redacted]	555
4	[redacted]司	435
5	[redacted]	278

- **Organization Resources**: displays the overview statistics about the organization resources. You can view data by organization, region, and cloud service.



Organization Resources

组织 [redacted] 地域 All Regions 云产品 全部产品 ···

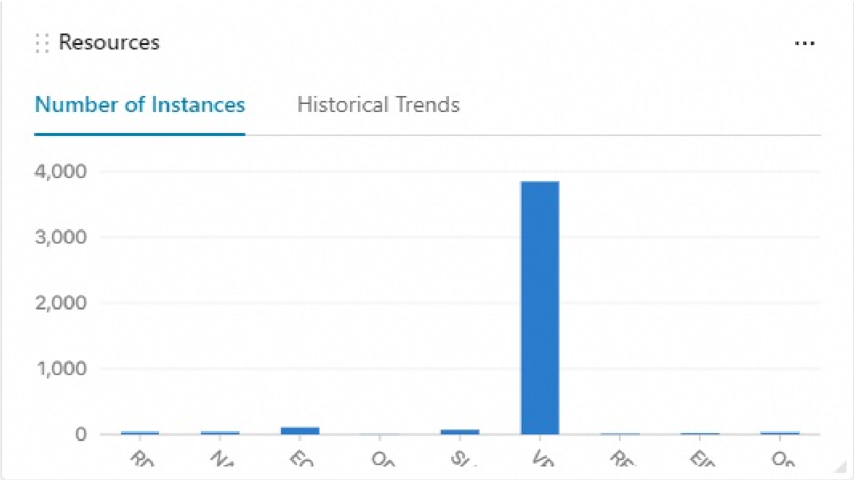
本月/实例总量

5303 /16922 月环比 ↑ 45.64%

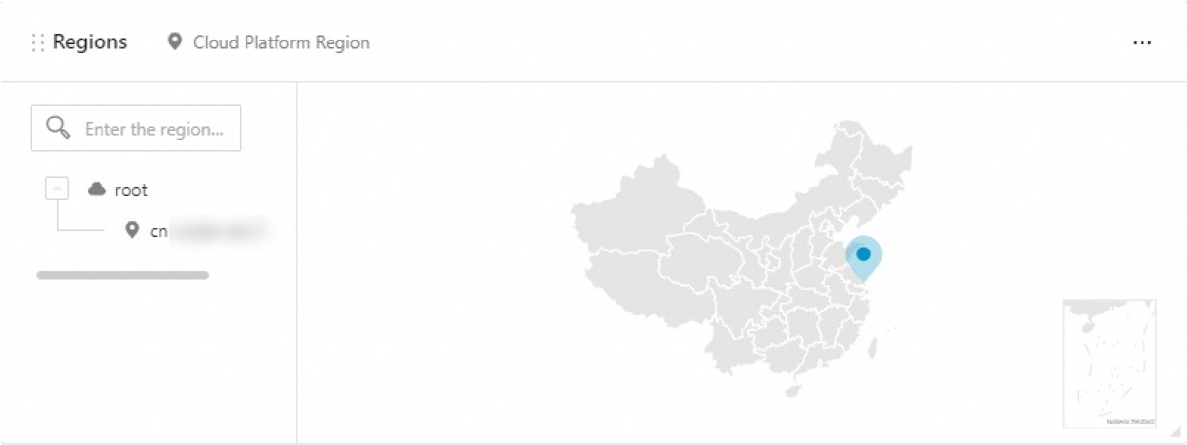
历史三个月资源增长趋势

Elastic Compute Service ›	ApsaraDB RDS ›	Log Service ›
1136 实例	35 实例	33 实例
Virtual Private Cloud ›	Resource Orchestration ROS ›	Automated Orchestration ... ›
15042 实例	106 实例	91 实例

- **Resources**: displays the total number of instances and the historical growth trend of instances.

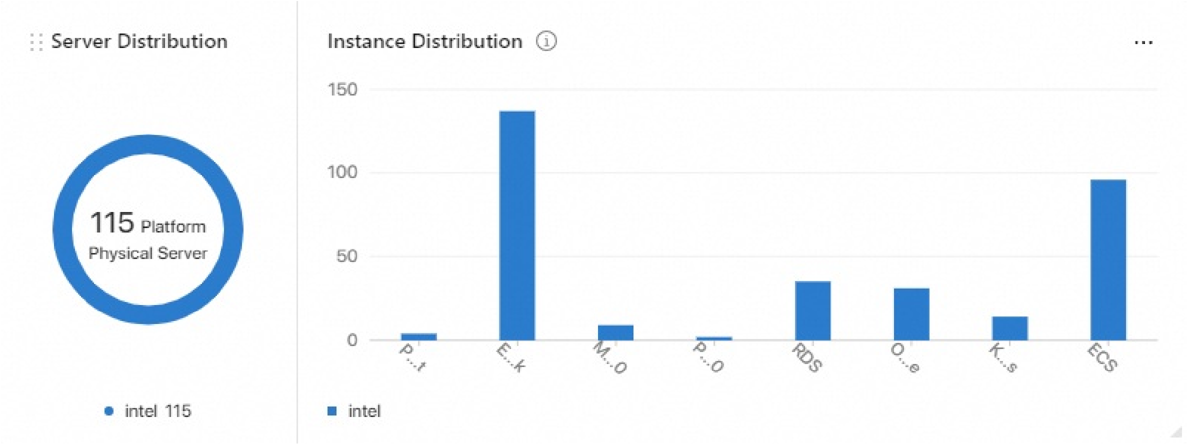


- **Regions**: displays the regions in which the cloud platforms reside in a map

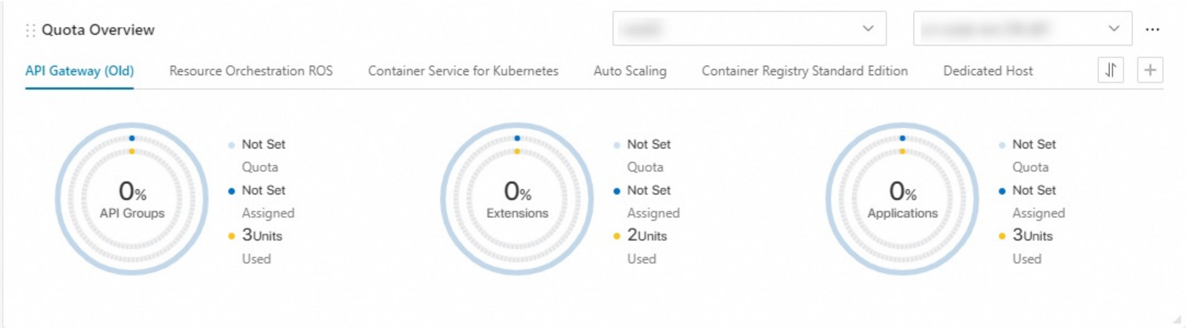


- **Server Distribution**: displays distribution statistics on instances and servers.

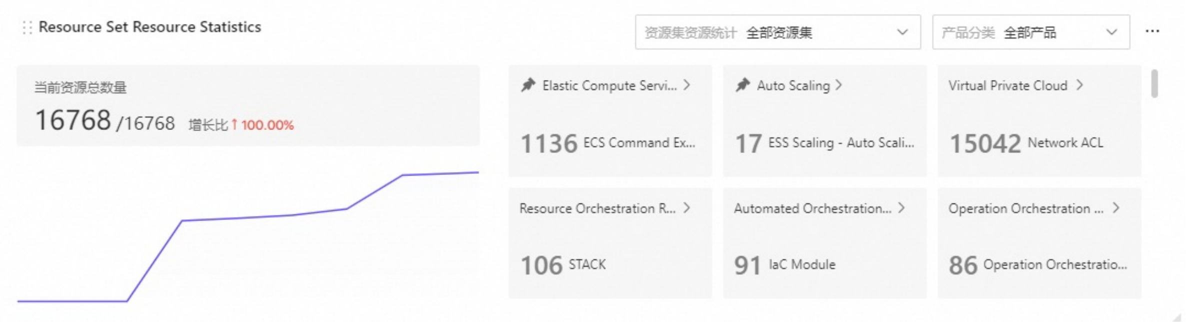
> **Note**
>
> The data source is the total amount of resources managed by the current role. The data update has a latency of more than 10 minutes.



- **Quota Overview**: displays the specification fields of services and the usage of resource quotas. You can view the usage of resource quotas by organization or region.



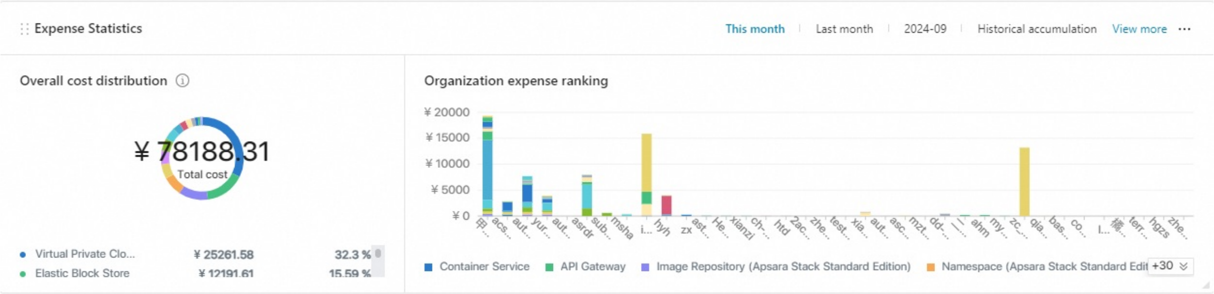
- **Resource Set Resource Statistics**: displays the resource statistics of resource sets. You can view statistical data by resource set or service.


Resource Set Resource Statistics
资源集资源统计 全部资源集
产品分类 全部产品
当前资源总数量
16768 /16768 增长比 ↑ 100.00%
Elastic Compute Servi...
1136 ECS Command Ex...
Auto Scaling
17 ESS Scaling - Auto Scali...
Virtual Private Cloud
15042 Network ACL
Resource Orchestration R...
106 STACK
Automated Orchestration...
91 IaC Module
Operation Orchestration ...
86 Operation Orchestratio...

Resource bills

The resource billing category includes the **Expense Statistics** card.

Expense Statistics: displays the statistics on and analysis of the traffic charges of resources by organization or resource set. You can click **View More** to go to the Overview of Organization Bill page under the Operations menu to view details.


Expense Statistics
This month
Last month
2024-09
Historical accumulation
View more
Overall cost distribution
¥ 78188.31
Total cost
Virtual Private Clo... ¥ 25261.58 32.3 %
Elastic Block Store ¥ 12191.61 15.59 %
Organization expense ranking
¥ 20000
¥ 15000
¥ 10000
¥ 5000
¥ 0
田... acs... aut... yur... aut... asrdr sub... msha i... hyh zx ast... He... xianzi ch-... htd 2ac... zhe... test... xia... aut... asc... mzt... dd-... \... ahm my... zc... qia... bas... co... l... 摇... terr... hgzs zhe...
Container Service
API Gateway
Image Repository (Apsara Stack Standard Edition)
Namespace (Apsara Stack Standard Edit
+30

4.Enterprise

4.1. Overview

Most modern enterprises are in hierarchical structures that are constantly evolving. To allow enterprises to manage cloud resources in a tiered manner, Apsara Stack provides the Enterprise component in the Apsara Uni-manager Management Console.

You can organize your resources on the platform by organizations and projects to implement cost-effective and refined resource management.

The Enterprise component consists of the following modules.

Module	Description
Resources	The resource management features, such as organization management, resource set management, region management, and change management, allow you to build a resource management structure that suits your enterprise. You can easily manage the ownership of resources to improve resource utilization.
Users	The user management and user group management features allow you to manage the structure and permissions of users and user groups in a centralized manner. This can improve management efficiency and meet the various requirements for system and resource access.
Permissions	The permission management features, such as role permissions, data permissions, access control, permission boundaries, and AccessKey logs, allow you to manage permissions based on scenarios, users, and cloud services, thereby improving the system security.

4.2. Resource management

4.2.1. Overview

In the Resources module, you can manage organizations, resource sets, regions, and changes. This way, you can build a resource management system that suits your enterprise. You can easily manage the ownership of resources to improve resource utilization.

Organizations

The Organizations page displays the organizational structure of your enterprise. Each organization can be defined as a company or department. You can build a resource management system that suits your enterprise on the Organizations page.

In the Apsara Uni-manager Management Console, organizations are where resources and resource sets belong. A root organization is created by default. It does not accommodate resources. Organizations that are directly subordinate to the root organization are level-1 organizations, and those that are directly subordinate to level-1 organizations are level-2 organizations, and so on. The lowest-level organizations are level-5 organizations.

After a level-1 organization is created, a cloud account and an AccessKey pair are automatically generated for the organization. The cloud account and the AccessKey pair are used to create resources in the system.

Operations for managing organizations:

- Basic operations: create organizations, modify organizations, delete organizations, change the sorting of organizations, and change the relationship between organizations.
- Manage the AccessKey pairs of organizations: create, disable, enable, and delete the AccessKey pairs of organizations.

Resource sets

Each time an organization is created, the system automatically creates a resource set for the organization.

A resource set is similar to a project and is a group of resources. Resource sets are isolated from each other. Therefore, you can use resource sets to isolate resources to solve complex issues such as user authorization. An organization can have multiple resource sets, but each resource set can belong to only a single organization.

When you create a resource, you need to select a resource set for the resource. Users who are added to the resource set can use the resources in the resource set.

Operations for managing resource sets:

- Create resource sets
- Change the names of resource sets
- Grant permissions to users in resource sets
- Delete resource sets

Regions

The Apsara Uni-manager Management Console allows you to manage multiple regions. You can manage and change the association between an organization and a region. This way, you can control the region in which the resources are created.

Regions can only be associated with level-1 organizations. An organization can be associated with multiple regions, and a region can be associated with multiple organizations.

Changes

The Apsara Uni-manager Management Console allows you to modify organizations, resources, and users in accordance with the changes of your organizations and projects. Changes cannot be made across level-1 organizations.

- Change organizations: You can change the hierarchical relationships of organizations at level 2 and lower. Level-1 organizations do not support changes in hierarchical relationships.
- Change resources: You can change the resource sets to which resources belong.
- Change users: You can change the organizations to which users belong and the roles of users, including the users that belong to level-1 organizations.

4.2.2. Organization management

4.2.2.1. Create an organization

Organizations reflect the architecture of an enterprise. An organization can be defined as a company or department, and is the core of personnel and resource management. Organizations can meet requirements for hierarchical management and resource isolation. You can build a resource management system that meets the requirements of your enterprise by using organizations based on the business environment of your enterprise. This helps you establish hierarchical relationships between resources.

Background information

- In the Apsara Uni-manager Management Console, organizations are where resources and resource sets belong. A root organization is created by default. It does not accommodate any resource.
- The root organization contains level-1 organizations, the level-1 organizations contain level-2 organizations, and so on.
- When you create an organization, the system creates a resource set for the organization by default.
- When a level-1 organization is created, an AccessKey pair is automatically generated for that organization. The AccessKey pair consists of an AccessKey ID and an AccessKey secret, which are used to authenticate and authorize cloud service resources. You can change the AccessKey pair on a regular basis based on your business requirements. This enhances security. The system records AccessKey logs. You can detect abnormal activities and track and identify potential security threats in a timely manner based on the AccessKey logs.

Limits

- You can create up to five levels of organizations.
- You can create a maximum of 500 organizations at a time.

Planning

Before you create an organization, you need to plan an organizational architecture based on the business requirements of your enterprise. Example:

- Plan the organizational architecture by department and responsibility

  An enterprise is usually divided into different departments based on their business requirements and responsibilities, such as the human resources department, the sales department, and the R&D department. Each department has different responsibilities and provides different services.

- Plan the organizational architecture by business unit and geographical distribution

  Large enterprises usually divide their business into different units. Each business unit may be responsible for a specific product line or region.

Create a single organization

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Organizations**.
4. In the left-side Organization Structure section of the **Organizations** page, select the parent organization and click **Create Organization** in the upper-right corner of the page.

   > **Note**
   >
   > - If you select the root organization, a level-1 organization is created.
   > - If you need to create a level-2 organization, you must select a level-1 organization. You can create up to five levels of organizations.
   > - An operations administrator can create level-1 to level-5 organizations. An organization administrator can create only subordinate organizations under the organization to which the organization administrator belongs.

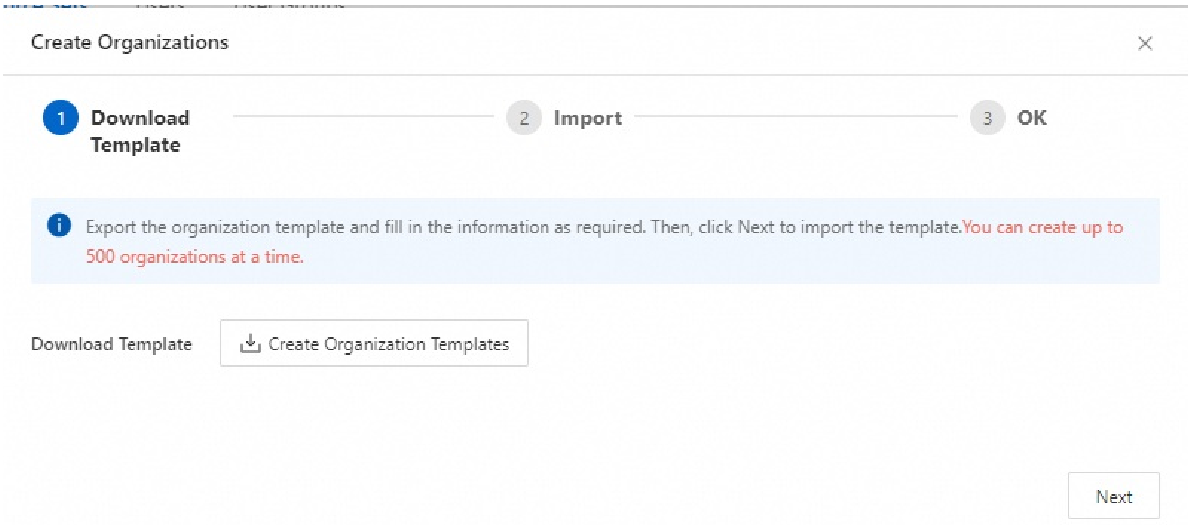
5. In the **Add Organization** dialog box, configure the parameters.

Parameter	Description
Name	The name of the organization. The name must be 2 to 128 characters in length. The name cannot begin or end with a space. **Note** The organization name must be unique in the organizational architecture.
Description	The description of the organization.
Associate Third-party Authentication	If no global identity provider (IdP) is configured on the Apsara Uni-manager Management Console, you can select **Set Now** or **Set Later**. ◦ If you select **Set Now**, you need to select a local IdP name from the**IdP Name** drop-down list. You can associate only one IdP. ◦ If you select **Set Later**, third-party authentication is not associated. **Important** ◦ The **Associate Third-party Authentication** parameter is displayed only when you create a level-1 organization. ◦ If a global IdP has been configured on the Apsara Uni-manager Management Console, the level-1 organization cannot be associated with third-party authentication, and the options **Set Now** and **Set Later** are unavailable.

6. Click **OK**.

Create multiple organizations at a time

1. In the left-side Organization Structure section of the **Organizations** page, click **Batch Create**.
2. In the **Create Organizations** dialog box, click **Create Organization Templates** and download the template file (**.xlsx** file) to your local computer.



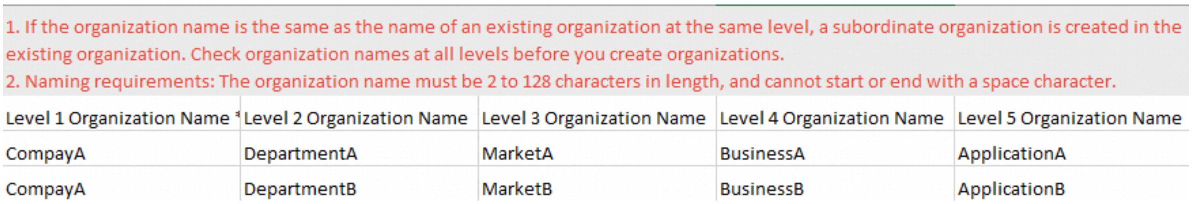
Create Organizations

1 Download Template — 2 Import — 3 OK

Export the organization template and fill in the information as required. Then, click Next to import the template.You can create up to 500 organizations at a time.

Download Template: Create Organization Templates

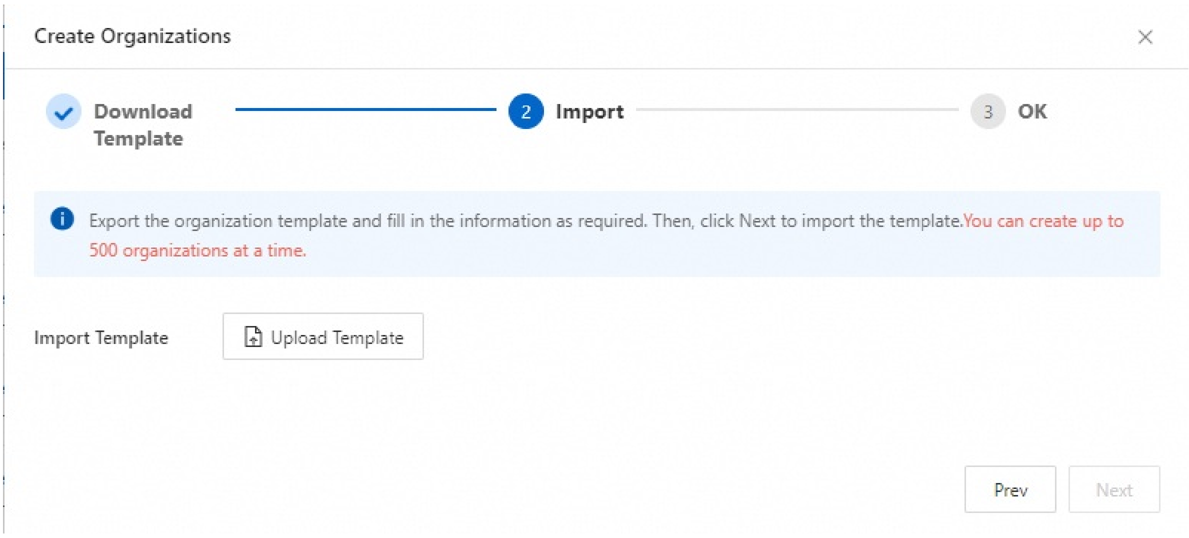
3. Fill the template file with the information of the organizations to be created and save the file. The following figure shows an example of the information.



1. If the organization name is the same as the name of an existing organization at the same level, a subordinate organization is created in the existing organization. Check organization names at all levels before you create organizations.
2. Naming requirements: The organization name must be 2 to 128 characters in length, and cannot start or end with a space character.

Level 1 Organization Name *	Level 2 Organization Name	Level 3 Organization Name	Level 4 Organization Name	Level 5 Organization Name
CompayA	DepartmentA	MarketA	BusinessA	ApplicationA
CompayA	DepartmentB	MarketB	BusinessB	ApplicationB

4. Click **Next** in the **Create Organizations** dialog box.



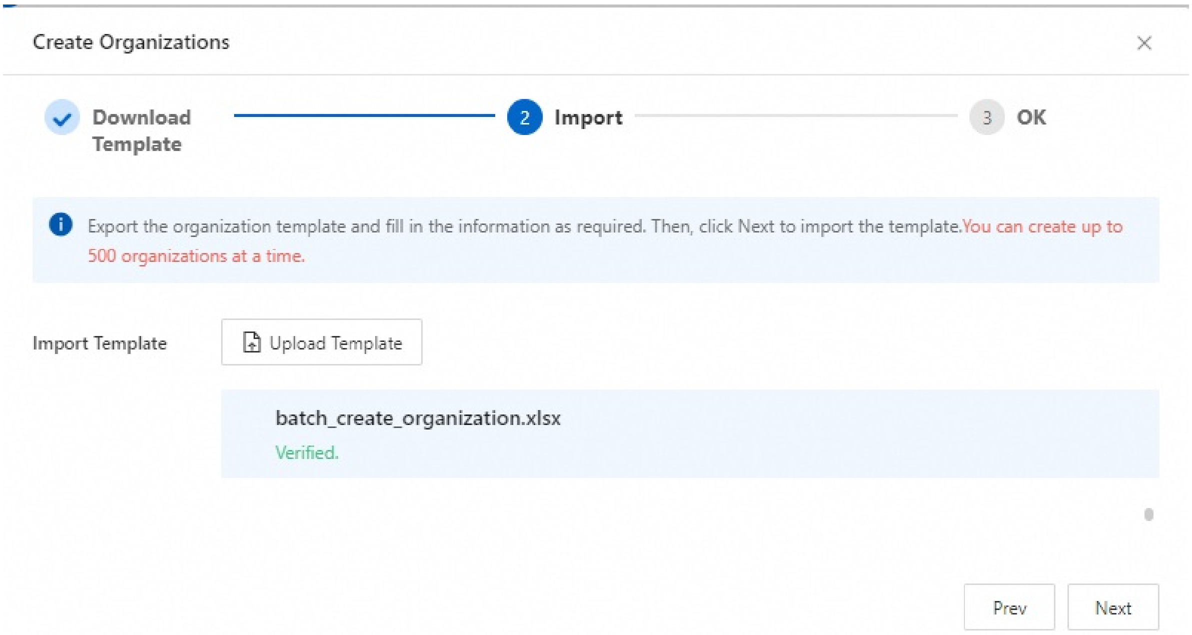
Create Organizations

Export the organization template and fill in the information as required. Then, click Next to import the template.You can create up to 500 organizations at a time.

Import Template: Upload Template

5. Click **Upload Template** and select the template file you edited. After the template file is verified, click **Next**.

> **Important**
> After the template file is uploaded, the system automatically checks whether the content of the template file is correct. If incorrect content exists, you cannot create the organizations. You must modify the template file and click **Re-upload**.



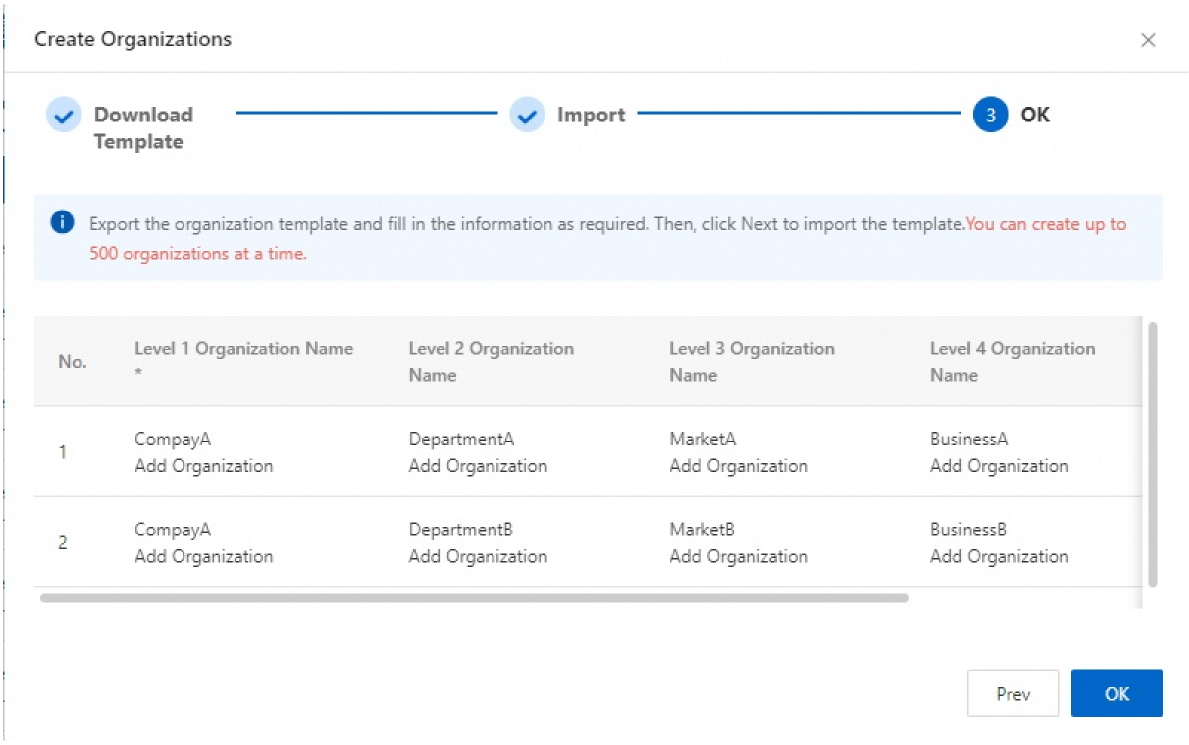
Create Organizations

Export the organization template and fill in the information as required. Then, click Next to import the template.You can create up to 500 organizations at a time.

Import Template: Upload Template

batch_create_organization.xlsx
Verified.

6. Confirm the organization information and click **OK**.

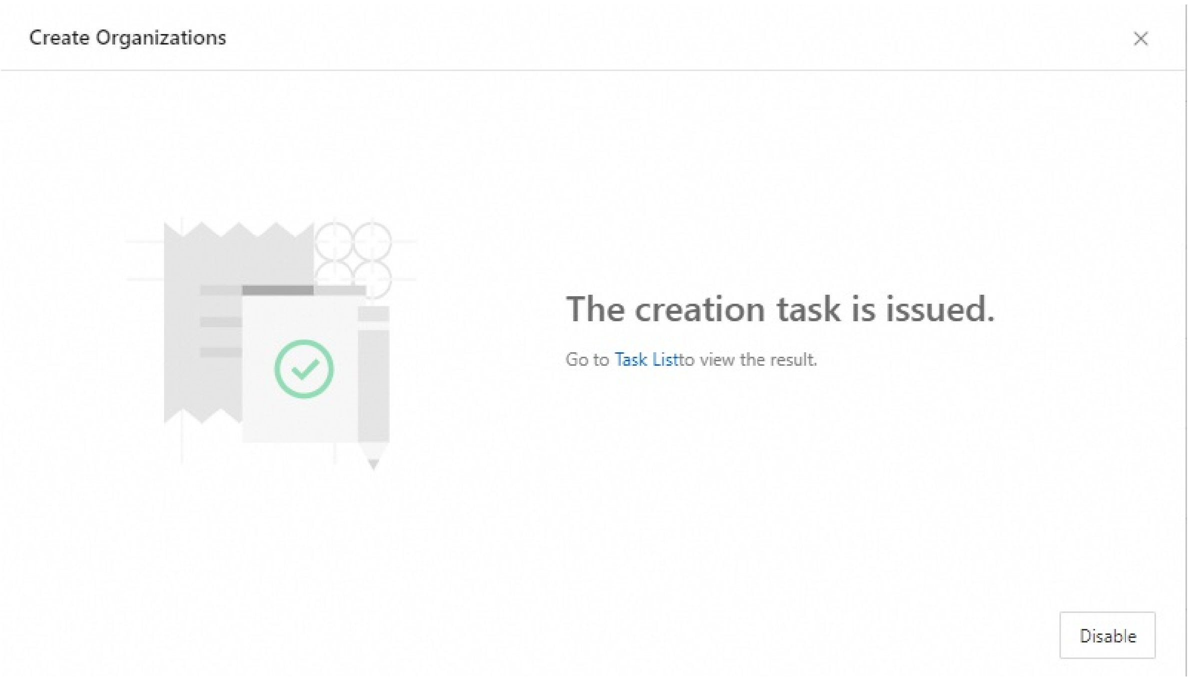


Create Organizations

Export the organization template and fill in the information as required. Then, click Next to import the template.You can create up to 500 organizations at a time.

No.	Level 1 Organization Name *	Level 2 Organization Name	Level 3 Organization Name	Level 4 Organization Name
1	CompayA Add Organization	DepartmentA Add Organization	MarketA Add Organization	BusinessA Add Organization
2	CompayA Add Organization	DepartmentB Add Organization	MarketB Add Organization	BusinessB Add Organization

7. Optional. Click **Task List** in the dialog box to view the organizations you created.



Create Organizations

The creation task is issued.

Go to Task Listto view the result.

4.2.2.2. Manage organizations

You can make corresponding adjustments to your organizations if the configurations of the organizations change.

Limits

Limits on the AccessKey pairs of an organization

You can create up to two AccessKey pairs for each level-1 organization. By default, only operations administrators and level-1 organization administrators have the permissions to obtain the AccessKey pairs of organizations.

- Operations administrators can manage the AccessKey pairs of all level-1 organizations.
- Level-1 organization administrators can manage only the AccessKey pairs of the corresponding level-1 organizations.

Limits on organization sorting

To perform organization sorting, you can drag and drop organization components within organization components only at the same level.

Limits on organization deletion

You cannot delete the root organization.

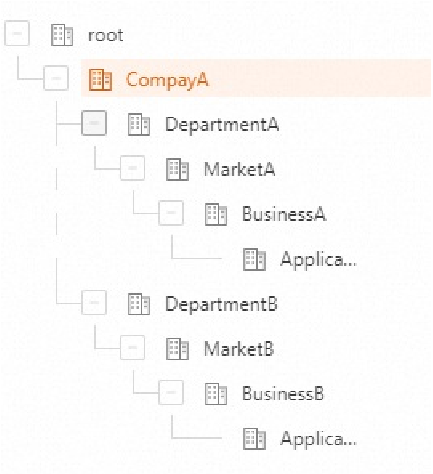
Limits on third-party authentication

- The third-party authentication information is displayed only in the basic information about level-1 organizations.
- Only level-1 organizations can be bound to identity providers (IdPs). Each level-1 organization can be bound to only one IdP including a global IdP.
    - After you bind a level-1 organization to an IdP, the identities of users of the level-1 organization and subordinate organizations are authenticated when the users log on to the system.
    - If a global IdP is configured for the platform, the global IdP is displayed and cannot be changed.
    - If a level-1 organization is bound to a local IdP, other level-1 organizations can still be bound to the same local IdP or other local IdPs.
    - When an organization is bound to a local IdP, the button for authorization logon is unavailable on the logon page of the system. This way, users can be redirected to the system only after they log on to the local IdP.
- Before you bind a level-1 organization to or unbind a level-1 organization from a local IdP or change the local IdP bound to the level-1 organization, make sure that you configure the local IdP. For more information, see Third-party authentication.

View the information about an organization

You can view the hierarchical architecture, basic information, resource sets, users, and user groups of an organization.

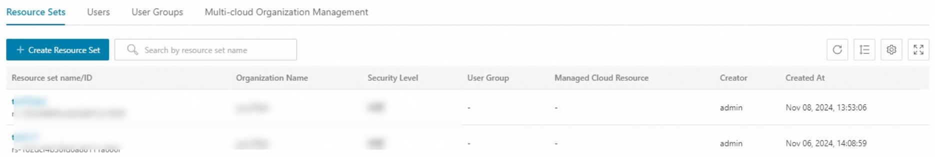
1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Organizations**.
4. Optional. In the left-side **Organization Structure** section of the **Organizations** page, enter a keyword in the search box to search for the organization that you want to manage.
5. View the organization hierarchy and organization names in the left-side organizational structure.

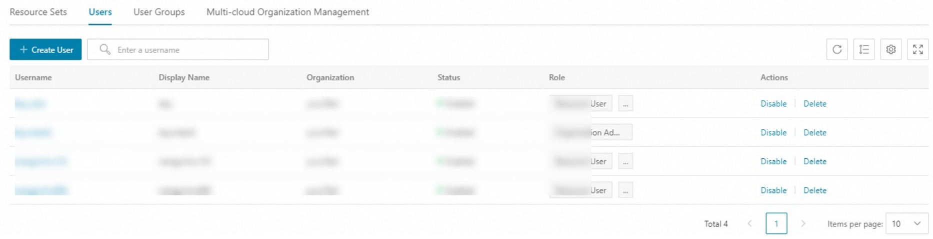


> **Note**
>
> If you bind a multi-cloud organization to a level-1 organization, the Multi-cloud tag is displayed next to the name of the level-1 organization.

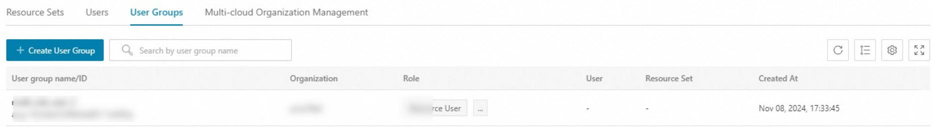
6. Click the name of an organization and view the information about the organization on the right side of the Organizations page.

<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td><b>Basic Information</b></td><td>The following parameters are displayed in the Basic Information section: <b>Organization Name</b>, <b>Organization ID</b>, <b>Organization Level</b>, <b>Description</b>, <b>Third-party Authentication</b>, <b>Created By</b>, and <b>Created At</b>.

<b>Note</b>
The <b>Third-party Authentication</b> parameter is displayed only for a level-1 organization. If an IdP is bound to the organization, the IdP name is displayed.</td></tr>
<tr><td><b>Resource Sets</b></td><td>The information about the resource sets of the organization is displayed on this tab in the following columns: <b>Resource Set Name/ID</b>, <b>Organization Name</b>, <b>Security Level</b>, <b>User Group</b>, <b>Managed Cloud Resource</b>, <b>Creator</b>, and <b>Created At</b>.

Resource Sets   Users   User Groups   Multi-cloud Organization Management
+ Create Resource Set   Search by resource set name
<table>
<tr><th>Resource set name/ID</th><th>Organization Name</th><th>Security Level</th><th>User Group</th><th>Managed Cloud Resource</th><th>Creator</th><th>Created At</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>-</td><td>-</td><td>admin</td><td>Nov 08, 2024, 13:53:06</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>-</td><td>-</td><td>admin</td><td>Nov 06, 2024, 14:08:59</td></tr>
</table>
<b>Note</b>
◦ You can click the name of a resource set to go to the details page of the resource set.
◦ You can click <b>Create Resource Set</b> above the resource set list to create a resource set.</td></tr>
</table>

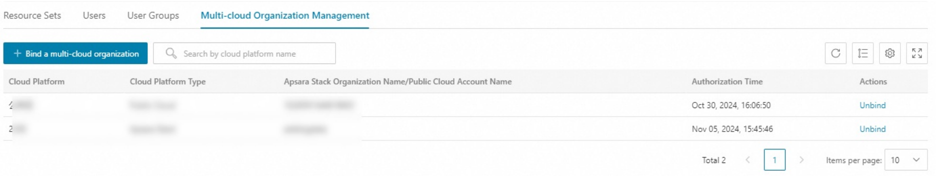
<table>
<tr>
<td><b>Users</b></td>
<td>
The information about the users of the organization is displayed on this tab in the following columns: <b>Username</b>, <b>Display Name</b>, <b>Organization</b>, <b>Status</b>, and <b>Role</b>.


Resource Sets | Users | User Groups | Multi-cloud Organization Management
+ Create User | Enter a username
<table>
<tr><th>Username</th><th>Display Name</th><th>Organization</th><th>Status</th><th>Role</th><th>Actions</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]User ...</td><td>Disable | Delete</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]ion Ad...</td><td>Disable | Delete</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]User ...</td><td>Disable | Delete</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]User ...</td><td>Disable | Delete</td></tr>
</table>
Total 4 &lt; 1 &gt; Items per page: 10

<b>Note</b>
○ You can click the name of a user to go to the details page of the user.
○ You can click <b>Create User</b> above the user list to create a user.
○ You can click <b>Disable</b> or <b>Enable</b> in the <b>Actions</b> column to disable or enable a user.
○ You can click <b>Delete</b> in the <b>Actions</b> column to delete a user.
</td>
</tr>
<tr>
<td><b>User Groups</b></td>
<td>
The information about the user groups of the organization is displayed on this tab in the following columns: <b>User Group Name/ID</b>, <b>Organization</b>, <b>Role</b>, <b>User</b>, <b>Resource Set</b>, and <b>Created At</b>.


Resource Sets | Users | User Groups | Multi-cloud Organization Management
+ Create User Group | Search by user group name
<table>
<tr><th>User group name/ID</th><th>Organization</th><th>Role</th><th>User</th><th>Resource Set</th><th>Created At</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]rce User ...</td><td>-</td><td>-</td><td>Nov 08, 2024, 17:33:45</td></tr>
</table>

<b>Note</b>
○ You can click <b>Create User Group</b> above the user group list to create a user group.
○ The number in the <b>User</b> column of a user group indicates the number of users who belong to the user group. When you move the pointer over the number, you can view the users who belong to the user group. If no users belong to the user group, a hyphen (-) is displayed in the User Group column.
</td>
</tr>
</table>

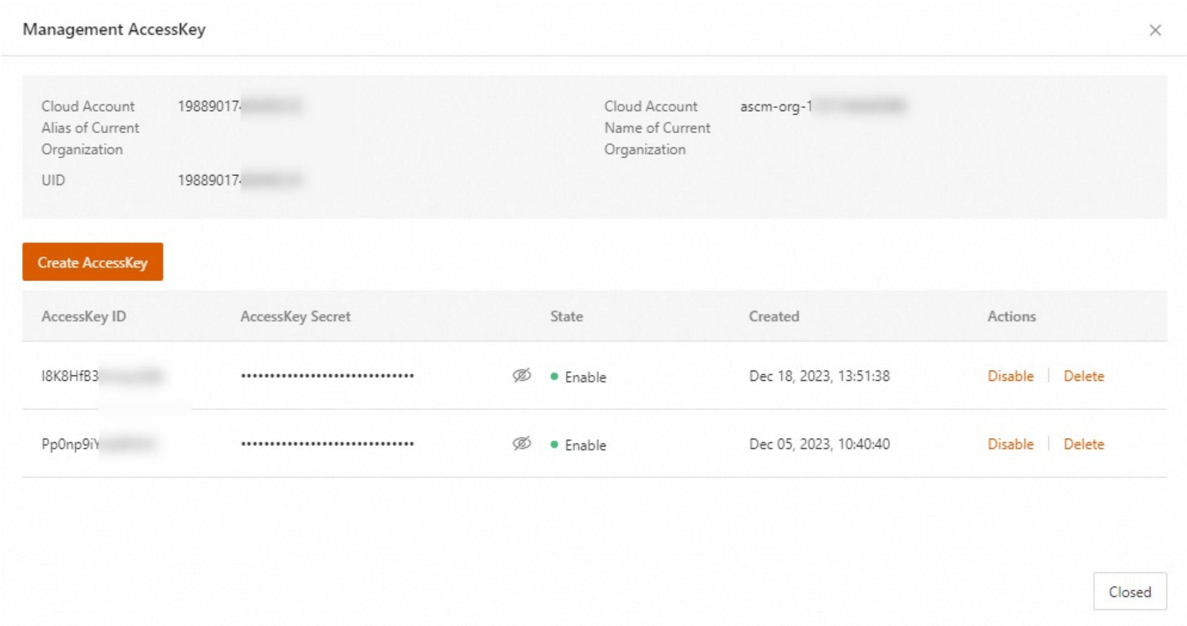
<table>
<tr><td><b>Multi-cloud Organization Management</b></td><td>
Only level-1 organizations are displayed. The information about the multi-cloud organizations that are bound to the level-1 organization is displayed in the following columns: <b>Cloud Platform</b>, <b>Cloud Platform Type</b>, <b>Apsara Stack Organization Name/Public Cloud Account Name</b>, and <b>Authorization Time</b>.

Resource Sets
Users
User Groups
Multi-cloud Organization Management
+ Bind a multi-cloud organization
Search by cloud platform name
<table>
<tr><th>Cloud Platform</th><th>Cloud Platform Type</th><th>Apsara Stack Organization Name/Public Cloud Account Name</th><th>Authorization Time</th><th>Actions</th></tr>
<tr><td>2[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>Oct 30, 2024, 16:06:50</td><td>Unbind</td></tr>
<tr><td>2[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>Nov 05, 2024, 15:45:46</td><td>Unbind</td></tr>
</table>
Total 2
1
Items per page: 10

<b>Important</b>
Only the operations administrator of the primary cloud can perform binding and unbinding operations on the Multi-cloud Organization Management tab. Other administrators can only view information on the Multi-cloud Organization Management tab.
○ To bind a multi-cloud organization to the required level-1 organization, you can click <b>Bind Multi-cloud Organization</b> on the Multi-cloud Organization Management tab. Before you perform binding operations, make sure that the cloud platform in which the multi-cloud organization resides is connected to the Apsara Uni-manager Management Console.
You can bind a level-1 organization to only one Alibaba Cloud account. An Alibaba Cloud account can be bound to only one level-1 organization.
○ To unbind a multi-cloud organization from a level-1 organization, you can click <b>Unbind</b> in the <b>Actions</b> column. After you unbind the organization, all resource sets of the organization are unbound and all temporary users in the organization are removed.
</td></tr>
</table>

Manage the AccessKey pairs of an organization

You can view, add, disable, enable, and delete the AccessKey pairs of an organization.

1. On the left side of the **Organizations** page, find the level-1 organization that you want to manage in the organizational structure and click its name.
2. Click **Management AccessKey** in the **Basic Information** section.
3. In the upper part of the **Management AccessKey** dialog box, view the following parameters: **Cloud Account Alias of Current Organization**, **Cloud Account Name of Current Organization**, and **UID**.



Management AccessKey

Cloud Account Alias of Current Organization	19889017[redacted]	Cloud Account Name of Current Organization	ascm-org-1[redacted]
UID	19889017[redacted]		

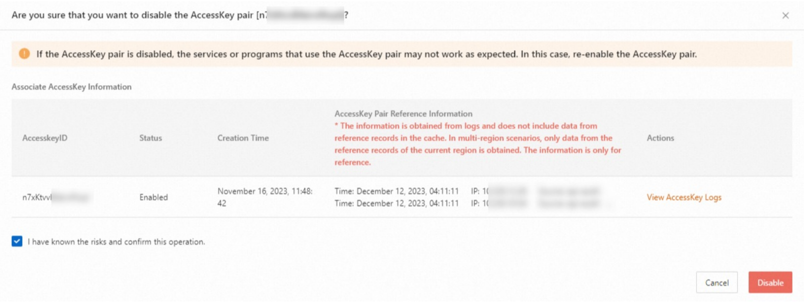
Create AccessKey

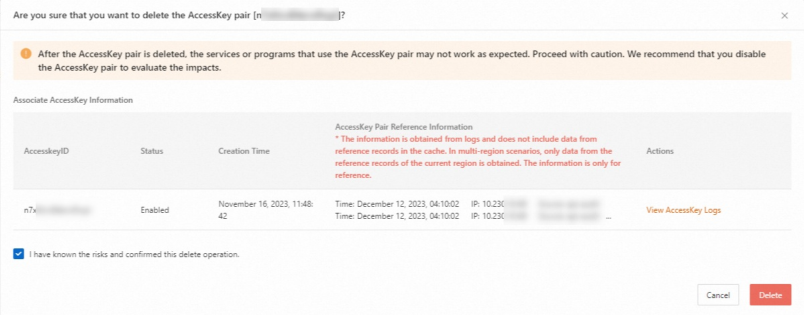
AccessKey ID	AccessKey Secret	State	Created	Actions
I8K8HfB3[redacted]	••••••••••••••••••••••••••••••	● Enable	Dec 18, 2023, 13:51:38	Disable | Delete
Pp0np9iY[redacted]	••••••••••••••••••••••••••••••	● Enable	Dec 05, 2023, 10:40:40	Disable | Delete

Closed

4. In the lower part of the **Management AccessKey** dialog box, manage the AccessKey pairs of the organization.

Operation	Procedure
View an AccessKey pair	View the AccessKey ID and AccessKey secret. ◦ Click the icon to display the hidden AccessKey secret. ◦ Click the icon to hide the AccessKey secret.
Create an AccessKey pair	Click **Create AccessKey**. **Note** You can create up to two AccessKey pairs for each level-1 organization.

Disable an AccessKey pair	i. Find the AccessKey pair that you want to disable and click**Disable** in the Actions column. ii. In the dialog box that appears, view the information about the AccessKey pair and the impacts after you disable the AccessKey pair. After you evaluate the impacts, select **I have known the risks and confirm this operation.** and click **Disable**. After you disable the AccessKey pair, the AccessKey pair changes to the **Disabled** state. **Important** - Find the desired AccessKey pair and click**View AccessKey Logs** in the **Actions** column to go to the **AccessKey Logs** page. View the logs of the AccessKey pair to evaluate the impacts. - After you disable the AccessKey pair, the services or programs that use the AccessKey pair become unavailable. Proceed with caution when you perform this operation.  Are you sure that you want to disable the AccessKey pair [n7[redacted]? If the AccessKey pair is disabled, the services or programs that use the AccessKey pair may not work as expected. In this case, re-enable the AccessKey pair. Associate AccessKey Information AccesskeyID / Status / Creation Time / AccessKey Pair Reference Information * The information is obtained from logs and does not include data from reference records in the cache. In multi-region scenarios, only data from the reference records of the current region is obtained. The information is only for reference. / Actions n7xKtvvl[redacted] / Enabled / November 16, 2023, 11:48:42 / Time: December 12, 2023, 04:11:11 IP: 1[redacted] [redacted] Time: December 12, 2023, 04:11:11 IP: 1[redacted] [redacted] / View AccessKey Logs ☑ I have known the risks and confirm this operation.
Enable an AccessKey pair	Find the AccessKey pair that you want to enable and click**Enable** in the Actions column. After you enable the AccessKey pair, the AccessKey pair changes to the **Enabled** state.

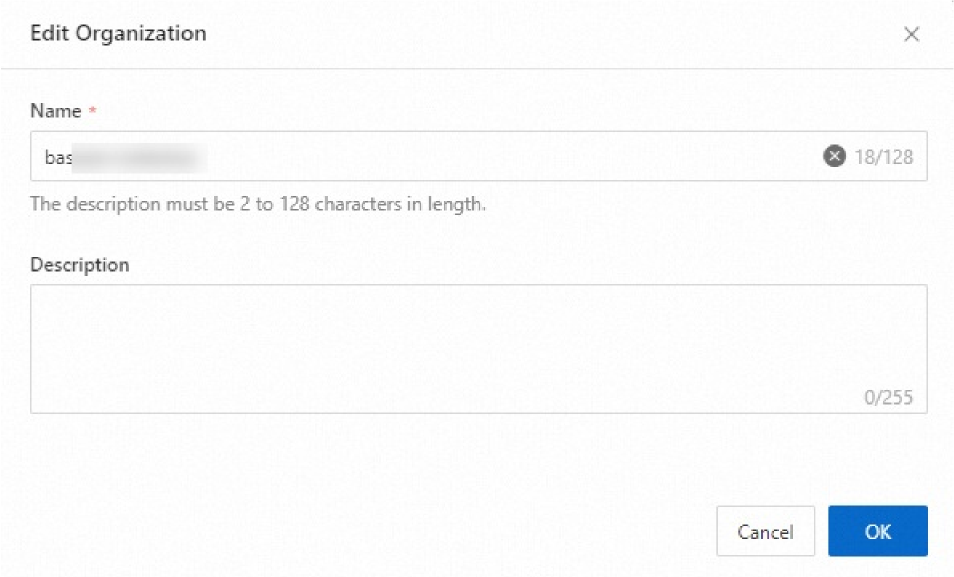
<table>
<tr>
<td>Delete an AccessKey pair</td>
<td>
i. On the Management AccessKey dialog box, find the AccessKey pair that you want to delete and click <b>Delete</b> in the Actions column.
ii. View the information about the AccessKey pair and the impacts after deletion. After you evaluate the impacts, select <b>I have known the risks and confirmed this delete operation</b> and click <b>Delete</b>.
<b>Important</b>
▪ Click <b>View AccessKey Logs</b> in the <b>Actions</b> column to go to the <b>AccessKey Logs</b> page. View the logs of the AccessKey pair to evaluate the impacts.
▪ After you delete the AccessKey pair, the applications that depend on the AccessKey pair may become unavailable. Proceed with caution when you perform this operation.

Are you sure that you want to delete the AccessKey pair [n[redacted]]?
After the AccessKey pair is deleted, the services or programs that use the AccessKey pair may not work as expected. Proceed with caution. We recommend that you disable the AccessKey pair to evaluate the impacts.
Associate AccessKey Information
<table>
<tr><th>AccesskeyID</th><th>Status</th><th>Creation Time</th><th>AccessKey Pair Reference Information
* The information is obtained from logs and does not include data from reference records in the cache. In multi-region scenarios, only data from the reference records of the current region is obtained. The information is only for reference.</th><th>Actions</th></tr>
<tr><td>n7x[redacted]</td><td>Enabled</td><td>November 16, 2023, 11:48:42</td><td>Time: December 12, 2023, 04:10:02 IP: 10.230[redacted]
Time: December 12, 2023, 04:10:02 IP: 10.230[redacted] ...</td><td>View AccessKey Logs</td></tr>
</table>
☑ I have known the risks and confirmed this delete operation.

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

Modify the name and description of an organization

You can modify only the name and description of an organization.

1. On the left side of the **Organizations** page, find the level-1 organization that you want to manage in the organizational structure and click its name.
2. In the **Basic Information** section, click **Edit**.
3. In the **Edit Organization** dialog box, modify the **Name** and **Description** parameters and click **OK**.



Edit Organization

Name *: bas[redacted] 18/128

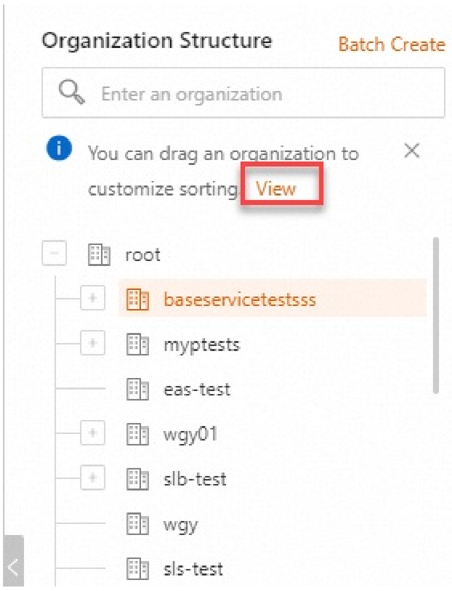
The description must be 2 to 128 characters in length.

Description: 0/255

Sort organizations

1. On the left side of the **Organizations** page, you can drag and drop an organization component in the organizational structure to perform custom sorting.

   You can click **View** above the organizational structure to learn how to drag and drop a component.

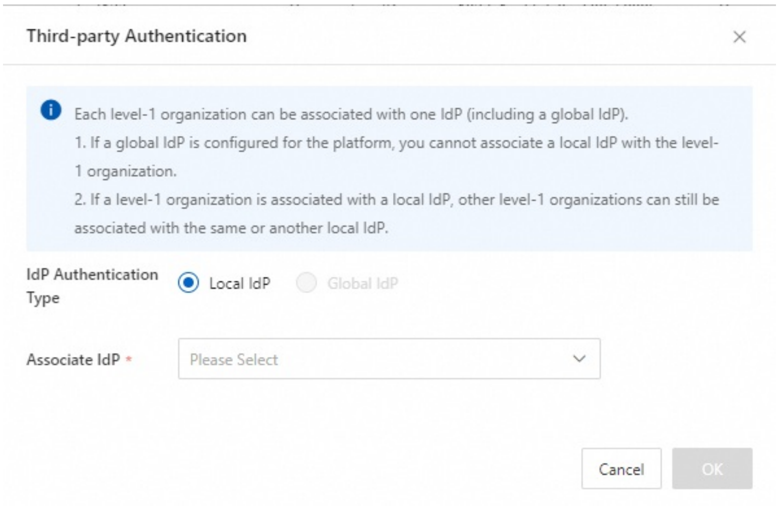
   

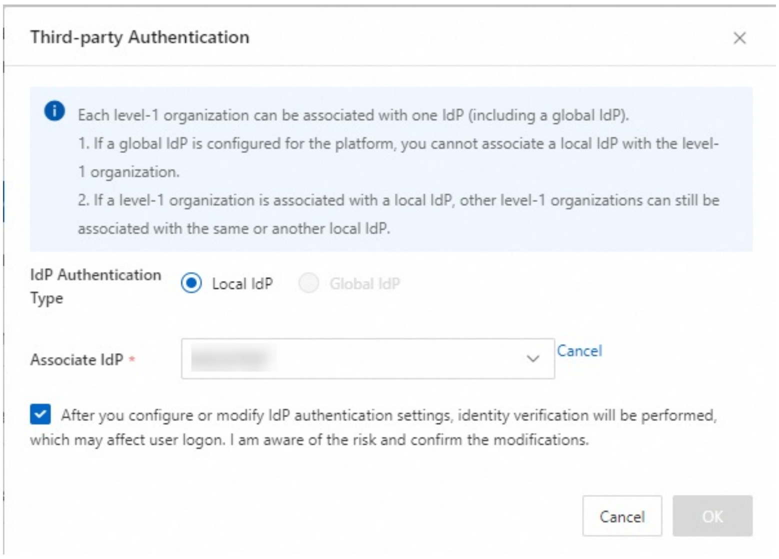
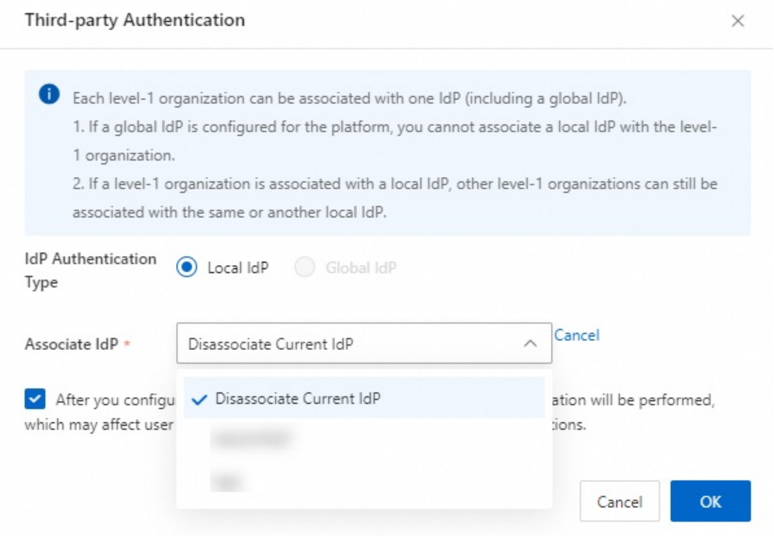
   You can drag an organization to customize sorting. View

Manage third-party authentication for an organization

1. On the left side of the **Organizations** page, find the level-1 organization that you want to manage in the organizational structure and click its name.
2. In the **Basic Information** section, click the ··· icon, and then click **Third-party Authentication**.
3. In the **Third-Party Authentication** dialog box, manage the local IdP bound to the organization.

Operation	Procedure

Bind the organization to a local IdP	If the level-1 organization is not bound to a local IdP and no global IdP is configured for the platform, you can bind the level-1 organization to a local IdP. i. Select an IdP from the **Associate IdP** drop-down list.  Third-party Authentication Each level-1 organization can be associated with one IdP (including a global IdP). 1. If a global IdP is configured for the platform, you cannot associate a local IdP with the level-1 organization. 2. If a level-1 organization is associated with a local IdP, other level-1 organizations can still be associated with the same or another local IdP. IdP Authentication Type ● Local IdP ○ Global IdP Associate IdP * Please Select Cancel OK ii. Click **OK**.

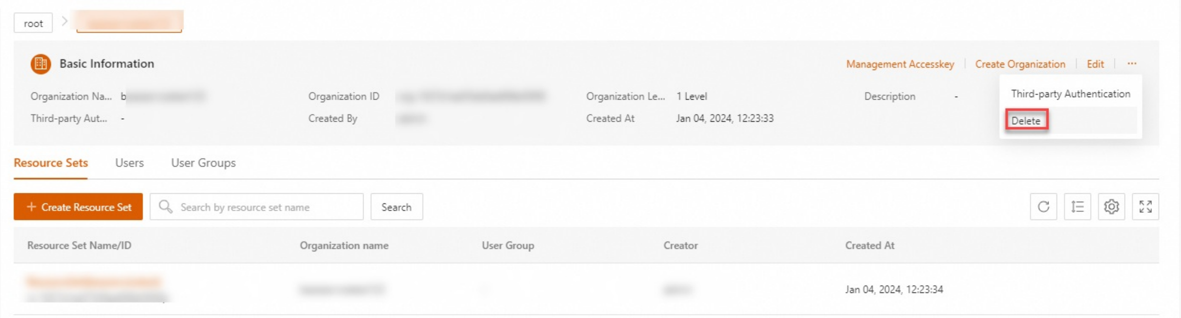
Change the local IdP bound to the organization	i. Click **Modify** next to **Associate IdP**. ii. Select another IdP from the **Associate IdP** drop-down list. **Note** You can click **Cancel** to cancel the change operation.  Third-party Authentication Each level-1 organization can be associated with one IdP (including a global IdP). 1. If a global IdP is configured for the platform, you cannot associate a local IdP with the level-1 organization. 2. If a level-1 organization is associated with a local IdP, other level-1 organizations can still be associated with the same or another local IdP. IdP Authentication Type: ● Local IdP ○ Global IdP Associate IdP *: [redacted] Cancel ☑ After you configure or modify IdP authentication settings, identity verification will be performed, which may affect user logon. I am aware of the risk and confirm the modifications. iii. Click **OK**.
Unbind the organization from the bound local IdP	i. Click **Modify** next to **Associate IdP**. ii. Select **Dissociate Current IdP** from the **Associate IdP** drop-down list.  Third-party Authentication Each level-1 organization can be associated with one IdP (including a global IdP). 1. If a global IdP is configured for the platform, you cannot associate a local IdP with the level-1 organization. 2. If a level-1 organization is associated with a local IdP, other level-1 organizations can still be associated with the same or another local IdP. IdP Authentication Type: ● Local IdP ○ Global IdP Associate IdP *: Disassociate Current IdP Cancel ✓ Disassociate Current IdP [redacted] [redacted] ☑ After you configu ation will be performed, which may affect user ions. iii. Click **OK**.

Delete an organization

1. On the left side of the **Organizations** page, find the organization that you want to delete in the organizational structure and click its name.

2. In the **Basic Information** section, click the ··· icon, and then click **Delete**.

   > **Important**
   >
   > - After the organization is deleted, the data of the organization cannot be recovered. Proceed with caution.
   > - Before you delete the organization, make sure that the organization does not have users, resource sets, and subordinate organizations.



Organization Na... b[redacted]

Organization ID [redacted]

Organization Le... 1 Level

Description -

Third-party Aut... -

Created By [redacted]

Created At Jan 04, 2024, 12:23:33

Resource Set Name/ID	Organization name	User Group	Creator	Created At
[redacted]	[redacted]	[redacted]	[redacted]	Jan 04, 2024, 12:23:34

3. In the message that appears, click **OK**.

4.2.3. Resource set management

4.2.3.1. Create a resource set

A resource set is a group of resources and is similar to a project. After a user or user group is added to a resource set, the user or users in the user group can manage resources in the resource set. The resource set management feature enables you to resolve complex issues such as user authorization. If an organization has multiple projects, you can create multiple resource sets in the organization. This allows users to use and manage resources by resource set.

Background information

A resource set is a logical container that associates multiple resources. Each resource must belong to a resource set. When you create a resource, you need to select a resource set for the resource.

- When you create an organization, the system creates a resource set for the organization by default.
- Resource sets are isolated from each other.
- An organization can have multiple resource sets, but each resource set can belong to only one organization.

Prerequisites

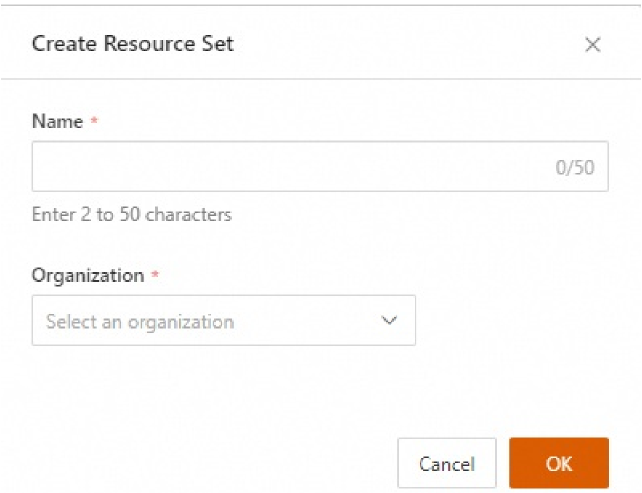
An organization is created.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.

3. In the left-side navigation pane, choose **Resources** > **Resource Sets**.
4. Click **Create Resource Set**.
5. In the **Create Resource Set** dialog box, set the **Name** and **Organization** parameters.

> **Note**
>
> If you enable the secret level access feature in the security policy, you must configure the Security Level parameter for your resource set when you create the resource set. You must make sure that the security level of the resource set is lower than the security level of the current operation role.



Create Resource Set

Name *

0/50

Enter 2 to 50 characters

Organization *

Select an organization

6. Click **OK**.

4.2.3.2. Manage a resource set

After you create a resource set, you can modify the resource set, add users to the resource set, and delete the resource set.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Resource Sets**.
4. Optional. In the upper part of the page, select an organization or specify the name of a resource set in the search box.
5. Find the required resource set and perform the following operations.

Operation	Step

View information about the resource set	Click the name of the resource set. ◦ In the **Basic Information** section of the page that appears, view information such as the name, ID, organization, creation time, and creator of the resource set. **Note** If you enable the secret level access feature in the security policy, you can view the security level of the resource set. ◦ On the **Resources** tab, view the resources in the resource set. ◦ On the **Users** tab, view the users or user groups in the resource set. **Note** ▪ Click **Member authorization**, select a role type, and then select a user or user group to add the user or user group to the resource set. ▪ Click **Remove Authorization** in the Actions column of a user or user group to remove the user or user group from the resource set. ◦ On the **Multi-cloud Resource Set** tab, view information about the required multi-cloud resource set. You can view information such as **Cloud Platform Code**, **Cloud Platform Display Name**, **Resource Set**, and **Cloud Platform Type**. **Important** The Multi-cloud Resource Set tab can be used only by the operations administrator and the level-1 organization administrator of the primary cloud to perform binding and unbinding operations. Other administrators can only view information on this tab. Before you can bind a multi-cloud resource set to a cloud platform, make sure that the cloud platform is connected. ▪ Click **Associate Multi-cloud Resource Set** and select a cloud platform, an organization, and a multi-cloud resource set to bind the multi-cloud resource set to the cloud platform and organization. ▪ Click **Unbind** in the Actions column of a multi-cloud resource set to unbind the multi-cloud resource set from the cloud platform and organization.
Modify the resource set	i. Click **Edit** in the Actions column. ii. In the Modify Resource Set dialog box, modify the name and security level of the resource set. **Note** If a user is being added to the resource set when you modify the security level, you can change the security level only from high to low. If no user is being added to the resource set, you can change the security level based on your business requirements. iii. Click **OK**.

Grant users the permissions on the resource set	i. Click **Member authorization** in the Actions column. ii. In the Member Authorization dialog box, select a role type and select a user or user group. **Important** When you create the resource set, if you configure the Security Level parameter in the Secret Level Access section, you can add only users or user groups whose security levels are higher than or equal to the security level of the resource set to the resource set. ▪ Grant the permissions to a user or a user group: In the lower-left section, select the required user or the user group. ▪ Revoke the permissions of a user or a user group: In the lower-right section, click **Remove** in the Actions column of the required user or user group. iii. Click **OK**.
Delete the resource set	**Important** ◦ You cannot delete the default resource set. ◦ Before you delete a resource set, you must make sure that the resource set does not contain resources and no users or user groups are added to the resource set. Otherwise, the resource set cannot be deleted. i. Find the resource set that you want to delete and click**Delete** in the Actions column. ii. Click **OK**.

4.2.4. Manage regions

You can manage the regions associated with organizations. Regions determine the geographical locations in which resources are created. Large-sized enterprises typically divide their business into different units. Each business unit may correspond to specific product lines or regions. In this case, they need to create different resources in specified regions. Enterprises can associate their organizations with regions to meet their requirements.

Background information

- An organization can be associated with multiple regions, and a region can be associated with multiple organizations.
- After an organization is associated with regions, resources of the organization can be created only in the associated regions.

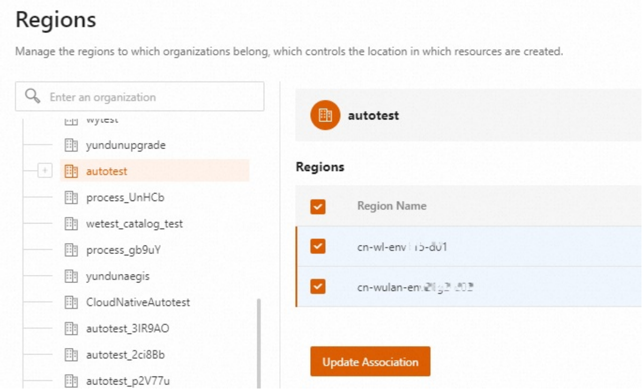
Limits

- After a level-1 organization is associated with a region, its subordinate organizations can also be associated with the region.
- If resources are activated in a region supported by an organization, you cannot disassociate the organization from the region.

Update the association between an organization and a region

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Regions**.
4. In the left-side organizational structure, click the name of the organization that you want to manage.
5. In the right-side Regions section, select or clear the name of the desired region.

   If you select the name of a region, the organization is associated with the region. Then, you can create resources in this region. If you clear the name of a region, the organization is disassociated from the region. Then, you cannot create resources in this region.



Regions

Manage the regions to which organizations belong, which controls the location in which resources are created.

Enter an organization

- wytest
- yundunupgrade
- autotest
- process_UnHCb
- wetest_catalog_test
- process_gb9uY
- yundunaegis
- CloudNativeAutotest
- autotest_3IR9AO
- autotest_2ci8Bb
- autotest_p2V77u

autotest

Regions

☑	Region Name
☑	cn-wl-env[redacted]-d01
☑	cn-wulan-en[redacted]

Update Association

6. Click **Update Association**.

4.2.5. Manage changes

You can modify the organizations, resources, and users in the console according to the changes of your organizations or projects.

Changes cannot be made across level-1 organizations, and names of organizations and users within a level-1 organization must be unique.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources > Changes**.
4. Optional. Search for the required organization in the search box above the organization navigation tree. Fuzzy search is supported.
5. Find the required organization and perform the following operations.

Operation	Step

Change the parent organization of an organization	i. Click the name of the required organization. ii. On the right side of the page, click**Change Organization**. iii. Select a new organization from the **Change Organization To** drop-down list. iv. Click **OK**. **Note** After you change the organization, the resource sets and users of the organization are also moved to the new organization.
Change the ownership of resources	i. Click the + icon to the left of the required organization and click a resource set under the organization. ii. On the right side of the page, configure the**Product Type** and **Resource Type** parameters. iii. Change the ownership of resources ▪ Change the ownership of a single resource: In the instance list, find the required resource and click **Change Ownership** in the Actions column. ▪ Change the ownership of multiple resources: In the instance list, select the target resources and click **Batch Change Ownership** at the bottom of the page. iv. In the dialog box that appears, select a resource set from the**Change Resource Set To** drop-down list. v. Click **OK**. **Note** ◦ Changing the ownership of a resource does not affect the organization and users. ◦ You can click **View Resource Relations** in the Actions column of a resource to view the parent resources of the resource. If the current resource has a parent resource, the ownership of the current resource cannot be changed. If you still want to change the ownership of the current resource, we recommend that you change the parent resource first. The ownership of the current resource automatically changes with the parent resource.

Change the organization to which a user belongs	i. Click the name of the required organization. ii. On the right side of the page, click **Users**. iii. Find the required user and click **Change** in the Actions column. iv. In the dialog box that appears, select an organization from the **Change Organization To** drop-down list and select roles from the **Assigned Roles** drop-down list. v. Click **OK**. **Note** Changing the organization of a resource does not affect the organization and users.

4.3. User management

4.3.1. Overview

The user management and user group management features allow you to centrally manage the structure and permissions of users and user groups. This can improve management efficiency and meet the various needs for system and resource access.

User management

You can perform management operations on users such as managing lifecycle for users, attaching roles to users, and controlling logons.

- On the System Users tab of the Users page, you can create, modify, disable, enable, and delete users. You can also grant permissions, configure logon policies, view user information, add users to user groups, remove users from user groups, configure multi-factor authentication (MFA), view the initial passwords of users, and view the resources sets of users.
- On the Historical Users tab, you can restore deleted users or permanently delete users.

User group management

You can add users to user groups to implement batch permission management. You can:

- Create user groups
- Modify user groups
- Add users to user groups
- Grant permissions to user groups
- Remove users from user groups
- Delete user groups

4.3.2. User management

4.3.2.1. Create a user

Administrators can create users and assign the users different roles to meet different requirements for system access control.

Create a single user

Procedure

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users** > **Users**.
4. Click the **System Users** tab. Click **Create a user**.
5. In the **Create a user** dialog box, configure the parameters.

Parameter	Required	Description
User name	Yes	The name of the user. The name must be 2 to 64 characters in length and can contain letters, digits, hyphens (-), underscores (_), and periods (.). ? **Note** User names must be unique.
Display name	Yes	The display name of the user. The name must be 1 to 128 characters in length and can contain letters, digits, hyphens (-), periods (.), and at signs (@).
Role	Yes	The roles to be assigned to the user. ? **Note** You can enter role names in the field. Fuzzy match is supported.
Organization	Yes	The organization to which the user belongs.
Logon policy	Yes	The logon policy that limits the logon time and IP address of the user. The default policy is automatically associated with new users. ? **Note** The default policy does not limit the logon time and IP address of the user. To impose limits, you can modify the default logon policy or create a new logon policy for the user. For more information, see Create an access policy.

Phone	Yes	The phone number of the user. This phone number is used to notify users of resource application and usage. Make sure that this mobile number is valid. **Note** If the phone number of the user changes, update it on the system in a timely manner.
Landline	No	The landline number of the user. The landline number must be 4 to 20 characters in length and can contain only digits and hyphens (-).
Email	Yes	The email address of the user. Emails about the resource application and usage are sent to this email address. Make sure that this email address is valid. **Note** If the email address changes, update it on the system in a timely manner.
DingTalk Key	No	The key of the chatbot for the DingTalk group to which the user belongs. For more information about how to configure the key, see DingTalk development documentation.
Notify User by Email	No	If this option is selected, the Apsara Uni-manager Management Console notifies the user configured as the alert contact by email whenever an alert is generated. **Note** You must configure an email server to notify the user by email. For more information, contact on-site O&M engineers.
Notify User by DingTalk	No	If this option is selected, the Apsara Uni-manager Management Console notifies the user configured as the alert contact by DingTalk whenever an alert is generated.

Create multiple users at a time

Procedure

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users** > **Users**.
4. Click the **System Users** tab. Click **Batch Create Users**.

> **Note**
>
> - To batch create users, you need to download the template file, fill in the information of the users in the spreadsheet, and then upload the file to the system.
> - A maximum of 100 users can be created at a time.

5. In the **Batch Create Users** dialog box, click **User Creation Template**.
6. In the downloaded template file, fill in the information of the users.

Parameter	Required	Description
Username	Yes	The name of the user. The name must be 2 to 64 characters in length and can contain letters, digits, hyphens (-), underscores (_), and periods (.). **Note** User names must be unique.
Display Name	Yes	The display name of the user. The name must be 1 to 128 characters in length and can contain letters, digits, hyphens (-), periods (.), and at signs (@).
Role	Yes	The role of the user. For a list of roles, click**Permissions** > **Role Permissions** in the left-side navigation pane in the console.
Organization	Yes	The path of the organization to which the user belongs. **Note** Format: root/<Level-1 organization>/<Level-2 organization> If the root organization has been renamed, use the actual name.
Logon Policy	Yes	The name of the logon policy of the user. For a list of logon policies, click **Permissions** > **Access control** in the left-side navigation pane in the console.
Country Code	Yes	The code of the country that the user is in.

Mobile Phone	Yes	The phone number of the user. This phone number is used to notify users of resource application and usage. Make sure that this mobile number is valid. **Note** If the phone number of the user changes, update it on the system in a timely manner.
Landline	No	The landline number of the user. The landline number must be 4 to 20 characters in length and can contain only digits and hyphens (-).
Email	Yes	The email address of the user. Emails about the resource application and usage are sent to this email address. Make sure that this email address is valid. **Note** If the email address changes, update it on the system in a timely manner.
Enable Email Notifications	No	Valid values: **Yes** and **No**. Default value: **No**. If you set the parameter to Yes, the Apsara Uni-manager Management Console notifies the user configured as the alert contact by email whenever an alert is generated. **Note** You must configure an email server to notify the user by email. For more information, contact on-site O&M engineers.
Enable DingTalk Notifications	No	Valid values: **Yes** and **No**. Default value: **No**. If you set the parameter to Yes, the Apsara Uni-manager Management Console notifies the user configured as the alert contact by DingTalk whenever an alert is generated.

DingTalk Key	No	The key of the chatbot for the DingTalk group to which the user belongs. For more information about how to configure the key, see DingTalk development documentation. **Note** This parameter takes effect only when Enable DingTalk Notifications is set to Yes.
Email me the password after the user is created.	No	Valid values: **Yes** and **No**. Default value: **No**. **Note** This parameter takes effect only when Enable Email Notifications is set to Yes.

7. Save the file. Click **Next** in the **Batch Create Users** dialog box. Click **Upload Template**.

> **Note**
>
> When the template file is uploaded, the system checks the validity of the parameter values. If invalid values exist, the users cannot be created. You need to modify the template file and re-upload it.

8. After the file is uploaded, click **OK**.
9. (Optional) On the **Batch Tasks** tab of the **Users** page, view the status and details of the batch user creation task. If **Succeeded** is displayed in the **Status** column of the task, the task has been completed.

4.3.2.2. Manage system users

You can perform management operations on users, including managing the lifecycle in the console, attaching roles to users, and controlling logons.

Background information

An operations administrator can manage the system users of all organizations. An organization administrator can manage only the system users of the corresponding organization and the subordinate organizations.

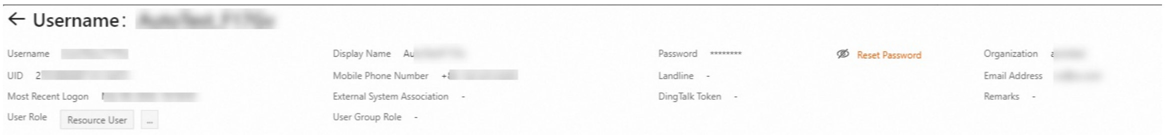
View the information about a user

View the basic information and details of a user.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users > Users**.
4. Click the **System Users** tab.

> **Note**
>
> You can click the ⚙ icon to select the fields that you want to display.

5. Find the system user that you want to manage and click its name or click **View Details** in the **Actions** column to go to the details page of the system user.
    - In the upper part of the details page, you can view the basic information about the system user in the following fields: **Username**, **Display Name**, **Password**, **Organization**, **UID**, **Mobile Phone Number**, **Landline**, **Email Address**, **Most Recent Logon**, **External System Association**, **DingTalk Token**, **Remarks**, **User Role**, and **User Group Role**.



← Username: [redacted]

Username [redacted]	Display Name [redacted]	Password ********	Reset Password	Organization [redacted]
UID [redacted]	Mobile Phone Number [redacted]	Landline -		Email Address [redacted]
Most Recent Logon [redacted]	External System Association -	DingTalk Token -		Remarks -
User Role Resource User ...	User Group Role -			

    - In the lower part of the details page, click the **Resource Set**, **User Group**, and **Role Permissions** tabs to view the resource sets and user groups to which the user belongs and the role permissions granted to the user.
        - **View the resource sets to which a user belongs** : On the **Resource Set** tab, select a role of the user from the Role drop-down list to view the information about the resource sets to which the user belongs.
        - **View the user groups to which a user belongs** : On the **User Group** tab, view the information about the user groups to which the user belongs.

> **Note**
>
> The number in the **User** field of a user group indicates the number of users added to the user group. The users who are added to the user group are displayed when you move the pointer over the number.

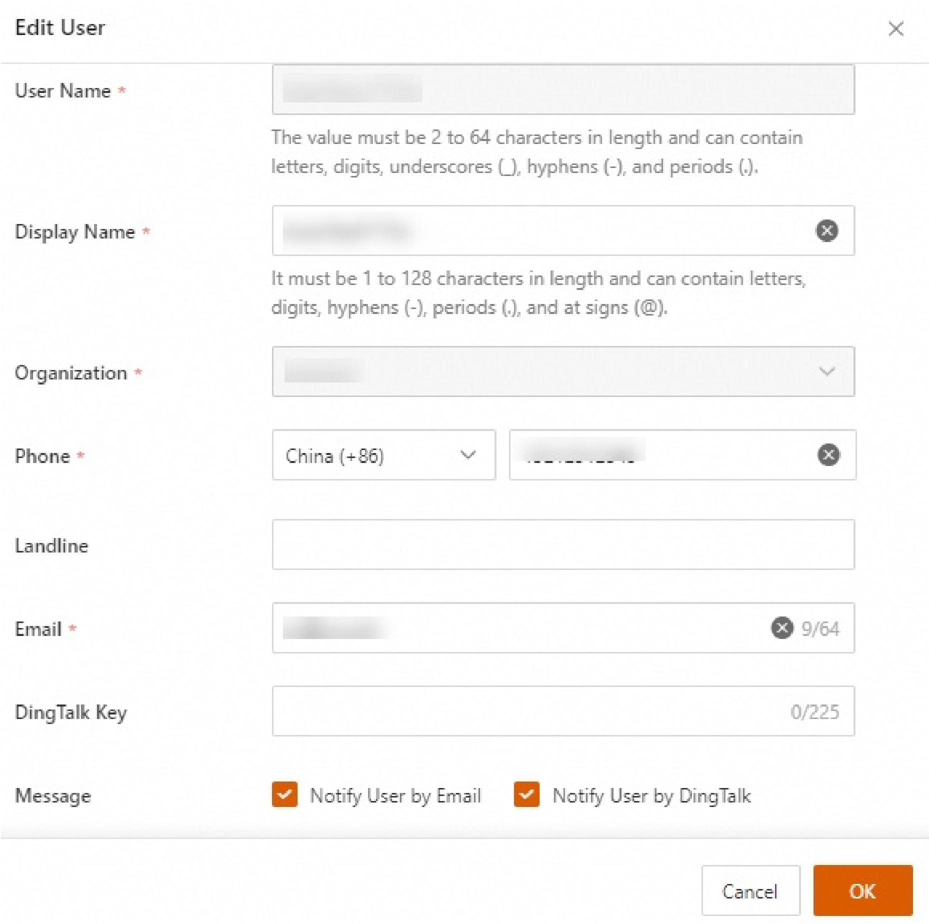
        - **View role permissions of a user**: On the **Role Permissions** tab, select a preset or custom role from the drop-down list to view the permissions of the role on the **Management Permissions**, **App Permissions**, and **Menu Permissions** tabs. You can also view the permissions of Resource Access Management (RAM) users.

Modify the basic information about a user

If the information about a user changes, perform the following steps to modify the information:

1. On the **System Users** tab, find the user that you want to manage in the list and click **Edit** in the Actions column.
2. In the **Edit User** dialog box, modify the values of the parameters.

> **Note**
>
> You cannot modify the values of the User Name and Organization parameters.



Edit User

User Name * [redacted]

The value must be 2 to 64 characters in length and can contain letters, digits, underscores (_), hyphens (-), and periods (.).

Display Name * [redacted]

It must be 1 to 128 characters in length and can contain letters, digits, hyphens (-), periods (.), and at signs (@).

Organization * [redacted]

Phone * China (+86) [redacted]

Landline

Email * [redacted] 9/64

DingTalk Key 0/225

Message ☑ Notify User by Email ☑ Notify User by DingTalk

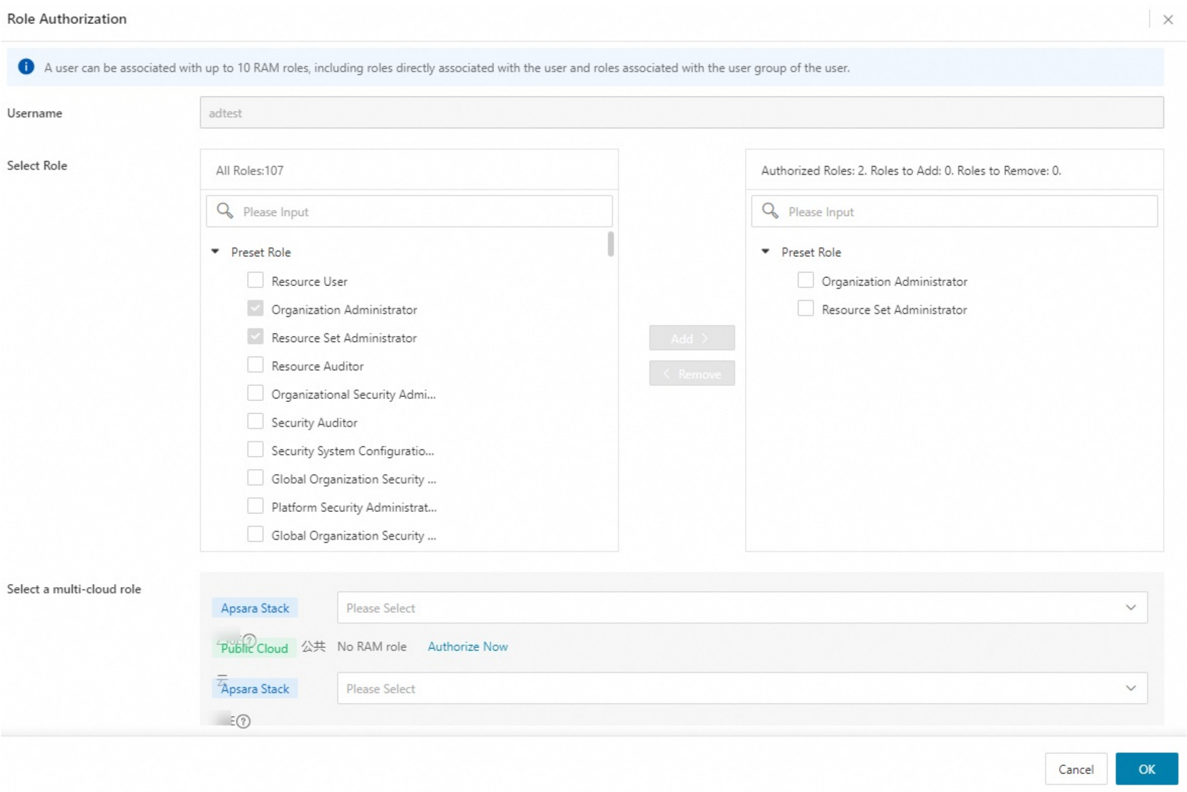
3. Click **OK**.

Manage the roles of a user

Perform the following steps to modify the roles of a user: Make sure that a role is created before you assign the role to a user.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Role Authorization**.
2. In the **Role Authorization** dialog box, select or deselect roles to assign roles to or revoke roles from the user.

> **Note**
>
> - You can assign up to 10 RAM roles to a user. The RAM roles include roles directly assigned to the user and roles assigned to the user group to which the user belongs.
> - If you select a multi-cloud role, each user can be assigned only one RAM role in the Alibaba Cloud public cloud. If no RAM role exists, click **Authorize** to create a RAM role. If a RAM role is assigned, you can update the policy of the RAM role or remove the RAM role.
> - When you select a multi-cloud role for Apsara Stack, you can select a role that has the permissions to manage only resource sets.



Role Authorization

A user can be associated with up to 10 RAM roles, including roles directly associated with the user and roles associated with the user group of the user.

Username: adtest

Select Role

All Roles:107

Please Input

▾ Preset Role
- □ Resource User
- ☑ Organization Administrator
- ☑ Resource Set Administrator
- □ Resource Auditor
- □ Organizational Security Admi...
- □ Security Auditor
- □ Security System Configuratio...
- □ Global Organization Security ...
- □ Platform Security Administrat...
- □ Global Organization Security ...

Add >
< Remove

Authorized Roles: 2. Roles to Add: 0. Roles to Remove: 0.

Please Input

▾ Preset Role
- □ Organization Administrator
- □ Resource Set Administrator

Select a multi-cloud role

Apsara Stack: Please Select

Public Cloud 公共 No RAM role Authorize Now

Apsara Stack: Please Select

Cancel OK

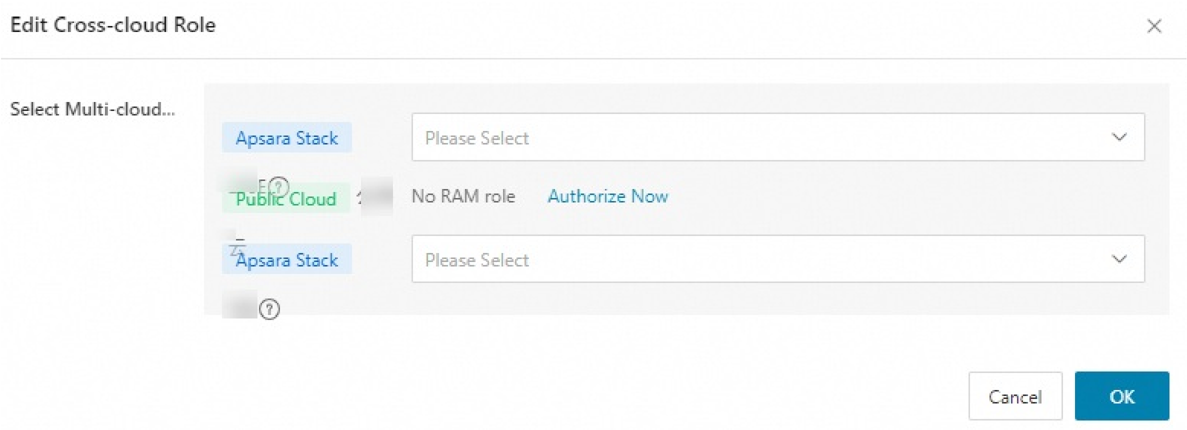
3. Click **OK**.

Modify a multi-cloud role

You can modify the multi-cloud role of a user.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Role Authorization**.
2. In the dialog box that appears, select a multi-cloud role and click **OK**.

> **Note**
>
> - If you select a multi-cloud role, each user can be assigned only one RAM role in the Alibaba Cloud public cloud. If no RAM role exists, click **Authorize** to create a RAM role.
> - When you select a multi-cloud role for Apsara Stack, you can select a role that has the permissions to manage only resource sets.



Edit Cross-cloud Role

Select Multi-cloud...

Apsara Stack: Please Select

Public Cloud [redacted]: No RAM role Authorize Now

Apsara Stack: Please Select

[redacted]

Manage the resource sets to which a user belongs

Perform the following steps to modify the resource sets to which a user belongs:

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Resource Sets**.
2. On the **Resource Set** tab of the **user details** page, select a role to view the information about the resource sets to which the user belongs.

   > **Note**
   >
   > Find the resource set that you want to manage and click **Remove** in the **Actions** column to remove the user from the resource set.

3. Click **My Resource Sets** above the list.

   > **Important**
   >
   > Make sure that a resource set is created before you add a user to the resource set.

4. In the **Add to Resource Set** dialog box, select a role type from the **Select a role type** drop-down list and select one or more resource sets to which you want to add the user in the resource set list.

   > **Note**
   >
   > If you enable the secret level access feature in the security policy, you must configure the Security Level parameter for your resource set when you create the resource set. You can add only users whose security level is higher than or equal to the security level of the resource set to the resource set.

5. Click **OK**.

Manage user groups to which a user belongs

Perform the following steps to modify the user groups to which a user belongs:

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **User Group Management**.

2. On the **User Group** tab of the user details page, view the information about the user groups to which the user belongs. The information is displayed in the following columns: **User Group Name/ID**, **Organization**, **Role**, **User**, **Associate Resource Set**, and **Creation Time**.

   > **Note**
   >
   > - The number in the **User** column of a user group indicates the number of users who are added to the user group. When you move the pointer over the number, you can view the users who are added to the user group.
   > - Find the user group that you want to manage and click **Remove** in the **Actions** column to remove the user from the user group.

3. Click **Add to User Group** above the list.

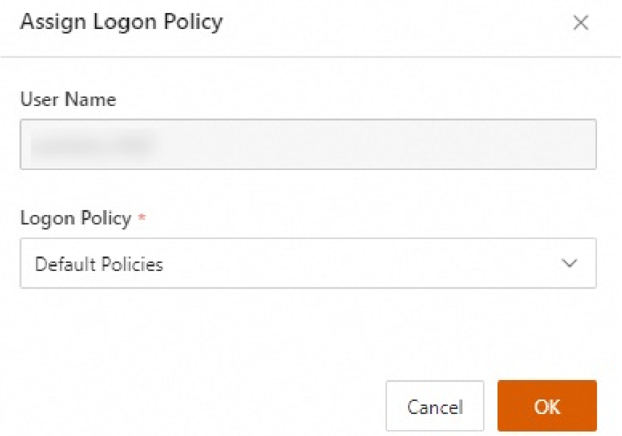
   > **Important**
   >
   > Make sure that a user group is created before you add a user to the user group.

4. In the **Add to User Group** dialog box, select one or more user groups to which you want to add the user.
5. Click **OK**.

Configure one or more access policies

Perform the following steps to modify the logon policies of one or more users:

- Configure a logon policy for a single user
   i. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Configure Access Control Policy**.
   ii. In the Assign Logon Policy dialog box, select an option from the **Logon Policy** drop-down list.

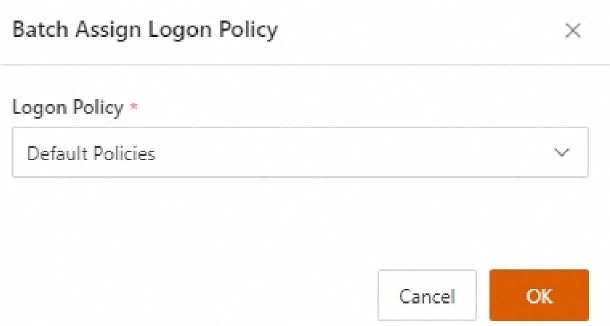


Assign Logon Policy

User Name: [redacted]

Logon Policy *: Default Policies

   iii. Click **OK**.
- Configure a logon policy for multiple users
   i. On the **System Users** tab, select multiple users in the list.
   ii. Click **Configure Logon Policy** below the list.
   iii. In the **Batch Assign Logon Policy** dialog box, select an option from the **Logon Policy** drop-down list.



Batch Assign Logon Policy

Logon Policy *

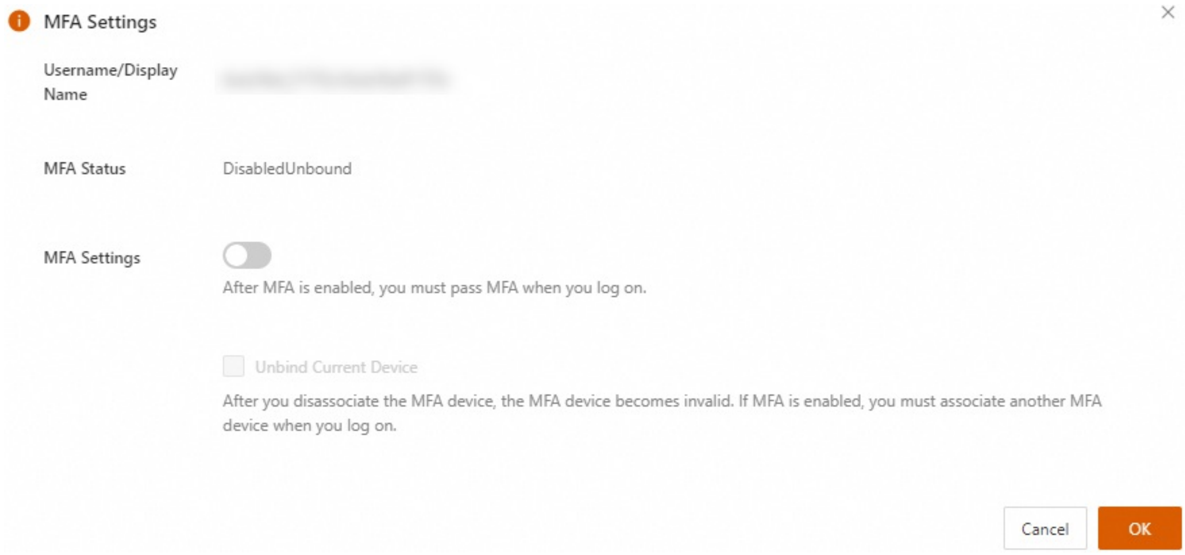
Default Policies

iv. Click **OK**.

Configure MFA settings

To implement Global Multi-factor Authentication (MFA), you must bind a virtual MFA device, such as Alibaba Cloud App. In this case, you must provide multiple identities for authentication when you log on to the console. This improves account security.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **MFA Settings**.
2. In the **MFA Settings** dialog box, turn on or off MFA Settings.



MFA Settings

Username/Display Name [redacted]

MFA Status DisabledUnbound

MFA Settings

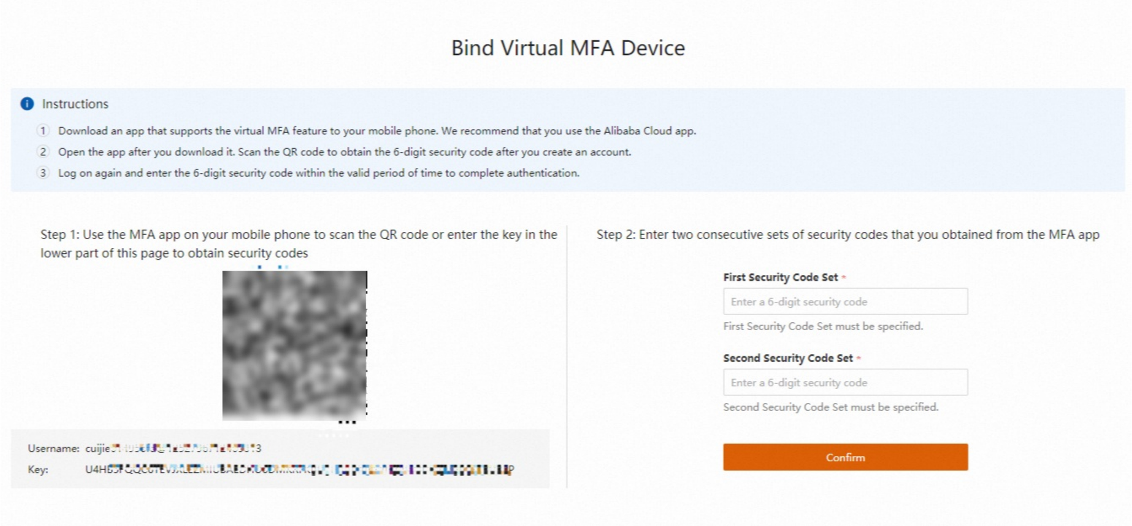
After MFA is enabled, you must pass MFA when you log on.

□ Unbind Current Device

After you disassociate the MFA device, the MFA device becomes invalid. If MFA is enabled, you must associate another MFA device when you log on.

- : MFA is enabled.

- **If MFA is enabled for a user but no MFA device is bound to the user** : When the user logs on to the console by using the username and password, the **Bind Virtual MFA Device** page appears and the user is required to bind an MFA device.

  Bind Virtual MFA Device

  Instructions

  1. Download an app that supports the virtual MFA feature to your mobile phone. We recommend that you use the Alibaba Cloud app.
  2. Open the app after you download it. Scan the QR code to obtain the 6-digit security code after you create an account.
  3. Log on again and enter the 6-digit security code within the valid period of time to complete authentication.

  Step 1: Use the MFA app on your mobile phone to scan the QR code or enter the key in the lower part of this page to obtain security codes

  [redacted]

  Username: cuijie[redacted]

  Key: U4H[redacted]

  Step 2: Enter two consecutive sets of security codes that you obtained from the MFA app

  First Security Code Set *

  Enter a 6-digit security code

  First Security Code Set must be specified.

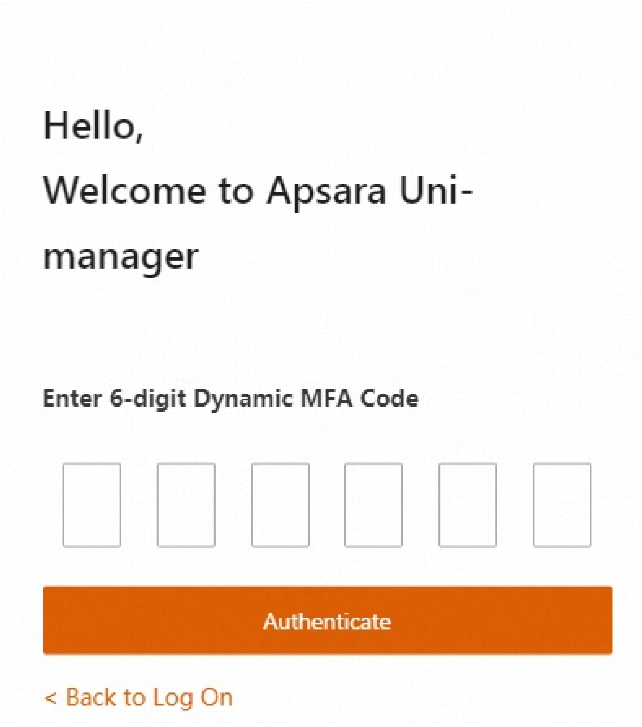
  Second Security Code Set *

  Enter a 6-digit security code

  Second Security Code Set must be specified.

- **MFA is enabled and an MFA device is bound** : When the user logs on to the console by using the username and password, a dynamic MFA code is required for authentication.

  > **Important**
  >
  > If you want to unbind an MFA device from a user, select **Unbind Current Device** in the **MFA Settings** dialog box. After you unbind the MFA device, the MFA device becomes invalid.

  Hello,

  Welcome to Apsara Uni-manager

  Enter 6-digit Dynamic MFA Code

  □ □ □ □ □ □

  - ○ : MFA is disabled.

- **If MFA is disabled for a user but an MFA device is bound to the user** : When the user logs on to the console by using the username and password, a dynamic MFA code is still required for authentication.

> **Important**
>
> If you want to unbind an MFA device from a user, select **Unbind Current Device** in the **MFA Settings** dialog box. After you unbind the MFA device, the MFA device becomes invalid.

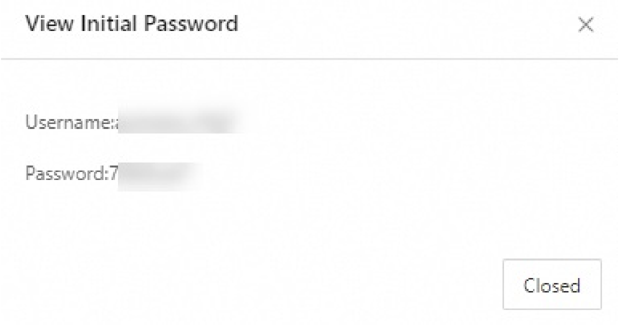
- **If MFA is disabled for a user and an MFA device is not bound to the user** : When the user logs on to the console by using the username and password, a dynamic MFA code is not required for authentication.

3. Click **OK**.

View the initial password of a user

You can view the initial password of a user only if the user has not been used to log on to the Apsara Uni-manager Management Console. If the user is already used to log on to the console, the password is not displayed.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **View Initial Password**.
2. In the View Initial Password dialog box, view the displayed initial password.



View Initial Password

Username:[redacted]

Password:[redacted]

Reset the password of a user

You can reset the password of an account if the password is forgotten.

1. On the **System Users** tab, find the user that you want to manage in the list and click its name to go to the user details page.
2. Click **Reset Password** next to the **Password** parameter and click the 👁 icon to view the reset password.

Manage the AccessKey pair of a user

The administrator can manually rotate the AccessKey pairs of users.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **AccessKey Management**.
2. In the **Manage User AccessKey Pairs** dialog box, manage the AccessKey pair.
   - In the AccessKey pair list, view information such as AccessKey ID, State, Created, and AccessKey Audit Logs.

> **Note**
>
> The administrator can view only the AccessKey ID of the AccessKey pair. To view the AccessKey secret, go to the Personal Information page.

- Click **Create AccessKey**. The system automatically creates an AccessKey pair. Each user can have up to two AccessKey pairs.
- In the AccessKey pair list, find the required AccessKey pair and click **Disable** in the Actions column. In the dialog box that appears, read and select **I have known the risks and confirm this operation.** and click **Disable**. After the AccessKey pair is disabled, the status of the AccessKey pair changes to Disabled.

> **Important**
>
> - Only AccessKey pairs in the **Enabled** state can be disabled.
> - After an AccessKey pair is disabled, the services or programs that use the AccessKey pair may be interrupted. If this issue occurs, enable the AccessKey pair to resolve the issue.

- In the AccessKey pair list, find the required AccessKey pair and click **Enable** in the Actions column. After the AccessKey pair is enabled, the status of the AccessKey pair changes to Enabled.

> **Important**
>
> Only AccessKey pairs in the **Disabled** state can be enabled.

- In the AccessKey pair list, find the required AccessKey pair and click **Delete** in the Actions column. In the dialog box that appears, read and select **I have known the risks and confirmed this delete operation.** and click **Delete**.

> **Important**
>
> After the AccessKey pair is deleted, the services or programs that use the AccessKey pair may be interrupted. Proceed with caution. We recommend that you disable the AccessKey pair to evaluate the impacts before you delete the AccessKey pair.

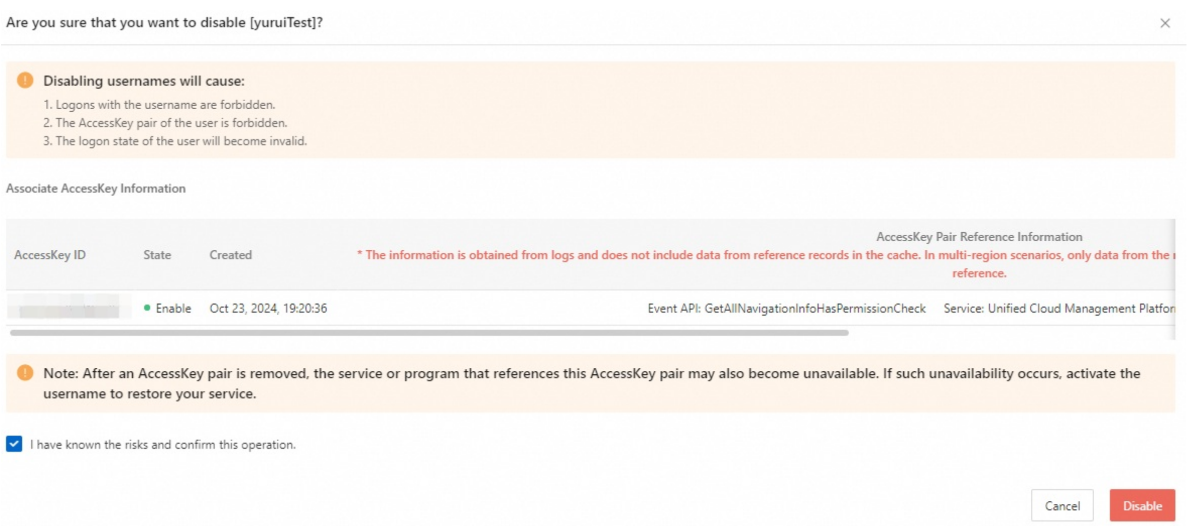
Disable a user

Perform the following steps to disable a user:

> **Important**
>
> - You can disable only users in the **Enabled** state. After a user is disabled, the user enters the **Disabled** state.
> - After you disable a user, the user is forbidden from logging on to the Apsara Uni-manager Management Console, the AccessKey pair of the user is disabled, and the user logon status is invalid.
> - After an AccessKey pair is disabled, the services or programs that use the AccessKey pair may be interrupted. If this issue occurs, enable the AccessKey pair to resolve the issue.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Disable**.
2. In the dialog box that appears, select **I have known the risks and confirm this operation**.

   > **Note**
   >
   > Move the pointer over the AccessKey Pair Reference Information column to view the information about the events that reference the AccessKey pair.

   Are you sure that you want to disable [yuruiTest]?

   Disabling usernames will cause:

   1. Logons with the username are forbidden.
   2. The AccessKey pair of the user is forbidden.
   3. The logon state of the user will become invalid.

   Associate AccessKey Information

AccessKey ID	State	Created	AccessKey Pair Reference Information * The information is obtained from logs and does not include data from reference records in the cache. In multi-region scenarios, only data from the r reference.
[redacted]	● Enable	Oct 23, 2024, 19:20:36	Event API: GetAllNavigationInfoHasPermissionCheck Service: Unified Cloud Management Platfor

   Note: After an AccessKey pair is removed, the service or program that references this AccessKey pair may also become unavailable. If such unavailability occurs, activate the username to restore your service.

   ☑ I have known the risks and confirm this operation.

3. Click **Disable**.

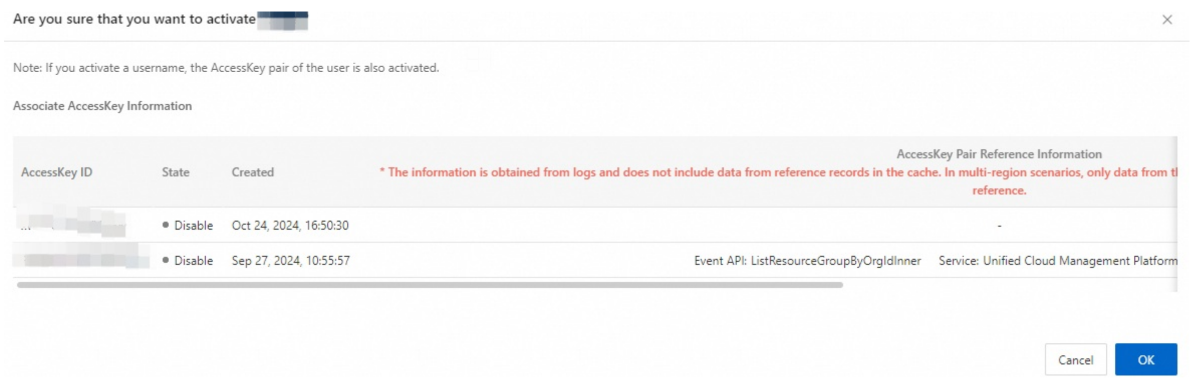
Enable a user

Perform the following steps to enable a disabled user:

> **Important**
>
> - You can enable only users in the **Disabled** state. After a user is enabled, the user enters the **Enabled** state.
> - After you enable a user, the associated AccessKey pair is also enabled.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Enable**.
2. In the message that appears, click **OK**.

   > **Note**
   >
   > Move the pointer over the AccessKey Pair Reference Information column to view the information about the events that reference the AccessKey pair.



Are you sure that you want to activate [redacted]

Note: If you activate a username, the AccessKey pair of the user is also activated.

Associate AccessKey Information

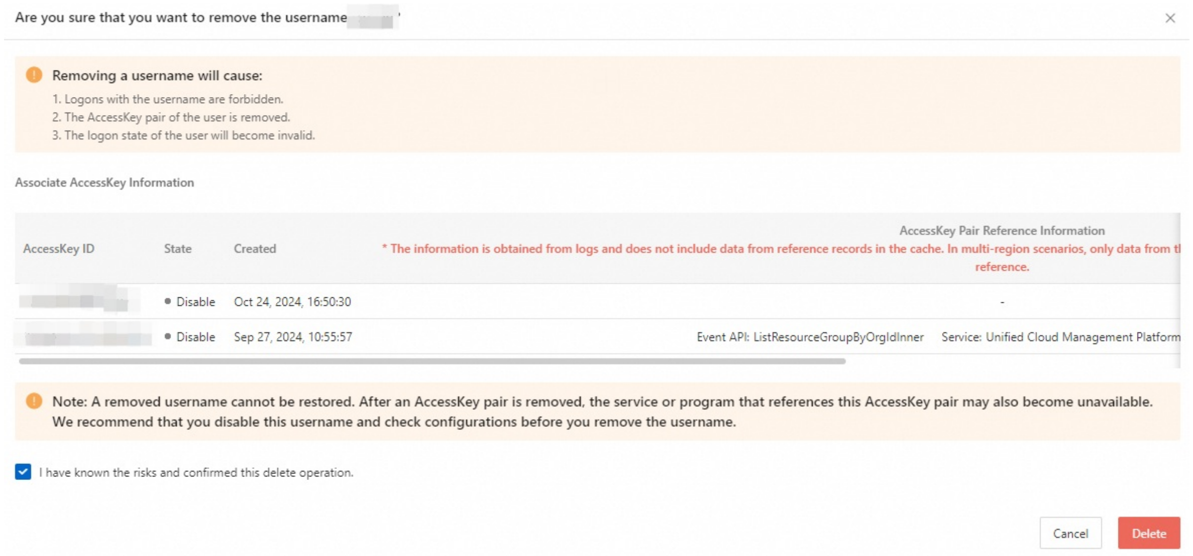
AccessKey ID	State	Created	AccessKey Pair Reference Information * The information is obtained from logs and does not include data from reference records in the cache. In multi-region scenarios, only data from t reference.
[redacted]	● Disable	Oct 24, 2024, 16:50:30	-
[redacted]	● Disable	Sep 27, 2024, 10:55:57	Event API: ListResourceGroupByOrgIdInner Service: Unified Cloud Management Platform

Delete a user

You can delete a user that you no longer use.

> **Important**
>
> - After you delete a user, if the user is forbidden from logging on to the Apsara Uni-manager Management Console or the AccessKey pair of the user is deleted, the user logon status is invalid.
> - After you delete a user, the user data cannot be recovered. After an AccessKey pair is deleted, the services or programs that use the AccessKey pair may not work as expected. We recommend that you disable the user first and troubleshoot issues before you delete the user.

1. On the **System Users** tab, find the user that you want to manage, click the ··· icon in the Actions column, and then click **Delete**
2. In the dialog box that appears, select **I have known the risks and confirmed this delete operation** and



Are you sure that you want to remove the username [redacted]

Removing a username will cause:
1. Logons with the username are forbidden.
2. The AccessKey pair of the user is removed.
3. The logon state of the user will become invalid.

Associate AccessKey Information

AccessKey ID	State	Created	AccessKey Pair Reference Information * The information is obtained from logs and does not include data from reference records in the cache. In multi-region scenarios, only data from t reference.
[redacted]	● Disable	Oct 24, 2024, 16:50:30	-
[redacted]	● Disable	Sep 27, 2024, 10:55:57	Event API: ListResourceGroupByOrgIdInner Service: Unified Cloud Management Platform

Note: A removed username cannot be restored. After an AccessKey pair is removed, the service or program that references this AccessKey pair may also become unavailable. We recommend that you disable this username and check configurations before you remove the username.

☑ I have known the risks and confirmed this delete operation.

3. Click **Delete**.

   The deleted system user is displayed on the **Historical Users** tab. You can restore or permanently delete the user on the Historical Users tab.

4.3.2.3. Manage historical users

You can restore or permanently delete deleted users.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users > Users**.
4. Click the **Historical Users** tab.

Operation	Procedure
Restore a user	After you restore a deleted user, the user will be added back to the System Users list. i. Click **Restore** in the Actions column corresponding to a user. ii. In the dialog box that appears, select the organization to which the user belongs and the roles of the user. iii. Click **OK**.
Permanently delete a user	After you permanently delete a user, the user will be removed from the Historical Users list and can no longer be restored. i. Click **Delete** in the Actions column corresponding to a user. ii. In the message that appears, click **Delete**.

4.3.3. User group management

4.3.3.1. Create a user group

This topic describes how to create user groups in an organization. You can use user groups to manage permissions of users in batch.

Prerequisites

An organization is created. For more information, see Create an organization.

Background information

Subjects	Description
User groups and organizations	• A user group belongs to only a single organization. • Multiple user groups can be created within an organization.
User groups and users	• A user group can contain multiple users. It can also contain no user. • A user does not necessarily need to belong to a user group. • A user can be added to multiple user groups.

User groups and roles	• A role can be assigned to multiple user groups. • When a role is assigned to a user group, the permissions that the role has are automatically granted to users within the user group.
User groups and resource sets	• A resource set can contain multiple user groups. It can also contain no user group. • A user group can be added to multiple resource sets.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users > User Groups**.
4. Click **Create a user group** in the upper-left corner.
5. In the dialog box that appears, set **User Group Name**, **Organization**, and **Role authorization**.

Parameter	Description
User Group Name	The name of the user group. The name must be 3 to 255 characters in length and can contain letters, digits, underscores (_), hyphens (-), periods (.), and at signs (@).
Organization	The organization to which the user group belongs.
Role authorization	The roles that are assigned to the user group.

6. Click **OK**.

4.3.3.2. Manage user groups

You can modify the name, permissions, and users of a user group.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users > User Groups**.
4. On the User Groups page, find the user group that you want to manage and perform operations. The following table describes the operations that you can perform.

Operation	Procedure
View user groups	On the User Groups page, view information about user groups, including the organization, assigned roles, number of users, and associated resource sets.

Modify a user group	You can modify the name of a user group. i. Click **Editing** in the Actions column. ii. In the Modify User Group dialog box, enter a new name. iii. Click **OK**.
Add a user	After a user is added to a user group, the user has the permissions of the role that is assigned to the user group. i. Find the user group to which you want to add users and click**Add User** in the Actions column. ii. In the left-side list of the Add User dialog box, select the users that you want to add to the user group and click the › icon to add the users to the right-side list. iii. Click **OK**.
Remove a user	After a user is removed from a user group, the user no longer has the permissions of the role that is assigned to the user group. i. Find the user group from which you want to remove users and move the pointer over the ··· icon in the Actions column. In the menu that appears, select **Remove User**. ii. In the left-side list of the Remove User dialog box, select the users you want to remove and click the › icon to add them to the right-side list. iii. Click **OK**.
Assign roles to a user group	You can assign a role to a user group to grant the role permissions to all users within the group. i. Find the user group that you want to manage and move the pointer over the ··· icon in the Actions column and click**Authorized**. ii. In the Authorized dialog box, select the roles you want to assign to the user group from the Role Permissions drop-down list. iii. Click **OK**.
Delete user groups	ⓘ **Important** When a user group is deleted, resources such as roles, users, and resource sets that are associated with the user group are automatically unbound. i. Find the user group that you want to manage and move the pointer over the ··· icon in the Actions column and click**Delete**. ii. Click **OK**.

4.4. Permission management

4.4.1. Overview

The Apsara Uni-manager Management Console allows you to manage permissions based on scenarios, users, and cloud services by using features such as the features for role permissions, data permissions, access control, permission boundaries, and AccessKey logs. These features improve system security.

Role permissions

You can create roles and assign the roles to users or user groups to implement fine-grained access control on users. The following operations are supported:

- Create roles
- Disable roles
- Enable roles
- Delete roles
- Replicate roles

Data permissions

You can grant users the data permissions to access specific cloud instances. You can also view and modify the data permissions granted to users. The following operations are supported:

- Configure the data permissions on cloud instances
- View user data permissions
- Modify user data permissions

Access control

You can configure access policies to control the time and IP addresses for user logon. After a user is associated with an access policy, user logons are limited based on the logon time and IP addresses specified in the policy. The following operations are supported:

- Create access policies
- Modify access policies
- Disable access policies
- Enable access policies
- Delete access policies

Permission boundaries

You can create service boundaries and configure API control policies to block API operations on the core gateway of Apsara Stack. Custom API control policies can be created. The following operations are supported:

- Create service boundaries and API control policies
- View service boundaries and API control policies
- Modify service boundaries and API control policies
- Edit service boundaries and API control policies
- Enable and disable service boundaries and API control policies
- Modify whitelists of service boundaries

- Delete service boundaries and API control policies

AccessKey logs

You can view AccessKey logs based on the AccessKey ID to facilitate security management of AccessKeys pairs. The following operations are supported:

- View the basic information about AccessKey pairs
- View the cloud services accessed by using an AccessKey pair

4.4.2. Role permissions

4.4.2.1. Overview

A role is a collection of access permissions. In the Apsara Uni-manager Management Console, role types include preset roles, custom roles, RAM role-based authorization, and RAM-based authorization.

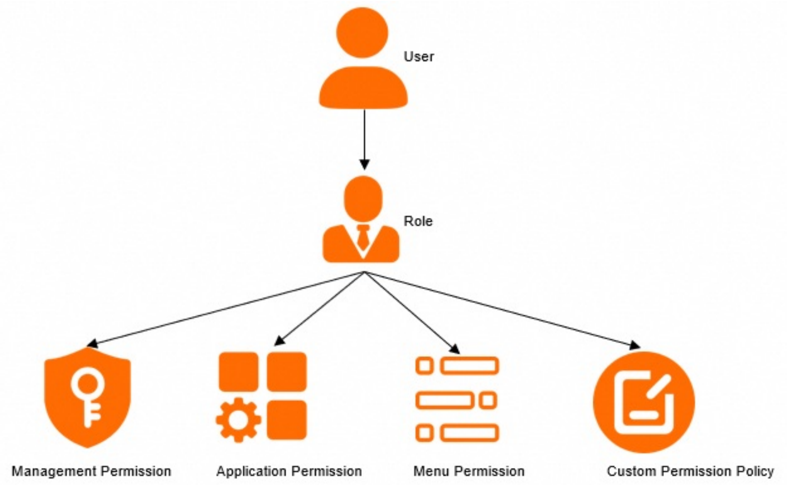
Role types

Preset role

A preset role is a collection of preset permissions for specific operations. To implement privilege separation, the Apsara Uni-manager Management Console provides preset roles based on the general use cases in cloud platforms. After a RAM user is assigned a preset role, the user has the corresponding operation permissions. During authentication, the system determines whether the user has the permissions to perform the corresponding operations based on the permissions that belong to the preset role assigned to the user. For more information, see Preset roles.

Custom role

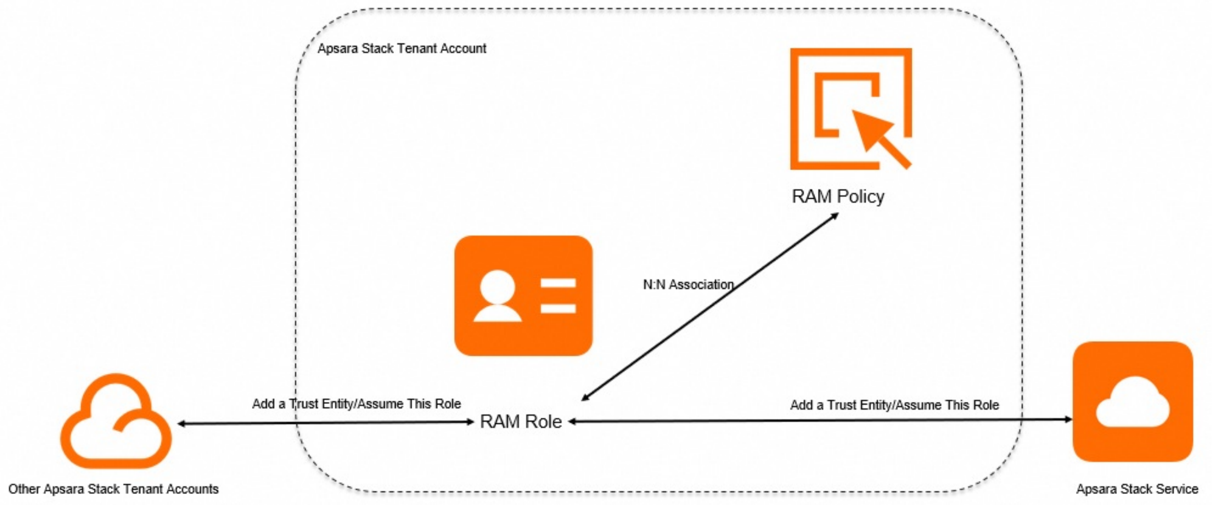
You can create a custom role to combine and set permission policies based on your business requirements. You can configure the sharing scope and permissions on resources, applications, and menus for the custom role, and configure custom permission policies to flexibly specify the services that can be accessed by the role, the operations that can be performed by the role, and the resources that can be managed by the role. Compared with preset roles, custom roles are more flexible and can be customized.



> **Note**
>
> Custom roles are commonly used to manage the permissions of users who log on to cloud service consoles. In addition, third-party independent software vendors (ISVs) can create custom roles when they require AccessKey pairs with limited permission scope to call cloud service APIs for application development.

RAM role-based authorization

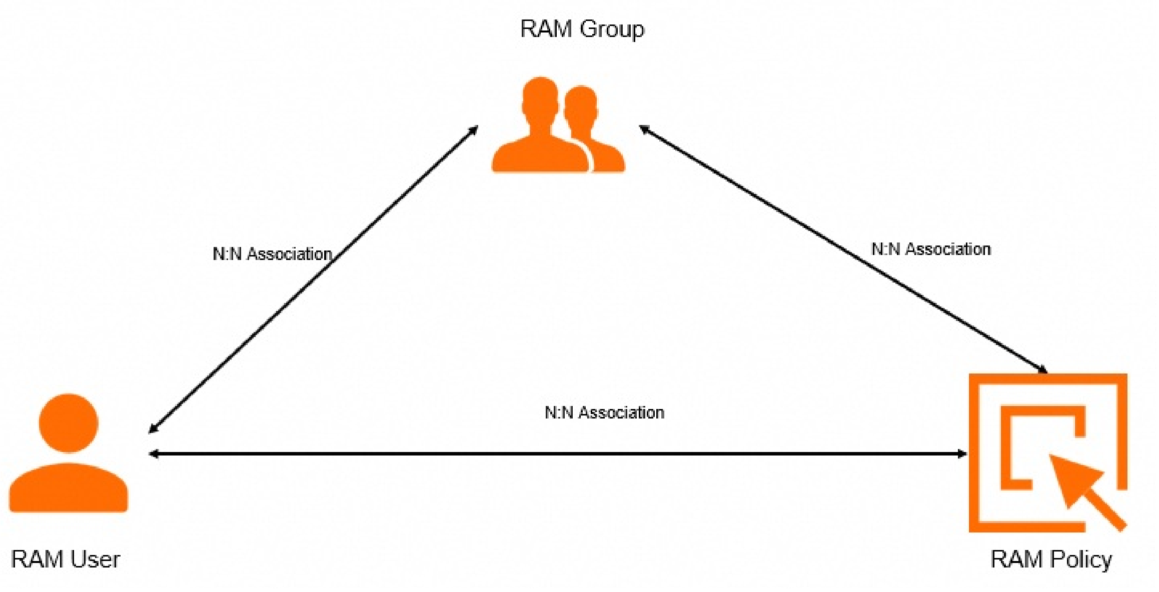
RAM role-based authorization is the process of associating a RAM role with RAM users, other Apsara Stack tenant accounts, or Apsara Stack services. An authorized entity can directly assume a RAM role to obtain the collection of permissions that belong to the role without the need to grant permission policies to the entity.


Apsara Stack Tenant Account
RAM Policy
N:N Association
Add a Trust Entity/Assume This Role
RAM Role
Add a Trust Entity/Assume This Role
Other Apsara Stack Tenant Accounts
Apsara Stack Service

> **Note**
>
> RAM role-based authorization can be divided into the role of Apsara Stack tenant accounts and the role of Apsara Stack services based on the types of trust entities.
>
> - Role of Apsara Stack tenant accounts: the role that can be assumed by RAM users. RAM users who assume this type of role can belong to the own Apsara Stack tenant accounts or other Apsara Stack tenant accounts. The roles of this type are used for cross-account access or temporarily authorized access.
> - Role of Apsara Stack services: the role that can be assumed by cloud services. The roles of this type are used for access across Apsara Stack services.

RAM-based authorization

Each RAM user is a user entity with a unique identity. You can assign custom policies to RAM users by using user groups. This way, the RAM users always have these permissions regardless of whether they assume a role.



Note

- RAM-based authorization is performed based on RAM user groups other than RAM roles.
- RAM-based authorization is used to enhance the fine-grained permission control of custom roles that are created on a GUI. After you create a custom role, you can use RAM-based authorization to attach a RAM policy to RAM users if some permissions cannot be granted by using the custom role.
- RAM-based authorization must be used together with user groups.

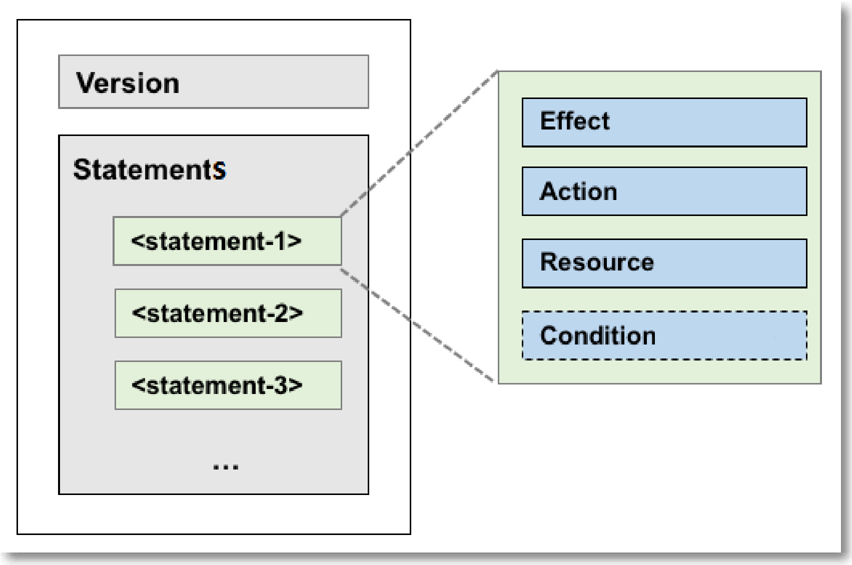
4.4.2.2. RAM policies

This topic describes the elements, structure, and syntax of RAM policies that are used to define the scope of permissions for custom roles, RAM authorization and RAM role-based authorization.

Structure

RAM policies are in the JSON format, containing two parts:

- Version: the version number of the policy.
- Statements: the statements that specify the permissions. The elements of statements include Effect, Action, Resource, Condition, and Principal.



Elements in statements

The elements of statements include Effect, Action, Resource, Condition, and Principal.

Effect (Required)

Specifies whether a statement result is an explicit allow or an explicit deny. Valid values: Allow and Deny.

> **Note**
>
> Precedence of Deny: Deny statements take precedence when a user is assigned multiple policies that contain Allow and Deny statements, and when a single policy contains both Allow and Deny statements.

Example

```
"Effect": "Allow"
```

Action (Required)

The specific API operations involved in the statement.

The Action element is in the following format: `<ram-code>:<action-name>` .

- `<ram-code>` : the product code.
- `<action-name>` : the API operation of the product involved in the policy.

> **Note**
>
> The values of the Action element are case-insensitive. However, to ensure consistency, we recommend that you follow the standard capitalization of the product code and API operation names.

Example

```
"Action": [
  "oss:ListBuckets",
  "ecs:Describe*",
  "rds:Describe*"
]
```

> **Note**
>
> You can use the asterisk (*) as a wildcard character. For example, in the preceding example, `ecs:Describe*` indicates that all the API operations of Elastic Compute Service (ECS) whose names start with Describe are involved in the policy.

Resource (Required)

The resources of cloud services involved in the statement, which are indicated by their Aliyun Resource Names (ARNs)

Resource elements are in the following format: `acs:<ram-code>:<region>:<account-id>:<relative-id>` .

- `acs` : the prefix of ARNs. It stands for Alibaba Cloud Service.
- `<ram-code>` : the product code.
- `<region>` : the region ID of the resource. You can use the asterisk (*) as a wildcard character to indicate regionless resources or resources in all regions.
- `<account-id>` : the user ID of the level-1 organization. This is used to specify the resources that belong to a specific level-1 organization.
- `<relative-id>` : the description of the specific resources. Its syntax is product-specific. For example, the relative-id for an OSS object is a path of that object, such as mybucket/dir1/object1.jpg.

Example

```
"Resource": [
 "acs:ecs:*:*:instance/inst-001",
 "acs:ecs:*:*:instance/inst-002",
 "acs:oss:*:*:mybucket",
 "acs:oss:*:*:mybucket/*"
]
```

Condition (Optional)

The conditions that are required for the policy to take effect. A Condition element, or a condition block, contains one or multiple conditions. Each condition consists of an operator, a condition key, and a condition value.

Condition keys are case-sensitive. The case-sensitivity of the condition values is determined by the operator. For example, assume that a condition key of the string type is specified. if the StringEquals operator is used, the system performs a case-sensitive match. If the StringEqualsIgnoreCase operator is used, the system performs a case-insensitive match.

Description:

- Evaluation logic

- You can specify one or more values for a condition key. If the value in a request matches one of the values, the condition is met.
- A condition can have multiple keys that are attached to a single conditional operator. The condition of this type is met only if all requirements for the keys are met.
- A condition block is met only if all of its conditions are met.

- Operators

  Operators are classified into the following types: string, number, data and time, Boolean, and IP address.

Category	Operator
String	◦ StringEquals ◦ StringNotEquals ◦ StringEqualsIgnoreCase ◦ StringNotEqualsIgnoreCase ◦ StringLike ◦ StringNotLike
Number	◦ NumericEquals ◦ NumericNotEquals ◦ NumericLessThan ◦ NumericLessThanEquals ◦ NumericGreaterThan ◦ NumericGreaterThanEquals
Date and time	◦ DateEquals ◦ DateNotEquals ◦ DateLessThan ◦ DateLessThanEquals ◦ DateGreaterThan ◦ DateGreaterThanEquals
Boolean	Bool
IP address	◦ IpAddress ◦ NotIpAddress

- Condition keys

- General condition keys are in the following format: `acs:<condition-key>` .

General condition key	Type	Description
acs:CurrentTime	Date and time	The time when the server receives the request. Specify the time in the ISO 8601 standard, for example, 2012-11-11T23:59:59Z.
acs:SecureTransport	Boolean	Specifies whether a secure channel is used to send a request. For example, a request can be sent over HTTPS.
acs:SourceIp	IP address	The IP address of the client that sends the requestIt can be a single IP address or a CIDR block. If the value is a single IP address, you must specify the specific IP address rather than a CIDR block. For example, you must specify 10.0.0.1 rather than 10.0.0.1/32.
acs:MFAPresent	Boolean	Specifies whether multi-factor authentication (MFA) is used when the user who sends the request logged on.
acs:PrincipalARN	String	The identity of the requester. This operator is only used in trust policies of RAM roles.

- Service-specific condition keys are in the following format: `<ram-code>:<condition-key>` .

Service-specific condition key	Cloud service	Type	Description
ecs:tag/<tag-key>	Elastic Compute Service (ECS)	String	The condition key for tags of ECS resources, which are customizable.
rds:ResourceTag/<tag-key>	ApsaraDB RDS	String	The condition key for tags of ApsaraDB RDS resources, which are customizable.
oss:Delimiter	Objective Storage Service (OSS)	String	The delimiter used by OSS to categorize object names.
oss:Prefix	OSS	String	The prefix of an OSS object name.

Principal

The entity that is allowed or denied to call the related API operations. This element is available only for resource-based policies. For example, in a trust policy attached to a RAM role, you can specify the resources that are allowed to assume the role in the Principle element. The Principal element is required in resource-based policies.

> **Note**
>
> You cannot specify the Principal element in identity-based policies. Identity-based policies are attached to RAM identities. The RAM identities to which identity-based policies are attached are the principals.

You can specify multiple types of principals for the Principal element in a policy. You can also specify multiple principals of the same type for the Principal element in a policy. If you specify multiple types of principals, separate the types with commas (,). If you specify multiple principals of the same type, separate the principals with commas (,) and enclose the principals with brackets ([]). Multiple principals are associated with each other by the OR operator, meaning that the policy is attached to all principals in the policy.

Example

```
"Principal": {
 "RAM": [
 "acs:ram::123456789012****:root",
 "acs:ram::987654321098****:root"
 ],
 "Service": "ecs.aliyuncs.com"
}
```

Principals are authenticated RAM entities, which are divided into the following types:

- Organization account

  Set the Principal element to the account of the level-1 organization. When you configure the trust policy of a RAM role-based authorization, the account ARN of the selected trust organization will be added to the policy as the principal, such as `acs:ram::165399189392****:root`.

- Cloud service

  Set the Principal element to a cloud service. When you configure the trust policy of a RAM role-based authorization, the identifier of the selected trust service will be added to the policy as the principal, such as `ecs.aliyuncs.com`.

Policy syntax

A RAM policy consists of the version_block and statement_block components.

```
policy = {
 <version_block>,
 <statement_block>
}
```

version_block

The version of the policy. By default, the value is 1.

```
<version_block> = "Version" : ("1")
```

statement_block

The statements. A RAM policy can contain multiple statements.

```
<statement_block> = "Statement" : [ <statement>, <statement>, ... ]
```

- Each statement consists of the effect_block, action_block, resource_block, and condition_block elements. condition_block is an optional element.

  ```
  <statement> = {
   <effect_block>,
   <action_block>,
   <resource_block>,
   <condition_block?>
  }
  ```

  - Valid values of an effect_block element are `Allow` and `Deny`.

    ```
    <effect_block> = "Effect" : ("Allow" | "Deny")
    ```

  - Multiple action_block and resource_block elements can be specified in each statement.

    ```
    <action_block> = "Action" :
     ("*" | [<action_string>, <action_string>, ...])
    <resource_block> = "Resource" :
     ("*" | [<resource_string>, <resource_string>, ...])
    ```

  - Each condition_block element can contain multiple operators and

    ```
    <condition_block> = "Condition" : <condition_map>

    <condition_map> = {
      <condition_type_string> : {
          <condition_key_string> : <condition_value_list>,
          <condition_key_string> : <condition_value_list>,
          ...
      },
      <condition_type_string> : {
          <condition_key_string> : <condition_value_list>,
          <condition_key_string> : <condition_value_list>,
          ...
      }, ...
    }
    ```

Valid values of elements

- If an element value is a string, number, date, time, Boolean value, or an IP address, the value must be enclosed in double quotation marks ("").
- If an element value is a string, you can use asterisks (*) and question marks (?) as wildcard characters.
  - An asterisk (*) indicates 0 or multiple letters. For example, `ecs:Describe*` indicates all the API operations of Elastic Compute Service (ECS) whose names start with Describe.
  - A question mark (?) indicates a single letter.

Policy syntax check

RAM policies follow the JSON format. When you create or update a RAM policy, the system automatically checks the validity of the JSON format. We recommend that you use JSON validators or formatters to help you ensure the validity of the policy. For more information about JSON syntax standards, see RFC 7159.

4.4.2.3. Create a role

You can create custom roles, Resource Access Management (RAM) role-based authorization, and RAM-based authorization to facilitate permission management.

Limits

Limits on the management scope of resource sets

If you set the Management Permissions parameter to Resource Sets when you create a custom role, the role has the permissions on the resource sets of the associated user by default. This role is mainly used to manage resources. The permissions described in the following table are beyond the management scope of resource sets and do not take effect even if you select them.

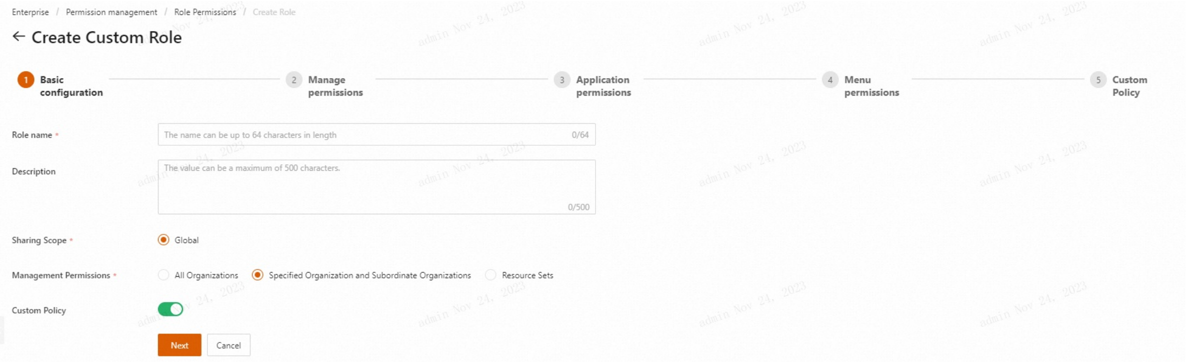
Management permission	Description
User management	The permissions to create a user, delete a user, activate a user, disable a user, lock a user, unlock a user, and perform other operations on the user.
Role management	The permissions to create or delete a role, lock or unlock a role, and perform other operations on the role.
User group management	The permissions to view a user group, create or delete a user group, and perform other operations on the user group.
Organization management	The permissions to create or delete an organization and perform other operations on the organization.
Resource set management	The permissions to create and delete a resource set.
AccessKey pair management	The permissions to view the AccessKey pair of an organization, create an AccessKey pair for an organization, delete the AccessKey pair of an organization, activate the AccessKey pair of an organization, disable the AccessKey pair of an organization, view the AccessKey pair of a user, and view AccessKey logs.
Access policy	The permissions to create or delete an access policy, and perform other operations on the access policy.

Change management	The permissions to change a resource set, change a resource, and change a user.
Bill management	The permissions to view the bills of a cloud service, an organization, and a resource set, export bills, and modify bills.
Service-linked role management	The permissions to create a service-linked role.
Process management	The permissions to view organization applications.
Multi-cloud management platform hosting	The permissions to configure multi-cloud management platform hosting.
Announcement management	The permissions to manage announcements.

Create a custom role

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions > Role Permissions**.
4. On the page that appears, click **Create Custom Role**.
5. In the **Basic Configuration** step, configure the parameters and click **Next**.

Create a custom role as an operations administrator



Enterprise / Permission management / Role Permissions / Create Role

← Create Custom Role

1 Basic configuration — 2 Manage permissions — 3 Application permissions — 4 Menu permissions — 5 Custom Policy

Role name *: The name can be up to 64 characters in length 0/64

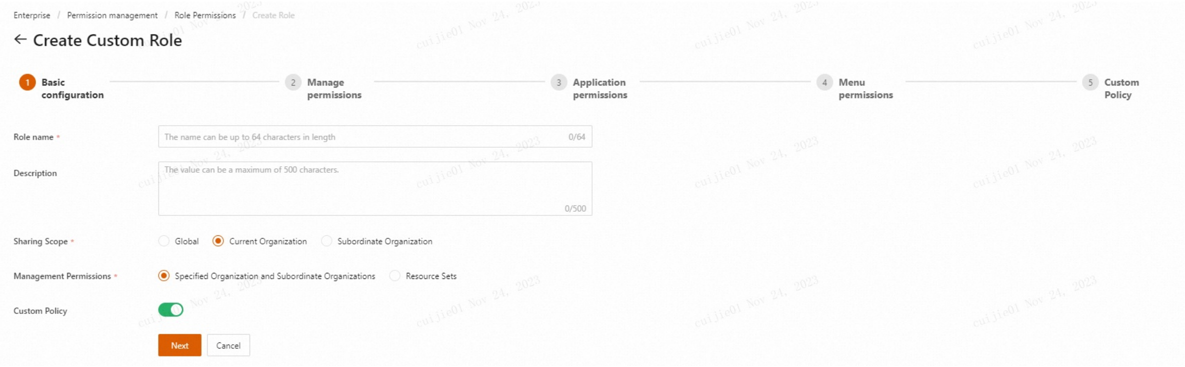
Description: The value can be a maximum of 500 characters. 0/500

Sharing Scope *: ● Global

Management Permissions *: ○ All Organizations ● Specified Organization and Subordinate Organizations ○ Resource Sets

Custom Policy: on

Create a custom role as an organization administrator



Enterprise / Permission management / Role Permissions / Create Role

← Create Custom Role

1 Basic configuration — 2 Manage permissions — 3 Application permissions — 4 Menu permissions — 5 Custom Policy

Role name *: The name can be up to 64 characters in length 0/64

Description: The value can be a maximum of 500 characters. 0/500

Sharing Scope *: ○ Global ● Current Organization ○ Subordinate Organization

Management Permissions *: ● Specified Organization and Subordinate Organizations ○ Resource Sets

Custom Policy: on

Parameter	Description
Role Name	The name of the role.
Description	The description of the role. This parameter is optional.
Sharing Scope	The scope in which the role is available. Only **Global** is available when you create a custom role as an operations administrator. Valid values: ◦ **Global**: The role is shared by all organizations. ◦ **Current Organization**: The role is shared within the current organization. ◦ **Subordinate Organization**: The role is shared by the current organization and its subordinate organizations.
Management Permissions	The scope of resources that can be managed by the role. Only **Specified Organization and Subordinate Organizations** and **Resource Sets** are available when you create a custom role as an organization administrator. Valid values: ◦ **All Organizations**: This role can manage cloud resources in all organizations. ◦ **Specified Organization and Subordinate Organizations**: This role can manage the cloud resources in the current organization and its subordinate organizations. ◦ **Resource Sets**: This role can manage only cloud resources in the specified resource sets. For more information about the limits on the management scope of resource sets, see Limits on the management scope of resource sets.

Secret Level Access	The security level that you want to configure for the role of a resource set. **Note** ◦ This parameter is required if you enable the secret level access feature in the security policy and set the **Management Permissions** parameter to Resource Sets. ◦ The security level of the current operation role must be higher than or equal to the security level of the role that you are creating.
Custom Policy	The status of the custom policy. Valid values: ○: disables the feature. Custom policies are not supported. ●: enables the feature. Custom policies are supported.

6. In the **Manage Permissions** step, configure the parameters and click **Next**.

   In this step, you can specify the management operations that this role can perform in the Apsara Uni-manager Management Console, such as operations on organizations, users, and resource sets.

   > **Important**
   >
   > If you set the Management Permissions parameter to Resource Sets, the role has the read-only permissions but does not have the write permissions.

7. In the **Application permissions** step, configure the parameters and click **Next**.

   In this step, you can specify the operations that this role can perform on cloud products. If you need to only grant the user the permissions to view ECS instances, you need to only select View instance in the ECS section.

   > **Important**
   >
   > The system selects the required permissions that the specified operation depends on. If you remove the dependency, the operation may fail.

8. In the **Menu permissions** step, configure the parameters and click **Next**.

   In this step, you can specify the menu items that are available to this role.

   > **Important**
   >
   > To authorize a role in the Apsara Uni-manager Management Console, you must select management permissions, application permissions, and menu permissions. Otherwise, the role cannot access the corresponding pages.

9. Optional. In the **Custom Policy** step, configure the parameters and click **Create**.

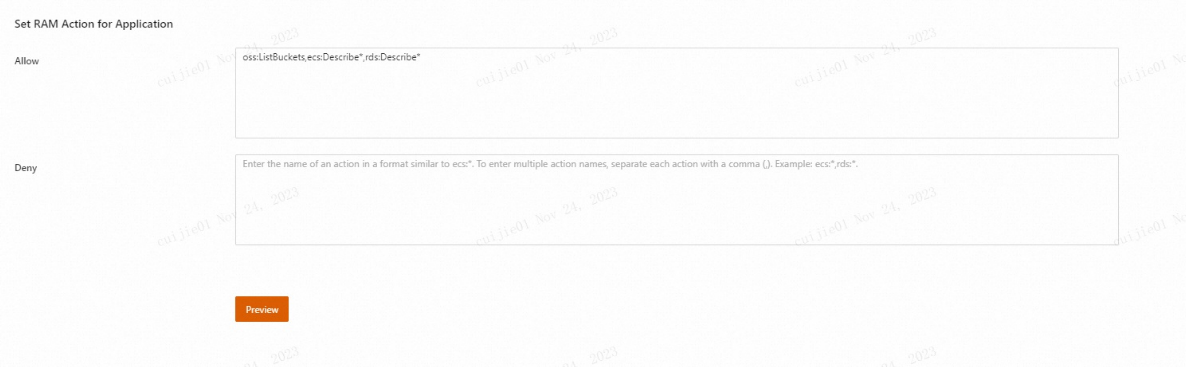
> **Important**
>
> The Custom Policy step is available only if you turn on Custom Policy in the Basic configuration step.

You can configure RAM actions to precisely describe authorized resources and operations on these resources. The Set RAM Action for Application section contains two parts: Allow and Deny. In the Allow field, you can specify the operations that are allowed to perform. In the Deny field, you can specify the operations that are not allowed to perform. If a RAM policy includes both an Allow statement and a Deny statement, the Deny statement takes precedence over the Allow statement.

A RAM action is specified in the <ram-code>:<action-name> format. Separate multiple actions with commas (,).

- <ram-code> indicates the RAM code of the cloud service, which is generally the code of the cloud service.
- <action-name> indicates the name of an open API operation of the cloud service.

If you specify `oss:ListBuckets,ecs:Describe*,rds:Describe*` in the Allow field, this role can list all the Object Storage Service (OSS) buckets, call all Elastic Compute Service (ECS) API operations whose names start with Describe, and call all ApsaraDB RDS API operations whose names start with Describe.



Set RAM Action for Application

Allow: oss:ListBuckets,ecs:Describe*,rds:Describe*

Deny: Enter the name of an action in a format similar to ecs:*. To enter multiple action names, separate each action with a comma (,). Example: ecs:*,rds:*.

0. In the **Create Custom Role** message, click **Complete**.

   You can also click **Authorize now** to assign the role to users or user groups on the **Authorized Personnel** tab.

Create RAM role-based authorization

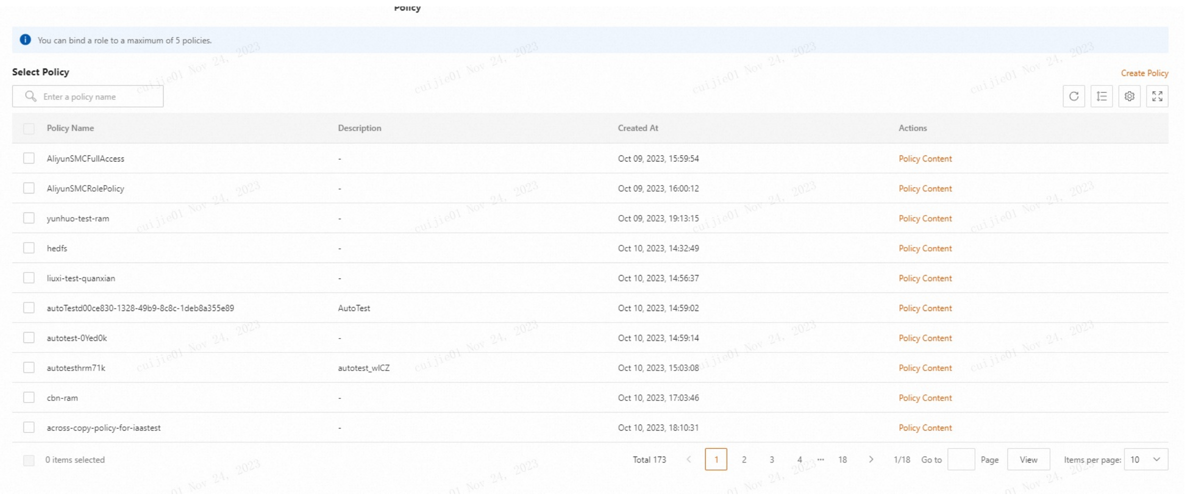
1. Click Create Custom Role. On the **Role Permissions** page that appears, click **Advanced Settings** at the lower part and click **Create RAM Role & Attach Policy** .
2. In the **Basic Configurations** step, configure the parameters and click **Next**.

Parameter	Description
Role Name	The name of the RAM role-based authorization.
Description	The description of the RAM role-based authorization. This parameter is optional.

Sharing Scope	The scope in which the RAM role-based authorization is available. You can select only **Global** when you create the RAM role-based authorization as an operations administrator. Valid values: ◦ Global: The RAM role-based authorization is shared by all organizations. ◦ Current Organization: The RAM role-based authorization is shared within the current organization. ◦ Subordinate Organization: The RAM role-based authorization is shared by the current organization and its subordinate organizations.

3. In the **Configure Custom Policy** step, select policies and click **Next**.

   If none of the listed policies meets your requirements, you can click **Create Policy** in the upper-right corner of the Select Policy section to create one. You can click **Policy Content** in the **Actions** column of a policy to view JSON-formatted policy content.



Policy

You can bind a role to a maximum of 5 policies.

Select Policy

Create Policy

Enter a policy name

□	Policy Name	Description	Created At	Actions
□	AliyunSMCFullAccess	-	Oct 09, 2023, 15:59:54	Policy Content
□	AliyunSMCRolePolicy	-	Oct 09, 2023, 16:00:12	Policy Content
□	yunhuo-test-ram	-	Oct 09, 2023, 19:13:15	Policy Content
□	hedfs	-	Oct 10, 2023, 14:32:49	Policy Content
□	liuxi-test-quanxian	-	Oct 10, 2023, 14:56:37	Policy Content
□	autoTestd00ce830-1328-49b9-8c8c-1deb8a355e89	AutoTest	Oct 10, 2023, 14:59:02	Policy Content
□	autotest-0Yed0k	-	Oct 10, 2023, 14:59:14	Policy Content
□	autotesthrm71k	autotest_wlCZ	Oct 10, 2023, 15:03:08	Policy Content
□	cbn-ram	-	Oct 10, 2023, 17:03:46	Policy Content
□	across-copy-policy-for-iaastest	-	Oct 10, 2023, 18:10:31	Policy Content

□ 0 items selected

4. In the **Configure Trust Policy** step, configure the **Trust Organization** and **Trust Cloud Service** parameters and click **Next**.

   A trust policy is used to define the entities that can assume this RAM role. For example, you can specify level-1 organizations (tenant accounts) and Apsara Stack services to assume this RAM role.

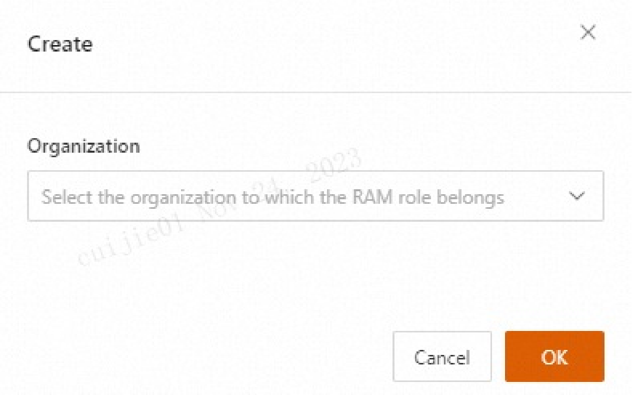
   > **Note**
   >
   > If you enable the Open ID Connect (OIDC) feature, you can also authorize an OIDC provider to assume the RAM role and configure the Limits parameter.

   - **Trust Organization**: Specify one or more level-1 organizations (tenant accounts) to assume this RAM role.
   - **Trust Cloud Service**: Specify one or more Apsara Stack services to assume this RAM role.

5. In the Preview Policy step, check the selected policies and the trust policy and click **Create**.

6. In the role list, find the RAM role template you created and click its name.

7. On the page that appears, click the **RAM Role** tab, click **Create**, and then select a level-1 organization to create a RAM role instance.

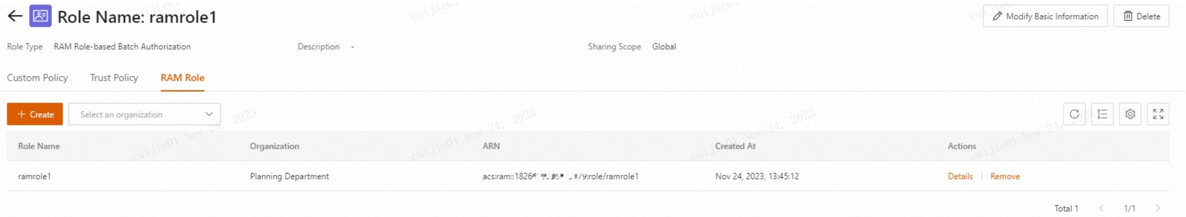


Create

Organization

Select the organization to which the RAM role belongs

8. After the RAM role instance is generated, the trust entities in the trust policy can assume this RAM role to access and manage the corresponding resources.



Role Name: ramrole1

Role Type RAM Role-based Batch Authorization

Description -

Sharing Scope Global

Select an organization

Role Name	Organization	ARN	Created At	Actions
ramrole1	Planning Department	acs:ram::1826[redacted]9:role/ramrole1	Nov 24, 2023, 13:45:12	Details | Remove

Total 1 1/1

Create RAM-based authorization

1. Click **Create Custom Role**. On the page that appears, click **Advanced Settings** at the lower part and click **Create RAM Authorization**.
2. Configure the parameters in the **Basic Information** step.

Parameter	Description
Role Name	The name of the RAM-based authorization.
Description	The description of the RAM-based authorization. This parameter is optional.
Sharing Scope	The scope in which the RAM-based authorization is available. Only **Global** is available when you create the RAM-based authorization as an operations administrator. ◦ **Global**: The RAM-based authorization is shared by all organizations. ◦ **Current Organization**: The RAM-based authorization is shared within the current organization. ◦ **Subordinate Organization**: The RAM-based authorization is shared by the current organization and its subordinate organizations.

3. Click **Create and Configure RAM Authorization**. In the **Role Permissions** step, configure the authorization.
   - **User Groups**: Configure the users to which you want to attach the policy. You can add or remove user groups.

- **Add a user group**
  a. Click the **User Groups** tab.
  b. Click **Add User Group**. In the **Add User Group** dialog box, select a user group and click **OK**.
- **Remove a user group**
  a. Click the **User Groups** tab.
  b. Find the user group that you want to manage and click **Remove** in the **Actions** column to remove the user group.

- **Permissions**: Configure access permissions on resources. You can add or remove permissions.
  - **Add a policy**
    a. Click the **Permissions** tab.
    b. Click **Add Policy**. In the **Add Policy** dialog box, select policies and click **OK**. If the listed policies do not meet your requirements, you can create a policy.
  - **Remove a policy**
    a. Find the permission that you want to manage and click **Remove permissions** in the **Actions** column.
    b. In the message that appears, click **OK**.

4. Click **OK**.

4.4.2.4. Manage roles

You can change the permissions and status of a role to change the permissions and logon status of the users that are assigned this role.

Limits

- Preset roles cannot be modified or deleted.
- Resource Access Management (RAM)-based batch authorization roles and RAM role-based batch authorization roles cannot be disabled, enabled, or copied.
- Before you delete a role, make sure that no users or user groups are associated with the role.
- If a role is locked, the role cannot be modified, deleted, disabled, or enabled. In addition, a locked role cannot be used to authorize users.
- Only custom roles support batch authorization.

View the details of a role

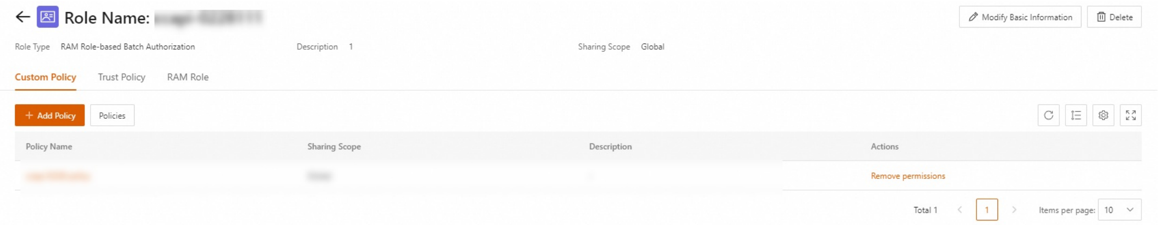
View the basic information and permissions of a role.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **Role Permissions**.
4. On the Role Permissions page, find the role that you want to view and c lick its name to go to the role details page and view the role details.
5. View the details of the role.
   - **View the details of a preset role or a custom role**

Click the **Management Permissions**, **Application Permissions**, **Menu Permissions**, and **Authorized Personnel** tabs to view the details of different permissions.

- **View the details of a RAM role-based batch authorization role**

  Click the **Custom Policy**, **Trust Policy**, and **RAM Role** tabs to view the information about the added policies, trust policy, and RAM roles.



Role Name: [redacted]

Role Type RAM Role-based Batch Authorization

Description 1

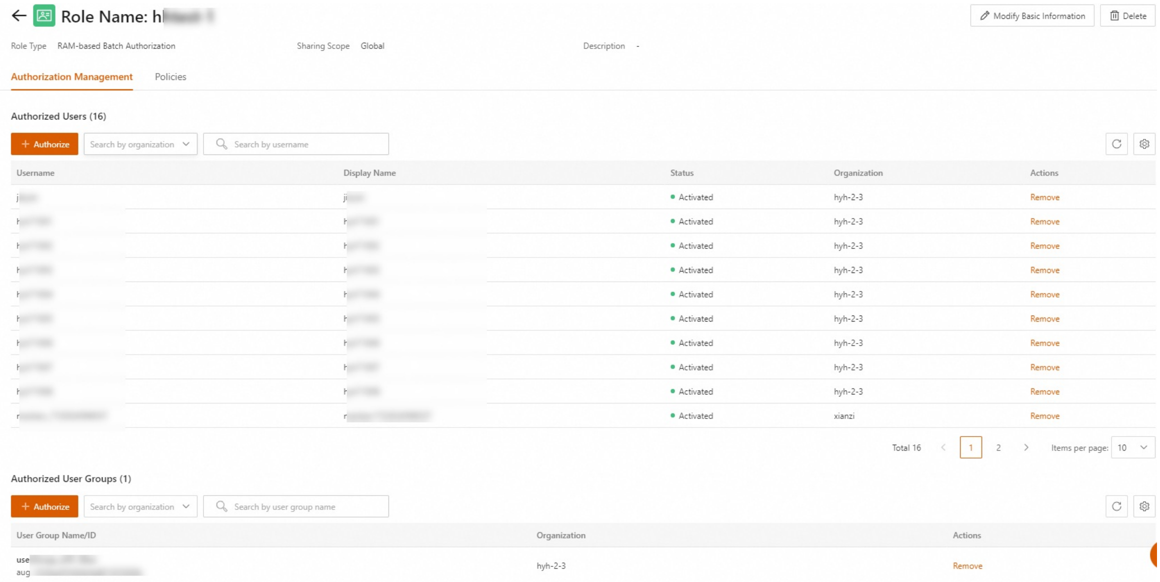
Sharing Scope Global

Policy Name	Sharing Scope	Description	Actions
[redacted]	[redacted]	[redacted]	Remove permissions

Total 1 1 Items per page: 10

- **View the details of a RAM-based batch authorization role**

  Click the **User Groups** and **Permissions** tabs to view the authorized user groups and policies.



Role Name: h[redacted]

Role Type RAM-based Batch Authorization

Sharing Scope Global

Description -

Authorized Users (16)

Username	Display Name	Status	Organization	Actions
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	hyh-2-3	Remove
[redacted]	[redacted]	● Activated	xianzi	Remove

Total 16 1 2 Items per page: 10

Authorized User Groups (1)

User Group Name/ID	Organization	Actions
use[redacted] aug[redacted]	hyh-2-3	Remove

Modify role information

You can update the basic information and permissions of a role.

> **Note**
>
> Preset roles cannot be modified.

1. On the **Role Permissions** page, find the role that you want to manage and click **Modify** in the Actions column.
2. On the page that appears, click **Modify Basic Information** in the upper-right corner.
3. Modify the permissions of the role.
   - **Modify the permissions of a custom role**

     Click the **Management Permissions**, **Application Permissions**, **Menu Permissions**, and **Authorized Personnel** tabs to modify the corresponding permissions.
   - **Modify the permissions of a RAM role-based batch authorization role**

        - On the **Custom Policy** tab, add or remove policies based on your business requirements.
        - On the **Trust Policy** tab, modify the values of the Trust Organization and Trust Cloud Service parameters.
        - On the **RAM Role** tab, add or remove RAM roles based on your business requirements.
    - **Modify the permissions of a RAM-based batch authorization role**
        - On the **User Groups** tab, add or remove user groups based on your business requirements.
        - On the **Permissions** tab, add or remove policies based on your business requirements.

Disable a role

When a role is disabled, all permissions of the role are revoked. All users associated with the role cannot log on to the console.

> **Note**
>
> RAM role-based batch authorization roles and RAM-based batch authorization roles cannot be disabled.

1. On the **Role Permissions** page, find the role that is in the **Enabled** state and you want to manage and click **Disable** in the Actions column.
2. In the message that appears, click **OK**.

Enable a role

You can enable a disabled role. After the role is enabled, all users associated with the role acquire the permissions of the role.

> **Note**
>
> RAM role-based batch authorization roles and RAM-based batch authorization roles cannot be enabled.

1. On the **Role Permissions** page, find the role that is in the **Disabled** state and you want to manage and click **Enable** in the Actions column.

Copy a role

> **Note**
>
> RAM role-based batch authorization roles and RAM-based batch authorization roles cannot be copied.

When you copy a role, a new role with the same sharing scope, management permissions, application permissions, and menu permissions is created. You can adjust the permissions of the new role based on your business requirements.

1. On the **Role Permissions** page, find the role that you want to copy, click the ··· icon in the Actions column, and then click **Copy**.
2. Modify the basic configurations, management permissions, application permissions, and menu permissions of the new role based on your business requirements.

> **Note**
>
> The name of the new role cannot be the same as that of the role that you copy.

Delete a role

You can delete a role if you no longer need it.

> **Note**
>
> - Preset roles cannot be deleted.
> - Before you delete a role, make sure that no users or user groups are associated with the role.

1. On the **Role Permissions** page, find the role that you want to delete, click the ··· icon in the Actions column, and then click **Delete**.
2. In the message that appears, click **OK**.

Lock a role

If an external system is associated with a role, you can lock the role.

> **Important**
>
> If a role is locked, the role cannot be modified, deleted, disabled, or enabled. In addition, a locked role cannot be used to authorize users.

1. On the **Role Permissions** page, find the role that you want to manage, click the ··· icon in the Actions column, and then click **Locked**.
2. In the message that appears, click **OK**.

Unlock a role

If a role is locked, you can unlock the role.

> **Important**
>
> If a locked role is associated with an external system, issues related to external system permissions and data synchronization may occur when you forcefully unlock the role. Proceed with caution.

1. On the **Role Permissions** page, find the role that you want to manage, click the ··· icon in the Actions column, and then click **Unlock**.
2. In the message that appears, click **OK**.

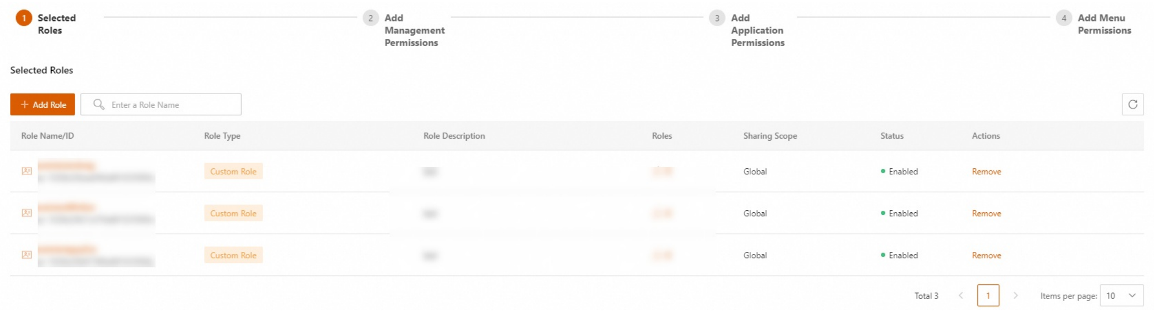
Grant permissions to multiple roles at a time

In specific service upgrade scenarios, new permissions are required to be granted to roles of a specific type. You can grant the permissions to multiple roles at a time to improve your work efficiency.

> **Important**

> In this case, new permissions are granted to the roles without reducing or overwriting the existing permissions of the roles.
>
> - If the selected roles do not have the new permissions, the permissions are added.
> - If the selected roles have the new permissions, the existing permissions are not affected.

1. On the **Role Permissions** page, select **Custom Role** from the **Role Type** drop-down list.
2. Select multiple custom roles to which you want to grant permissions.
3. Click **Add Permissions** in the lower-left corner of the page. In the message that appears, click **OK**.
4. Perform the following steps to grant permissions to the selected roles:
    i. **Selected Roles**: Confirm the selected custom roles.
        - If you want to add roles, you can click **Add Role**.
        - If you want to delete a selected role, find the role that you want to manage and click **Remove** in the **Actions** column.



Selected Roles

Role Name/ID	Role Type	Role Description	Roles	Sharing Scope	Status	Actions
[redacted]	Custom Role	[redacted]	[redacted]	Global	● Enabled	Remove
[redacted]	Custom Role	[redacted]	[redacted]	Global	● Enabled	Remove
[redacted]	Custom Role	[redacted]	[redacted]	Global	● Enabled	Remove

Total 3 < 1 > Items per page: 10

    ii. **Add Management Permissions**: Select the management permissions that you want to add to the selected roles.
    iii. **Add Application Permissions**: Select the operations permissions on products that you want to add to the selected roles.
    iv. **Add Menu Permissions**: Select the menu permissions that you want to add to the selected roles.
5. Optional. After the Batch Role Authorization task is created, go to the Asynchronous Task page to view the execution details of the task.

Manage multi-cloud roles

1. On the **Role Permissions** page, click the required multi-cloud role tab.
2. View and manage multi-cloud roles.
    - **Multi-cloud roles for Apsara Stack**

      On the multi-cloud role tab for Apsara Stack, view the Apsara Stack roles that are connected. You can view only the roles that have the permissions to manage resource sets.
    - **Multi-cloud roles for the Alibaba Cloud public cloud**

      On the multi-cloud role tab for the Alibaba Cloud public cloud, view and manage the connected public cloud roles.

- **Create a RAM role**

  a. Click **Create RAM Role**.

  b. In the Create RAM Role dialog box, configure the Resource Access Management (RAM) role and click **OK**. After the RAM role is created, you have the permissions of the RAM role.

Parameter	Description
Role Name	Specify the name of the RAM role for the Alibaba Cloud public cloud. The name can be up to 64 characters in length.
Organization	Select an organization that is bound to the Alibaba Cloud public cloud from the drop-down list.
Bind User	Select a user that has been bound to an Alibaba Cloud public cloud organization from the drop-down list to authorize the user to use the RAM role.
Remarks	Enter the description of the RAM role.
Permission Policy	Select the policy of the RAM role. You can select multiple policies.

- **View information about a RAM role**

  a. In the RAM role list, view the RAM role that you create. You can view information such as Role Name, Authorized Object, Description, and Created At.

  b. Find the RAM role that you want to view and click **View** in the Actions column. In the panel that appears, view the policy that is attached to the RAM role.

- **Update a RAM role**

  a. In the role list, find the RAM role that you want to update and click **Update** in the Actions column.

  b. In the dialog box that appears, update the description and policy of the RAM role and click **OK**.

- **Delete a RAM role**

  a. In the RAM role list, find the RAM role that you want to delete and click **Delete** in the Actions column.

  b. In the dialog box that appears, click **Delete**. After you delete a RAM role, the permissions granted to the RAM role become unavailable.

4.4.2.5. Limits on roles

Limits on the management scope of resource sets

If you select Resource Sets for Management Permissions when you create a custom role, the role has permissions on the resource sets of the associated user by default. This role is mainly used to manage resources. The permissions described in the following table are beyond the management scope of resource sets and do not take effect even if you select them.

Management permission	Description
User management	Create, delete, enable, disable, lock, unlock, and manage users.
Role management	Create, delete, lock, unlock, and manage roles.
User group management	View, create, delete, and manage user groups.
Organization management	Create, delete, and manage organizations.
Resource set management	Create and delete resource sets.
AccessKey management	View the AccessKey pairs of organizations and users, create AccessKey pairs for organizations, delete, enable, and disable the AccessKey pairs of organizations, and view AccessKey logs.
Access policy	Create, delete, and manage access policies.
Change management	Change resource sets, resources, or users.
Bill management	View the bills of cloud services, organizations, and resource sets, and export and modify bills.
Service-linked role	Create service-linked roles.
Process management	View organization applications.
Multi-cloud management platform hosting	Configure multi-cloud management platform hosting.
Announcement	Manage announcements.

4.4.2.6. Examples

4.4.2.6.1. Example: Create a custom role with ECS read-only permissions

Background information

Company A (level-1 organization) needs to grant only view permissions on Elastic Compute Service (ECS) resources to an ECS resource administrator named Administrator A. This way, Administrator A can view all ECS resources of the company to implement O&M.

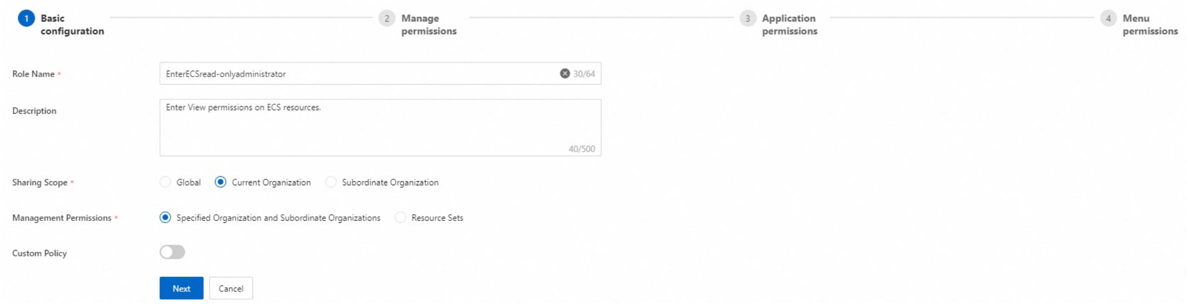
Planning

As an O&M engineer for ECS resources of the company, Administrator A needs to view all ECS resources of the company. In this case, you can create a custom role, set the management scope of the role to the level-1 organization and its subordinate organizations, grant only view permissions on ECS resources to the role, and then add menu permissions for accessing ECS resources.

Procedure

By default, the level-1 organization administrator of Company A is Organization A. The following section describes how to create a custom role as Organization A.

1. Log on to the Apsara Uni-manager Management Console as Organization A.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions > Role Permissions**.
4. On the **Role Permissions** page, click **Create Custom Role**.
5. On the Basic configuration wizard page, specify the required parameters and click **Next**.
   - **Role Name**: Enter ECS read-only administrator.
   - **Description**: Enter View permissions on ECS resources.
   - **Sharing Scope**: Select Current Organization.
   - **Management Permissions**: Select Specified Organization and Subordinate Organizations.



Role Name *: EnterECSread-onlyadministrator 30/64

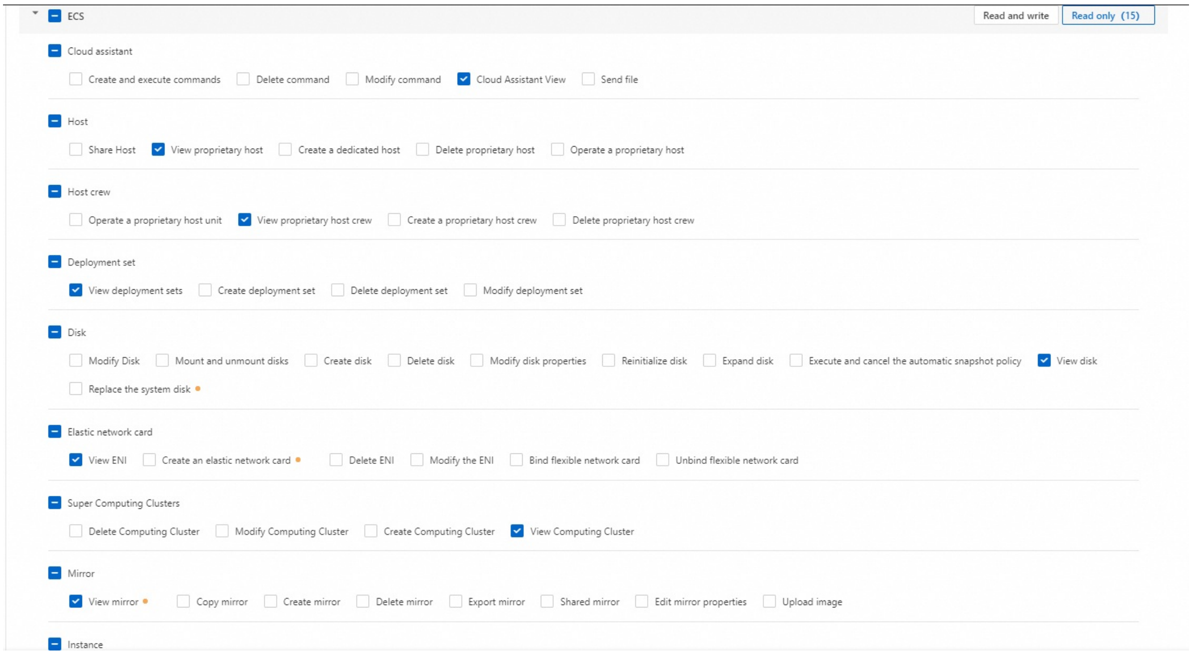
Description: Enter View permissions on ECS resources. 40/500

Sharing Scope *: ○ Global ● Current Organization ○ Subordinate Organization

Management Permissions *: ● Specified Organization and Subordinate Organizations ○ Resource Sets

Custom Policy: ○

6. On the **Manage permissions** wizard page, you can specify parameters to allow the role to perform specific operations on specific organizations or specific resource sets in the console. You can skip this step and click **Next** when you create an ECS read-only role.
7. On the **Application permissions** wizard page, search for **ECS** in the Cloud products section. Select the desired view permissions on ECS resources or click **Read only** in the upper-right corner of the section. Then, click **Next**.



☐ ECS — Read and write | Read only (15)

☐ Cloud assistant

☐ Create and execute commands ☐ Delete command ☐ Modify command ☑ Cloud Assistant View ☐ Send file

☐ Host

☐ Share Host ☑ View proprietary host ☐ Create a dedicated host ☐ Delete proprietary host ☐ Operate a proprietary host

☐ Host crew

☐ Operate a proprietary host unit ☑ View proprietary host crew ☐ Create a proprietary host crew ☐ Delete proprietary host crew

☐ Deployment set

☑ View deployment sets ☐ Create deployment set ☐ Delete deployment set ☐ Modify deployment set

☐ Disk

☐ Modify Disk ☐ Mount and unmount disks ☐ Create disk ☐ Delete disk ☐ Modify disk properties ☐ Reinitialize disk ☐ Expand disk ☐ Execute and cancel the automatic snapshot policy ☑ View disk

☐ Replace the system disk

☐ Elastic network card

☑ View ENI ☐ Create an elastic network card ☐ Delete ENI ☐ Modify the ENI ☐ Bind flexible network card ☐ Unbind flexible network card

☐ Super Computing Clusters

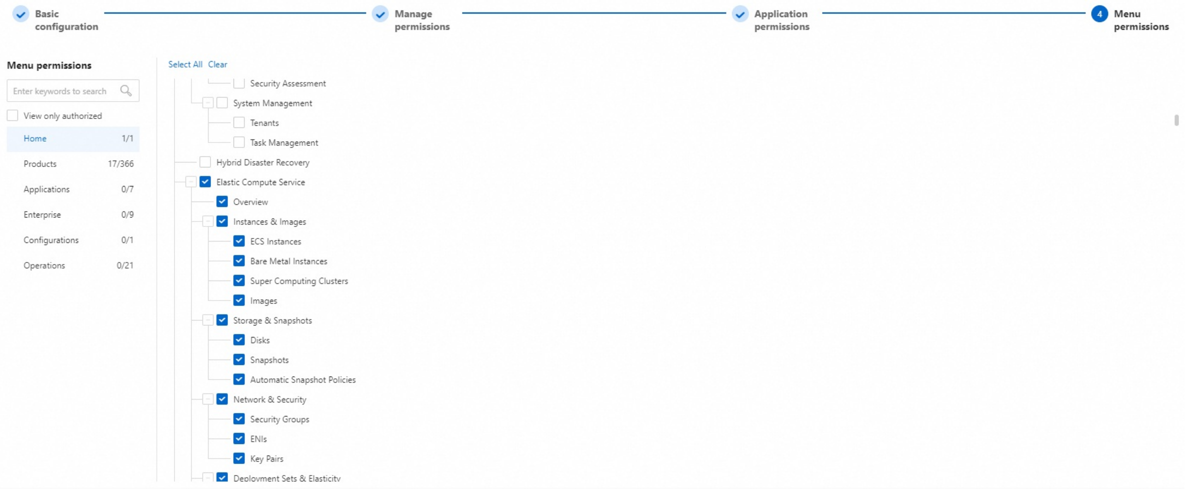
☐ Delete Computing Cluster ☐ Modify Computing Cluster ☐ Create Computing Cluster ☑ View Computing Cluster

☐ Mirror

☑ View mirror ☐ Copy mirror ☐ Create mirror ☐ Delete mirror ☐ Export mirror ☐ Shared mirror ☐ Edit mirror properties ☐ Upload image

☐ Instance

8. On the **Menu permissions** wizard page, add menus for accessing ECS resources. Otherwise, the user associated with the role cannot see the menus for accessing ECS resources after the user logs on to the console.



Menu permissions

Enter keywords to search

☐ View only authorized

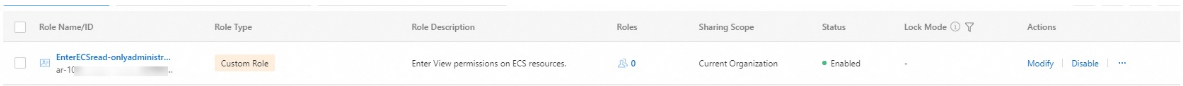
Home	1/1
Products	17/366
Applications	0/7
Enterprise	0/9
Configurations	0/1
Operations	0/21

Select All Clear

```
    ☐ Security Assessment
  ☐ System Management
    ☐ Tenants
    ☐ Task Management
☐ Hybrid Disaster Recovery
☑ Elastic Compute Service
  ☑ Overview
  ☑ Instances & Images
    ☑ ECS Instances
    ☑ Bare Metal Instances
    ☑ Super Computing Clusters
    ☑ Images
  ☑ Storage & Snapshots
    ☑ Disks
    ☑ Snapshots
    ☑ Automatic Snapshot Policies
  ☑ Network & Security
    ☑ Security Groups
    ☑ ENIs
    ☑ Key Pairs
  ☑ Deployment Sets & Elasticity
```

9. After you add the menus for accessing ECS resources, click **Create**. The administrator role with ECS read-only permissions is created.

After the role is created, you can associate the role with the desired user Administrator A. This way, Administrator A can view all ECS resources of Company A.



☐	Role Name/ID	Role Type	Role Description	Roles	Sharing Scope	Status	Lock Mode	Actions
☐	EnterECSread-onlyadministr... ar-10[redacted]..	Custom Role	Enter View permissions on ECS resources.	0	Current Organization	● Enabled	-	Modify | Disable | ···

4.4.2.6.2. Example: Modify a custom role with ECS read-only permissions

Background information

Due to the business changes of Company A, Administrator A not only needs to view all Elastic Compute Service (ECS) resources of Company A but also needs to view all Virtual Private Cloud (VPC) resources of Company A. The ECS read-only role of Administrator A is created. For more information, see Example: Create a custom role with ECS read-only permissions.

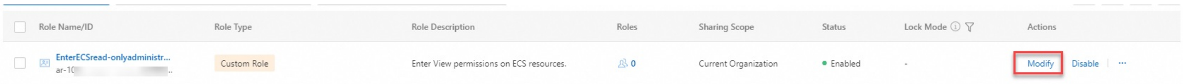
Planning

To allow the ECS read-only role to view all VPC resources of Company A, you can grant read-only permissions on VPC resources to the role.

Procedure

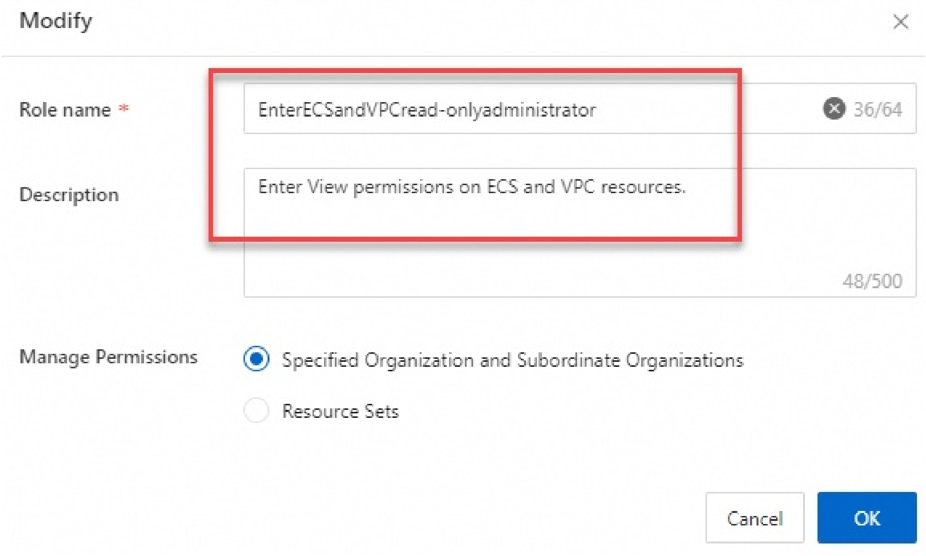
By default, the level-1 organization administrator of Company A is Organization A. The following section describes how to modify a custom role as Organization A.

1. Log on to the Apsara Uni-manager Management Console as Organization A.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions > Role Permissions**.
4. On the **Role Permissions** page, click the created ECS read-only role.
5. Click **Modify** in the **Actions** column that corresponds to the role.



□	Role Name/ID	Role Type	Role Description	Roles	Sharing Scope	Status	Lock Mode	Actions
□	EnterECSread-onlyadministr... ar-10 [redacted] ..	Custom Role	Enter View permissions on ECS resources.	0	Current Organization	● Enabled	-	Modify Disable ···

6. On the details page of the role, modify the basic information and grant VPC read-only permissions to the role.
   - Modify basic information: Change the role name to ECS and VPC read-only administrator and the description of the role to View permissions on ECS and VPC resources. You can click **Modify Basic Information** in the upper-right corner of the page to modify the basic information about the role.



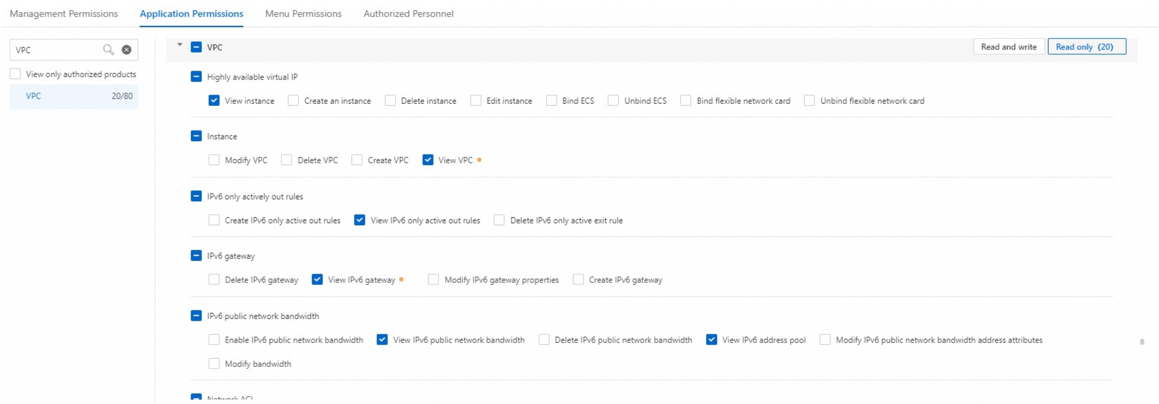
Modify

Role name * EnterECSandVPCread-onlyadministrator 36/64

Description Enter View permissions on ECS and VPC resources. 48/500

Manage Permissions ● Specified Organization and Subordinate Organizations ○ Resource Sets

   - Add read-only permissions on VPC resources: Click the **Application Permissions** tab. Enter VPC in the search box below the Cloud products section and select the desired view permissions on ECS resources or click **Read only** in the upper-right corner of the tab.



Management Permissions | Application Permissions | Menu Permissions | Authorized Personnel

VPC

☐ View only authorized products

VPC 20/80

VPC — Read and write | Read only (20)

Highly available virtual IP
- ☑ View instance ☐ Create an instance ☐ Delete instance ☐ Edit instance ☐ Bind ECS ☐ Unbind ECS ☐ Bind flexible network card ☐ Unbind flexible network card

Instance
- ☐ Modify VPC ☐ Delete VPC ☐ Create VPC ☑ View VPC

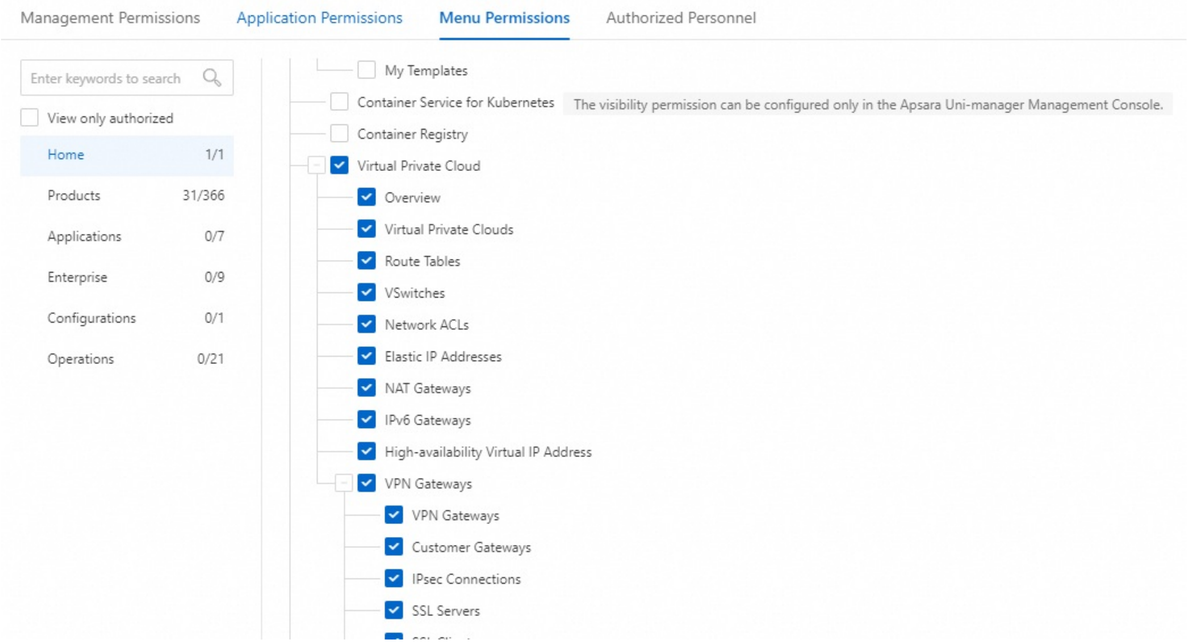
IPv6 only actively out rules
- ☐ Create IPv6 only active out rules ☑ View IPv6 only active out rules ☐ Delete IPv6 only active exit rule

IPv6 gateway
- ☐ Delete IPv6 gateway ☑ View IPv6 gateway ☐ Modify IPv6 gateway properties ☐ Create IPv6 gateway

IPv6 public network bandwidth
- ☐ Enable IPv6 public network bandwidth ☑ View IPv6 public network bandwidth ☐ Delete IPv6 public network bandwidth ☑ View IPv6 address pool ☐ Modify IPv6 public network bandwidth address attributes
- ☐ Modify bandwidth

Network ACL

7. On the **Menu Permissions** tab, select menus for accessing VPC resources.



Management Permissions | Application Permissions | Menu Permissions | Authorized Personnel

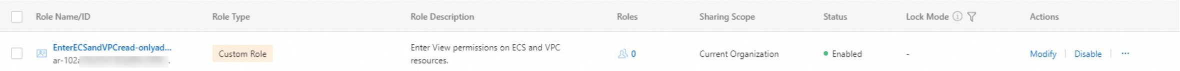
Enter keywords to search

☐ View only authorized

Home	1/1
Products	31/366
Applications	0/7
Enterprise	0/9
Configurations	0/1
Operations	0/21

- ☐ My Templates
- ☐ Container Service for Kubernetes — The visibility permission can be configured only in the Apsara Uni-manager Management Console.
- ☐ Container Registry
- ☑ Virtual Private Cloud
  - ☑ Overview
  - ☑ Virtual Private Clouds
  - ☑ Route Tables
  - ☑ VSwitches
  - ☑ Network ACLs
  - ☑ Elastic IP Addresses
  - ☑ NAT Gateways
  - ☑ IPv6 Gateways
  - ☑ High-availability Virtual IP Address
  - ☑ VPN Gateways
    - ☑ VPN Gateways
    - ☑ Customer Gateways
    - ☑ IPsec Connections
    - ☑ SSL Servers

8. Click **Update** to modify the ECS read-only role. View the modified role in the role list.



☐	Role Name/ID	Role Type	Role Description	Roles	Sharing Scope	Status	Lock Mode	Actions
☐	EnterECSandVPCread-onlyad... ar-102[redacted].	Custom Role	Enter View permissions on ECS and VPC resources.	0	Current Organization	● Enabled	-	Modify | Disable | ···

4.4.2.6.3. Use a RAM role to grant users the permissions to restart ECS instances

Background information

You need to use a Resource Access Management (RAM) role to grant O&M Engineer A of a level-1 organization named Company A the permissions to restart all Elastic Compute Service (ECS) instances.

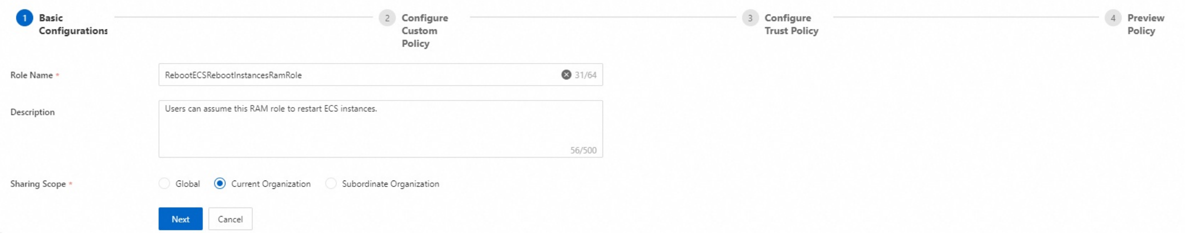
Planning

You can configure a policy that grants the specified role the permissions to restart all ECS instances in RAM role-based authorization, and then configure a trust policy to specify O&M Engineer A to assume this role.

Procedure

By default, the level-1 organization administrator of Company A is orgA. In this example, orgA is used as the organization administrator.

1. Log on to the Apsara Uni-manager Management Console as the organization administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions > Role Permissions**.
4. On the **Role Permissions** page, click **Create Custom Role**.
5. On the page that appears, click **Advanced Settings** and click **Create RAM Role & Attach Policy**.
6. In the **Basic Configurations** step, configure the basic information about the RAM role by referring to the following parameter values and click **Next**.
    - **Role Name**: RebootECSRebootInstancesRamRole
    - **Description**: Users can assume this RAM role to restart ECS instances.
    - **Sharing Scope**: Current Organization



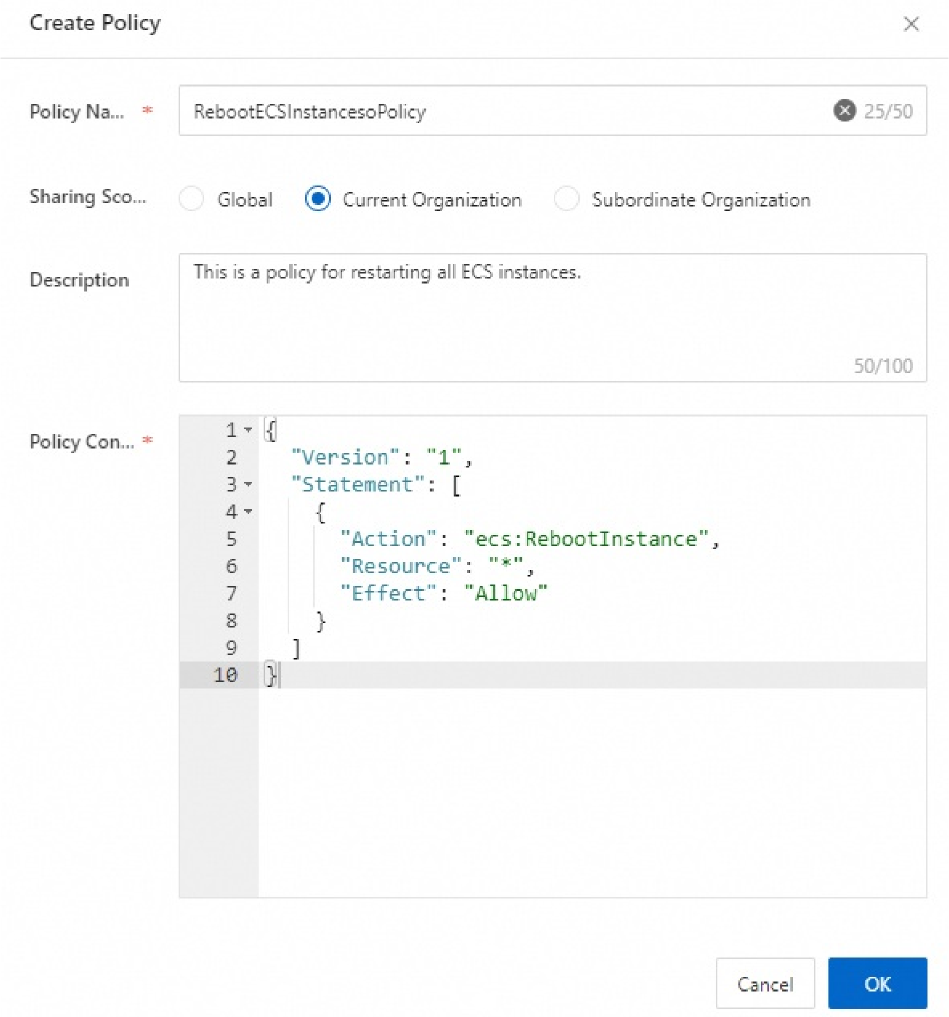
Role Name *: RebootECSRebootInstancesRamRole 31/64

Description: Users can assume this RAM role to restart ECS instances. 56/500

Sharing Scope *: ○ Global ● Current Organization ○ Subordinate Organization

7. In the **Configure Custom Policy** step, click **Create Policy** and create a policy that grants permissions to restart all ECS instances by referring to the following parameter values.
    - **Policy Name**: RebootECSInstancesoPolicy
    - **Sharing Scope**: Current Organization
    - **Description**: This is a policy for restarting all ECS instances.
    - **Policy Content**:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ecs:RebootInstance",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```



Policy Na... * RebootECSInstancesoPolicy 25/50

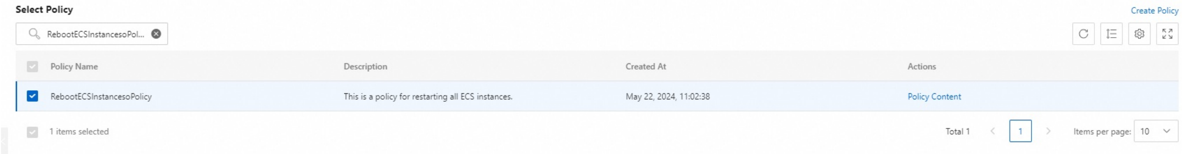
Sharing Sco... ○ Global ● Current Organization ○ Subordinate Organization

Description: This is a policy for restarting all ECS instances. 50/100

Policy Con... *

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ecs:RebootInstance",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

8. In the Select Policy section, select the policy you created and click **Next**.



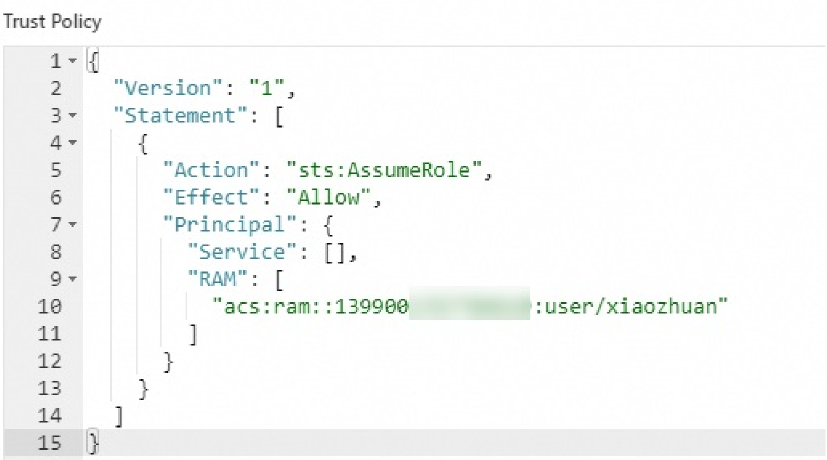
☑	Policy Name	Description	Created At	Actions
☑	RebootECSInstancesoPolicy	This is a policy for restarting all ECS instances.	May 22, 2024, 11:02:38	Policy Content

9. In the **Configure Trust Policy** step, specify O&M Engineer A whose username is xiaozhuan to assume this role.

i. Select Company A from the Trust Organization drop-down list. This grants the permissions to assume this role to all RAM users and RAM roles within the Apsara Stack tenant account of Company A. The Alibaba Cloud Resource Name (ARN) of the Apsara Stack tenant account is automatically filled in the trust policy. Example: `acs:ram::139900176770****:root` .

> **Note**
>
> - ARN format for the Apsara Stack tenant account: `acs:ram::<account-id>:root` , which specifies the RAM users and RAM roles within the Apsara Stack tenant account.
> - ARN format for RAM users: `acs:ram::<account-id>:user/<user-name>` , which specifies the RAM users within the Apsara Stack tenant account.
> - ARN format for RAM roles: `acs:ram::<account-id>:role/<role-name>` , which specifies the RAM roles within the Apsara Stack tenant account.
> - <account-id>: the ID of the Apsara Stack tenant account.

ii. Change the ARN to `acs:ram::139900176770****:user/xiaozhuan` in the trust policy. This grants the permissions only to O&M Engineer A whose username is xiaozhuan.

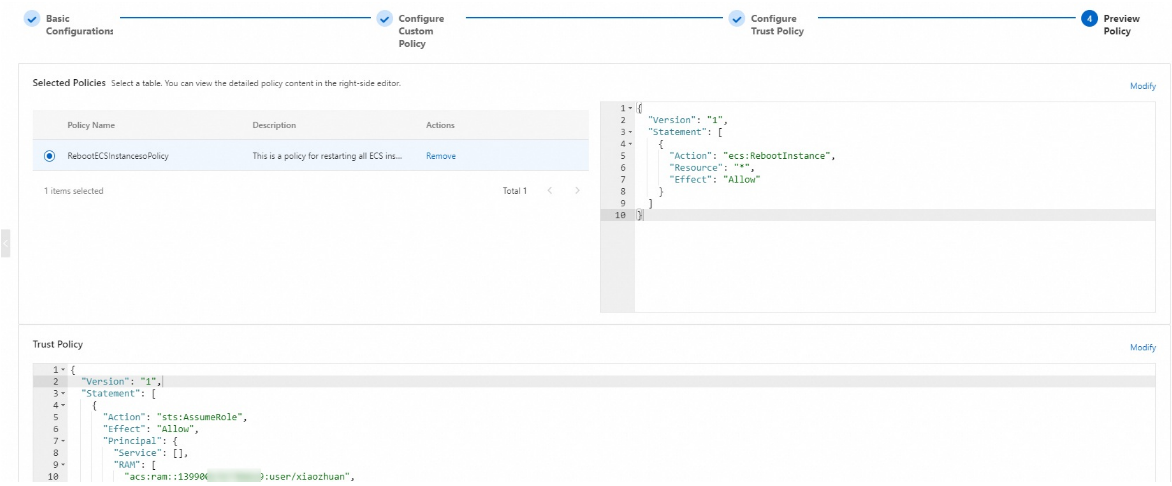


Trust Policy

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [],
        "RAM": [
          "acs:ram::139900[redacted]:user/xiaozhuan"
        ]
      }
    }
  ]
}
```

0. In the Preview Policy step, confirm the policy and the trust policy, and click **Create**.

The RAM role template is created.



Selected Policies Select a table. You can view the detailed policy content in the right-side editor.

	Policy Name	Description	Actions
●	RebootECSInstancesoPolicy	This is a policy for restarting all ECS ins...	Remove

1 items selected Total 1

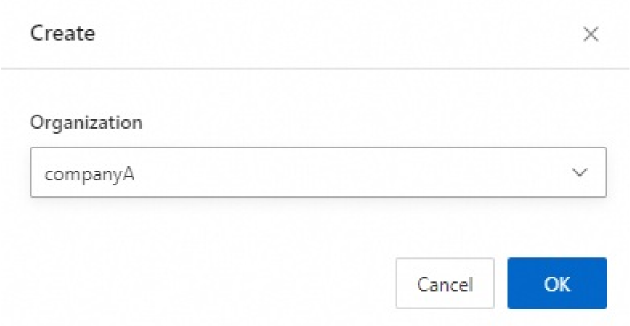
```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ecs:RebootInstance",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

Trust Policy

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [],
        "RAM": [
          "acs:ram::13990[redacted]:user/xiaozhuan",
```

1. On the Role Permissions page, click the name of the RAM role you created.

2. On the role details page, click the **RAM Role** tab and click **Create**. In the dialog box that appears, select Company A from the **Organization** drop-down list and click OK. This way, the RAM role is created within the Apsara Stack tenant account of Company A, and O&M Engineer A whose username is xiaozhuan can assume this role to restart ECS instances.



Create

Organization: companyA

4.4.2.6.4. Example: Use RAM-based authorization to grant users the permissions to view and delete VPC instances

Background information

You need to use RAM-based authorization to grant users in the VPC-Group user group of Company A (level-1 organization) the permissions to view and delete VPC instances.

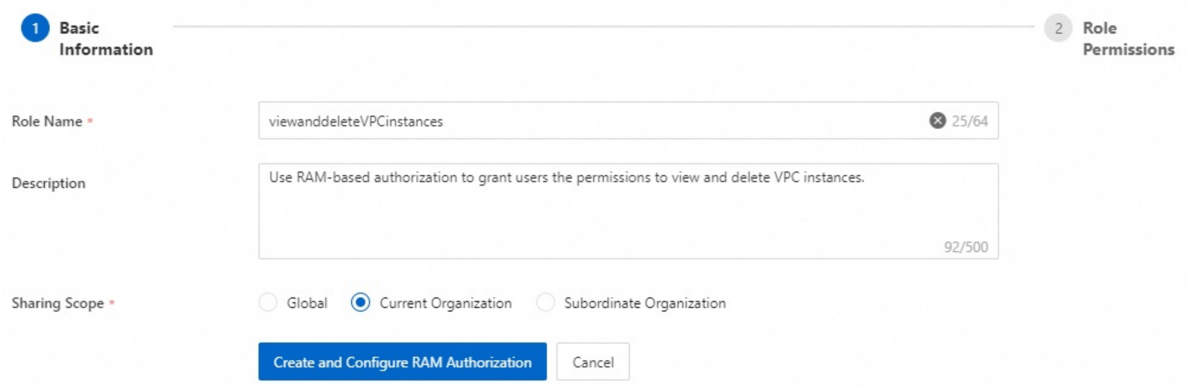
Planning

You can define a policy that contains the permissions to view and delete all VPC instances in RAM-based authorization, and then attach the policy to the user group to grant the users in the user group the permissions.

Procedure

By default, the level-1 organization administrator of Company A is orgA. In the following example, orgA is used as the organization administrator.

1. Log on to the Apsara Uni-manager Management Console as the organization administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions > Role Permissions**.
4. In the upper-left corner of the **Role Permissions** page, click **Create Custom Role**.
5. On the page that appears, expand **Advanced Settings** and click **Create RAM Authorization**.
6. In the **Basic Information** step, configure the parameters and click **Create and Configure RAM Authorization**.
   - **Role Name**: viewanddeleteVPCinstances
   - **Description**: Use RAM-based authorization to grant users the permissions to view and delete VPC instances.
   - **Sharing Scope**: Current Organization



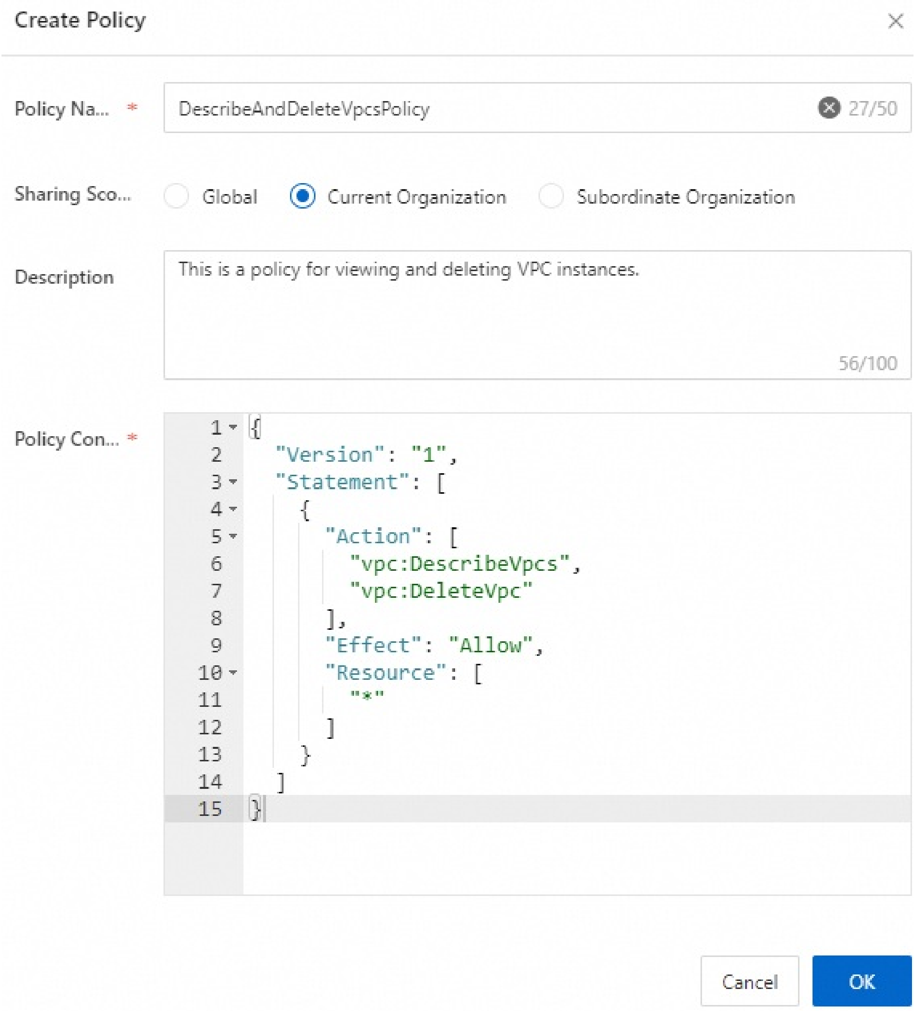
Role Name * viewanddeleteVPCinstances 25/64

Description: Use RAM-based authorization to grant users the permissions to view and delete VPC instances. 92/500

Sharing Scope * ○ Global ● Current Organization ○ Subordinate Organization

7. Click the **Permissions** tab, and click **Add Policy**.
8. In the **Add Policy** dialog box, click **Create Policy**.
   - **Policy Name**: DescribeAndDeleteVpcsPolicy
   - **Sharing Scope**: Current Organization
   - **Description**: This is a policy for viewing and deleting VPC instances.
   - **Policy Content**:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DeleteVpc"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ]
}
```



Create Policy

Policy Na... * DescribeAndDeleteVpcsPolicy 27/50

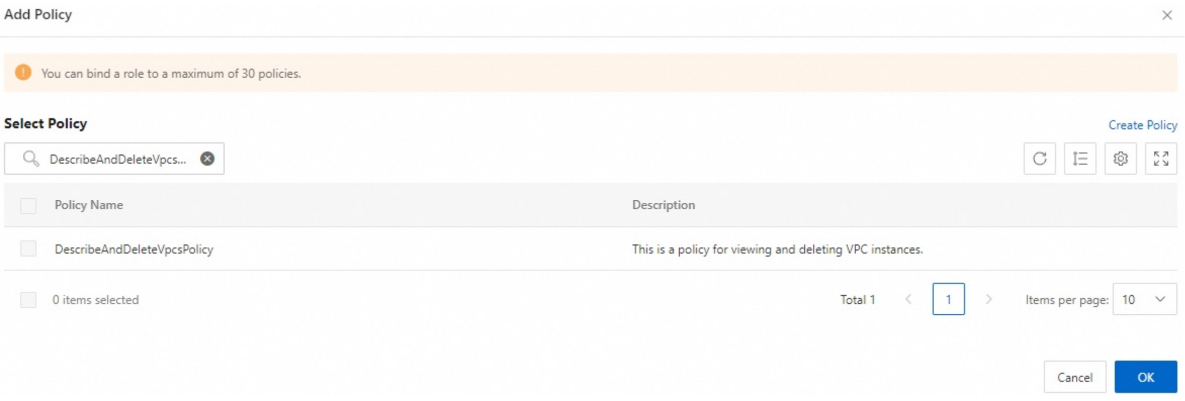
Sharing Sco... ○ Global ● Current Organization ○ Subordinate Organization

Description This is a policy for viewing and deleting VPC instances. 56/100

Policy Con... *

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DeleteVpc"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ]
}
```

9. After the policy is created, select the policy in the Add Policy dialog box and click **OK** to add the policy for the RAM-based authorization.



Add Policy

You can bind a role to a maximum of 30 policies.

Select Policy

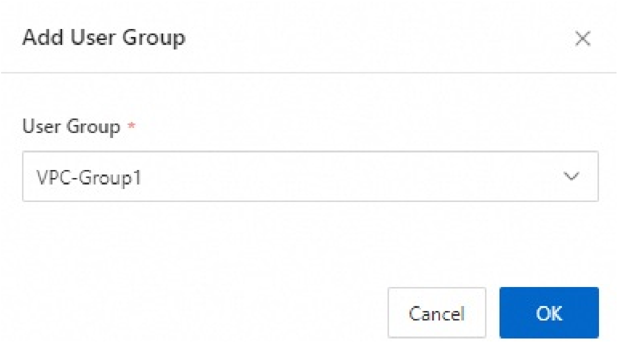
DescribeAndDeleteVpcs...

	Policy Name	Description
□	DescribeAndDeleteVpcsPolicy	This is a policy for viewing and deleting VPC instances.

□ 0 items selected Total 1 Items per page: 10

0. Click the **User Groups** tab, and click **Add User Group**.

1. In the **Add User Group** dialog box, select VPC-Group1 from the drop-down list and click **OK**. The DescribeAndDeleteVpcsPolicy policy is attached to the user group.



Add User Group

User Group *

VPC-Group1

2. On the page that appears, click **OK**. The RAM-based authorization is created, and users in the VPC-Group user group have the permissions to view and delete VPC instances.

4.4.3. Data permissions

On the Data Permissions page, you can authorize specific users to access specific cloud service instances. You can also view and change all data permissions granted to specific users.

Background information

In the Apsara Uni-manager Management Console, you can view and manage the management permissions, application permissions, and menu permissions granted to users. The preceding permissions allow users to manage resource sets or organizations. However, the scopes of the preceding permissions are still not fine-grained enough to meet the business requirements of customers in specific scenarios. Therefore, the Apsara Uni-manager Management Console allows you to grant data permissions to a user on a specific resource instance. This way, you can not only control access to resource sets or resources, but also manage the operations of a specific user on a specific resource instance.

To simplify and optimize data permissions on instances, the Apsara Uni-manager Management Console provides an intuitive and easy-to-use data permission feature. This way, you can grant permissions on cloud service instances to users on the Data Permissions page.

Alternatively, you can create policies to grant permissions to users. In this case, you can grant data permissions to users on cloud services that include the cloud services displayed on the Data Permissions page.

Cloud services that are displayed on the Data Permissions page

You can grant data permissions on the instances of the following cloud services to users on the Data Permissions page: ApsaraMQ, Object Storage Service (OSS), Simple Log Service, DataHub, Container Service for Kubernetes (ACK), Key Management Service (KMS), and Tablestore.

Use cases

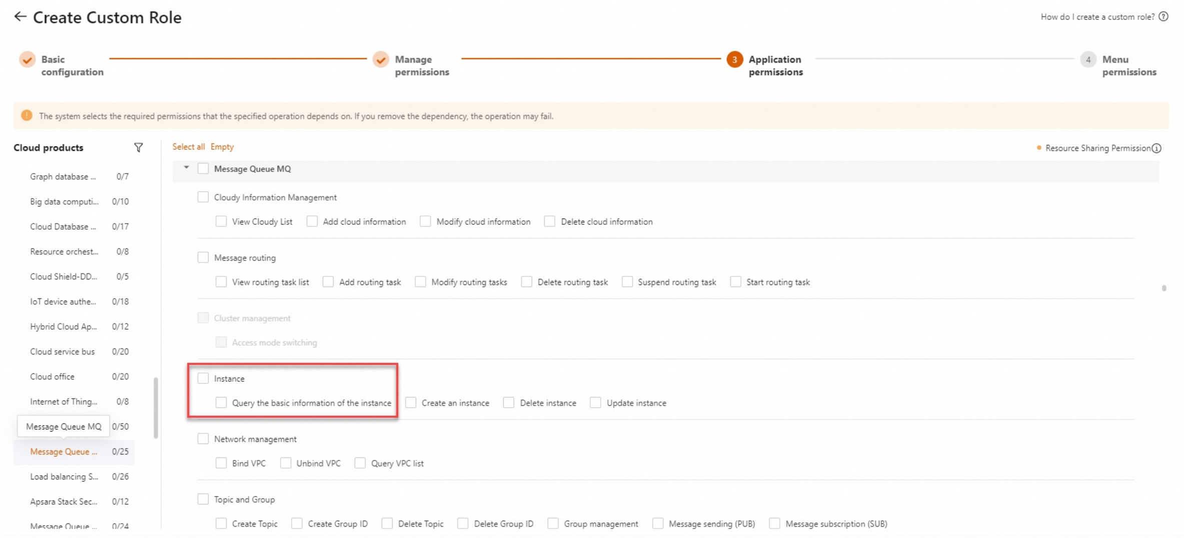
To grant operation permissions on resource instances to users in the console, you can perform the following steps to create a custom role and grant data permissions to the role:

1. Create a custom role to define access permissions on services of resource sets or organizations. For more information, see the "Create a custom role" section of the Create a role topic.

2. Grant access and operation data permissions on specific resource instances. For more information, see the Grant data permissions on specific instances on the Data Permissions page section of this topic.

For example, you can perform the following authorization to grant the view permissions on all ApsaraMQ instances of resource sets and operation permissions on topics or groups in a specific ApsaraMQ instance.

- **First authorization**: You can create a custom role to grant the view permissions on ApsaraMQ instances of resource sets. This way, users can only view all the ApsaraMQ instances of resource sets in the console.



← Create Custom Role

How do I create a custom role?

Basic configuration — Manage permissions — 3 Application permissions — 4 Menu permissions

The system selects the required permissions that the specified operation depends on. If you remove the dependency, the operation may fail.

Cloud products	
Graph database ...	0/7
Big data computi...	0/10
Cloud Database ...	0/17
Resource orchest...	0/8
Cloud Shield-DD...	0/5
IoT device authe...	0/18
Hybrid Cloud Ap...	0/12
Cloud service bus	0/20
Cloud office	0/20
Internet of Thing...	0/8
Message Queue MQ	0/50
Message Queue ...	0/25
Load balancing S...	0/26
Apsara Stack Sec...	0/12
Message Queue ...	0/24

Select all Empty

Resource Sharing Permission

□ Message Queue MQ

□ Cloudy Information Management

□ View Cloudy List □ Add cloud information □ Modify cloud information □ Delete cloud information

□ Message routing

□ View routing task list □ Add routing task □ Modify routing tasks □ Delete routing task □ Suspend routing task □ Start routing task

□ Cluster management

□ Access mode switching

□ Instance

□ Query the basic information of the instance □ Create an instance □ Delete instance □ Update instance

□ Network management

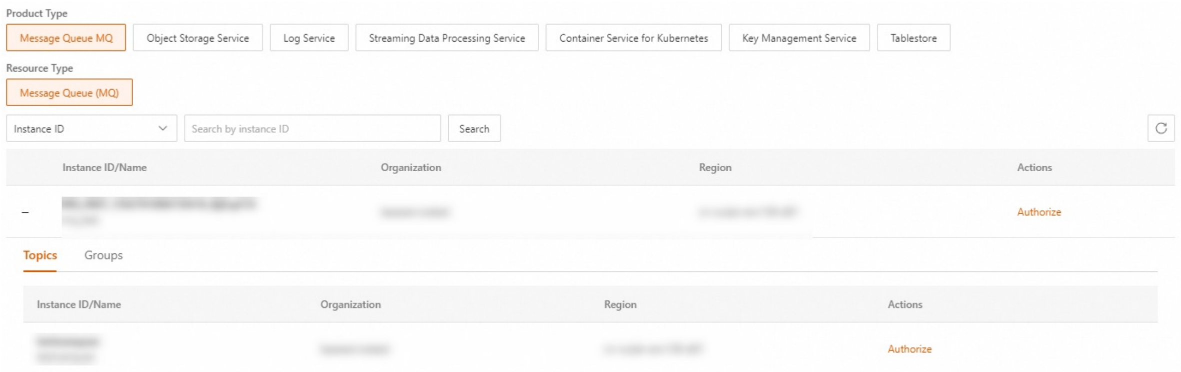
□ Bind VPC □ Unbind VPC □ Query VPC list

□ Topic and Group

□ Create Topic □ Create Group ID □ Delete Topic □ Delete Group ID □ Group management □ Message sending (PUB) □ Message subscription (SUB)

- **Second authorization**: YYou can grant operation permissions on a specific ApsaraMQ instance or a specific topic or group in an ApsaraMQ instance on the Data Permissions page.

Service instances



Product Type

Message Queue MQ | Object Storage Service | Log Service | Streaming Data Processing Service | Container Service for Kubernetes | Key Management Service | Tablestore

Resource Type

Message Queue (MQ)

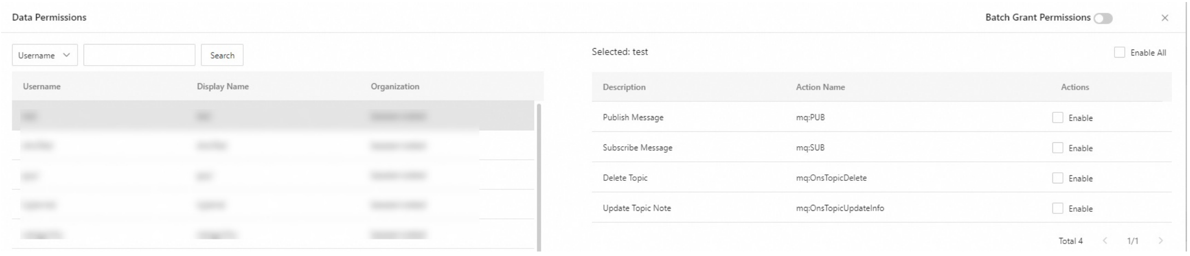
Instance ID ⌄ | Search by instance ID | Search

	Instance ID/Name	Organization	Region	Actions
–	[redacted]	[redacted]	[redacted]	Authorize

Topics Groups

Instance ID/Name	Organization	Region	Actions
[redacted]	[redacted]	[redacted]	Authorize

Data permissions



Data Permissions

Batch Grant Permissions

Username ⌄ | Search

Username	Display Name	Organization
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Selected: test

□ Enable All

Description	Action Name	Actions
Publish Message	mq:PUB	□ Enable
Subscribe Message	mq:SUB	□ Enable
Delete Topic	mq:OnsTopicDelete	□ Enable
Update Topic Note	mq:OnsTopicUpdateInfo	□ Enable

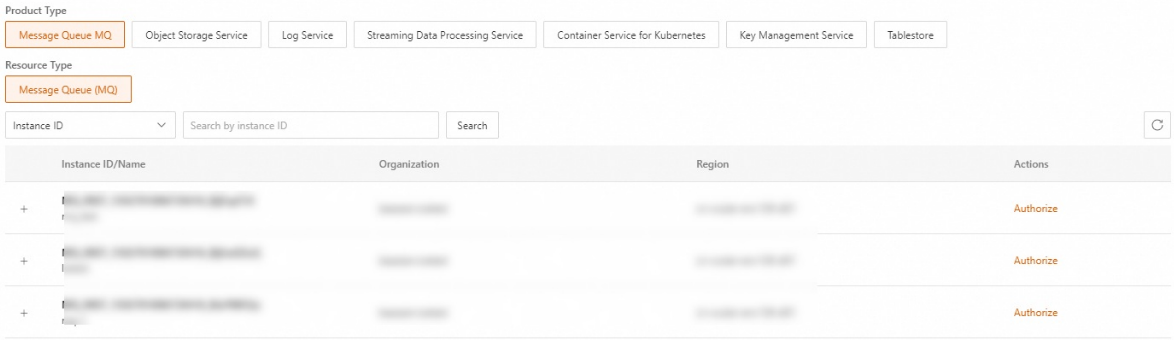
Total 4 < 1/1 >

Grant data permissions on specific instances on the Data Permissions page

> **Note**
>
> You can grant data permissions on specific instances on the Data Permissions page.

Grant data permissions on ApsaraMQ

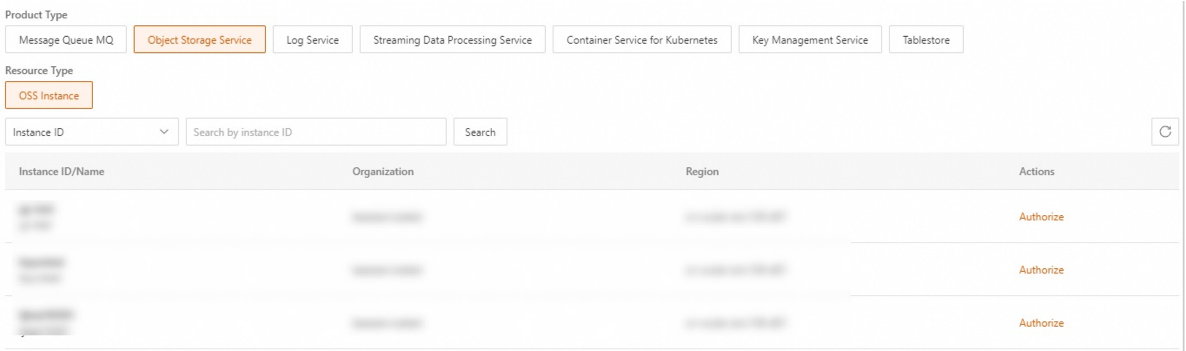
1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **Data Permissions**.
4. On the left side of the **Data Permissions** page, click a resource set to which the ApsaraMQ instance that you want to manage belong. On the right side of the page, select **Message Queue MQ** for the **Product Type** parameter.



5. Grant data permissions on an ApsaraMQ instance
   i. In the ApsaraMQ instance list, find the instance that you want to manage and click **Authorize** in the **Actions** column.
   ii. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
   iii. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions to or from the specified users. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the instance.
   iv. Click **OK**.
6. Grant permissions on a topic or a group in an ApsaraMQ instance
   i. In the ApsaraMQ instance list, find the ApsaraMQ instance that you want to manage and click the + icon before the instance name to display the topics and groups in the instance.
   ii. Find the topic or group that you want to manage and click **Authorize** in the **Actions** column.
   iii. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
   iv. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions to or from the specified users on the topic or group. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the topic or group.

Grant data permissions on OSS

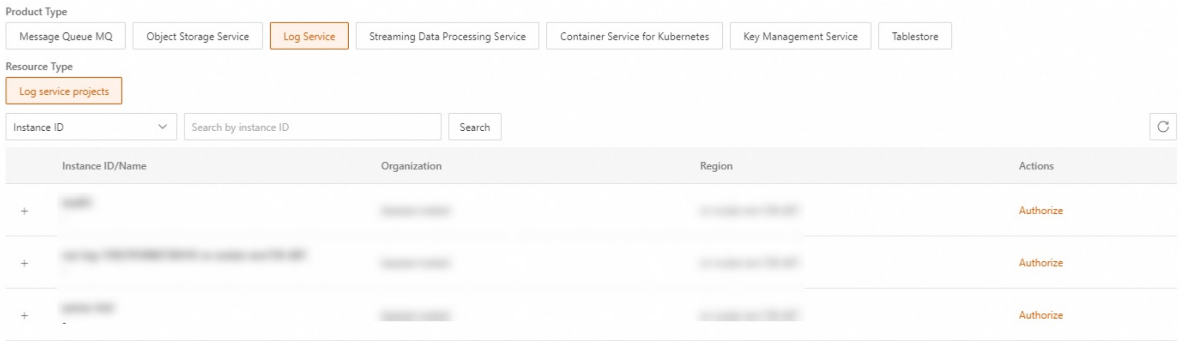
1. On the left side of the **Data Permissions** page, click a resource set to which the OSS instance that you want to manage belongs. On the right side of the page, select **Object Storage Service** for the **Product Type** parameter.



2. In the OSS instance list, find the instance that you want to manage and click **Authorize** in the **Actions** column.
3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions to or from the specified users. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the instance.
5. Click **OK**.

Grant data permissions on Simple Log Service

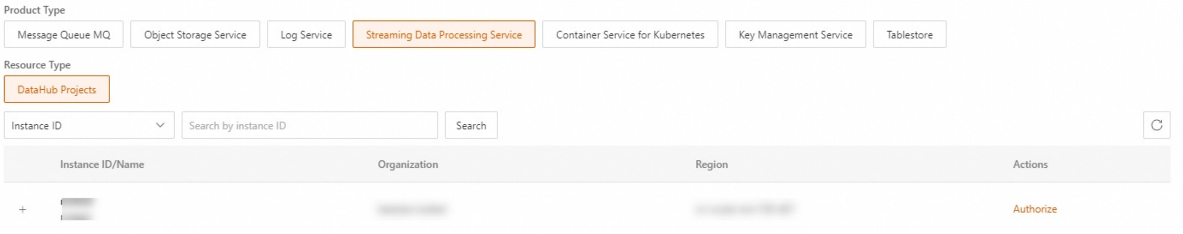
1. On the left side of the **Data Permissions** page, click a resource set to which the Simple Log Service project that you want to manage belongs. On the right side of the page, select **Log Service** for the **Product Type** parameter.



2. In the list of Simple Log Service projects, find the project that you want to manage and click **Authorize** in the **Actions** column.
3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions to or from the specified users. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the project.
5. Click **OK**.

Grant data permissions on DataHub

1. On the left side of the **Data Permissions** page, click a resource set to which the DataHub project that you want to manage belongs. On the right side of the page, select **Streaming Data Processing Service** for the **Product Type** parameter.



Product Type

Resource Type

	Instance ID/Name	Organization	Region	Actions
+	[illegible]	[illegible]	[illegible]	Authorize

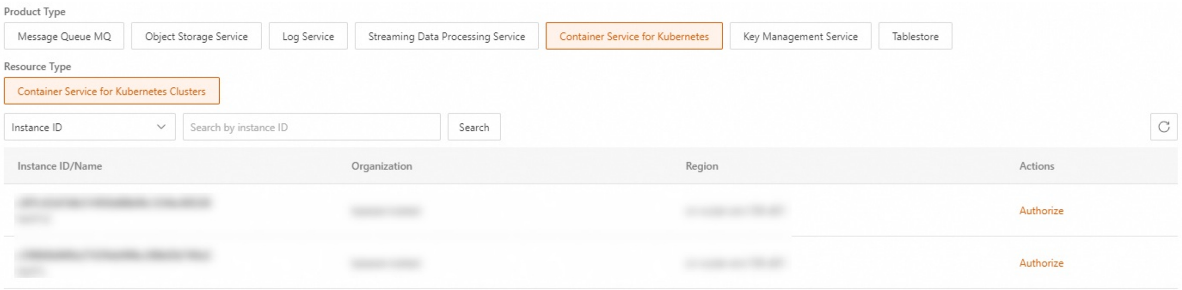
2. Grant data permissions on a DataHub project.
   1. In the DataHub project list, find the project that you want to manage and click **Authorize** in the **Actions** column.
   2. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
   3. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions to or from the specified users. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the project.
   4. Click **OK**.
3. Grant permissions on a topic in a DataHub project
   1. In the DataHub project list, find the DataHub project that you want to manage and click the + icon before the project name to display the topics in the project.
   2. Find the topic that you want to manage and click **Authorize** in the **Actions** column.
   3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
   4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions on the topic. You can also select **Enable All** in the upper-right corner of the section to grant users all operation permissions on the topic.
   5. Click **OK**.

Grant data permissions on ACK

Perform authorization in the Apsara Uni-manager Management Console

> **Note**
>
> You can grant operation permissions on an ACK cluster to users in the Apsara Uni-manager Management Console.

1. On the left side of the **Data Permissions** page, click a resource set to which the ACK cluster that you want to manage belongs. On the right side of the page, select **Container Service for Kubernetes** for the **Product Type** parameter



Instance ID/Name	Organization	Region	Actions
[redacted]	[redacted]	[redacted]	Authorize
[redacted]	[redacted]	[redacted]	Authorize

2. In the ACK cluster list, find the cluster that you want to manage and click **Authorize** in the **Actions** column.
3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions on the cluster. You can also select **Enable All** in the upper-right corner of the section to grant all operation permissions on the cluster.
5. Click **OK**.

Perform authorization in the ACK console

> **Note**
>
> You can configure fine-grained role-based access control (RBAC) for Resource Access Management (RAM) users or RAM roles in the ACK console. This way, you can grant access or operation permissions on resources in clusters. For example, you can authorize RAM users or RAM roles to manage resources only in the specified namespace in a cluster.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose > **Products** > **Elastic Computing** > **Container Service for Kubernetes**.
3. In the left-side navigation pane, click **Authorizations**.
4. On the RAM Users or RAM Roles tab, find the RAM user or RAM role that you want to manage and click **Modify Permissions** in the **Actions** column.
5. In the **Configure Role-Based Access Control (RBAC)** step, click **Add Permissions**. Select all clusters or a cluster from the Cluster drop-down list. If you select a cluster, you also need to select one or more namespaces of the cluster. Select the preset role or custom role that you want to manage and click **Next Step**.

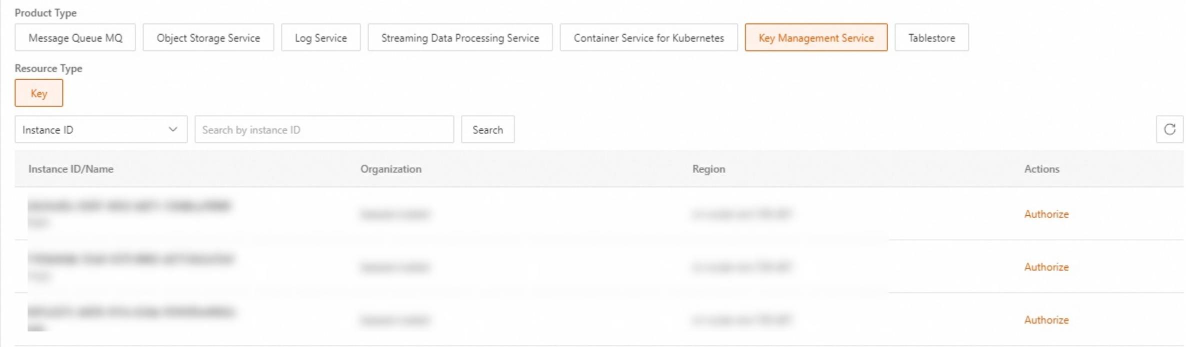
   The following table describes the permissions that roles have on clusters and namespaces.

Role	RBAC permissions on cluster resources
Administrator	This role has the read and write permissions on all resources in all namespaces of the corresponding cluster.
O&M engineer	This role has the read and write permissions on resources in all namespaces and read-only permissions on nodes, persistent volumes (PVs), namespaces, and service quotas of the corresponding cluster.

Developer	This role has the read and write permissions on resources in a specific namespace or all namespaces.
Restricted user	This role has the read-only permissions on resources in a specific namespace or all namespaces.
Custom role	The permissions of a custom role are determined by the ClusterRole that you select. Before you select a ClusterRole, check the permissions of the ClusterRole to ensure that you grant only the required permissions to the RAM user.

Grant data permissions on KMS

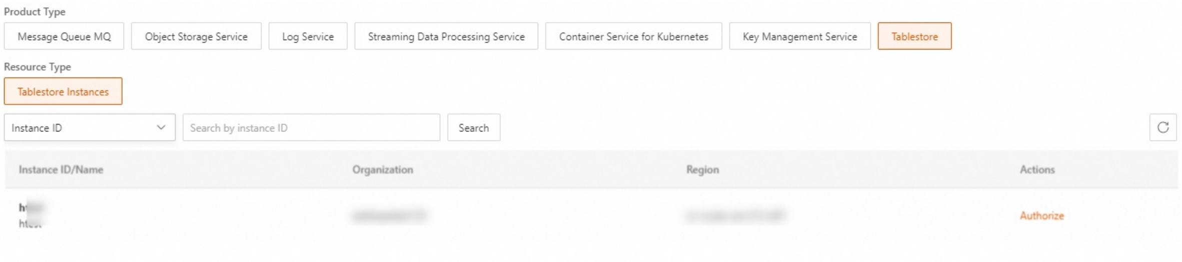
1. On the left side of the **Data Permissions** page, click a resource set to which the KMS instance that you want to manage belongs. On the right side of the page, select **Key Management Service** for the **Product Type** parameter.



2. In the KMS instance list, find the instance that you want to manage and click **Authorize** in the **Actions** column.
3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions on the key. You can also select **Enable All** in the upper-right corner of the section to grant all operation permissions on the key.
5. Click **OK**.

Grant data permissions on Tablestore

1. On the left side of the **Data Permissions** page, click a resource set to which the Tablestore instance that you want to manage belongs. On the right side of the page, select **Tablestore** for the **Product Type** parameter.

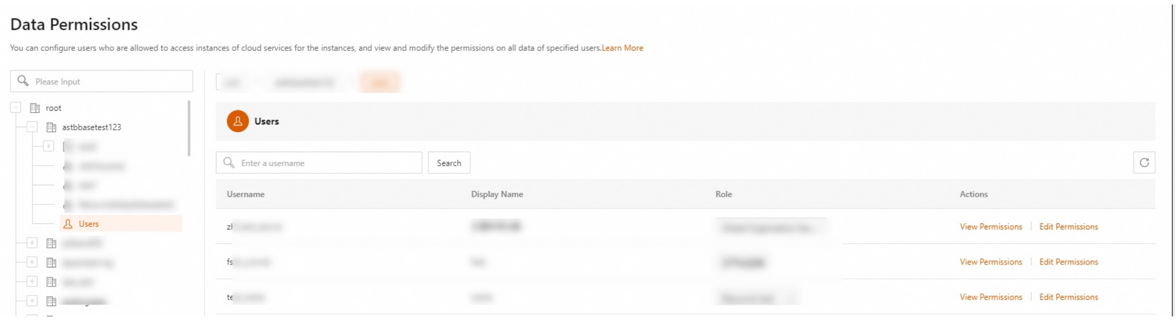


2. In the Tablestore instance list, find the instance that you want to manage and click **Authorize** in the **Actions** column.

3. On the left side of the **Data Permissions** dialog box, select one or more users to whom you want to grant data permissions. You can also turn on **Batch Grant Permissions** in the upper-right corner of the dialog box to grant permissions to multiple users at a time.
4. In the Instance Permission Settings section on the right side of the dialog box, select or deselect **Enable** to grant or remove specific operation permissions on the instance. You can also select **Enable All** in the upper-right corner of the section to grant all operation permissions on the instance.
5. Click **OK**.

Grant permissions to a user by creating a policy

1. On the left side of the **Data Permissions** page, click a user group to which the user that you want to manage belongs. On the right side of the page, find the desired user.



Data Permissions

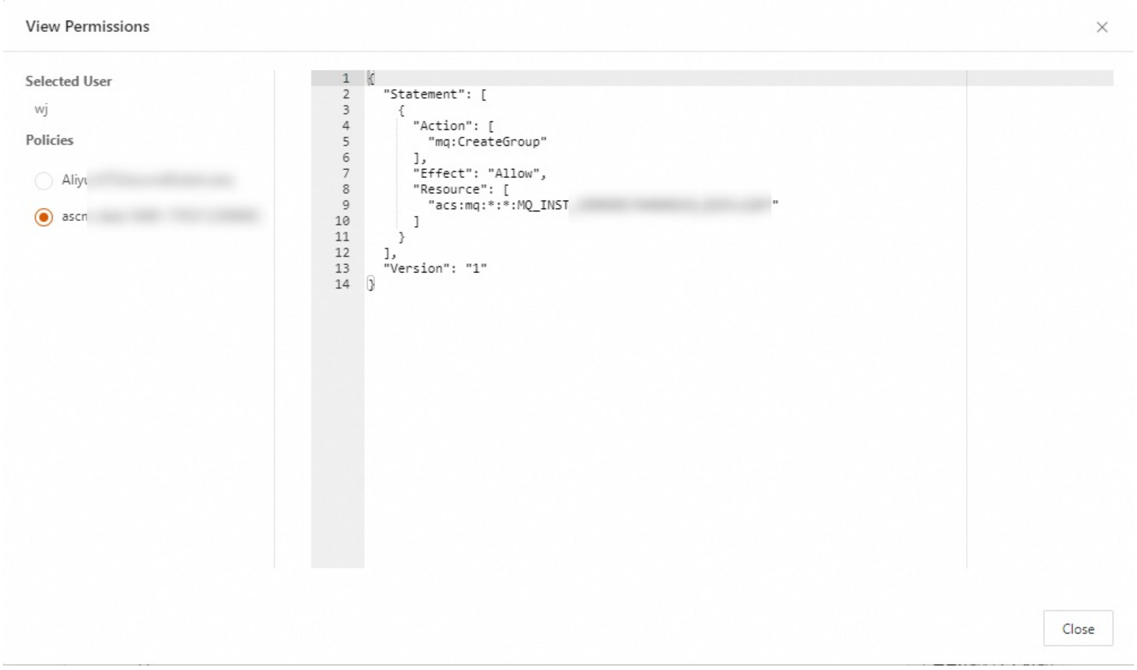
You can configure users who are allowed to access instances of cloud services for the instances, and view and modify the permissions on all data of specified users.Learn More

Username	Display Name	Role	Actions
zl[redacted]	[redacted]	[redacted]	View Permissions | Edit Permissions
fs[redacted]	[redacted]	[redacted]	View Permissions | Edit Permissions
te[redacted]	[redacted]	[redacted]	View Permissions | Edit Permissions

2. View or modify the policies of the user. For more information, see RAM policies.
   - **View the policies of the user**

   a. Click **View Permissions** in the **Actions** column.

b. In the **View Permissions** dialog box, view all the policies of the user. Click a policy in the **Policies** section to view the policy content.

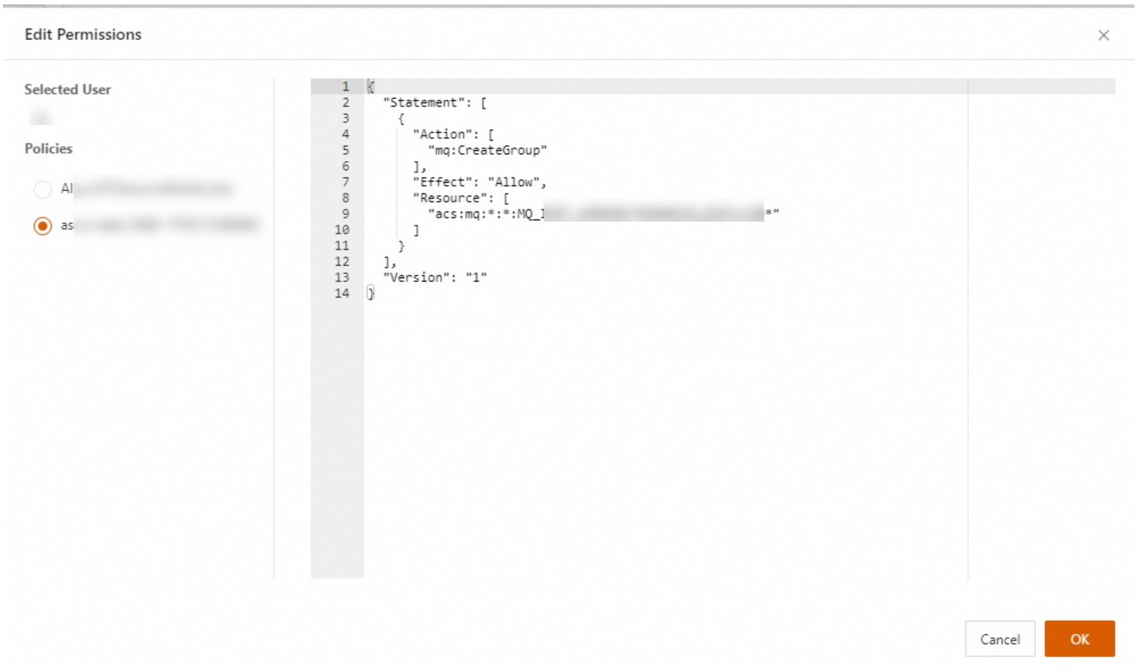


```
{
  "Statement": [
    {
      "Action": [
        "mq:CreateGroup"
      ],
      "Effect": "Allow",
      "Resource": [
        "acs:mq:*:*:MQ_INST[redacted]"
      ]
    }
  ],
  "Version": "1"
}
```

> **Note**
>
> The policy shown in the preceding figure specifies a set of permissions on the resource asc:mq:MQ****. The policy allows the user to create a group on the ApsaraMQ instance. You can attach this policy to a user to allow the user to create a group on the ApsaraMQ instance.

- **Modify a policy of the user**
  - Click **Edit Permissions** in the **Actions** column.

- In the **Edit Permissions** dialog box, click a policy in the **Policies** section to modify the policy in the right-side code editor.



```
{
  "Statement": [
    {
      "Action": [
        "mq:CreateGroup"
      ],
      "Effect": "Allow",
      "Resource": [
        "acs:mq:*:*:MQ_I[redacted]*"
      ]
    }
  ],
  "Version": "1"
}
```

4.4.4. Access control

4.4.4.1. Create an access policy

To improve the security of the Apsara Uni-manager Management Console, you can create access policies as an administrator to control logon access based on the logon time and IP addresses of users.

Background information

Access policies are used to control the time periods and IP addresses valid for user logon. After a user is associated with an access policy, user logons are limited based on the logon time and IP addresses specified in the policy.

The default policy generated by the Apsara Uni-manager Management Console does not have limits on the time and IP addresses valid for user logon. This policy cannot be deleted.

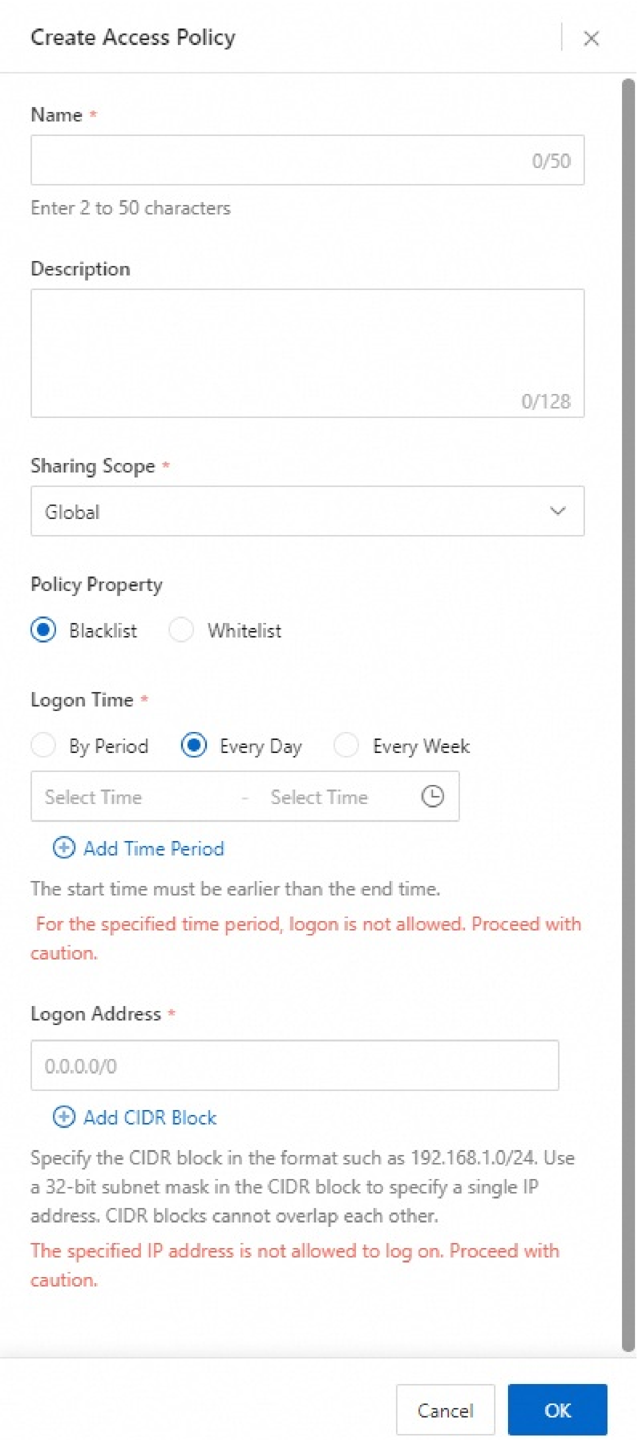
Limits

- The super administrator can only create access policies that are shared within the current organization, and these policies can only be configured for custom operations administrators.
- Operations administrators can only create globally shared access policies.
- If you use a custom role whose permissions are shared by all organizations, you can create globally shared access policies, access policies that are shared within the current organization, and access policies that are shared within the current organization and its subordinate organizations.
- If you use a role whose permissions are shared within the current organization and its subordinate organizations, you can only create access policies that are shared within the current organization and access policies that are shared within the current organization and its subordinate organizations.

- If you use a custom role whose permissions are shared by resource sets, you cannot create access policies even if you are granted the required permissions.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **Access Control**.
4. On the page that appears, click **Create Access Policy** in the upper-left corner.
5. In the **Create Access Policy** dialog box, set the Name, Description, Sharing Scope, Policy Property, Logon Time, and Logon Address parameters.



Create Access Policy

Name *

0/50

Enter 2 to 50 characters

Description

0/128

Sharing Scope *

Global

Policy Property

● Blacklist ○ Whitelist

Logon Time *

○ By Period ● Every Day ○ Every Week

Select Time - Select Time

Add Time Period

The start time must be earlier than the end time.

For the specified time period, logon is not allowed. Proceed with caution.

Logon Address *

0.0.0.0/0

Add CIDR Block

Specify the CIDR block in the format such as 192.168.1.0/24. Use a 32-bit subnet mask in the CIDR block to specify a single IP address. CIDR blocks cannot overlap each other.

The specified IP address is not allowed to log on. Proceed with caution.

Parameters for creating an access policy

Parameter	Description
Name	The name of the access policy. The name can be 2 to 50 characters in length and can contain only letters and digits. The name must be unique in the system.

Description	The description of the access policy.
Sharing Scope	The scope in which the policy is available. Valid values: ◦ **Global**: The policy is available in all organizations. ◦ **Current Organization**: The policy is available only in the current organization but is unavailable in the subordinate organizations of the current organization. ◦ **Subordinate Organization**: The policy is available in the current organization and its subordinate organizations.
Policy Property	The authentication method of the access policy. **Important** The authentication method takes effect only when the settings of both the **Logon Time** and **Logon Address** parameters are matched. ◦ **Whitelist**: Logon is allowed for users that match the settings of both the Logon Time and Logon Address parameters. ◦ **Blacklist**: Logon is not allowed for users that match the settings of both the Logon Time and Logon Address parameters.
Logon Time	The permitted logon time period. Valid values: **By Period**, **Every Day**, and **Every Week**. You can click **Add Time Period** to add a logon time period. ◦ **By Period**: You must specify a start date, an end date, and a specific logon period. ◦ **Every Day**: You need to only specify a logon period. ◦ **Every Week**: You need to select one or more days of the week (from Monday to Sunday) and specify a logon period. **Note** The start time of the login period must be earlier than the end time of the logon period.
Logon Address	The permitted CIDR block. You can click **Add CIDR Block** to add CIDR blocks. The CIDR block is in the IP address/Subnet mask format, such as 192.168.1.0/24. If the subnet mask of a logon IP address is 32 bits in length, only this IP address is allowed to log on. The CIDR block cannot be empty or duplicate.

6. Click **OK**.

4.4.4.2. Manage an access policy

After you create an access policy, you can view, modify, disable, enable, or delete the access policy.

Limits

- The default policy of the system is globally shared and is in the valid state. You cannot modify, disable, or delete the default policy.
- You can view the default policy of the system and the access policies you created as the super administrator. You can also modify, disable, enable, or delete the access policies you created as the super administrator.
- If you use a role whose permissions are shared by all organizations, you can view the access policies that are globally shared, and that are shared in the current organization and its subordinate organizations. You can also modify, disable, enable, or delete all available access policies except the default policy.
- If you use a role whose permissions are shared by the current organization and its subordinate organizations, you can view the access policies that are globally shared, and that are shared in the current organization and its subordinate organizations. You can also modify, disable, enable, or delete the access policies that are available within the management scope.
- If you use a custom role whose permissions are shared by resource sets, you can view the access policies that are globally shared, and that are shared in the current organization and its subordinate organizations. You cannot modify, disable, enable, or delete the access policies even if you are granted the required permissions.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **Access Control**.
4. Find the target access policy and perform the operations described in the following table.

Operation	Procedure
View the access policy	i. On the Access Control page, view the information of the access policy, such as Policy Property, Status, Sharing Scope, Users, Access Time, Endpoint, and Description. ii. Click the number (not 0) in the **Users** column to view the users who are configured with this access policy.
Modify the access policy	i. Click **Modify** in the Actions column. ii. Modify the access policy, including Name, Description, Logon Time, and Logon Address. iii. Click **OK**.
Disable the access policy	You can disable the access policy that is not needed at the moment. **Important** After the access policy is disabled, users that are associated with the policy cannot log on to the Apsara Uni-manager Management Console. i. Click **Disable** in the **Actions** column. ii. In the message that appears, click **OK**.

Enable the access policy	Click **Enable** in the Actions column.
Delete the access policy	ⓘ **Important** Before you delete an access policy, make sure that it is not associated with any user. i. Click **Delete** in the Actions column. ii. Click **OK**.

4.4.5. Permission boundary

4.4.5.1. Service boundary management

The Apsara Uni-manager Management Console leverages the API control capabilities of the core gateway of Apsara Stack to provide the service boundary feature. You can create service boundaries to implement fine-grained control on API operations based on organizations, usage methods, and time periods.

4.4.5.1.1. Create a service boundary

You can associate API control policies with service boundaries to implement fine-grained control on API operations.

Background information

The Apsara Uni-manager Management Console allows you to control operations by organizations, time, and operation methods through setting service boundaries. You can also use service boundaries to trigger approval processes when cloud operations are performed.

Service boundaries take effect on operations performed through all methods, including cloud accounts, RAM users, and STS tokens. Specially, they also take effect on operations performed on the console. This is because when users perform operations on the console, the system is calling API operations under the hood.

> ⓘ **Important**
>
> API operations performed across cloud services (such as when Resource Orchestration Service calls an Elastic Compute Service operation to manage the resources) are also controlled by service boundaries. Therefore, inappropriate configurations may interrupt the normal usage of cloud services. You need to add the ARNs of relevant resources to the whitelist of the service boundaries and make sure that you are aware of the impact of the service boundaries before you enable them.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Permission Boundary** > **Service Boundary**.
3. On the **Service Boundary Management** page, click **Create Service Boundary**. On the page that appears, configure the parameters.

Section	Parameter	Description
Basic Information	Service Boundary Name	The name of the service boundary.
	Description	The description of the service boundary.
Management Scope	Management Scope	The organizations for which the service boundary takes effect. Valid values: **Global** and **Specified Organization**. When you select Specified Organization, you need to select one or more organizations from the **Authorize Organization** drop-down list.
	Associate API Control Policy	The API control policies with which the service boundary is associated. You can select one or more API control policies. In an API control policy, you can specify conditions based on the parameter values of specific API operations.
Control Mode	Console Calls	The action on an operation that hits the control policy. Valid values: ◦ **Reject**: rejects the operation. ◦ **Process Approval**: initiates a preconfigured approval process for the operation. If you select this option, you must configure the **Process** parameter in the **Configure Resource Application Process** dialog box. You can select an existing process or create a new process
	API Calls	The action on an API call that hits the control policy. The value is set to **Reject** and cannot be changed.
Period Settings	Effective Period	The periods of time during which the service boundary takes effect. Valid values: ◦ **By Period**: If you select this option, you must configure the **Start and End Time** parameter. ◦ **Every Day**: If you select this option, you must configure the **Start and End Time** and **Effective Time per Day** parameters. ◦ **Every Week**: If you select this option, you must configure the **Start and End Time**, **Effective Days per Week**, and **Effective Time per Day** parameters.

Settings	Status	The status the service boundary enters immediately when it is created. Valid values: ◦ **Enable** ◦ **Disable** **Important** We recommend that you disable the service boundary first, and enable it after you have comprehensive knowledge about its influence.
	Whitelist	The resources (RAM authorizations), RAM users, and RAM roles that are exempt from the service boundary. Specify the entities by ARNs. You can perform a fuzzy search and select existing ARNs from the drop-down list, or specify a custom ARN by following the format. **Note** Up to 10 ARNs can be specified in the whitelist of a service boundary.

4. Click **Submit**.

4.4.5.1.2. Manage service boundaries

You can view, modify, enable, disable, and delete service boundaries and manage their whitelists in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Permission Boundary** > **Service Boundary**.
3. On the Service Boundary Management page, manage the service boundaries.

Description	Procedure
View the details of service boundaries	Click the name or ID of the target service boundary. On the page that appears, you can view the details of the service boundary, including its basic information, associated API control policies, approval processes, and whitelists.

Modify service boundaries	○ Modify the configurations of a service boundary: Click**Edit** in the **Actions** column corresponding to the target service boundary. On the page that appears, you can modify the basic information, management scope, control mode, and effective period of the service boundary. ○ Modify the API control policies associated with a service boundary: Click **Modify Policy** in the **Actions** column corresponding to a service boundary. On the **Associate Policy** tab of the page that appears, click **Add API Control Policy** or **Remove** to associate or disassociate control policies.
Enable or disable service boundaries	Click **Enable** or **Disable** in the **Actions** column corresponding to the target service boundary.
Manage whitelists	Move your pointer over the More icon in the**Actions** column corresponding to a service boundary and click **Manage Whitelist**. On the **Whitelist** tab of the page that appears, you can click**Add** or **Edit** to add or modify the ARNs that are exempt from the service boundary.
Delete service boundaries	Move your pointer over the More icon in the**Actions** column corresponding to a service boundary and click **Delete**.

4.4.5.2. Control policy management

API control policies are associated with service boundaries to implement fine-grained access control. In an API control policy, you can specify conditions based on parameter values of specific API operations. After it is associated with a service boundary, actions will be taken when the conditions in the API control policy are met. For example, you can define a control policy that enables service boundaries to take actions when users query details of instances whose names contain a specific string.

Supported services

The following table lists the cloud services and their API versions that are supported by API control policies.

> **Note**
>
> The services and API versions listed in the console prevail. We recommend that you refer to relevant API documentation to learn about the operations and their parameters.

Service name	Service code	API version
Elastic Compute Service (ECS)	Ecs	2014-05-26

		2016-03-14
Apsara File Storage NAS	NAS	2017-06-26
Virtual Private Cloud (VPC)	Vpc	2016-04-28
ApsaraDB RDS	Rds	2014-08-15
PolarDB	polardb	2017-08-01
KVStore for Redis	R-kvstore	2015-01-01
ApsaraDB for MongoDB	Dds	2015-12-01
		2022-11-21
API Gateway	CloudAPI	2016-02-01
		2016-07-01
		2016-07-14

Content of control policies

The content of a control policy consists of a coordinate and parameters. The policies are stored as a JSON file that can be modified on the control policy details page.

Element	Description
coordinate	The coordinate of the API operation. Format: `${popCode}:${version}:${action}` . popCode indicates the product code; version indicates the API version; action indicates the API operation. You can use an asterisk (*) as a wildcard character to replace ${version} so that all API versions are included.
parameters	An array that contains details about the rule, including the name of the parameter (key), logical expression (condition), and specified value (value).
└ condition	The logical relationship between the actual value of the parameter and the specified value.

ㄴ value	The specified value. ⓘ **Note** The value can be left empty only if condition is set to NotNull or IsNull.
ㄴ key	The name of the controlled API operation.

Example

```
[
 {
  "coordinate": "CloudAPI:2016-02-01:AbolishApi",
  "parameters": [
   {
    "condition": "IsNull",
    "value": "",
    "key": "AccessKeyId"
   }
  ]
 }
]
```

Data types of parameter values and logical expressions

The following table lists the logical expressions that can be specified in API control policies.

Type	Logical expression	Description
Numeric (such as INTEGER, LONG, and FLOAT)	NumericEquals	The actual value equals the specified value in the policy.
	NumericNotEquals	The actual value does not equal the specified value in the policy.
	NumericLessThan	The actual value is smaller than the specified value in the policy.
	NumericGreaterThan	The actual value is larger than the specified value in the policy.
	NumericLessThanEquals	The actual value is smaller than or equal to the specified value in the policy.

	NumericGreaterThanEquals	The actual value is larger than or equal to the specified value in the policy.
	IsNull	The parameter is left empty.
	NotNull	The parameter is not empty.
String	StringLike	The actual value includes the specified string in the policy.
	StringNotLike	The actual value does not include the specified string in the policy.
	StringEquals	The actual value matches the specified string in the policy (case-sensitive).
	StringNotEquals	The actual value does not match the specified string in the policy (case-sensitive).
	StringEqualsIgnoreCase	The actual value matches the specified string in the policy (case-insensitive).
	IsNull	The parameter is left empty.
	NotNull	The parameter is not empty.
BOOLEAN	Boolean_Equals	The actual value matches the specified value in the policy.
	IsNull	The parameter is left empty.
	NotNull	The parameter is not empty.

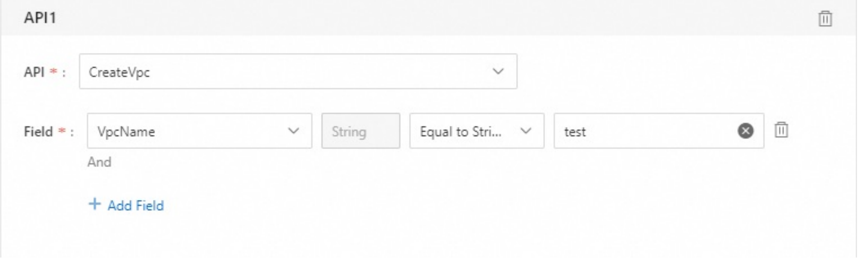
4.4.5.2.1. Create an API control policy

In the Apsara Uni-manager Management Console, you can create API control policies to control API operations on cloud resources based on values of the request parameters.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Permission Boundary** > **Control Policies**.
3. On the **API control policy management** page, click **Create an API control policy**.
4. On the **Create Control Policy** page, specify the name and description of the policy and click **Create** in the Control Content section. In the dialog box that appears, configure the following parameters.

Parameter	Description
Cloud Services	The cloud services whose API operations are to be controlled.
Version	The API version. Some cloud services may have multiple API versions. We recommend that you select All Versions for this parameter.
API	The API operation that is controlled. **Note** Each rule is set for a single operation. If you want to specify rules for multiple operations in a single policy, you can click **Add Rule**. The rules in a policy are in **OR** logical relations. This means that when the policy is attached to a service boundary, the policy takes effect as long as one of the rules is met.

Field	The request parameter to be controlled, a specified value, and the logical relation between the values in actual requests and the specified value. The logical relations vary with the types of the selected request parameters. Valid values include **Similar To**, **Equal to String**, **Equal to (case-insensitive)**, **Empty**, **Not Empty**. **Note** You can click **Add Field** to specify multiple conditions. The conditions in a rule are in **AND** logical relations. This means that the rule takes effect only if all conditions are met. **Example**: The following figure shows how to configure the Field parameter for a rule that is created to control the action of creating a VPC named "test".  API1 API * : CreateVpc Field * : VpcName String Equal to Stri... test And + Add Field

5. Click **Create**. Then, you can attach the API control policy to service boundaries.

4.4.5.2.2. Manage API control policies

You can view the details of existing API control policies, including their content and association with service boundaries. You can also modify and delete the policies.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Permission Boundary** > **Control Policies**.
3. On the page that appears, the existing policies are listed, and you can perform operations on them.

Operation	Procedure
View details of an API control policy	Click the ID of an API control policy. On the**Policy Details** tab of the page that appears, you can view the basic information and control content of the policy. On the **Reference Information** tab, you can view information of the service boundaries with which the policy is associated. You can click **Disassociate** in the Actions column corresponding to a service boundary to cancel the association.

Modify an API control policy	◦ Click **Modify** in the **Actions** column corresponding to a policy. In the dialog box that appears, you can modify its name and description. ◦ Click **Modify Control Content** in the **Actions** column corresponding to a policy. On the policy details page that appears, you can modify or delete the existing rules in the policy, or create new rules. **Note** ▪ When you modify a rule, you cannot change the cloud service, API version, or the API operation involved. ▪ After you delete a rule, service boundaries with which the policy is associated will be affected. Proceed with caution. If you are familiar with the format of control policies, you can click **Custom Edit** to modify the JSON file of the policy. This way, you can modify the cloud service, API version, and the API operation involved. You need to make sure that the modifications comply with the JSON format and that you are aware of the modifications' impact on relevant service boundaries.
Delete an API control policy	Click **Delete** in the **Actions** column corresponding to a policy. **Note** Policies that are associated with service boundaries cannot be deleted.

4.4.6. AccessKey logs

You can learn about the use of AccessKey pairs from AccessKey logs to improve security.

Background information

AccessKey pairs are supported for the following cloud products.

Cloud service category	Cloud service name
Elastic computing	• Bare-metal Management Service (BMS) • Operation Orchestration Service (OOS) • Resource Orchestration Service (ROS) • Auto Scaling • Dedicated Host (DDH) • Container Registry • Container Service for Kubernetes (ACK)

Storage	- Elastic Block Storage (EBS) - Apsara File Storage NAS (NAS) - Log Service **Note** This service is partially supported. Fat client authentication may be used for Log Service. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information. - Tablestore **Note** This service is partially supported. Fat client authentication may be used for Tablestore. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information.
Networking	- VPN Gateway - Virtual Private Cloud (VPC) - Server Load Balancer (SLB) - NAT Gateway - IPv6 Gateway - High-availability Virtual IP Address (HAVIP) - Express Connect - Elastic IP Address - Apsara Stack DNS
Database	- PolarDB-X V1.0 - ApsaraDB RDS SQL Server - KVStore for Redis - PolarDB-X V2.0 - PolarDB - ApsaraDB for MongoDB - Data Transmission Service (DTS) - Data Management (DMS) - Database Backup (DBS)

Middleware	- - Message Queue Note This service is partially supported. Fat client authentication may be used for Message Queue for Apache RocketMQ. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information.
Application services	- API Gateway
Security	- Key Management Service (KMS) Note This service is partially supported. Fat client authentication may be used for KMS. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information.
Big data	- DataHub - MaxCompute Note This service is partially supported. Fat client authentication may be used for MaxCompute. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information. - DataWorks Note This service is partially supported. Fat client authentication may be used for DataWorks. If an AccessKey pair is used for fat client authentication, the AccessKey logs may not record complete information.
Monitoring and O&M	- CloudMonitor

Disaster recovery	• Apsara Stack Resilience for Zone-disaster Recovery

View AccessKey logs

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **AccessKey Logs**.
4. Enter the AccessKey ID to be queried in the search box and click the 🔍 icon. The **Basic Information About AccessKey Pair** section and the **Accessed Services** section display the information about the AccessKey pair.

    > **Note**
    >
    > AccessKey logs may be generated 1 hour after the AccessKey pair is used. By default, AccessKey logs are stored for seven days. Exercise caution when you modify the AccessKey pair. If you want to store the logs for a longer period of time, you need to configure log storage, which is supported by Log Service. For more information about how to configure log storage, see Log storage settings.

    - **Basic Information About AccessKey Pair**
        - **Type**: the type of the AccessKey pair. An AccessKey pair may be a user AccessKey pair or an organization AccessKey pair.
        - **User Logon Name**: the logon name of the user.

            > **Note**
            >
            > This parameter is empty if the queried AccessKey pair is an organization AccessKey pair.

        - **UID**: the ID of the user or organization to which the AccessKey pair belongs.
        - **Organization**: the name of the organization to which the AccessKey pair belongs.

            > **Note**
            >
            > This parameter is empty if the queried AccessKey pair is a user AccessKey pair.

        - **AccessKeyID**: the ID of the AccessKey pair.
        - **Last Used At**: the last time when the AccessKey pair was used. Format: `YYYY:MM:DD:hh:mm:ss` .
        - **Last Used Service**: the cloud service that the AccessKey pair was used to access last time.
    - **Accessed Services**
        - **Events**: Click **Events** in the **Actions** column corresponding to a service to view the API operations called by using the AccessKey pair.
        - **IP Addresses**: Click **IP Addresses** in the **Actions** column corresponding to a service to view the IP addresses of the user of the AccessKey pair.

- **Resources**: Click **Resources** in the **Actions** column corresponding to a service to view the instances accessed by using the AccessKey pair.

> **Note**
>
> If the AccessKey pair has not been used to access any instance, no record is displayed.

4.5. Cloud instances

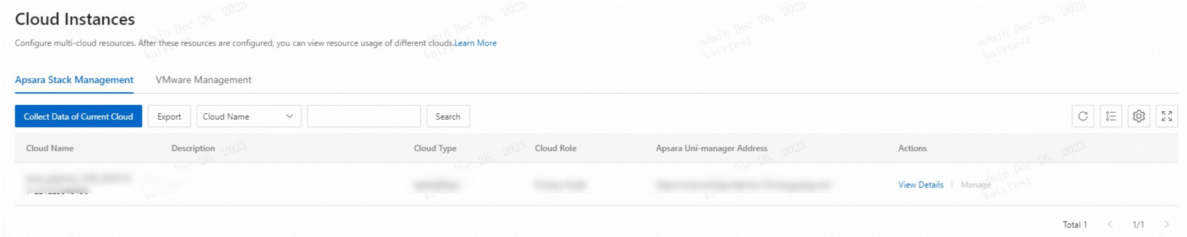
4.5.1. Manage Apsara Stack cloud instances

4.5.1.1. Export data of Apsara Stack

You can export the information about the Apsara Stack system to a JSON file.

Procedure:

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, click **Cloud Instances**.
4. On the Cloud Instances page, click the **Apsara Stack Management** tab.
5. Click **Collect Data of Current Cloud** to collect the deployment information about the current Apsara Stack system.



Cloud Instances

Configure multi-cloud resources. After these resources are configured, you can view resource usage of different clouds.Learn More

Cloud Name	Description	Cloud Type	Cloud Role	Apsara Uni-manager Address	Actions
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	View Details | Manage

Total 1 < 1/1 >

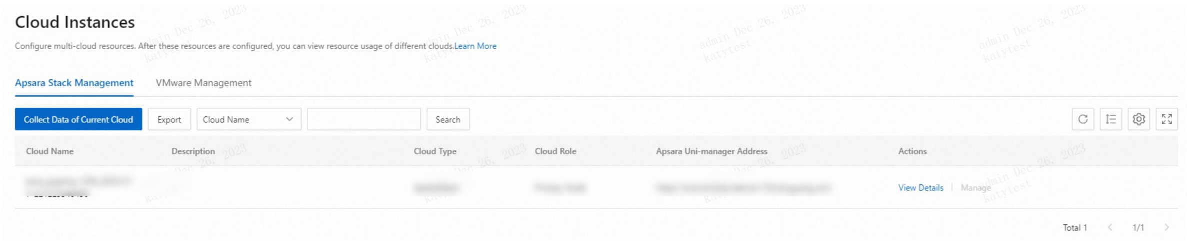
6. Click **Export** to export the information in the JSON format.

4.5.1.2. View the details of managed cloud instances

You can use the multi-cloud management feature to view the details of all managed cloud instances.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, click **Cloud Instances**.
4. On the Cloud Instances page, click the **Apsara Stack Management** tab.
5. Find the cloud instance that you want to manage and click **View Details** in the **Actions** column.



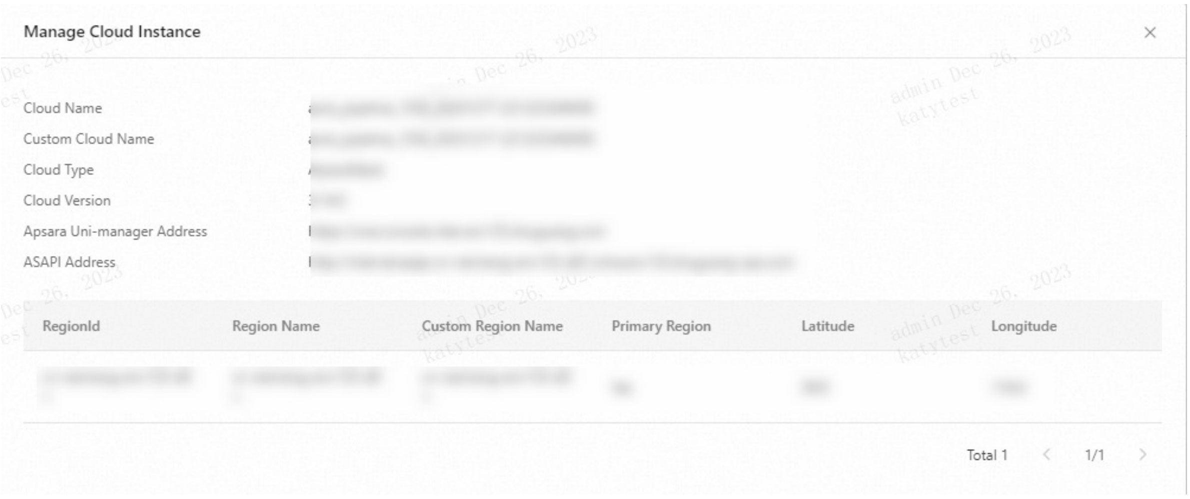
Cloud Instances

Configure multi-cloud resources. After these resources are configured, you can view resource usage of different clouds.Learn More

Cloud Name	Description	Cloud Type	Cloud Role	Apsara Uni-manager Address	Actions
[illegible]		[illegible]	[illegible]	[illegible]	View Details | Manage

Total 1 < 1/1 >

6. In the **Manage Cloud Instance** message, view the version, Apsara Stack API (ASAPI) address, and region in which the cloud is deployed.



Manage Cloud Instance

Cloud Name [illegible]
Custom Cloud Name [illegible]
Cloud Type [illegible]
Cloud Version [illegible]
Apsara Uni-manager Address [illegible]
ASAPI Address [illegible]

RegionId	Region Name	Custom Region Name	Primary Region	Latitude	Longitude
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Total 1 < 1/1 >

4.5.2. Manage VMware nodes

4.5.2.1. Add a VMware node

You can add the configuration information of VMware nodes to the Apsara Stack VMware management configuration for centralized management.

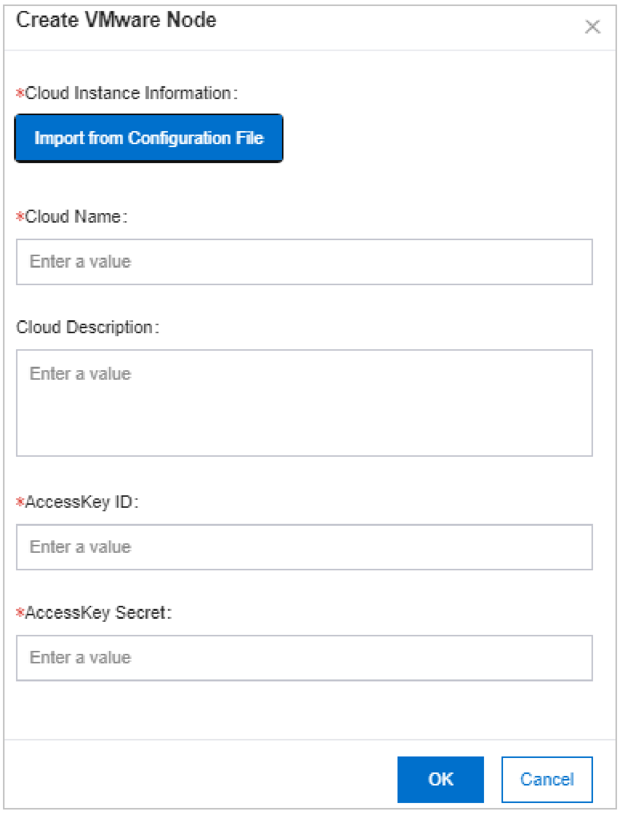
Prerequisites

- The configuration file of a VMware node is obtained from the deployment personnel.
- The VMware node is configured.

Procedure:

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane of the Enterprise page, click **Cloud Instances**.
4. Click the **VMware Management** tab.
5. Click **Create VMware Node**.

6. In the **Create VMware Node** dialog box, enter the configuration information of a VMware node and click **OK**.



Create VMware Node

*Cloud Instance Information:

Import from Configuration File

*Cloud Name:

Enter a value

Cloud Description:

Enter a value

*AccessKey ID:

Enter a value

*AccessKey Secret:

Enter a value

Parameter	Description
Cloud Instance Information	The configuration file of the VMware node.
Cloud Name	The name of the VMware node.
Cloud Description	The description of the VMware node.
AccessKey ID	The AccessKey ID in the configuration file of the VMware node.
AccessKey Secret	The AccessKey secret in the configuration file of the VMware node.

4.5.2.2. Modify a VMware node

If you want to change the information of a VMware node for more efficient management, you can modify it in the Apsara Uni-manager Management Console.

Procedure

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

2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane of the Enterprise page, click **Cloud Instances**.
4. Click the **VMware Management** tab.
5. Enter the name of the VMware node that you want to modify in the search box and click **Search** to search for the VMware node.
6. Click **Edit** in the **Actions** column corresponding to the VMware node.
7. In the **Edit Cloud Instance** dialog box, set **Cloud Name**, **Cloud Description**, **AccessKey ID**, and **AccessKey Secret**, and click **OK**.

4.5.2.3. Test VMware node connectivity

You can manage VMware nodes to check whether they can be connected.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane of the Enterprise page, click **Cloud Instances**.
4. Click the **VMware Management** tab.
5. Enter a VMware node name in the search box and click **Search** to search for the VMware node.
6. Click **Manage** in the **Actions** column corresponding to the VMware node.
7. In the **Manage Cloud Instance** dialog box, click **Test Connectivity**.

4.6. Asynchronous task

You can view the progress and results of asynchronous tasks on the Asynchronous Task page.

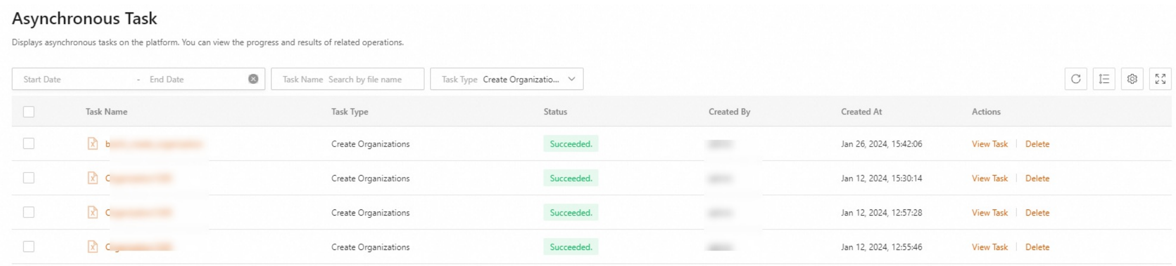
Background information

On the Asynchronous Task page, you can view the information about each asynchronous task, including the task name, task type, status, creator, and creation time. The system updates the execution situation of each task in real time. This way, users can know whether the task is running as expected at any time.

Asynchronous tasks are classified into the following types: batch creation of organizations and users and batch authorization of roles.

View the information about a task

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, click **Asynchronous Task**.
4. On the **Asynchronous Task** page, specify the **Start Date**, **End Date**, **Task Type**, and **Task Name** parameters to search for the desired task.
5. View the task information in the task list.



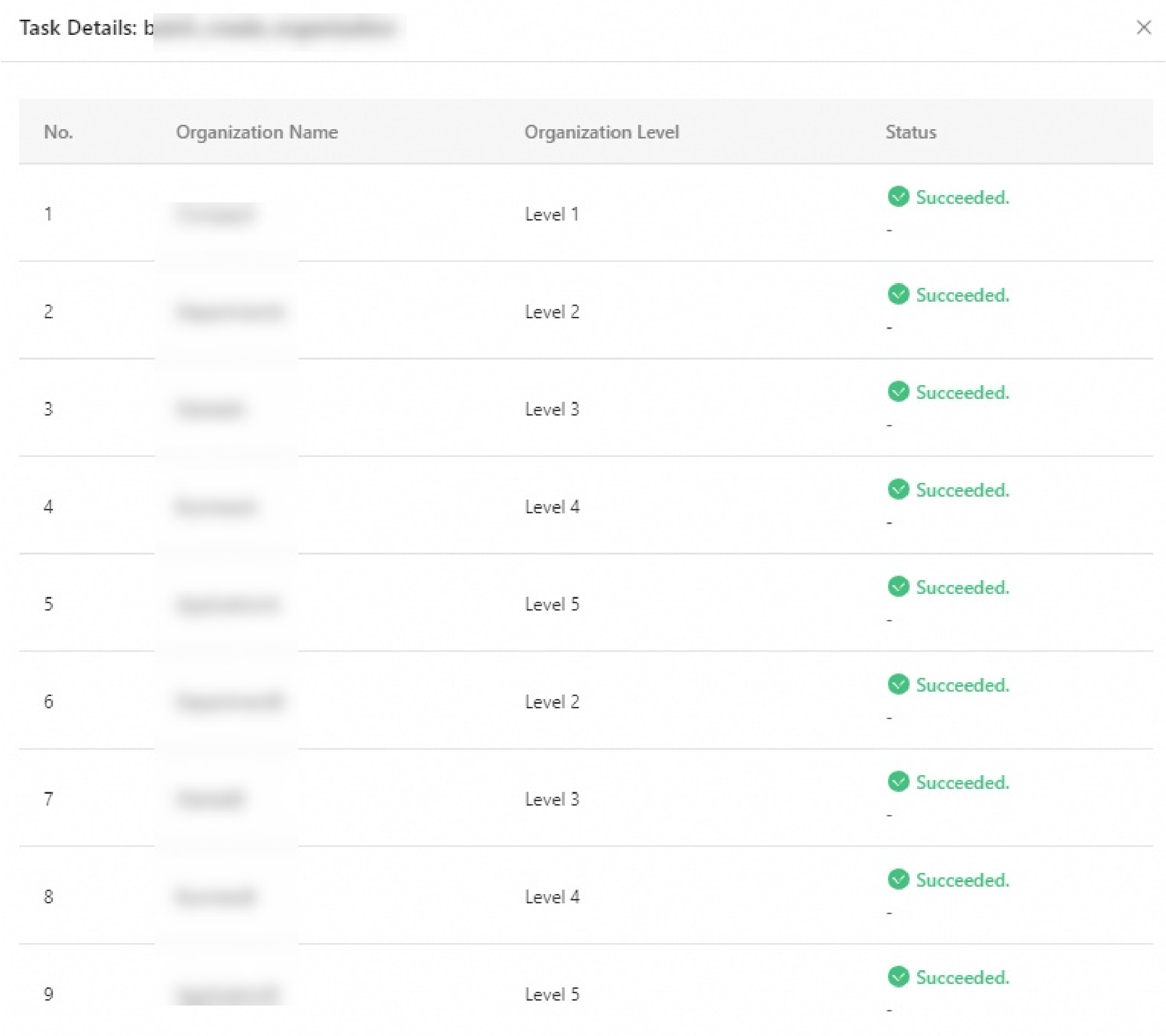
Asynchronous Task

Displays asynchronous tasks on the platform. You can view the progress and results of related operations.

Start Date - End Date | Task Name Search by file name | Task Type Create Organizatio...

□	Task Name	Task Type	Status	Created By	Created At	Actions
□	b[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 26, 2024, 15:42:06	View Task | Delete
□	C[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 15:30:14	View Task | Delete
□	C[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 12:57:28	View Task | Delete
□	C[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 12:55:46	View Task | Delete

6. Find the desired task and click the task name or click **View Task** in the **Actions** column. The **Task Details** panel appears.

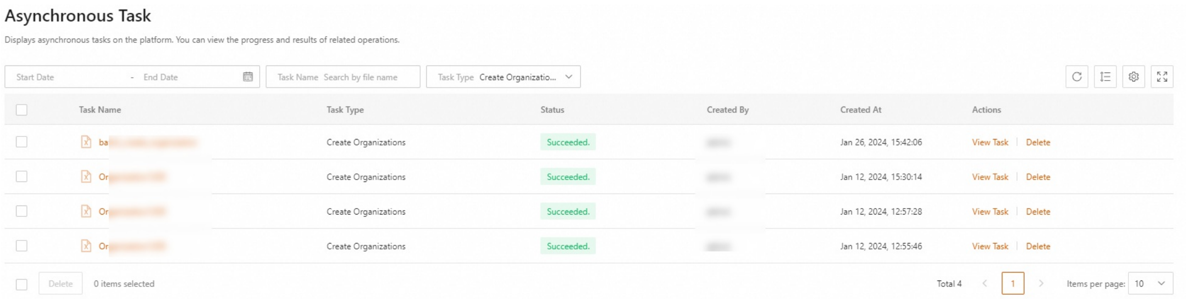


Task Details: b[redacted]

No.	Organization Name	Organization Level	Status
1	[redacted]	Level 1	Succeeded. -
2	[redacted]	Level 2	Succeeded. -
3	[redacted]	Level 3	Succeeded. -
4	[redacted]	Level 4	Succeeded. -
5	[redacted]	Level 5	Succeeded. -
6	[redacted]	Level 2	Succeeded. -
7	[redacted]	Level 3	Succeeded. -
8	[redacted]	Level 4	Succeeded. -
9	[redacted]	Level 5	Succeeded. -

Delete a task

1. On the **Asynchronous Task** page, find the desired task and click **Delete** in the **Actions** column.



Asynchronous Task

Displays asynchronous tasks on the platform. You can view the progress and results of related operations.

Start Date - End Date
Task Name Search by file name
Task Type Create Organizatio...

□	Task Name	Task Type	Status	Created By	Created At	Actions
□	ba[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 26, 2024, 15:42:06	View Task | Delete
□	Or[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 15:30:14	View Task | Delete
□	Or[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 12:57:28	View Task | Delete
□	Or[redacted]	Create Organizations	Succeeded.	[redacted]	Jan 12, 2024, 12:55:46	View Task | Delete

2. In the **Delete** message, click **OK**.

> **Important**
>
> After a task is deleted, the information about the task cannot be queried. Exercise caution when you delete a task. The information about task deletion is recorded in an operation log.

5.Configurations

5.1. Configure resource pools

You can manage the logical inventory of cloud resources to control the maximum usage of resources.

Background information

The amount of resources on the cloud platform is limited. Therefore, it is important to control the amount of resources available for each organization based on the scope of its responsibilities. This ensures that each organization is allocated with the right amount of resources.

The procedure to set resource quotas includes the following stages:

1. The platform administrator sets the maximum amount of resources that can be used for each cloud service on the cloud platform on the Resource Pool Configuration page.
2. The operations administrator allocates the cloud service quotas to each level-1 organizations by referring to the logical inventory set by the platform administrator.
3. Each organization administrator allocates resource quotas to subordinate organizations or resource sets in sequence.

> **Note**
>
> For more information about how an operations administrator or organization administrator allocates quotas, see Manage quotas.

If you perform operations on a cloud service, including activating the cloud service, changing the resource specifications, deleting resources, or changing the ownership of resources, the organizations and resource sets that have been allocated quotas directly use the quotas for resource verification and cost calculation update. For an organization or resource set that does not have quotas set, the quotas of the parent organization of the organization or resource set are used for verification.

Limits

- If the physical inventory of a cloud service is unlimited, the logical inventory cannot be less than the allocated inventory.
- If the physical inventory of a cloud service is limited, the default logical inventory cannot be less than the used inventory nor be greater than the physical inventory.

> **Important**
>
> - If the logical inventory is less than the used inventory, resources cannot be created.
> - To set a quota for the logical inventory that is greater than the physical inventory, you can contact technical support to disable physical inventory verification. This way, the physical inventory is unlimited.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Configure quota items

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Resource Pool Configuration**.
4. Select a region from the region drop-down list in the upper-left corner. In the upper-right corner of the page, select **Only View Cloud Services That Trigger Alerts** to display only the cloud services that trigger alerts.
5. Click the cloud service whose quotas you want to modify. The **Resource Pool Details** panel appears.

   In this example, an ECS instance is used. View the following parameters: **Resource Item**, **Logical Inventory**, **Physical Inventory**, and **Total Activated Resources**.
6. Click **Configure Quota** in the lower part of the panel.
7. In the **Configure Quota** dialog box, add or remove configuration items.
   - **Add quota items**: In the **Available Quotas** list on the left side, find the desired quota item and click **Add** in the **Actions** column to add the quota item to the **Added Quotas** list on the right side.
   - **Remove quota items**: In the **Added Quotas** list on the right side, find the desired quota item and click **Delete** in the **Actions** column to remove the quota item.
8. Click **OK**.

Create or modify the inventory

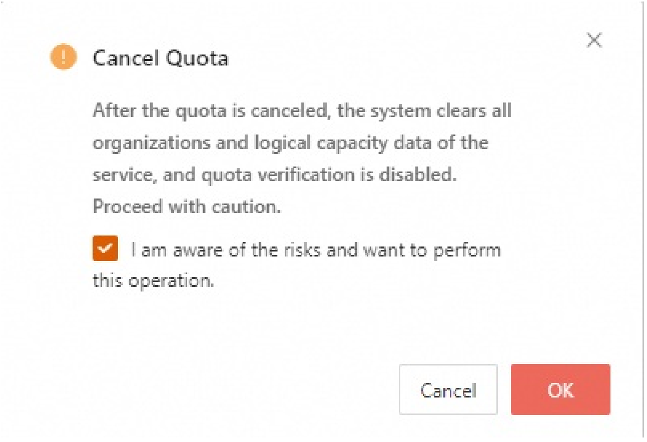
1. In the **Resource Pool Details** panel, click **Create Inventory** or **Modify Inventory**.
2. Modify the inventory quotas in the **Logical Inventory** column to limit the maximum usage of resources.

   > **Note**
   >
   > If you do not specify a quota for a resource item, no quota is configured for the resource item by default. The system does not limit the overhead of the corresponding resources.
3. Click **Save**.

Cancel quotas

> **Important**
>
> - If the total number of resources to be activated and activated resources is greater than the physical inventory, you can cancel quotas to clear the quota data of the service. When resources are created after the quota data is cleared, the console no longer verifies the resources of the service to allow resources to be oversold.
> - If you cancel quotas, the capacity data of the logical inventory of the cloud service is cleared in all organizations and the quota verification feature is disabled. Proceed with caution.

1. In the **Resource Pool Details** panel, click **Cancel Quota**.
2. In the **Cancel Quota** dialog box, select **I am aware of the risks and want to perform this operation.**



Cancel Quota

After the quota is canceled, the system clears all organizations and logical capacity data of the service, and quota verification is disabled. Proceed with caution.

☑ I am aware of the risks and want to perform this operation.

3. Click **OK**.

5.2. Manage regions

This topic describes how to associate a region with a geographical location. You can modify the location information when the location changes.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Region Settings**.
4. On the Region Settings page, view the names of regions and associated provinces, cities, and districts.
5. Find the region that you want to manage, click **Modify Location** in the Actions column, and then modify the information about the province, city, and district in the map.

   > **Note**
   >
   > District information is required.

6. Click **OK**.

5.3. Multi-cloud management

All cloud platforms that are managed in the Apsara Uni-manager Management Console are displayed on the Cloud Platform page. You can manage the cloud resources of Apsara Stack and Alibaba Cloud in a centralized manner.

Prerequisites

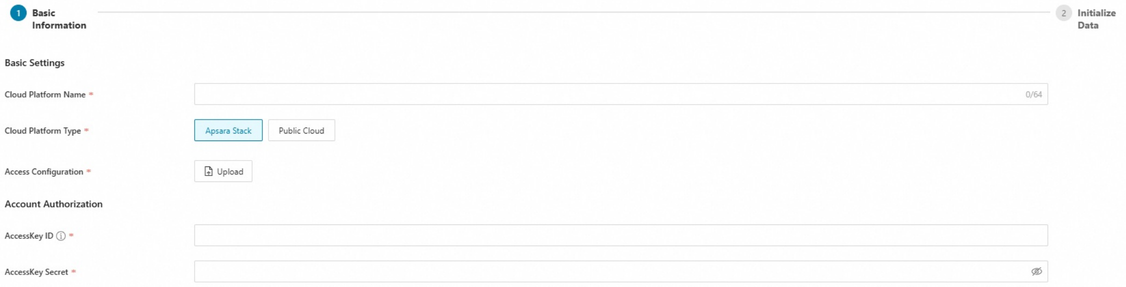
- Multi-cloud management is enabled.
- You are a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Multi-cloud Management**.
4. On the page that appears, click **Create Platform** to connect to an Apsara Stack platform or Alibaba Cloud platform.

   - **Connect to an Apsara Stack platform**

     a. In the Basic Settings section, complete the basic configurations of the required Apsara Stack platform, specify account authorization information, and then click **Create, and Continue**. The following table describes the required parameters.



1 Basic Information

2 Initialize Data

Basic Settings

Cloud Platform Name * 0/64

Cloud Platform Type * Apsara Stack | Public Cloud

Access Configuration * Upload

Account Authorization

AccessKey ID ⓘ *

AccessKey Secret *

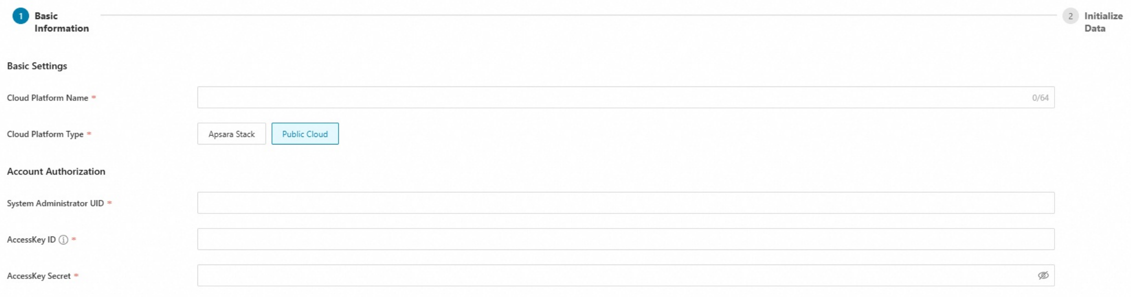
Parameter		Description
Basic Settings	**Cloud Platform Name**	Specify the name of the Apsara Stack platform.
	Cloud Platform Type	Select the type of the cloud platform. In this example, **Apsara Stack** is selected.
	Access Configuration	Click **Upload** to upload the configuration file of the Apsara Stack platform. You can export the configuration file of the required Apsara Stack platform on the Cloud Instances page.
Account Authorization	**AccessKey ID**	Specify the AccessKey ID of the Apsara Stack administrator account. By default, the Apsara Stack administrator account is the super account.
	Accesskey Secret	Specify the AccessKey secret of the Apsara Stack administrator account. By default, the Apsara Stack administrator account is the super account.

     b. In the Initialize Data step, select the required operations administrators from the **Bind Operations Administrator** drop-down list and click **Submit**.

> **Note**
>
> You can select multiple operations administrators.

   - **Connect to an Alibaba Cloud platform**

a. In the Basic Settings section, complete the basic configurations of the required Alibaba Cloud platform, specify account authorization information, and then click **Create, and Continue**. The following table describes the required parameters.



Basic Settings

Cloud Platform Name * 0/64

Cloud Platform Type * Apsara Stack [✓ Public Cloud]

Account Authorization

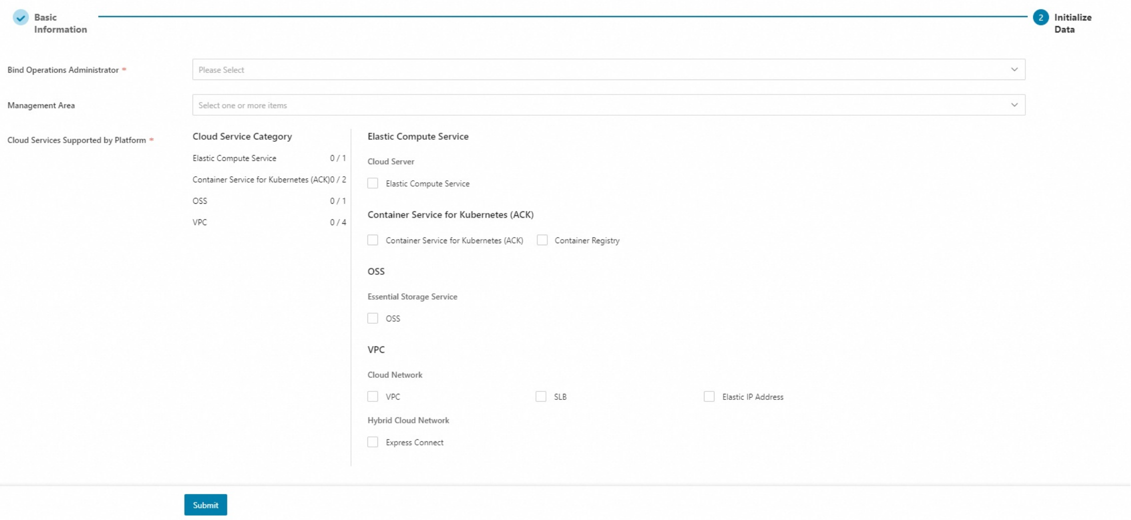
System Administrator UID *

AccessKey ID ⓘ *

AccessKey Secret *

Parameter		Description
Basic Settings	**Cloud Platform Name**	Specify the name of the Alibaba Cloud platform.
	Cloud Platform Type	Select the type of the cloud platform. In this example, **Public Cloud** is selected.
Account Authorization	**System Administrator UID**	Specify the ID of the Alibaba Cloud account that is used to log on to the required Alibaba Cloud platform.
	AccessKey ID	Specify the AccessKey ID of the Resource Access Management (RAM) user of the required Alibaba Cloud platform. The AdministratorAccess policy is attached to the RAM user.
	AccessKey Secret	Specify the AccessKey secret of the RAM user of the required Alibaba Cloud platform. The AdministratorAccess policy is attached to the RAM user.

b. In the Initialize Data step, configure the **Bind Operations Administrator (Primary Cloud)**, **Management Area**, and **Cloud Services Supported by Platform** parameters, and click **Submit**.



Basic Information — 2 Initialize Data

Bind Operations Administrator * Please Select

Management Area Select one or more items

Cloud Services Supported by Platform *

Cloud Service Category	
Elastic Compute Service	0 / 1
Container Service for Kubernetes (ACK)	0 / 2
OSS	0 / 1
VPC	0 / 4

Elastic Compute Service

Cloud Server

□ Elastic Compute Service

Container Service for Kubernetes (ACK)

□ Container Service for Kubernetes (ACK) □ Container Registry

OSS

Essential Storage Service

□ OSS

VPC

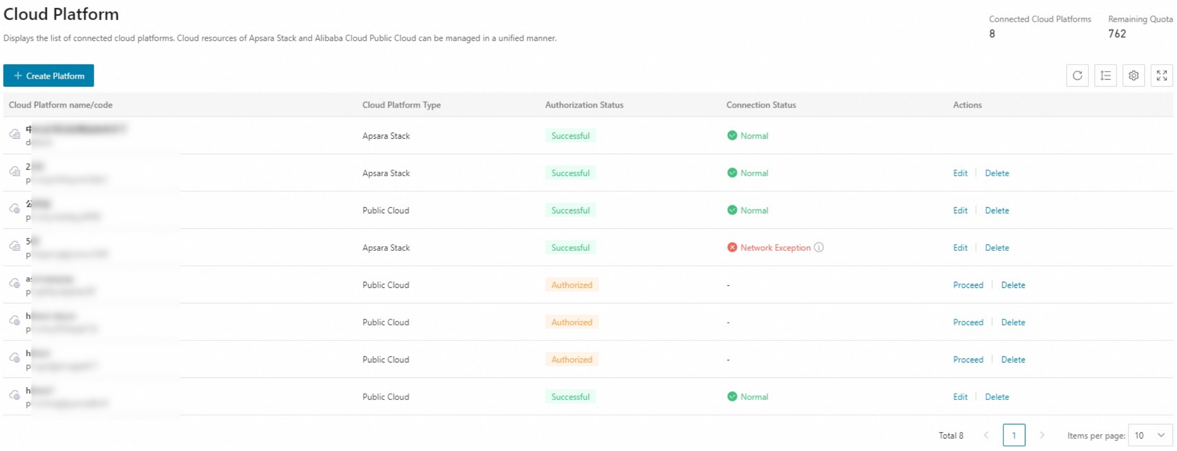
Cloud Network

□ VPC □ SLB □ Elastic IP Address

Hybrid Cloud Network

□ Express Connect

5. View and manage the connected cloud platform in the cloud platform list.



Cloud Platform

Displays the list of connected cloud platforms. Cloud resources of Apsara Stack and Alibaba Cloud Public Cloud can be managed in a unified manner.

Connected Cloud Platforms 8

Remaining Quota 762

Cloud Platform name/code	Cloud Platform Type	Authorization Status	Connection Status	Actions
[redacted]	Apsara Stack	Successful	✓ Normal	
[redacted]	Apsara Stack	Successful	✓ Normal	Edit | Delete
[redacted]	Public Cloud	Successful	✓ Normal	Edit | Delete
[redacted]	Apsara Stack	Successful	✗ Network Exception ⓘ	Edit | Delete
[redacted]	Public Cloud	Authorized	-	Proceed | Delete
[redacted]	Public Cloud	Authorized	-	Proceed | Delete
[redacted]	Public Cloud	Authorized	-	Proceed | Delete
[redacted]	Public Cloud	Successful	✓ Normal	Edit | Delete

Total 8 < 1 > Items per page: 10

- **View cloud platforms**

  a. In the upper-right corner of the Cloud Platform page, view the number of **connected cloud platforms** and the **remaining quota for connections**.

  b. In the cloud platform list, view the information about the connected cloud platforms in the following columns: **Cloud Platform Name/Code**, **Cloud Platform Type**, **Cloud Platform Status**, and **Connection Status**.

  > **Note**
  >
  > In the cloud platform list, the local cloud platforms and the connected cloud platforms are displayed. You can only change the names of the local cloud platforms.

- **Change the name of a cloud platform**

  a. Move the pointer over the name of the cloud platform that you want to manage and click the ✎ icon.

  b. Enter a new name and click **OK**.

- **Resume the creation of a cloud platform**

  If you complete the basic configurations when you create a cloud platform but do not proceed to the data initialization step, the system retains the configured settings to allow you to resume the platform creation process at a later time.

  a. Find the cloud platform that you want to manage and click **Proceed**.

  b. In the Initialize Data step, configure the required parameters and click **Submit**.

- **Modify a cloud platform**

  > **Note**
  >
  > When you modify a cloud platform, you cannot modify information such as the cloud platform type, access configuration, and account authorization.

  a. Find the cloud platform that you want to modify and click **Edit** in the Actions column.

  b. On the Modify Platform page, change the cloud platform name, modify initialization data, and then click **Submit**.

- **Delete a cloud platform**

  > **Important**
  >
  > After you delete a cloud platform, the temporary users or RAM roles created in the cloud platform are also deleted.

  a. Find the cloud platform that you want to delete and click **Delete** in the Actions column.

  b. Click **OK**.

5.4. Configure security policies

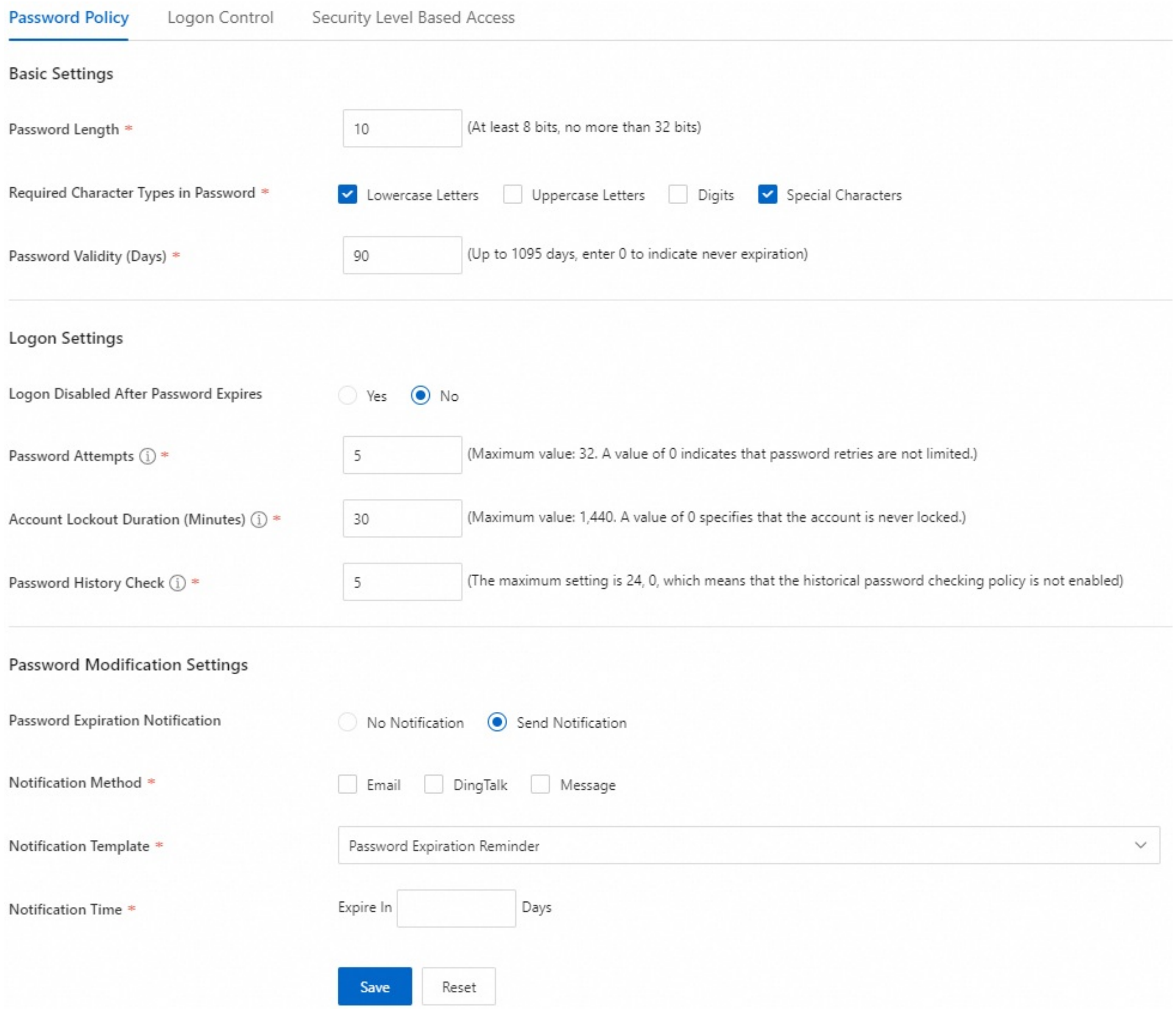
You can configure logon password policies, logon control settings, and resource security levels.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Configure password policies

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Security Policies** to the **Password Policy** tab.



Basic Settings

Password Length * 10 (At least 8 bits, no more than 32 bits)

Required Character Types in Password * ☑ Lowercase Letters □ Uppercase Letters □ Digits ☑ Special Characters

Password Validity (Days) * 90 (Up to 1095 days, enter 0 to indicate never expiration)

Logon Settings

Logon Disabled After Password Expires ○ Yes ● No

Password Attempts ⓘ * 5 (Maximum value: 32. A value of 0 indicates that password retries are not limited.)

Account Lockout Duration (Minutes) ⓘ * 30 (Maximum value: 1,440. A value of 0 specifies that the account is never locked.)

Password History Check ⓘ * 5 (The maximum setting is 24, 0, which means that the historical password checking policy is not enabled)

Password Modification Settings

Password Expiration Notification ○ No Notification ● Send Notification

Notification Method * □ Email □ DingTalk □ Message

Notification Template * Password Expiration Reminder

Notification Time * Expire In Days

Parameter		Description
Basic Settings	Password Length	The minimum length of a password. Valid values: 8 to 32.
	Required Character Types in Password	The character types that must be included in a password. You can select multiple options. Valid values: ◦ **Lowercase Letters** ◦ **Uppercase Letters** ◦ **Digits** ◦ **Special Characters**

	Password Validity (Days)	The validity period of a password. Unit: **days**. After the validity period ends, the password becomes invalid. Valid values: 0 to 1095. **Note** A value of 0 indicates that the password never expires.
Logon Settings	Logon Disabled After Password Expires	Specifies whether to allow a user to log on to the console after the password expires. Valid values: **Yes** and **No**. ◦ If you select **Yes**, the user cannot log on to the console after the password expires. In the drop-down list, select **Allow Users to Change Password** or **Do Not Allow Users to Change Password**. ▪ If you select **Allow Users to Change Password**, the user can change the password on the logon page after the password expires. After the password is changed, the user can log on to the console. ▪ If you select **Do Not Allow Users to Change Password**, the user cannot change the password on the logon page after the password expires. The user must contact the administrator to change the password before the user can log on to the console. ◦ If you select **No**, the user can log on to the console after the password expires. **Important** To prevent security risks caused by password disclosure, we recommend that you change your password at the earliest opportunity. You can change your password on the logon page or contact the administrator to change the password.
	Password Attempts	The maximum number of logon attempts within 1 hour. After the maximum number is reached, the account is locked and cannot be used to log on for a specific period of time. Valid values: 0 to 32. **Note** A value of 0 indicates that password retries are not limited.

	Account Lockout Duration (Minutes)	The period of time during which logons from an account are prohibited. Unit: **minutes**. If the maximum number of attempts is reached, the account becomes locked. During the lockout period, the account cannot be used to log on to the console. Valid values: 0 to 1440. **Note** A value of 0 indicates that account lockout is disabled.
	Password History Check	The number of previous passwords that cannot be the same with the current password. Valid value: 0 to 24. **Note** A value of 0 indicates that the system does not check historical passwords. For example, if you set this parameter to 3, the current password cannot be the same as one of the previous five passwords that are used.
Password Modification Settings	Password Expiration Notification	Specifies whether the system notifies you after a password expires. Valid values: ○ **Send Notification** ○ **No Notification**
	Notification Method	The notification method. Valid values: ○ **Email** ○ **DingTalk** ○ **Message** **Note** This parameter is displayed only if the Password Expiration Notification parameter is set to Send Notification.

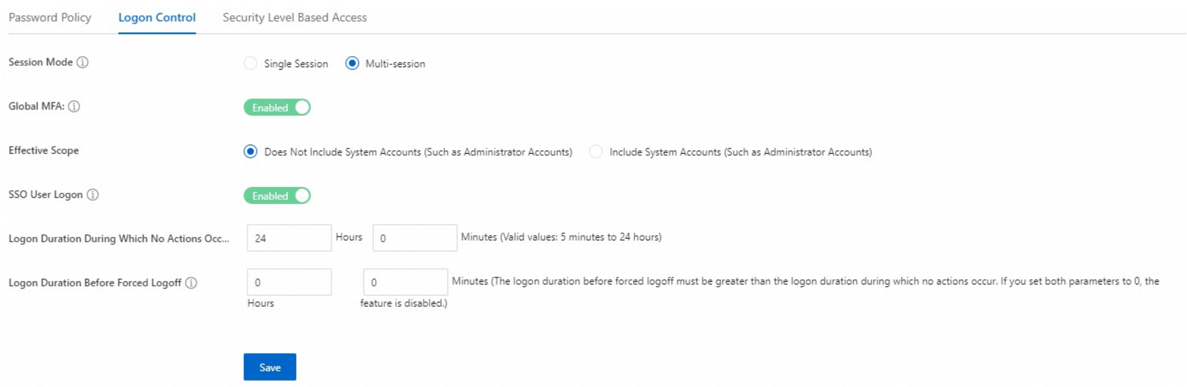
	Notification Template	The template based on which the system sends notifications. For information about how to configure template content, see the Configure a message template section of the Message gateway topic. **Note** This parameter is displayed only if the Password Expiration Notification parameter is set to Send Notification.
	Notification Time	The number of days before the expiration of a password on which the system sends notifications. Valid values: 1 to 30 **Note** This parameter is displayed only if the Password Expiration Notification parameter is set to Send Notification.

4. Click **Save**.

   You can click **Reset** to use the default settings.

Logon Control

1. On the **Security Policies** page, click the **Logon Control** tab.
2. Configure the parameters described in the following table based on your business requirements.



Session Mode ⓘ ○ Single Session ● Multi-session

Global MFA: ⓘ Enabled

Effective Scope ● Does Not Include System Accounts (Such as Administrator Accounts) ○ Include System Accounts (Such as Administrator Accounts)

SSO User Logon ⓘ Enabled

Logon Duration During Which No Actions Occ... 24 Hours 0 Minutes (Valid values: 5 minutes to 24 hours)

Logon Duration Before Forced Logoff ⓘ 0 Hours 0 Minutes (The logon duration before forced logoff must be greater than the logon duration during which no actions occur. If you set both parameters to 0, the feature is disabled.)

Parameter	Description

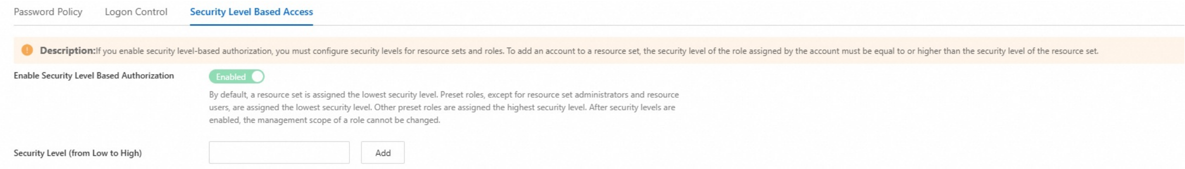
Session Mode	The session mode. Valid values: ◦ Single Session: A user can log on by using only a single client at the same time. ◦ Multi-session: A user can log on by using multiple clients at the same time.
Global MFA	Specifies whether to enable global multi-factor authentication (MFA). ◦ Enabled: MFA is required for all accounts on the platform. ◦ Disabled: MFA is not required for accounts on the platform.
Effective Scope	The scope of accounts for which **global MFA** is enabled. Valid values: ◦ Does Not Include System Accounts (Such as Administrator Accounts) ◦ Include System Accounts (Such as Administrator Accounts) **Note** This parameter is displayed only if Global MFA is turned on.
SSO User Logon	Specifies whether to allow single sign-on (SSO) users to log on to the platform. ◦ When the switch is turned on, SSO users can directly log on to the platform. ◦ When the switch is turned off, SSO users cannot directly log on to the platform and can log on only by using SSO. **Note** Platform administrators are not subject to this configuration.
Logon Duration During Which No Actions Occur	The specific period of time during which no operations are performed before the system logs off a user. Valid values: 5 minutes to 24 hours. If no actions are performed for the specified number of minutes, the user is forcefully logged off. The user must re-log on.
Logon Duration Before Forced Logoff	The specific period of time before the system forcefully logs off a user. The system prompts and forcefully logs off a user within the specified duration. The user must re-log on. **Important** The logon duration before the user is forcefully logged off must be greater than or equal to the logon duration during which no operations are performed. A value of 0 indicates that this feature is disabled.

3. Click **Save**.

Security level-based access

If you enable security level-based authorization, you must configure security levels for resource sets and roles. To add an account to a resource set, the security level of the role assigned by the account must be higher than or equal to the security level of the resource set.

1. On the **Security Policies** page, click the **Security Level Based Access** tab.
2. Configure the parameters based on your business requirements. The following table describes the parameters.



Description: If you enable security level-based authorization, you must configure security levels for resource sets and roles. To add an account to a resource set, the security level of the role assigned by the account must be equal to or higher than the security level of the resource set.

Enable Security Level Based Authorization: Enabled

By default, a resource set is assigned the lowest security level. Preset roles, except for resource set administrators and resource users, are assigned the lowest security level. Other preset roles are assigned the highest security level. After security levels are enabled, the management scope of a role cannot be changed.

Security Level (from Low to High)

Parameter	Description
Enable Security Level Based Authorization	Specifies whether to enable security level-based authorization. **Important** - After you enable security level-based authorization, you cannot disable it in the console. If you want to disable security level-based authorization, contact technical support. - By default, after you enable security level-based authorization, a resource set is assigned the lowest security level. Preset roles, such as resource set administrators and resource users, are assigned the lowest security level. Other preset roles are assigned the highest security level. The management scope of a role cannot be changed.
Security Level (from Low to High)	Default levels: **Non-secret**, **Secret**, **General**, and **Enhanced**. **Important** - You can add up to 10 security levels. - If you do not enable security level-based authorization, you can add, modify, and delete security levels. - After you enable security level-based authorization, you can modify the description of a security level and add security levels. You cannot delete existing security levels.

5.5. Authentication modes

5.5.1. Authentication modes

This topic describes the authentication modes. Authentication modes are classified into the token mode and the hybrid mode. You can configure an authentication mode based on your business requirements.

Token mode

In token mode, Resource Access Management (RAM) and Security Token Service (STS) are required. Temporary STS tokens are issued to users and cloud services to assist in permission management.

- In token mode, all cloud services use STS tokens to authenticate users. Cloud services that do not support STS may be affected. For example, only operations administrators and level-1 organization administrators can log on to the console of a cloud service.

  > ⓘ **Note**
  >
  > On the **Authentication Mode** page, you can view the cloud services that support the token mode.

- After you enable the token mode, authentication of northbound APIs may be affected.

  For example, if you use the AccessKey pair of a RAM user to call an API operation to add, delete, modify, or query specified resources in a specified organization and resource set, and the required RAM policies are not attached to the RAM user, an error may be returned.

  > ⚠ **Warning**
  >
  > Before you enable the token mode, we recommend that you contact Alibaba Cloud to evaluate the situation. If an error occurs when you call an API operation, disable the token mode.

Hybrid mode

In hybrid mode, cloud services that support RAM and STS can still authenticate users based on STS tokens. For cloud services that do not support STS, permissions are managed based on the authentication logic of Apsara Stack tenant accounts and RAM users. In hybrid mode, if you select one or more cloud services, the cloud services use STS tokens to authenticate users. Cloud services that are not selected still authenticate users in hybrid mode.

5.5.2. Configure an authentication mode

You can configure an authentication mode based on the scenario.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Authentication Mode**.
4. Select **Token Mode** or **Hybrid** based on the scenario.

   If you select **Hybrid**, you can control the authentication model of a cloud service by selecting or clearing the cloud service. If you select a cloud service, Security Token Service (STS)-based authentication is enabled for the cloud service.

> **Important**
>
> After token-based authentication is enabled, the authentication mode of northbound API operations is affected. We recommend that you contact the Alibaba Cloud service team for evaluation before you enable token-based authentication. If an error occurs when an API operation is called, roll back and disable token-based authentication for the service.

5. In the lower part of the page, click **Save**.

5.6. Specification management

5.6.1. Specifications

A platform administrator can enable and disable specifications for cloud services to control the specifications that are available when users create cloud resources. This topic describes the specification parameters of each configurable cloud service.

Elastic computing

Elastic Compute Service (ECS)

Parameter	Description
Region	The region in which ECS can be deployed.
GPUs	The number of GPUs that can be configured for ECS.
Instance Family	The instance family that is divided into different instance types based on the scenarios for which they are suitable.
Instance Type	The instance type that can be configured for ECS.
Disk Type	The disk type that can be configured for ECS.
CPU Model	The CPU model that can be configured for ECS.
Edition	The category of the instance family that can be configured for ECS.
CPUs	The number of CPU cores that can be configured for ECS.
Support Hot Configuration Changes	Specifies whether ECS supports the hot configuration change feature.
Memory (GB)	The memory size that can be configured for ECS.

CPU Brand	The CPU type that can be configured for ECS.
Specifications Level	The level of the instance family that can be configured for ECS.
Supported ENIs	The number of Elastic network interfaces (ENIs) that can be configured for ECS.
Support Deployment Set	Specifies whether ECS supports deployment sets.
Zone	The zone in which ECS can be deployed.
Architecture	The architecture that can be configured for ECS.
GPU Specifications	The GPU type that can be configured for ECS.
Private IP Addresses	The number of private IP addresses that can be configured for ECS.
Specification Source	The specification source that can be configured for ECS.

Storage

Object Storage Service (OSS)

Parameter	Description
Region	The region in which OSS can be deployed.
Storage Type	The storage type that can be configured for OSS.
Specification Source	The specification source that can be configured for OSS.

Networking

NAT Gateway

Parameter	Description
Region	The region in which NAT Gateway can be deployed.
Storage Type	The storage type that can be configured for NAT Gateway.

Specification Source	The specification source that can be configured for NAT Gateway.

Server Load Balancer (SLB)

Parameter	Description
Region	The region in which SLB can be deployed.
New Connections	The number of new connections that can be configured for SLB.
QPS	The queries per second (QPS) that can be configured for SLB.
Instance Type	The specification that can be configured for SLB.
Name	The specification description that can be configured for SLB.
Specifications	The instance type that can be configured for SLB.
Max. Connections	The maximum number of connections that can be configured for SLB.
Specification Source	The specification source that can be configured for SLB.

IPv6 Gateway

Parameter	Description
Region	The region in which IPv6 Gateway can be deployed.
Specifications	The specification that can be configured for IPv6 Gateway.
Specification Source	The specification source that can be configured for IPv6 Gateway.

Database services

ApsaraDB RDS

Parameter	Description

Region	The region in which ApsaraDB RDS can be deployed.
Engine Version	The engine version that can be configured for ApsaraDB RDS.
Maximum Storage	The maximum storage capacity that can be configured for ApsaraDB RDS.
Chip Type	The chip type that can be configured for ApsaraDB RDS.
Instance Type	The instance type that can be configured for ApsaraDB RDS.
Memory	The memory size that can be configured for ApsaraDB RDS.
CPU	The number of CPU cores that can be configured for ApsaraDB RDS.
Storage Type	The storage type that can be configured for ApsaraDB RDS.
Default Storage	The default amount of storage capacity that can be configured for ApsaraDB RDS.
Database Engine	The database engine that can be configured for ApsaraDB RDS.
Edition	The instance edition that can be configured for ApsaraDB RDS.
IOPS	The IOPS that can be configured for ApsaraDB RDS.
Step Size	The step size that can be configured for ApsaraDB RDS.
Minimum Storage	The minimum amount of storage capacity that can be configured for ApsaraDB RDS.
Connections	The number of connections that can be configured for ApsaraDB RDS.
Specification Source	The specification source that can be configured for ApsaraDB RDS.

PolarDB-X 1.0

Parameter	Description

Region	The region in which PolarDB-X 1.0 can be deployed.
Memory	The memory size that can be configured for PolarDB-X 1.0.
CPU	The number of CPU cores that can be configured for PolarDB-X 1.0.
Specifications	The instance type that can be configured for PolarDB-X 1.0.
Instance Edition	The instance edition that can be configured for PolarDB-X 1.0.
Specification Source	The specification source that can be configured for PolarDB-X 1.0.

PolarDB-X 2.0

Parameter	Description
Region	The region in which PolarDB-X 2.0 can be deployed.
Engine Version	The engine version that can be configured for PolarDB-X 2.0.
Instance Type	The instance type that can be configured for PolarDB-X 2.0.
Chip Type	The chip type that can be configured for PolarDB-X 2.0.
Memory	The memory size that can be configured for PolarDB-X 2.0.
Node Specification	The node specifications that can be configured for PolarDB-X 2.0. The specifications include the specification name, the memory size, and the number of CPU cores.
Edition	The instance edition that can be configured for PolarDB-X 2.0.
Instance Family	The instance family that can be configured for PolarDB-X 2.0.
Instance Type	The instance type that can be configured for PolarDB-X 2.0.
CPU	The number of CPU cores that can be configured for PolarDB-X 2.0.
Specification Source	The specification source that can be configured for PolarDB-X 2.0.

ApsaraDB for MongoDB

Parameter	Description
Region	The region in which ApsaraDB for MongoDB can be deployed.
Version	The engine version that can be configured for ApsaraDB for MongoDB.
Maximum Storage	The maximum storage capacity that can be configured for ApsaraDB for MongoDB.
Chip Type	The chip type that can be configured for ApsaraDB for MongoDB.
Memory	The memory size that can be configured for ApsaraDB for MongoDB.
CPU	The number of CPU cores that can be configured for ApsaraDB for MongoDB.
Storage Capacity	The storage capacity that can be configured for ApsaraDB for MongoDB.
Node Type	The node type that can be configured for ApsaraDB for MongoDB.
Edition	The instance edition that can be configured for ApsaraDB for MongoDB.
Specifications	The instance type that can be configured for ApsaraDB for MongoDB.
Database Instance Type	The database instance type that can be configured for ApsaraDB for MongoDB.
IOPS	The IOPS that can be configured for ApsaraDB for MongoDB.
Step Size	The step size that can be configured for ApsaraDB for MongoDB.
Connections	The number of connections that can be configured for ApsaraDB for MongoDB.
Minimum Storage	The minimum storage capacity that can be configured for ApsaraDB for MongoDB.

Specification Source	The specification source that can be configured for ApsaraDB for MongoDB.

Tair (Redis OSS-compatible)

Parameter	Description
Region	The region in which Tair (Redis OSS-compatible) can be deployed.
Engine Version	The engine version that can be configured for Tair (Redis OSS-compatible).
Bandwidth	The bandwidth that can be configured for Tair (Redis OSS-compatible).
Memory	The memory that can be configured for Tair (Redis OSS-compatible).
Edition	The instance edition that can be configured for Tair (Redis OSS-compatible).
Plan Type	The plan type that can be configured for Tair (Redis OSS-compatible).
Specifications	The instance type that can be configured for Tair (Redis OSS-compatible).
Name	The name of the instance type that can be configured for Tair (Redis OSS-compatible).
Node Type	The node type that can be configured for Tair (Redis OSS-compatible).
Architecture	The architecture that can be configured for Tair (Redis OSS-compatible).
CPU	The number of CPU cores that can be configured for Tair (Redis OSS-compatible).
Connections	The number of connections that can be configured for Tair (Redis OSS-compatible).
Specification Source	The specification source that can be configured for Tair (Redis OSS-compatible).

PolarDB

Parameter	Description
Region	The region in which PolarDB can be deployed.
Proxy Memory (GB)	The proxy memory size that can be configured for PolarDB.
Chip Type	The CPU chip type that can be configured for PolarDB.
Node Specifications	The node specifications that can be configured for PolarDB.
Instance Family	The instance family that can be configured for PolarDB.
Memory (GB)	The memory size that can be configured for PolarDB.
Database Edition	The database edition that can be configured for PolarDB.
Nodes	The number of nodes that can be configured for PolarDB.
Proxy Type	The proxy type that can be configured for PolarDB.
Compatibility	The database type that can be configured for PolarDB.
CPU (Cores)	The number of CPU cores that can be configured for PolarDB.
Proxy Specifications	The proxy specification that can be configured for PolarDB.
Proxy CPU (Cores)	The number of proxy CPU cores that can be configured for PolarDB.
Service Type	The service type that can be configured for PolarDB.
Specification Source	The specification source that can be configured for PolarDB.

5.6.2. Create or synchronize specifications

You can create or synchronize specifications of cloud resources.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Specifications**.
4. On the Specifications page, select a cloud service from the **Resource Specification Settings** drop-down list.
5. Click the **Resource Specifications** tab.
    - **Create specifications**

        > **Note**
        >
        > You can create specifications for the following cloud services: NAT Gateway, Server Load Balancer (SLB), IPv6 Gateway, ApsaraDB RDS, Tair (Redis OSS-compatible), PolarDB-X 1.0, PolarDB-X 2.0, ApsaraDB for MongoDB, and PolarDB.

        a. Click **Create Specifications**.

        b. In the Create Specifications dialog box, configure the parameters. For more information about the specification parameters, see Specifications.

        c. Click **OK**.
    - **Synchronize specifications**

        > **Note**
        >
        > The specifications of cloud services are synchronized to the current system by calling API operations. You can manually synchronize the specifications of Elastic Compute Service (ECS).

        a. Click **Synchronize Specifications**.

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

5.6.3. Manage specifications

You can enable or disable specifications of different cloud resources. This way, only enabled specifications can be configured when resources are created.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Specifications**.

i. On the Specifications page, configure the **Specification Synchronization Settings** parameter to specify the specification synchronization mechanism.

> ⓘ **Important**
>
> New specifications may be released after cloud services are updated. You can configure the specification synchronization mechanism to make sure the specifications are up-to-date.

a. Click **Edit**. Select **Maintain Current Specifications** or **Synchronize Specifications**.

- **Maintain Current Specifications**: New specifications are not synchronized after version updates.

  > ⓘ **Note**
  >
  > Select this option if you want to retain the existing configurations after version updates.

- **Synchronize Specifications**: New specifications are synchronized after version updates.

  > ⓘ **Note**
  >
  > We recommend that you select this option to make sure that specifications are up-to-date.

b. Click **Save**.

ii. Select a cloud service from the **Resource Specification Settings** drop-down list.

Operation	Procedure
View specifications	- Click the **Resource Specifications** tab to view the information about resource specifications, such as the status. - Click the **Specifications History** tab to view the information about historical specifications. - Click the **Existing Specifications** tab to view the used specifications and the number of resources that use the specifications.
Disable a specification	You can disable an enabled specification. The disabled specification is unavailable when users create the corresponding resources. a. Click the **Resource Specifications** tab. b. Find the resource specification that you want to disable and click**Disable** in the Actions column. c. In the message that appears, click**OK**.
Enable a specification	You can enable disabled specifications. a. Click the **Resource Specifications** tab. b. Find the resource type that you want to enable and click**Enable** in the Actions column. c. In the message that appears, click**OK**.
Export specifications	You can export the specification information to your computer for backup. a. Click the **Resource Specifications** tab. b. Click **Export** above the specification list. c. Configure the storage path, enter a file name, and then click**Download** to export specifications of the cloud service as a .csv file to your computer.

5.6.4. Examples

5.6.4.1. Create an ApsaraDB RDS instance specification

Background information

Company A uses ApsaraDB RDS to deploy and manage database instances. The company needs to create a new ApsaraDB RDS instance specification to meet the requirements of different departments and applications.

Planning

Company A analyzes the specific requirements of departments and applications and poses the following requirements on the specification: The vCPU performance must be high and content resources must be extensive to support large-scale database operations. The storage capacity and the maximum number of connections can be expanded based on business requirements. SSD storage is required. High-speed read and write performance and a low failure rate are required. Company A then plans specification configurations based on these requirements. Example:

vCPU: 8 cores

Memory: 16 GB

Storage: 500 GB SSD

Maximum number of connections: 1,000

Database engine: MySQL 8.0

> ⓘ **Important**
>
> Before you create specifications, check with cloud service technical support to make sure that the specifications are available.

Prerequisites

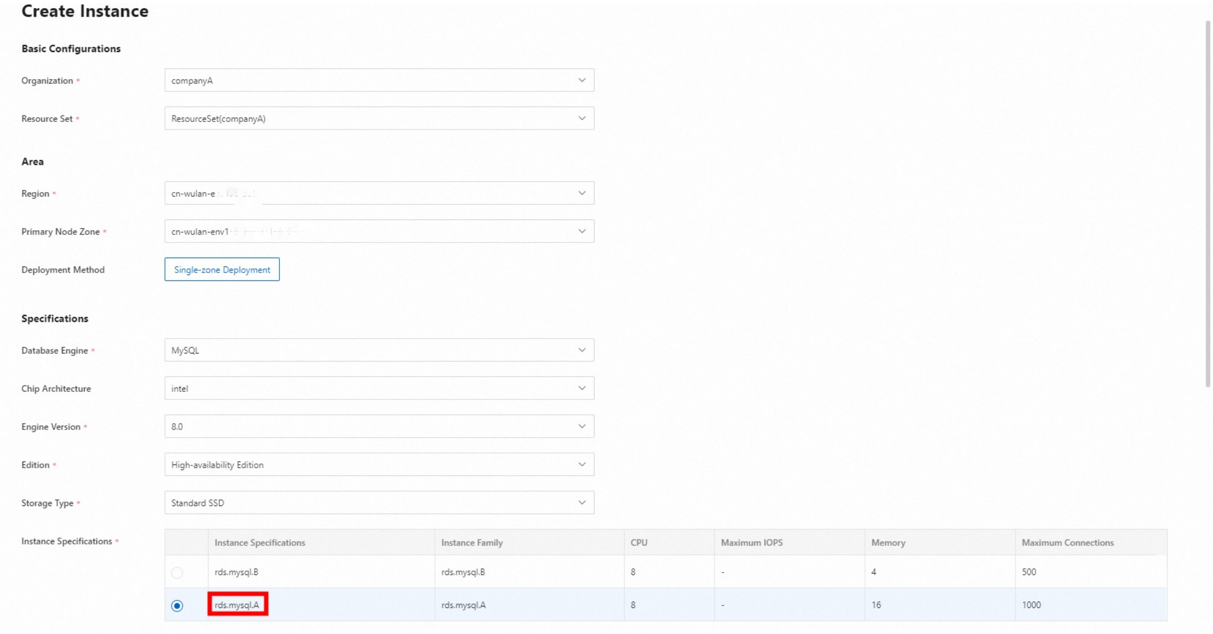
You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Specifications**.
4. On the **Specifications** page, choose **Database Services** > **ApsaraDB RDS** from the **Resource Specification Settings** drop-down list.
5. On the **Resource Specifications** tab, click **Create Specifications**.
6. In the **Create Specifications** dialog box, configure the parameters.
   - Database Engine: MySQL
   - Minimum Storage: 500
   - Maximum Storage: 3000
   - Instance Type: rds.mysql.A
   - Chip Type: intel
   - Engine Version: 8.0
   - cpu: 8
   - Connections: 1,000
   - Memory: 16
   - Edition: dual_ha
   - Storage Type: cloud_ssd
7. Click **OK**. View the specification you created in the specification list.

Subsequent impact

The administrator named orgA of the level-1 organization of Company A can select the created specification when orgA creates an ApsaraDB RDS instance.



Create Instance

Basic Configurations

Organization * companyA

Resource Set * ResourceSet(companyA)

Area

Region * cn-wulan-e[redacted]

Primary Node Zone * cn-wulan-env1[redacted]

Deployment Method: Single-zone Deployment

Specifications

Database Engine * MySQL

Chip Architecture: intel

Engine Version * 8.0

Edition * High-availability Edition

Storage Type * Standard SSD

Instance Specifications *

	Instance Specifications	Instance Family	CPU	Maximum IOPS	Memory	Maximum Connections
○	rds.mysql.B	rds.mysql.B	8	-	4	500
●	rds.mysql.A	rds.mysql.A	8	-	16	1000

5.6.4.2. Disable an ApsaraDB RDS instance specification

Background information

Due to changes in business, Company A needs to disable the ApsaraDB RDS instance specification rds.mysql.A. After this specification is disabled, the related departments and applications can no longer use the specification. For more information about how to create the specification rds.mysql.A, see Create an ApsaraDB RDS instance specification.

Planning

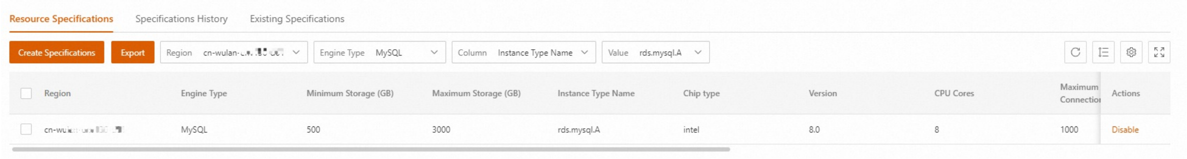
After the specification rds.mysql.A is disabled, it is unavailable when users create ApsaraDB RDS instances.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Procedure

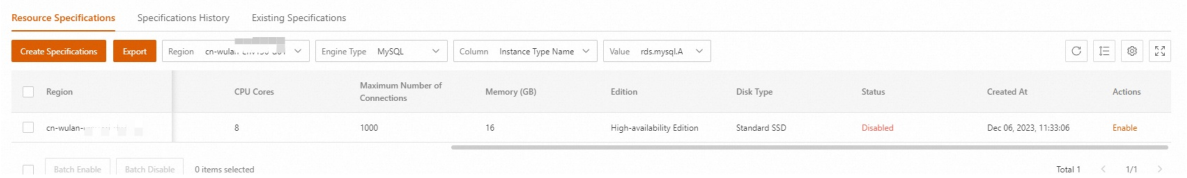
1. Log on to the Apsara Uni-manager Management Console as the super administrator.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Specifications**.
4. On the **Specifications** page, choose **Database Services** > **ApsaraDB RDS** from the **Resource Specification Settings** drop-down list.
5. On the **Resource Specifications** tab, find the specification rds.mysql.A and click **Disable** in the **Actions** column.



Region cn-wulan-[redacted] | Engine Type MySQL | Column Instance Type Name | Value rds.mysql.A

□	Region	Engine Type	Minimum Storage (GB)	Maximum Storage (GB)	Instance Type Name	Chip type	Version	CPU Cores	Maximum Connectio	Actions
□	cn-wu[redacted]	MySQL	500	3000	rds.mysql.A	intel	8.0	8	1000	Disable

6. In the message that appears, click **OK**. After the specification is disabled, the value in the **Status** column of the specification changes to **Disabled**.



Region cn-wula[redacted] | Engine Type MySQL | Column Instance Type Name | Value rds.mysql.A

□	Region	CPU Cores	Maximum Number of Connections	Memory (GB)	Edition	Disk Type	Status	Created At	Actions
□	cn-wulan-[redacted]	8	1000	16	High-availability Edition	Standard SSD	Disabled	Dec 06, 2023, 11:33:06	Enable

□ Batch Enable Batch Disable 0 items selected Total 1 < 1/1 >

Subsequent impact

The specification rds.mysql.A is unavailable when the level-1 organization administrator orgA of Company A creates an ApsaraDB RDS instance.

5.7. Menu management

5.7.1. Configure a main menu item

You can configure the menu bar to manage access to services and operations based on your business requirements.

Background information

You can add external links to the Apsara Uni-manager Management Console for centralized management and easy access. This greatly simplifies operations, avoids frequent switching between different platforms, and improves work efficiency.

In addition, to implement personalized and categorized management, you can group and name menu items that you create for easy management and search. The highly flexible and user-friendly configuration method allows you to create, edit, and organize various submenu items based on your requirements. You can categorize related features into different groups to quickly and accurately locate the required features to better meet the requirements of different scenarios.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Menu item parameters

Parameter	Description
Title	The display name of the menu item.
URL	The URL of the menu item.

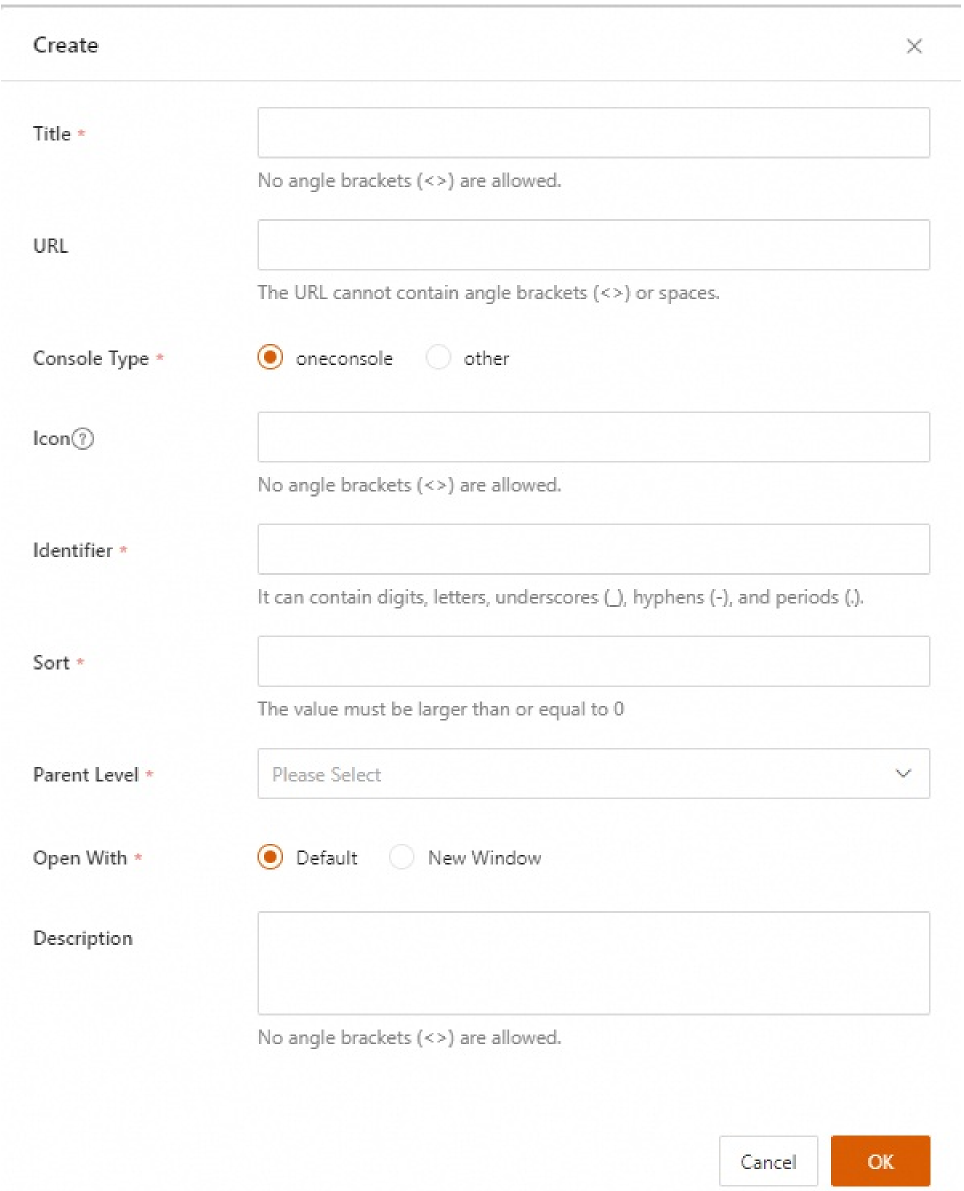
Console Type	The type of the console. Different consoles have different domain names. Valid values: oneconsole and other. - **oneconsole**: You need to only enter the path in the URL field. The domain name is automatically matched. The URL starts with one.console. - **other**: You must enter the domain name in the URL field.
Icon	The icon displayed in the left-side navigation pane. Enter an icon name based on the icons of hybrid cloud services in the component library.
Identifier	The unique identifier of the menu item in the system. This identifier can be used to indicate whether the menu item is selected in the navigation bar. The identifier cannot be changed.
Sort	The display order among the same-level menu items. The larger the value, the lower it is displayed.
Parent Level	The parent level to which the menu item belongs.
Group	The group to which the menu item belongs. This parameter is available and required when Parent Level is set to **Products**.
Open With	The method to open the page of the menu item. Valid values:**Default** and **New Window**. - **Default**: opens the page in the current window. - **New Window**: opens the page in a new window.
Description	The description of the menu item.

Create a menu item

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, choose **Menu Settings** > **Main Menu Configuration**.
4. On the **Main Menu Configuration** page, click the **Single-cloud Menu** or **Multi-cloud Menu** tab and click **Create**.

   > **Note**
   >
   > - **Single-cloud menu**: manages the menu items of a single-cloud role.
   > - **Multi-cloud Menu**: manages the menu items of a multi-cloud role.

5. In the **Create** dialog box, configure the parameters. For more information, see the Menu item parameters section of this topic.



Create ×

Title *

No angle brackets (<>) are allowed.

URL

The URL cannot contain angle brackets (<>) or spaces.

Console Type * ● oneconsole ○ other

Icon

No angle brackets (<>) are allowed.

Identifier *

It can contain digits, letters, underscores (_), hyphens (-), and periods (.).

Sort *

The value must be larger than or equal to 0

Parent Level * Please Select

Open With * ● Default ○ New Window

Description

No angle brackets (<>) are allowed.

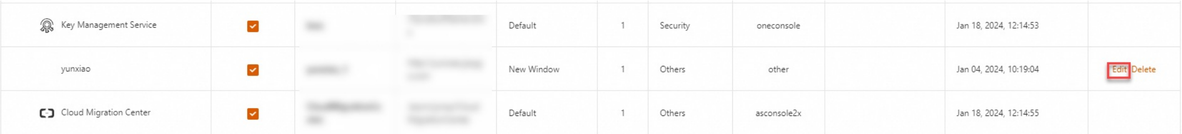
6. Click **OK**.

Modify a menu item

You modify the information about a menu item when it is changed.

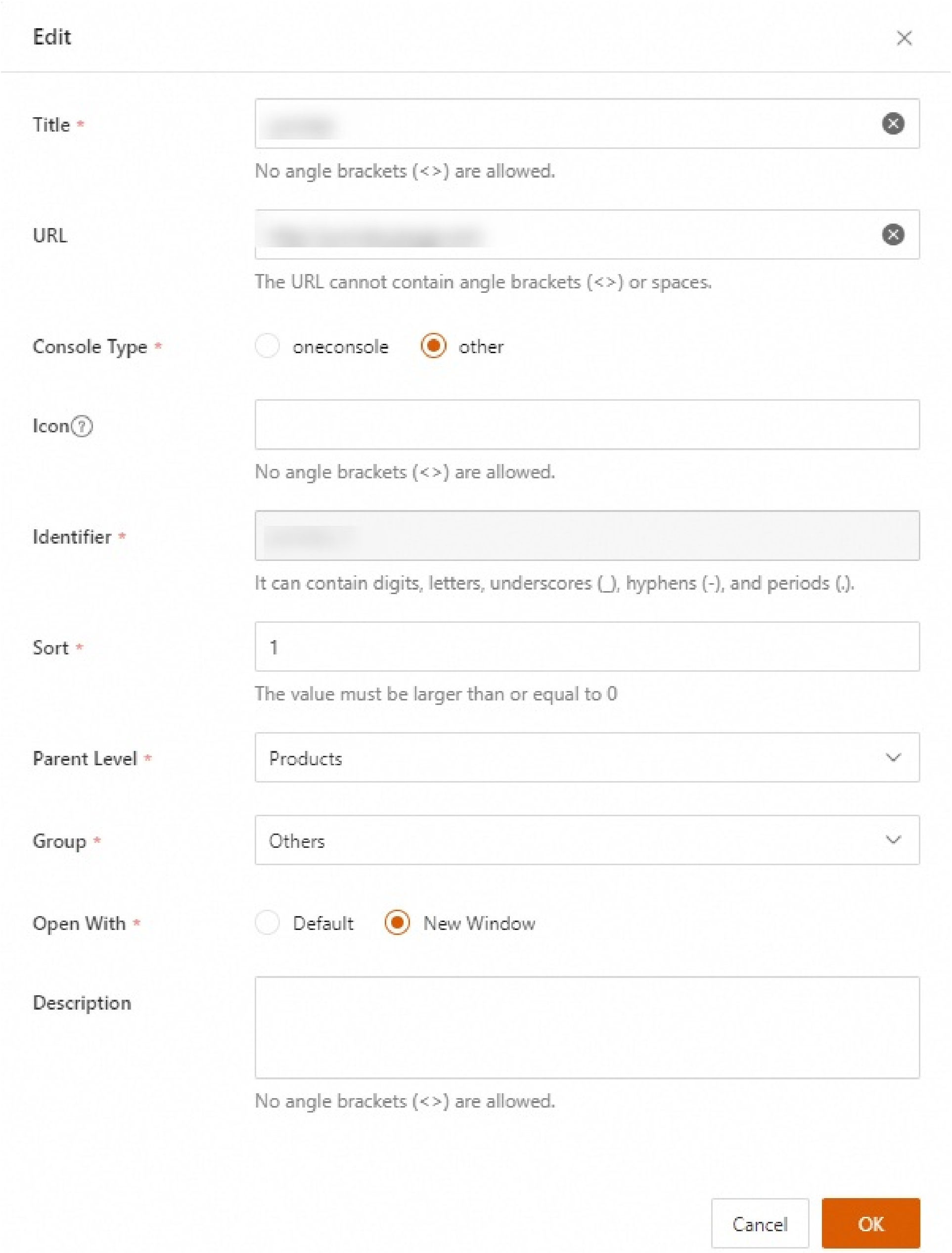
> **Important**
>
> The default menu items cannot be modified.

1. On the **Main Menu Configuration** page, click the **Single-cloud Menu** or **Multi-cloud Menu** tab, find the menu item that you want to manage, and then click **Edit** in the Actions column.



Key Management Service	☑	[redacted]	[redacted]	Default	1	Security	oneconsole		Jan 18, 2024, 12:14:53	
yunxiao	☑	[redacted]	[redacted]	New Window	1	Others	other		Jan 04, 2024, 10:19:04	Edit Delete
Cloud Migration Center	☑	[redacted]	[redacted]	Default	1	Others	asconsole2x		Jan 18, 2024, 12:14:55	

2. In the **Edit** dialog box, modify the menu item information and click **OK**.



Edit

Title * [redacted]

No angle brackets (<>) are allowed.

URL [redacted]

The URL cannot contain angle brackets (<>) or spaces.

Console Type * ○ oneconsole ● other

Icon

No angle brackets (<>) are allowed.

Identifier * [redacted]

It can contain digits, letters, underscores (_), hyphens (-), and periods (.).

Sort * 1

The value must be larger than or equal to 0

Parent Level * Products

Group * Others

Open With * ○ Default ● New Window

Description

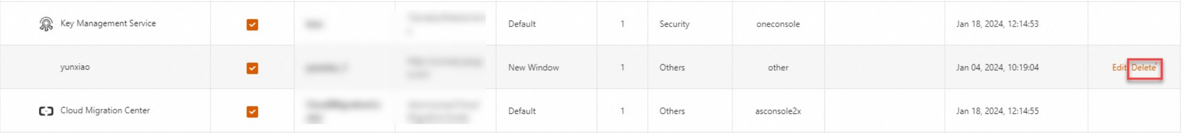
No angle brackets (<>) are allowed.

Delete a menu item

You can delete a menu item if you no longer need it.

> **Important**
>
> The default menu items cannot be deleted.

1. On the **Main Menu Configuration** page, click the **Single-cloud Menu** or **Multi-cloud Menu** tab, find the menu item that you want to manage, and then click **Delete** in the Actions column.



Key Management Service	☑	[redacted]	[redacted]	Default	1	Security	oneconsole		Jan 18, 2024, 12:14:53	
yunxiao	☑	[redacted]	[redacted]	New Window	1	Others	other		Jan 04, 2024, 10:19:04	Edit Delete
Cloud Migration Center	☑	[redacted]	[redacted]	Default	1	Others	asconsole2x		Jan 18, 2024, 12:14:55	

2. In the **Delete** message, click **OK**.

Display or hide a menu item

1. On the **Main Menu Configuration** page, click the **Single-cloud Menu** or **Multi-cloud Menu** tab, find the menu item that you want to manage, and then select or clear the check box in the **Display** column.

   - ☑: the menu item is displayed in the console.
   - □: the menu item is not displayed in the console.

5.7.2. Configure a service creation page

The Apsara Uni-manager Management Console allows you to configure service creation pages based on your business requirements of users. This feature allows administrators to globally adjust the parameters and layout of a series of service creation pages.

Background information

The feature of configuring creation pages allows you to specify the fields to be displayed and hidden, and specify required and optional fields. For example, if you want users to provide detailed descriptions in the Description field when the users create virtual private clouds (VPCs), you can use this feature to configure the Description field as mandatory.

This feature allows you to configure the following items for a service creation page:

- Required fields: Specify the fields that are required on the service creation page.
- Hidden fields: Hide some fields so that they are unavailable on the service creation page.
- Options: Display or hide some options of fields based on the requirements of users, and adjust the order of options based on the habits of users.

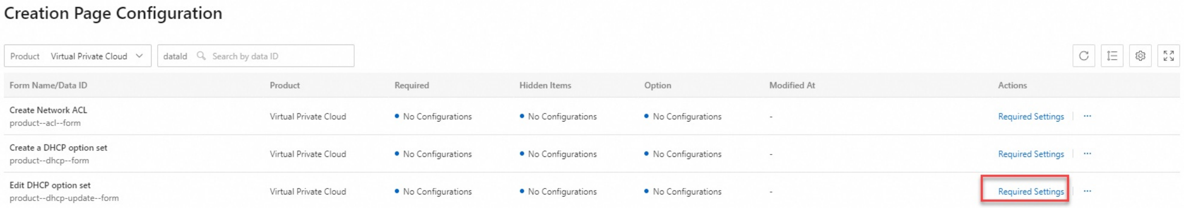
Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

Configure required fields

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, choose **Menu Settings** > **Creation Page Configuration**.
4. On the **Creation Page Configuration** page, find the form for the service whose creation page you want to manage.

   You can select the service name from the **Product** drop-down list and enter a **data ID** to quickly find the form.
5. Click **Required Settings** in the **Actions** column.



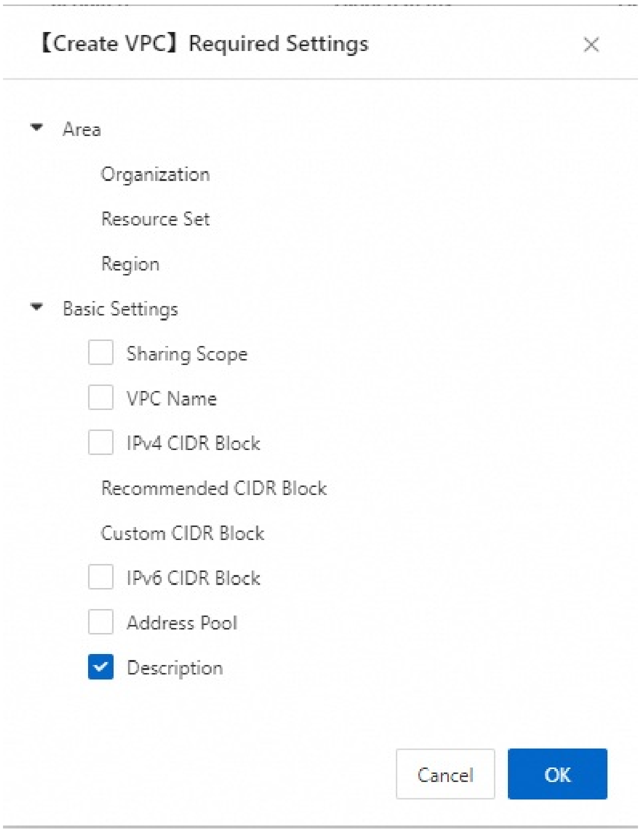
Creation Page Configuration

Product Virtual Private Cloud | dataId Search by data ID

Form Name/Data ID	Product	Required	Hidden Items	Option	Modified At	Actions
Create Network ACL product--acl--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Create a DHCP option set product--dhcp--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Edit DHCP option set product--dhcp-update--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···

6. In the **Required Settings** dialog box, select the fields that are required. For example, if you select the **Description** field, users must configure this parameter on a creation page.

> **Note**
>
> This configuration is applicable only to the fields that have a check box.



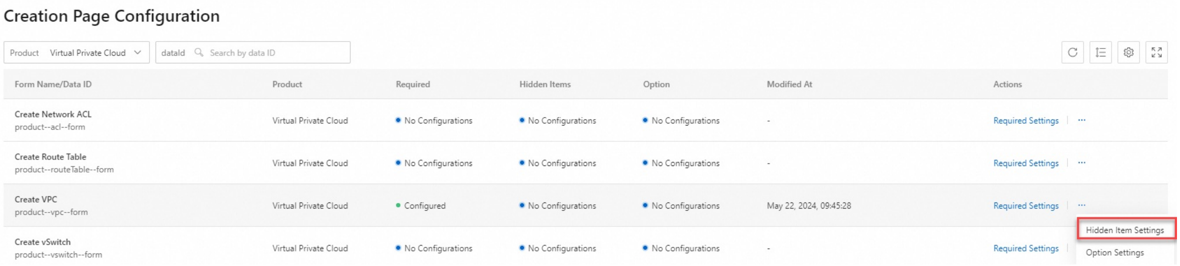
【Create VPC】 Required Settings

- Area
  - Organization
  - Resource Set
  - Region
- Basic Settings
  - ☐ Sharing Scope
  - ☐ VPC Name
  - ☐ IPv4 CIDR Block
  - Recommended CIDR Block
  - Custom CIDR Block
  - ☐ IPv6 CIDR Block
  - ☐ Address Pool
  - ☑ Description

7. Click **OK**.

Configure hidden fields

1. Find the form for the service whose creation page you want to manage, click the ... icon in the **Actions** column, and then click **Hidden Item Settings**.



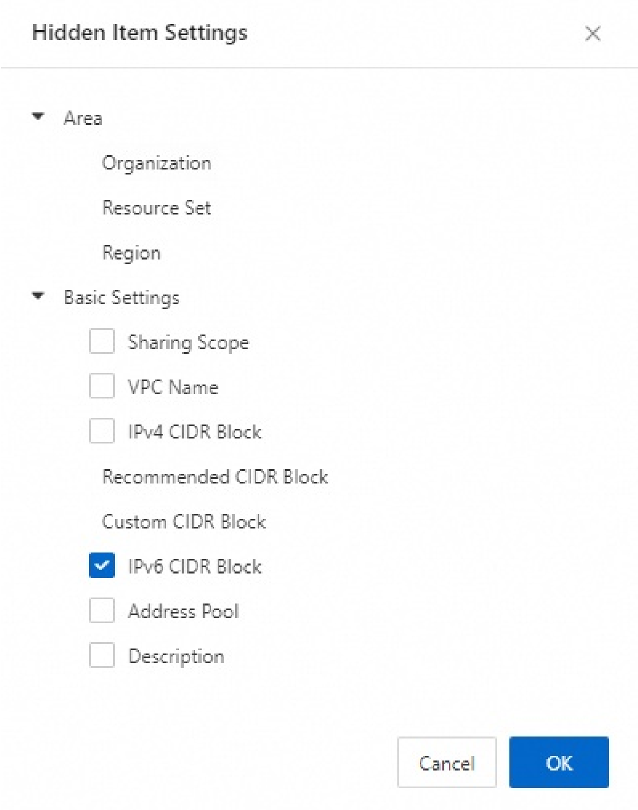
Creation Page Configuration

Product: Virtual Private Cloud | dataId: Search by data ID

Form Name/Data ID	Product	Required	Hidden Items	Option	Modified At	Actions
Create Network ACL product--acl--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Create Route Table product--routeTable--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Create VPC product--vpc--form	Virtual Private Cloud	● Configured	● No Configurations	● No Configurations	May 22, 2024, 09:45:28	Required Settings | ···
Create vSwitch product--vswitch--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings |

2. In the **Hidden Item Settings** dialog box, select the fields that you do not want to display. For example, if you select the **IPv6 CIDR Block** field, the field is not displayed on the creation page.

> **Note**
>
> This configuration is applicable only to the fields that have a check box.



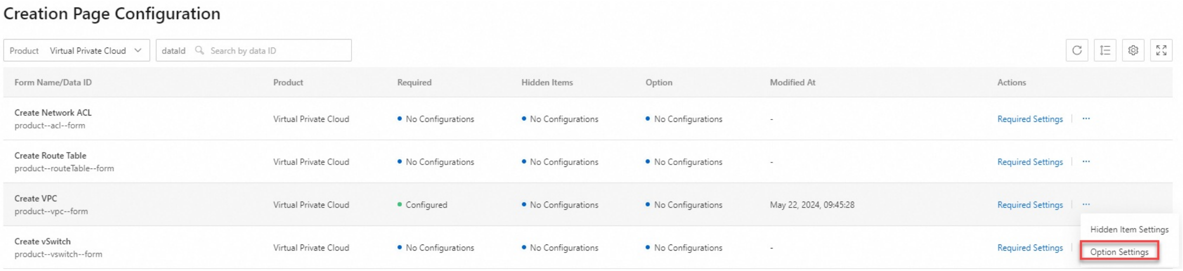
Hidden Item Settings

- Area
  - Organization
  - Resource Set
  - Region
- Basic Settings
  - ☐ Sharing Scope
  - ☐ VPC Name
  - ☐ IPv4 CIDR Block
  - Recommended CIDR Block
  - Custom CIDR Block
  - ☑ IPv6 CIDR Block
  - ☐ Address Pool
  - ☐ Description

3. Click **OK**.

Configure options

1. Find the form for the service whose creation page you want to manage, click the ... icon in the **Actions** column, and then click **Option Settings**.



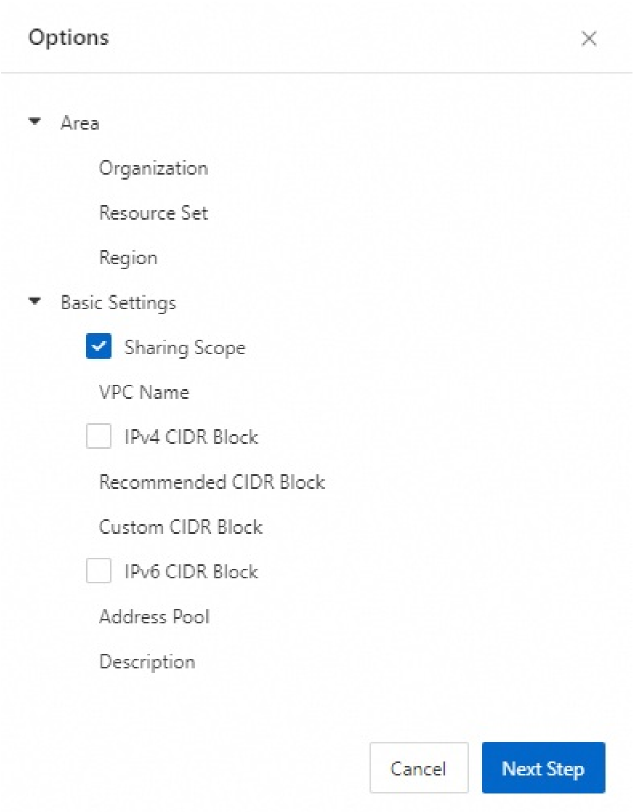
Creation Page Configuration

Product: Virtual Private Cloud | dataId: Search by data ID

Form Name/Data ID	Product	Required	Hidden Items	Option	Modified At	Actions
Create Network ACL product--acl--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Create Route Table product--routeTable--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings | ···
Create VPC product--vpc--form	Virtual Private Cloud	● Configured	● No Configurations	● No Configurations	May 22, 2024, 09:45:28	Required Settings | ···
Create vSwitch product--vswitch--form	Virtual Private Cloud	● No Configurations	● No Configurations	● No Configurations	-	Required Settings |

2. In the **Options** dialog box, select the fields for which you want to configure options and click **Next Step**. For example, select the **Sharing Scope** field.

> **Note**
>
> This configuration is applicable only to the fields that have a check box.



Options ✕

▾ Area

Organization

Resource Set

Region

▾ Basic Settings

☑ Sharing Scope

VPC Name

□ IPv4 CIDR Block

Recommended CIDR Block

Custom CIDR Block

□ IPv6 CIDR Block

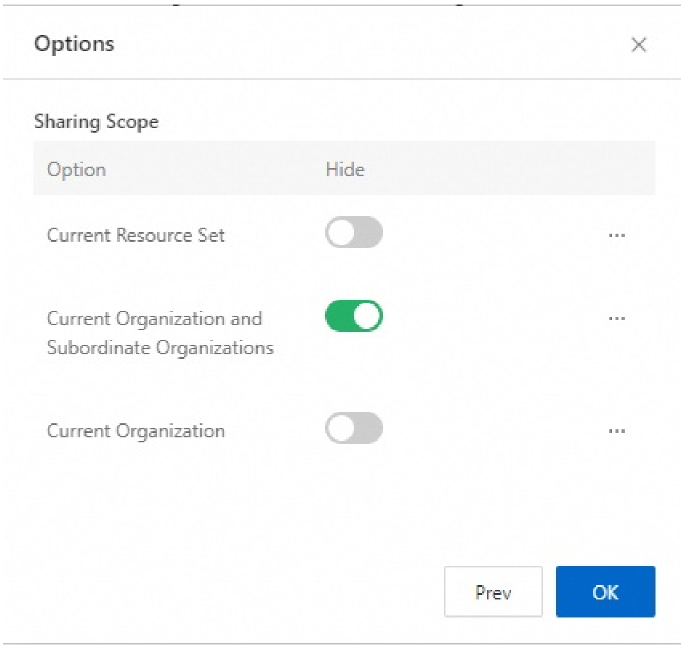
Address Pool

Description

Cancel | Next Step

3. Specify whether to hide the options and adjust the order of the options.

> **Note**
>
> - ●: the corresponding option is not displayed on the creation page.
> - ○: the corresponding option is displayed on the creation page.
> - You can click the ... icon next to an option and click **Move Up** or **Move Down** to adjust the order of the option.



Sharing Scope

Option	Hide
Current Resource Set	○
Current Organization and Subordinate Organizations	●
Current Organization	○

4. Click **OK**.

5.8. Manage announcements

You can create announcements on the platform to inform users about events such as O&M, updates, and daily operations.

Background information

- After an announcement is published, users can view the announcement in the Announcement section of the homepage.

> **Important**
>
> - The announcements that a user can view vary based on the role of the user:
>   - If the user assumes a global role, the user can view all published announcements.
>   - If the user assumes a non-global role, the user can view the published announcements of the organization to which the user belongs and the published announcements of which the Visible for Organization parameter is set to All.
> - The announcements are displayed in descending order based on the publish time.

- The announcement management feature allows you to create, modify, view, edit, and delete announcements. Tenant isolation is also implemented to ensure that announcements are separately managed for each tenant.

> **Important**
>
> - When a platform administrator creates or edits an announcement, the platform administrator can set the Visible for Organization parameter to All or SystemDefaultOrganization. However, only All is a valid value. If the Visible for Organization parameter is set to SystemDefaultOrganization, an error is reported when the announcement is saved.

> - Global roles can view and manage announcements of all organizations.
> - Non-global roles can view only the announcements of the level-1 organization to which the current account belongs. If you create or edit an announcement by assuming a non-global role, you can select only All or the corresponding level-1 organization from the Visible for Organization drop-down list.

- You can limit the visibility of announcements to specified organizations.
- Announcement content supports rich text. You can adjust the content style and insert images or links based on your business requirements.
- Announcements are automatically published or unpublished based on the specified publish or unpublish time.
- You can delete an announcement if you no longer need it. After the announcement is deleted, it cannot be restored.

Prerequisites

You are a platform administrator or operations administrator.

Create an announcement

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Announcement Management**.
4. On the **Announcement Management** page, click **Create Announcement**.
5. On the **Create Announcement** page, configure the parameters described in the following table.

Section and parameter	Description
Title	The title of the announcement. The title must be 2 to 120 characters in length and can contain letters, digits, and the following characters: periods (.), commas (,), semicolons (;), colons (:), single quotation marks ('), double quotation marks (''), question marks (?), angle brackets (<>), exclamation points (!), and spaces.
Type	The type of the announcement. Valid values:**Upgrade Announcement**, **O&M Notifications**, **Security Notifications**, **Urgent Events**, and **Daily Announcement**.

Visible for Organization	The organizations to which the announcement is visible. By default,**All** is selected. In this case, users in all organizations can view the announcement. You can also select a level-1 organization from the drop-down list. In this case, only the users in the selected level-1 organization can view the announcement. **Note** ◦ If you use a platform administrator account, the displayed values of the Visible for Organization parameter are All and SystemDefaultOrganization. To create the announcement, you must select All for the Visible for Organization parameter. Otherwise, the configuration is invalid. ◦ If you use an operations administrator account, you can view all level-1 organizations in the drop-down list. You can select All or a specific level-1 organization to create the announcement. ◦ If you use a custom Resource Access Management (RAM) role that has the permissions to manage announcements, take note of the following items: ▪ If you use a global RAM role, you can view all level-1 organizations in the drop-down list. You can select All or a specific level-1 organization to create the announcement. ▪ If you use a non-global RAM role, you can view only the level-1 organization to which the current account belongs in the drop-down list. You can select All or the corresponding level-1 organization to create the announcement.
Publish - Unpublish Time	The time that you want to publish and unpublish the announcement. The time is accurate to seconds. Announcements are automatically published or unpublished based on the specified publish or unpublish time. The publish time must be later than the current time, and the unpublish time must be later than the publish time.
Announcement content	Announcement content supports rich text. You can adjust the content style and insert images or links based on your business requirements.

6. Click **Create**.

> **Note**
>
> - After an announcement is created and automatically published, the announcement is displayed in the Announcement section of the **homepage**. Only the users in the specified organizations can view the announcement.
> - Automatic publishing and unpublishing of announcements may be delayed by 1 to 5 seconds.

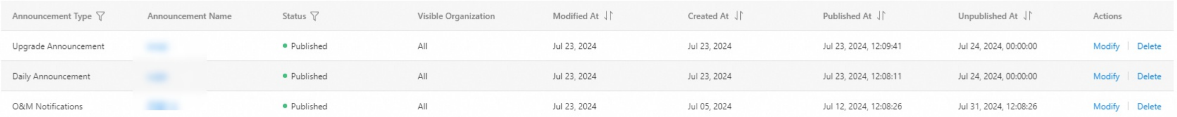
View the announcement list and details of an announcement

After an announcement is created, you can view the created announcement in the announcement list.

1. Optional. On the **Announcements** page, enter an announcement name in the search box to search for the announcement.

2. View the information about the announcement displayed in the following columns: **Announcement Type**, **Announcement Name**, **Status**, **Visible Organization**, **Modified At**, **Created At**, **Published At**, and **Unpublished At**.

   > **Note**
   >
   > - Click the ▽ icon next to the **Status** column to filter announcements by status.
   >
   >   Valid values of the Status column: **Pending**, **Published**, and **Unpublished**.
   > - Click the ⇅ icon next to the **Modified At**, **Created At**, **Published At**, or **Unpublished At** column to sort announcements in ascending or descending order based on the corresponding time.



Announcement Type ▽	Announcement Name	Status ▽	Visible Organization	Modified At ⇅	Created At ⇅	Published At ⇅	Unpublished At ⇅	Actions
Upgrade Announcement	[redacted]	● Published	All	Jul 23, 2024	Jul 23, 2024	Jul 23, 2024, 12:09:41	Jul 24, 2024, 00:00:00	Modify | Delete
Daily Announcement	[redacted]	● Published	All	Jul 23, 2024	Jul 23, 2024	Jul 23, 2024, 12:08:11	Jul 24, 2024, 00:00:00	Modify | Delete
O&M Notifications	[redacted]	● Published	All	Jul 23, 2024	Jul 05, 2024	Jul 12, 2024, 12:08:26	Jul 31, 2024, 12:08:26	Modify | Delete

3. Click the name of the announcement to go to the announcement details page and view the announcement details.

   > **Note**
   >
   > You can go to the details pages of only announcements in the **Published** state.

Modify an announcement

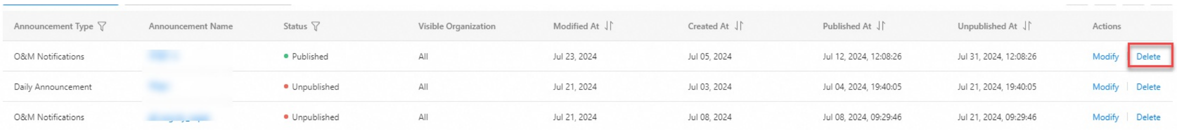
You can modify an announcement to reflect information changes.

1. On the **Announcement Management** page, find the announcement that you want to modify and click **Modify** in the Actions column.
2. On the **Modify Announcement** page, modify the title, type, organizations to which the announcement is visible, publish and unpublish time, and content based on your business requirements.
3. Click **Modify**.

Delete an announcement

You can delete an announcement if it is no longer needed.

1. On the **Announcement Management** page, find the announcement that you want to delete and click **Delete** in the Actions column.



Announcement Type ▽	Announcement Name	Status ▽	Visible Organization	Modified At ⇅	Created At ⇅	Published At ⇅	Unpublished At ⇅	Actions
O&M Notifications	[redacted]	● Published	All	Jul 23, 2024	Jul 05, 2024	Jul 12, 2024, 12:08:26	Jul 31, 2024, 12:08:26	Modify Delete
Daily Announcement	[redacted]	● Unpublished	All	Jul 21, 2024	Jul 03, 2024	Jul 04, 2024, 19:40:05	Jul 21, 2024, 19:40:05	Modify | Delete
O&M Notifications	[redacted]	● Unpublished	All	Jul 21, 2024	Jul 08, 2024	Jul 08, 2024, 09:29:46	Jul 21, 2024, 09:29:46	Modify | Delete

2. In the **Confirm** message, click **OK**.

5.9. Custom settings

You can customize logon pages and platform logos for the Apsara Uni-manager Management Console based on your business requirements.

Background information

- Multiple languages are supported, including Simplified Chinese, Traditional Chinese, and English. You can select a default language for the platform.
- You can select a dark or light mode. You can also change the theme color of the console.
- You can enable and customize the page watermark.
- You can configure multi-language brand information in the console, including the browser ICO image, platform logo, platform name, and information displayed on the logon page.
- You can restore the page to factory settings. The restoration is irreversible.

Prerequisites

You are a platform administrator.

Customize configurations

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Custom Configurations**.

Parameter	Description
Platform Language	You can select one or more languages supported by the platform. Valid values: ◦ Simplified Chinese ◦ Traditional Chinese ◦ English You can select a default language for the platform among the supported languages.
Appearance and Theme	You can select the appearance (light mode or dark mode) and theme color of the console. **Note** You can select a recommended theme color or use the custom palette.
Page Watermark	Specifies whether to add a watermark on the console. ○: does not add a watermark. ●: adds the specified watermark.
Preset information	User profile picture: We recommended that you use a 1:1 aspect ratio such as 100 × 100 pixels. Format: GIF, PNG, JPG, or JPEG.

Brand Setting	You can specify the logos, versions, and copyright notices of the console in the supported languages: Simplified Chinese, Traditional Chinese, and English. Parameters: ◦ **Browser Ico Icon**: We recommended that you set the aspect ratio to 1:1 such as 32 pixel × 32 pixel. Format: GIF, PNG, JPG, or JPEG. ◦ **Platform Logo**: We recommended that you set the resolution to 160 pixel × 36 pixel. Format: GIF, PNG, JPG, or JPEG. ◦ **Platform Name**: We recommend that you specify a name for the platform. ◦ **Login Page**: You can configure up to three pages. Each page can have their specific background image and slogan. We recommend that you use an image whose resolution is 1,880 pixel × 1,600 pixel in the GIF, PNG, JPG, or JPEG format. The slogan must not exceed 120 characters in length. ◦ **Version Information**: the version information. ◦ **Copyright Notice**: the declaration of the copyright.

4. Click **OK**.

   To restore factory settings, you can click **Restore Factory Settings** in the upper-right corner of the page. The configurations take effect next time you log on to the console.

5.10. Third-party authentication

You can configure third-party authentication to implement single sign-on (SSO) in which the Apsara Uni-manager Management Console serves as a service provider (SP) and the system that is developed by a customer serves as an identity provider (IdP). This way, users can access the resources provided by the SP without additional authentication after they pass the authentication of the IdP. You can configure a global IdP or a local IdP for third-party authentication.

Terms

- SSO: allows users to log on to multiple systems with a single action of logon without the need to re-enter the username and password for authentication.
- Single log-out (SLO): allows users to log out from multiple systems with a single action of logout.
- IdP: provides identity management services.
- SP: provide users with specific services by using the identity management services provided by IdPs.
- Security Assertion Markup Language 2.0 (SAML 2.0): a protocol that is designed for enterprise-level user identity authentication. SAML 2.0 is used for communication between SPs and IdPs by exchanging authentication and authorization data within security domains.
- Open Authorization (OAuth) 2.0: an authorization protocol that specifies the following grant types for different scenarios: authorization code, client credentials, resource owner password credentials, and implicit. The Apsara Uni-manager Management Console uses the authorization code grant type.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as a platform administrator.

User-based SSO

Configure a global IdP

> **Important**
>
> - The following section describes how to configure a global IdP which is an enterprise system when the Apsara Uni-manager Management Console serves as an SP. In One Cloud with Multiple Regions scenarios, users from all regions must be authenticated by the global IdP.
> - When a global IdP is configured for the cloud platform, users are authenticated by the global IdP after they click the button for authentication on the logon page of the platform.
> - If a global IdP is configured for the cloud platform, you can no longer configure a local IdP. You must clear the global IdP before you configure a local IdP.
> - If a local IdP is configured for the cloud platform, you no longer configure a global IdP. You must clear the local IdP before you configure a global IdP.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Authentication by Third Party**. The User-based SSO tab is displayed by default.
4. On the **Global IdP Settings** tab, separately click the **Edit** button in the **Global Authorization Redirect** and **Global IdP Settings** sections to specify parameters.

   > **Note**
   >
   > - If the **Protocol Type** parameter is set to **OAuth 2.0**, you must specify the parameters in the **Obtain Verified User Information** section.
   > - The parameters in the **Obtain Verified User Information** section are not required in OAuth 2.0. Configure the parameters based on your business requirements.

Parameter		Description
Global Authorization Redirect	**Enable Redirect**	Specify whether users are redirected to the configured URL upon logon or logout. Valid values: **Yes** and **No**.
	Authorized URL	If you set the **Enable Redirect** parameter to **Yes**, specify this parameter. Enter the URL to which users are redirected upon logon. If you leave this parameter empty, users are redirected to the URL for IdP authentication upon logon.
	Exit URL	If you set the **Enable Redirect** parameter to **Yes**, specify this parameter. Enter the URL to which users are redirected upon logout. If you leave this parameter empty, users are redirected to the logon page of the Apsara Uni-manager Management Console upon logout.

	Authorized Logon Custom Name	Enter a custom name for the button that is used for**authorization logon** on the logon page of the platform. If you do not specify this parameter, the default value**Authorize Logon** is used.
Global IdP Settings	**IdP Service Name**	Enter the name for the IdP. The name can be up to 64 characters in length and can contain letters, digits, and underscores (_). The name cannot start with a digit.
	Protocol Type	Select **SAML 2.0** or **OAuth 2.0**. **Note** If you select **SAML 2.0**, use the SAML SP metadata of Apsara Stack. You can click **Download Metadata File** to download the metadata.
	IdP Authentication Address	Enter a URL for IdP authentication. Format: `http://URL` or `https://URL`.
	IdP Certificate	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Enter the Base64-encoded third-party certificate.
	SLO Endpoint	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Enter a URL for SLO. Format: `http://URL` or `https://URL`. **Note** The Apsara Uni-manager Management Console calls this URL when it responds to an SLO request from the IdP.
	SLO Request Method	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Select an SLO request method.
	Client ID	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a client ID.
	Client Key	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a client key.

	Service Address for Obtaining Access Token	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a URL for obtaining the access token. Format: `http://URL` or `https://URL` . By default, the POST method is used for this request. **Note** Click **Test** to test whether the service address can be connected as expected.
	Content-Type	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Valid values: **application/json; charset=utf-8** and **application/x-www-form-urlencoded**. **Note** The value of the Content-Type parameter depends on the requirements of the global IdP. Forms and JSON data are supported. ◦ If the global IdP accepts requests in forms, set the **Content-Type** parameter to **application/x-www-form-urlencoded**. ◦ If the global IdP accepts requests in JSON, set the **Content-Type** parameter to **application/json; charset=utf-8**.
	Service Address for Obtaining Verified User	Enter a URL for user authentication. Format: `http://URL` and `https://URL` . **Note** Click **Test** to test whether the service address can be connected as expected.
	Request Type	Valid values: **GET** and **POST**.

Obtain Verified User Information	**Content-Type**	If you set the Request Type parameter to**POST**, specify this parameter. Valid values: **application/json; charset=utf-8** and **application/x-www-form-urlencoded**. **Note** The value of the Content-Type parameter depends on the requirements of the global IdP. Forms and JSON data are supported. ◦ If the global IdP accepts requests in forms, set the **Content-Type** parameter to **application/x-www-form-urlencoded**. ◦ If the global IdP accepts requests in JSON, set the **Content-Type** parameter to **application/json; charset=utf-8**.
	Access Token Request Header Template	Default value: `[{ "key": "access_token", "value": "{{access_token}}" }]` . **Note** ◦ {{access_token}} will be replaced with the obtained access token information and is a required parameter. ◦ The Apsara Uni-manager Management Console will add the key and value in the template to the header of the requests sent to the user authentication URL.
	Access Token Request Parameter Template	If you set the Request Type parameter to**Get**, specify this parameter. Default value: `[{ "key": "access_token", "value": "{{access_token}}" }]` . **Note** ◦ {{access_token}} will be replaced with the obtained access token information and is a required parameter. ◦ The Apsara Uni-manager Management Console will add the key and value in the template to the header of the requests sent to the user authentication URL.

	Access Token Request Body Template	If you set the Request Type parameter to**POST**, specify this parameter. ◦ If the **Content-Type** parameter is set to **application/json; charset=utf-8**, the default value of the Access Token Request Body Template parameter is `{ "access_token": "{{access_token}}" }` . ◦ If the **Content-Type** parameter is set to **application/x-www-form-urlencoded**, the default value of the Access Token Request Body Template parameter is `[{ "key": "access_token", "value": "{{access_token}}" }]` . **Note** ◦ {{access_token}} will be replaced with the obtained access token information and is a required parameter. ◦ The Apsara Uni-manager Management Console will add the key and value in the template to the header of the requests sent to the user authentication URL.
	Obtain Path for Parsing Verified Username	Enter a parsing path for the verified username. The objects returned from the service must be JSON objects. **Note** Use periods (.) to indicate the level of the username in the object. For example, `user` indicates that the username is at the root level, and `ascm.user` indicates that the username is at the second level.

5. Click **Save** for each section.

> **Important**
>
> If you click **Restore Factory Settings**, the global IdP settings are cleared. Users are not authenticated by the global IdP when they log on to the platform. Exercise caution when you perform this operation.

Configure a local IdP

> **Important**
>
> - If a local IdP is created and bound to a level-1 organization, the button for authentication is unavailable on the logon page of the platform for the users of the level-1 organization and subordinate organizations. The users are redirected to the platform only after they log on from the local IdP.
> - After you create a local IdP, you can bind the IdP to a level-1 organization to implement IdP authentication at the organization level. Each level-1 organization can be bound to only one IdP including a global IdP.

- If a global IdP is configured for the cloud platform, you can no longer configure a local IdP. You must clear the global IdP before you configure a local IdP.
- If a local IdP is configured for the cloud platform, you no longer configure a global IdP. You must clear the local IdP before you configure a global IdP.
- If a level-1 organization is bound to a local IdP, you can still configure local IdPs for other level-1 organizations.

Create a local IdP

1. On the **Local IdP Settings** tab, click **Create Local IdP**.
2. In the **Create Local IdP** dialog box, specify parameters.

> **Note**
>
> - If the **Protocol Type** parameter is set to **OAuth 2.0**, you must specify the parameters in the **Obtain Verified User Information** section.
> - The parameters in the **Obtain Verified User Information** section are not required in OAuth 2.0. Configure the parameters based on your business requirements.

Parameter		Description
	IdP Service Name	Enter the name for the IdP. The name can be up to 64 characters in length and can contain letters, digits, and underscores (_). The name cannot start with a digit.
	Description	Enter a description for the IdP.
	Protocol Type	Select **SAML 2.0** or **OAuth 2.0**. **Note** If you select **SAML 2.0**, use the SAML SP metadata of Apsara Stack. You can click **Download Metadata File** to download the metadata in the Basic Information section on the details panel of the local IdP after you create the IdP.
	IdP Authentication Address	Enter a URL for IdP authentication. Format: `http://URL` or `https://URL` .
	IdP Certificate	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Enter the Base64-encoded third-party certificate.

IdP Settings	**SLO Endpoint**	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Enter a URL for SLO. Format: `http://URL` or `https://URL`. **Note** The Apsara Uni-manager Management Console calls this URL when it responds to an SLO request from the IdP.
	SLO Request Method	If you set the **Protocol Type** parameter to **SAML 2.0**, specify this parameter. Select an SLO request method.
	Client ID	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a client ID.
	Client Key	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a client key.
	Service Address for Obtaining Access Token	If you set the **Protocol Type** parameter to **OAuth 2.0**, specify this parameter. Enter a URL for obtaining the access token. Format: `http://URL` or `https://URL`. By default, the POST method is used for this request. **Note** Click **Test** to test whether the service address can be connected as expected.
	Content-Type	Valid values: **application/json; charset=utf-8** and **application/x-www-form-urlencoded**. **Note** The value of the Content-Type parameter depends on the requirements of the local IdP. Forms and JSON data are supported. ◦ If the local IdP accepts requests in forms, set the **Content-Type** parameter to **application/x-www-form-urlencoded**. ◦ If the local IdP accepts requests in JSON, set the**Content-Type** parameter to **application/json; charset=utf-8**.

Obtain Verified User Information	**Service Address for Obtaining Verified User**	Enter a URL for user authentication. Format: `http://URL` and `https://URL` . **Note** Click **Test** to test whether the service address can be connected as expected.
	Request Type	Valid values: **GET** and **POST**.
	Content-Type	If you set the Request Type parameter to**POST**, specify this parameter. Valid values: **application/json; charset=utf-8** and **application/x-www-form-urlencoded**. **Note** The value of the Content-Type parameter depends on the requirements of the local IdP. Forms and JSON data are supported. ◦ If the local IdP accepts requests in forms, set the **Content-Type** parameter to **application/x-www-form-urlencoded**. ◦ If the local IdP accepts requests in JSON, set the**Content-Type** parameter to **application/json; charset=utf-8**.
	Access Token Request Header Template	Default value: `[{ "key": "access_token", "value": "{{access_token}}" }]` . **Note** ◦ {{access_token}} will be replaced with the obtained access token information and is a required parameter. ◦ The Apsara Uni-manager Management Console will add the key and value in the template to the header of the requests sent to the user authentication URL.

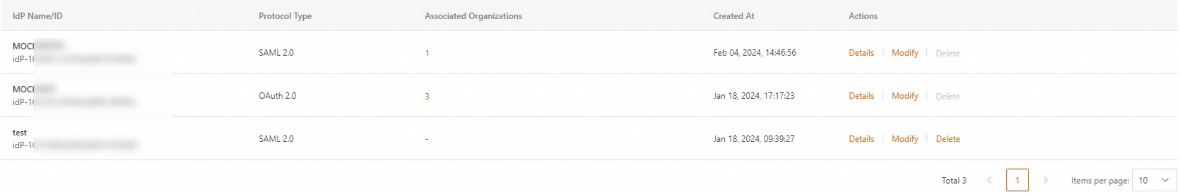
	Access Token Request Body Template	◦ If the **Request Type** parameter is set to **GET**: Default value: `[{ "key": "access_token", "value": "{{access_token}}" }]` . ◦ If the **Request Type** parameter is set to **POST**: ▪ If the **Content-Type** parameter is set to **application/json; charset=utf-8**, the default value of the Access Token Request Body Template parameter is `{ "access_token": "{{access_token}}" }` . ▪ If the **Content-Type** parameter is set to **application/x-www-form-urlencoded**, the default value of the Access Token Request Body Template parameter is `[{ "key": "access_token", "value": "{{access_token}}" }]` . **Note** ◦ {{access_token}} will be replaced with the obtained access token information and is a required parameter. ◦ The Apsara Uni-manager Management Console will add the key and value in the template to the body of the requests sent to the user authentication URL.
	Obtain Path for Parsing Verified Username	Enter a parsing path for the verified username. The objects returned from the service must be JSON objects. **Note** Use periods (.) to indicate the level of the username in the object. For example, `user` indicates that the username is at the root level, and `ascm.user` indicates that the username is at the second level.

3. Click **OK**.

View local IdPs

1. On the **Local IdP Settings** tab, view the information about created local IdPs, such as **IdP Name/ID**, **Protocol Type**, **Associated Organizations**, and **Created At**.

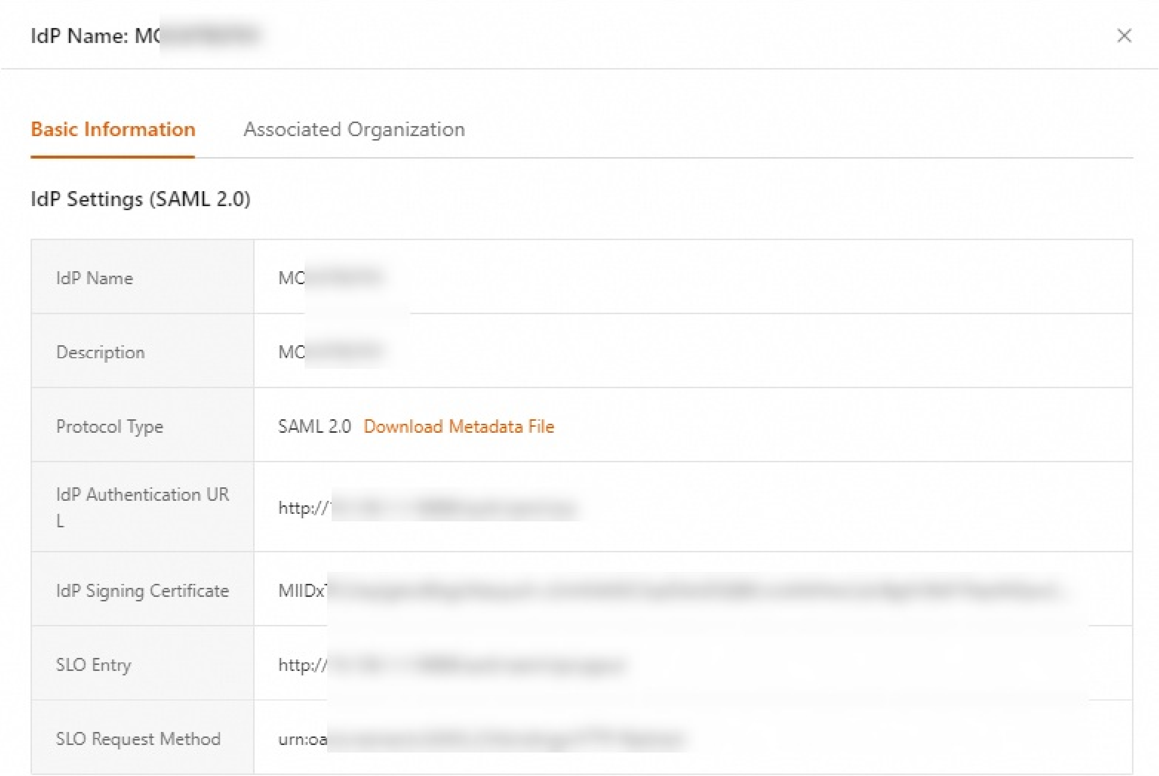
> **Note**
>
> After you click a number in the **Associated Organizations** column that corresponds to an IdP, you are redirected to the **Associated Organization** tab.



IdP Name/ID	Protocol Type	Associated Organizations	Created At	Actions
MOC[redacted] idP-1[redacted]	SAML 2.0	1	Feb 04, 2024, 14:46:56	Details | Modify | Delete
MOC[redacted] idP-1[redacted]	OAuth 2.0	3	Jan 18, 2024, 17:17:23	Details | Modify | Delete
test idP-1[redacted]	SAML 2.0	-	Jan 18, 2024, 09:39:27	Details | Modify | Delete

2. Click **Details** in the **Actions** column that corresponds to an IdP. The details panel of the IdP is displayed.
3. In the details panel, view the basic information and associated organizations of the IdP.
   - **Basic Information**: The basic information about the local IdP is displayed on this tab.

     > **Note**
     >
     > If the protocol type of the IdP is **SAML 2.0**, you can click **Download Metadata File** in the Basic Information section to download the metadata file.

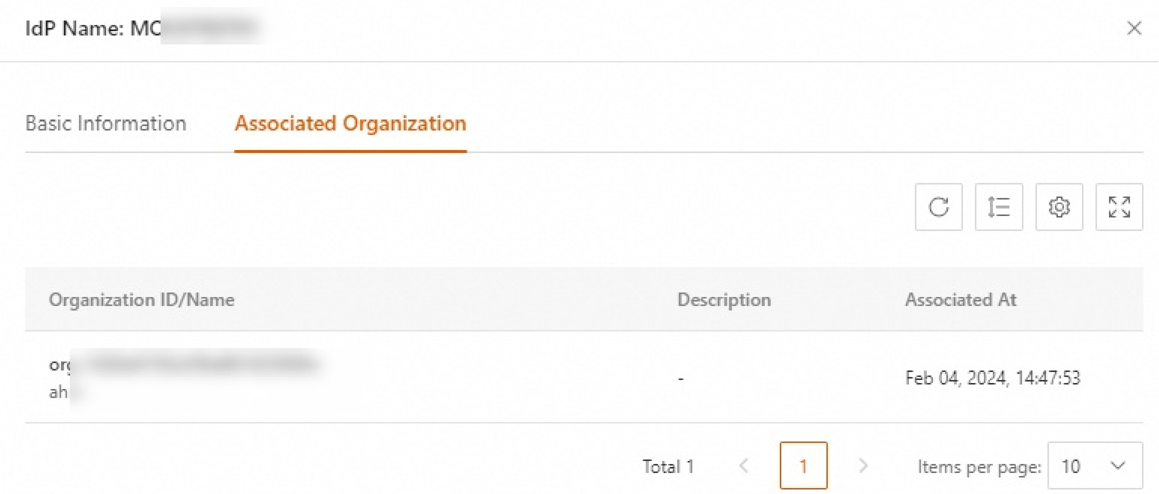


IdP Name: MC[redacted]

IdP Settings (SAML 2.0)

IdP Name	MC[redacted]
Description	MC[redacted]
Protocol Type	SAML 2.0 Download Metadata File
IdP Authentication URL	http://[redacted]
IdP Signing Certificate	MIIDx[redacted]
SLO Entry	http://[redacted]
SLO Request Method	urn:oa[redacted]

   - **Associated Organization**: The information about organizations associated with the local IdP is displayed on this tab. The information includes **Organization ID/Name**, **Description**, and **Associated At**.

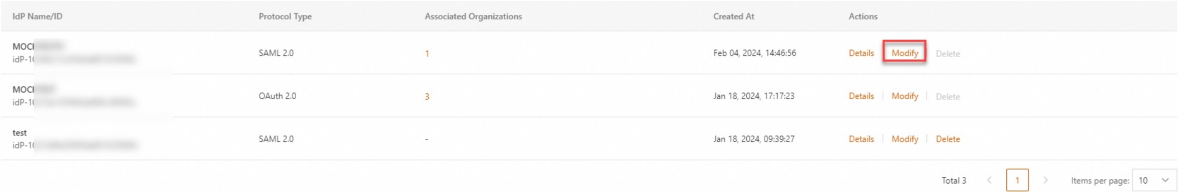


IdP Name: MC[redacted]

Organization ID/Name	Description	Associated At
org[redacted] ah[redacted]	-	Feb 04, 2024, 14:47:53

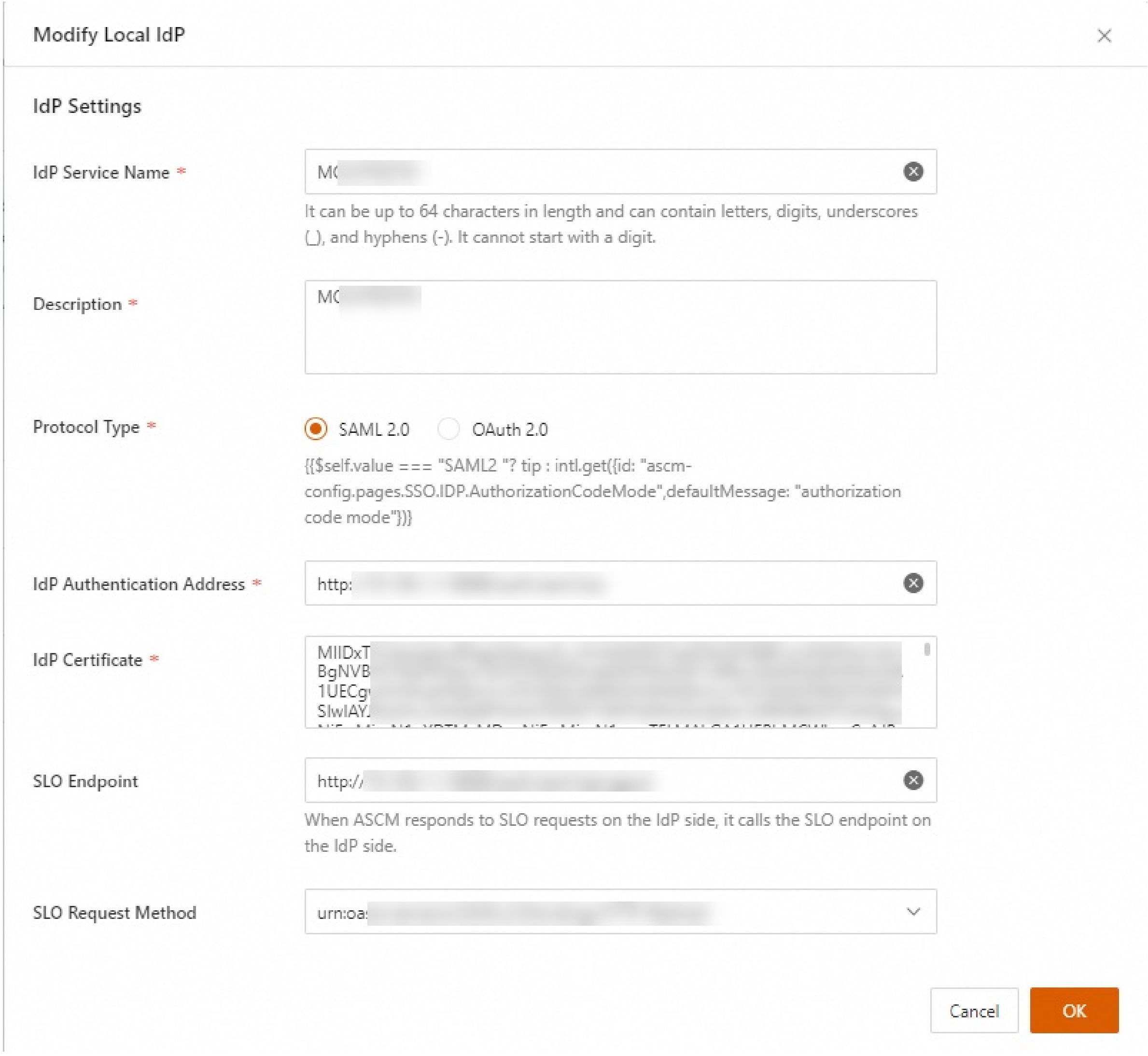
Modify a local IdP

1. On the **Local IdP Settings** tab, click **Modify** in the **Actions** column that corresponds to a local IdP.



IdP Name/ID	Protocol Type	Associated Organizations	Created At	Actions
MOC[redacted] idP-1[redacted]	SAML 2.0	1	Feb 04, 2024, 14:46:56	Details Modify Delete
MOC[redacted] idP-1[redacted]	OAuth 2.0	3	Jan 18, 2024, 17:17:23	Details | Modify | Delete
test idP-1[redacted]	SAML 2.0	-	Jan 18, 2024, 09:39:27	Details | Modify | Delete

2. In the **Modify Local IdP** dialog box, modify the values of the desired parameters.



Modify Local IdP

IdP Settings

IdP Service Name *: MO[redacted]

It can be up to 64 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with a digit.

Description *: MO[redacted]

Protocol Type *: ● SAML 2.0 ○ OAuth 2.0

{{$self.value === "SAML2 "? tip : intl.get({id: "ascm-config.pages.SSO.IDP.AuthorizationCodeMode",defaultMessage: "authorization code mode"})}}

IdP Authentication Address *: http:[redacted]

IdP Certificate *: MIIDxT[redacted] BgNVB[redacted] 1UECg[redacted] SlwlAY[redacted]

SLO Endpoint: http:/[redacted]

When ASCM responds to SLO requests on the IdP side, it calls the SLO endpoint on the IdP side.

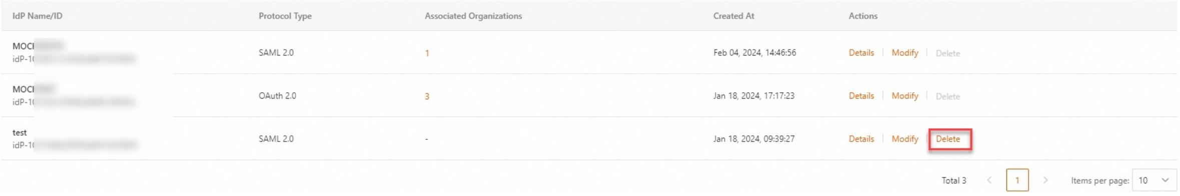
SLO Request Method: urn:oa[redacted]

3. Click **OK**.

Delete a local IdP

> **Important**
>
> Before you delete a local IdP, you must unbind the local IdP from bound organizations. For more information, see the "Manage third-party authentication for an organization" section of the Manage organizations topic.

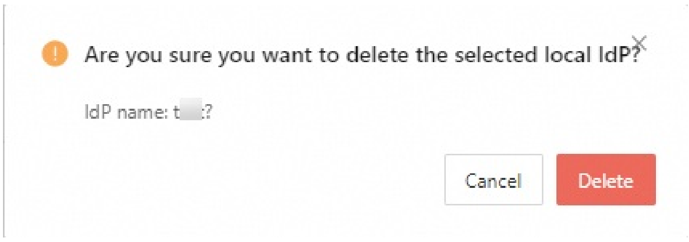
1. On the **Local IdP Settings** tab, click **Delete** in the **Actions** column that corresponds to a local IdP.



IdP Name/ID	Protocol Type	Associated Organizations	Created At	Actions
MOC[redacted] idP-1[redacted]	SAML 2.0	1	Feb 04, 2024, 14:46:56	Details | Modify | Delete
MOC[redacted] idP-1[redacted]	OAuth 2.0	3	Jan 18, 2024, 17:17:23	Details | Modify | Delete
test idP-1[redacted]	SAML 2.0	-	Jan 18, 2024, 09:39:27	Details | Modify | Delete

Total 3 1 Items per page: 10

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



Are you sure you want to delete the selected local IdP?

IdP name: t[redacted]?

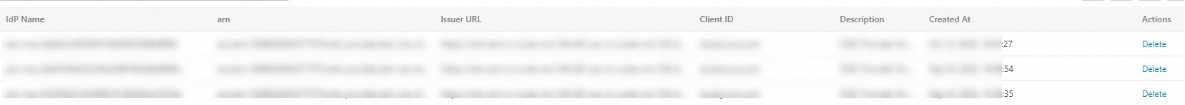
OIDC Authentication

Important

- OpenID Connect (OIDC) is an authentication protocol on top of OAuth 2.0. Applications can use this protocol for authentication based on the relationship between external IdPs and Apsara Stack Resource Access Management (RAM).
- You can use OIDC authentication to implement access control on different pods that are deployed in a Container Service for Kubernetes (ACK) cluster. This achieves fine-grained API permission control on pods and reduces security risks.
- Only ACK supports OIDC authentication, and the OIDC IdP list displays OIDC IdPs created by ACK clusters. You cannot directly create an OIDC IdP. You must contact technical support to enable OIDC authentication for ACK clusters.
- After ACK clusters create OIDC IdPs, the platform administrator can view and delete the OIDC IdPs on the OIDC Authentication tab.

View OIDC IdPs

1. On the **Authentication by Third Party** page, click the **OIDC Authentication** tab.
2. In the OIDC IdP list, view information about an OIDC IdP. The information includes **IdP Name**, **arn**, **Issuer URL**, **Client ID**, **Description**, and **Created At**.
   - **IdP Name**: the name of the OIDC IdP.
   - **arn**: the Alibaba Cloud Resource Name (ARN) of the OIDC IdP.
   - **Issuer URL**: the URL of the OIDC IdP. The URL is used by the client to authenticate the source of the ID token.
   - **Client ID**: the ID that the OIDC IdP uses to authenticate an application.
   - **Description**: the description of the OIDC IdP.
   - **Created At**: the time when the OIDC IdP was created.



IdP Name	arn	Issuer URL	Client ID	Description	Created At	Actions
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]:27	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]:54	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]:35	Delete

Delete an OIDC IdP

If an OIDC IdP is no longer required, you can delete it.

> ⓘ **Important**
>
> After you delete an OIDC IdP, RAM roles that reference the OIDC IdP cannot be used. This may adversely affect cloud service authentication and cause risks to your business. Proceed with caution.

1. In the OIDC IdP list, find an OIDC IdP that you want to delete and click **Delete** in the Actions column.
2. In the dialog box that appears, select **I am aware of the risks and want to delete the OIDC provider**.
3. Click **OK**.

5.11. Message gateway

You can send messages to users through email, SMS, and DingTalk. Before you send notifications, you must configure the methods.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Message Gateway**.
4. Perform the operations described in the following table.

Operation	Procedure
Configure the email gateway	i. Click the **Mail Gateway** tab. ii. Configure the parameters. ▪ **Sender mailbox**: The email address that is used to send messages. ▪ **Sender mailbox password**: The password of the email address. ▪ **Smtp server address**: The address of the SMTP server. Format: smtp.*xxx*.com ▪ **Port**: The port of the SMTP server. ▪ **Encrypted**: Valid values: **No encryption**, **SSL**, and **TLS**. ▪ **Enabled**: Valid values: **Enabled** and **Do not enable**. ▪ **Email Attachment**: Valid values: **Enabled** and **Do not enable**. iii. Click **Submit**. You can click **Reset** to clear the configurations. You can click **Test Mail** and specify a destination mailbox in the dialog box that appears to test the email gateway.

Configure the SMS gateway	i. Click the **SMS Gateway** tab. ii. Configure the parameters. ▪ **SMS gateway address**: The API URL of the SMS gateway. ▪ **Receive Number Parameter Name**: The name of the parameter that specifies the recipient's number in the SMS gateway API. ▪ **SMS content parameter name**: The name of the parameter that specifies the content in the SMS gateway API. ▪ **Request header parameters**: The header parameters for requesting the SMS gateway API. ▪ **Request body parameters**: When the POST method is used, the recipient number parameter name and the content parameter name are included in the request body . When the GET method is used, the two parameter names are included in the query string. ▪ **Content coding**: Valid values: **UTF-8** and **GBK**. ▪ **Transfer mode**: Valid values: **GET** and **POST**. When the parameter is set to GET, the recipient number parameter name and the content parameter name are included in the query string. When the parameter is set to POST, the two parameters are included in the request body. ▪ **Enabled**: Valid values: **Enabled** and **Do not enable**. iii. Click **Submit**. You can click **Reset** to clear the configurations. You can click **Test SMS** and specify a recipient phone number in the dialog box that appears to test the SMS gateway.

Configure the DingTalk method	i. Click the **DingTalk settings** tab. ii. Configure the parameters. **Note** Procedure for obtaining the parameter values: a. Create a DingTalk group chat. b. In the Group Settings panel, click Bot. In the Robot Management dialog box, create a custom robot. c. Go to the robot details page. Set the Security Settings parameter to **Additional Signature** and copy the generated secret. - **Hook address**: The webhook URL of the custom robot. - **Secret key**: The secret key generated in the **Security Settings** parameter of the custom robot. - **Enabled**: Valid values: **Enabled** and **Do not enable**. iii. Click **Submit**. You can click **Reset** to clear the configurations. You can click **Test DingTalk** to test the DingTalk method.

Configure a message template	Note ◦ Message templates cannot be created. You can only modify the existing templates. ◦ By default, 17 message templates are provided, including 1 application O&M message template, 1 product message template, 4 operations message templates, and 11 process approval message templates. i. Click **Edit Template** in the **Operation** column corresponding to a template. In the dialog that appears, modify the template. ▪ **Business Type**: The business type of the template. Valid values:**Product Messages**, **Operations Messages**, **Process Approval Message**, **Application O&M Messages**, and **Announcement**. ▪ **Business Name**: The name of the template. The name must be 2 to 50 characters in length. ▪ **Message header template**: The template for titles of messages. You can use the `${}` syntax to specify system built-in variables that are associated with templates. The title template must be 2 to 50 characters in length. Note The supported template literals are included in the template content. The system automatically replaces the template literals with the actual values. ▪ **Message content template**: The template for message content. You can use the `${}` syntax to specify system built-in variables that are associated with templates. The content template must be 0 to 1,000 characters in length. Note The supported template literals are included in the template content. The system automatically replaces the template literals with the actual values. ▪ **Message default sending method**: Valid values: **Mail**, **SMS**, and **DingTalk**. ii. Click **OK**.

5.12. Manage service-linked roles

You can create a Resource Access Management (RAM) role to authorize cloud services in a level-1 organization to view and manage other resources in the organization.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as an operations administrator, organization administrator, global organization security administrator, or organization security administrator.

Create a service-linked role

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Configurations**.
3. In the left-side navigation pane, click **Service-linked Roles**.
4. On the **Service-Linked Roles** page, click **Create Service-linked Role**.
5. On the page that appears, select a service from the **Service Name** drop-down list and select one or more organizations from the **Authorized Organization Name** drop-down list.
    - After you select a service, the permissions of the service-linked role are displayed.
    - You can select multiple organizations.
6. Click **OK**.

View the details of a service-linked role

1. On the **Service-linked Roles** page, configure the **Role Name**, **Organization Name**, and **Service Name** parameters to filter RAM roles.
2. Find the RAM role that you want to manage and click **View Details** in the **Actions** column to go to the details page of the RAM role.
3. On the **role details** page, view the details and policy of the RAM role.
    - Click the **Role Details** tab to view the name, creation time, description, and trust policy of the RAM role.
    - Click the **Role Policy** tab to view the policy information, including the policy name, policy type, default version, description, and time when the policy is attached to the RAM role.

    > ? **Note**
    >
    > You can click **View Details** in the **Actions** column to view the policy details.

5.13. Billing switch

You can use the billing switch to change the billing period for generated resources.

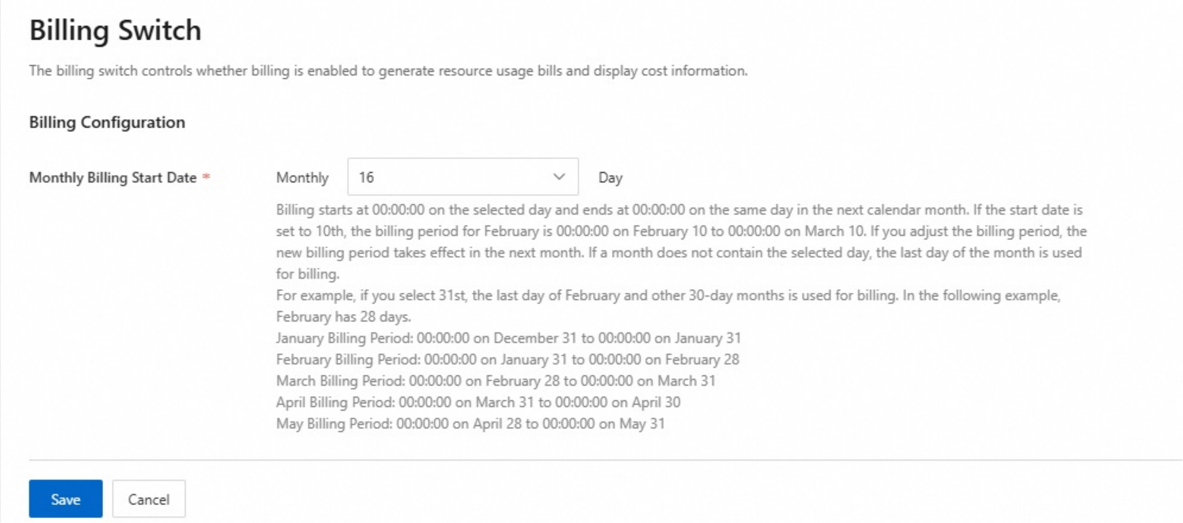
Prerequisites

You are an operations administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Billing Switch**.
4. In the lower part of the page, click **Edit**.
5. Configure the Monthly Billing Start Date parameter and click **Save**.

> **Note**
>
> - Billing starts at 00:00:00 on the selected day and ends at 00:00:00 on the same day in the following calendar month. If you set the start date to the 15th day of the month or a day before the 15th day, the billing period begins in the current month and ends in the following month. If you set the start date to a day after the 15th day of the month, the billing period starts in the previous month and ends in the current month. If you change the billing period, the change takes effect in the following month.
>
>   Examples:
>
>   - If you set the start date to the 10th day of the month, the billing period for February starts at 00:00:00 on February 10 and ends at 00:00:00 on March 10.
>   - If you set the start date to the 18th day of the month, the billing period for February starts at 00:00:00 on January 18 and ends at 00:00:00 on February 18.
>
> - If the date you selected does not exist in a calendar month, the system uses the last day of the calendar month as the start date. For example, if you set the start date to the 31st day of the month, the system uses the last day of February and other 30-day months as the start date of the billing period.
>
>   - January billing period: 00:00:00 on December 31 to 00:00:00 on January 31
>   - February billing period: 00:00:00 on January 31 to 00:00:00 on February 28
>   - March billing period: 00:00:00 on February 28 to 00:00:00 on March 31
>   - April billing period: 00:00:00 on March 31 to 00:00:00 on April 30
>   - May billing period: 00:00:00 on April 30 to 00:00:00 on May 31



Billing Switch

The billing switch controls whether billing is enabled to generate resource usage bills and display cost information.

Billing Configuration

Monthly Billing Start Date * Monthly 16 Day

Billing starts at 00:00:00 on the selected day and ends at 00:00:00 on the same day in the next calendar month. If the start date is set to 10th, the billing period for February is 00:00:00 on February 10 to 00:00:00 on March 10. If you adjust the billing period, the new billing period takes effect in the next month. If a month does not contain the selected day, the last day of the month is used for billing.

For example, if you select 31st, the last day of February and other 30-day months is used for billing. In the following example, February has 28 days.

January Billing Period: 00:00:00 on December 31 to 00:00:00 on January 31

February Billing Period: 00:00:00 on January 31 to 00:00:00 on February 28

March Billing Period: 00:00:00 on February 28 to 00:00:00 on March 31

April Billing Period: 00:00:00 on March 31 to 00:00:00 on April 30

May Billing Period: 00:00:00 on April 28 to 00:00:00 on May 31

5.14. Configure log storage settings

You can configure a storage mode for the operation logs and AccessKey logs of cloud services. This way, security administrators can query logs to check the resource usage and component status in the Apsara Uni-manager Management Console. Security administrators can also export operation logs as a file and download the file to a local device.

Background information

- The log storage settings apply to the storage of operation logs and AccessKey logs of cloud services.
- By default, logs are stored in the underlying storage of Simple Log Service. If no Logstore exists in the sales cloud, logs are stored in the Logstore of the Apsara Infrastructure Management cluster. By default, logs are retained for seven days.
- The capacity required for log storage is calculated based on the following formula: 5,000,000 × Log retention period × Number of organizations/1,024/1,024/1,024.

  For example, if the number of organizations is 300 and the log retention period is 180 days, approximately 251.46 GB of capacity is required for log storage.

  > **Note**
  >
  > - 5,000,000 is the estimated amount of log data generated in one day, measured in bytes. The log data includes the data generated by using Apsara Stack consoles, calling API operations, and using developer tools.
  > - The storage capacity is measured in GB.

Prerequisites

You have logged on to the Apsara Uni-manager Management Console as an operations administrator.

Procedure

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

   > **Note**
   >
   > We recommend that you log on to the Apsara Uni-manager Management Console as the preset operations administrator. This ensures the security of created Simple Log Service projects and Logstores and prevents accidental deletion.

2. In the top navigation bar, click **Configurations**.
3. In the left-side navigation pane, click **Log Storage Settings**.
4. In the lower-left part of the Log Storage Settings page, click **Edit**.

   The following log storage modes are available: **Default**, **Log Storage for All Organizations**, and **Log Storage for Specified Organization**.

Storage Mode	Description
Default	The operation logs of the users of all organizations are stored in the system Logstore for seven days. Only **All Events** is available for the **Event Type** parameter.

Log Storage for All Organizations	The operation logs of the users of all organizations are stored in the configured Logstore. You need to purchase Simple Log Service in advance. ◦ You can set the **Storage Duration** parameter to 30 Days, 60 Days, 90 Days, 180 Days, 360 Days, or 720 Days. The maximum storage duration is 720 days. ◦ You can set the **Event Type** parameter to **All Events**, **Write Event**, or **Read Event**.
Log Storage for Specified Organization	The operation logs of the users of the specified organizations are stored in the configured Logstore. You need to purchase Simple Log Service in advance. ◦ You can set the **Storage Duration** parameter to 30 Days, 60 Days, 90 Days, 180 Days, 360 Days, or 720 Days. The maximum storage duration is 720 days. ◦ You can set the **Event Type** parameter to **All Events**, **Write Event**, or **Read Event**. ◦ In the **Settings** section, configure the parameters in the **Organization** and **Log Service Configuration** sections. In the Log Service Configuration section, the **Log Service Region**, **Project Name**, and **Logstore Name** parameters are required. You can click the ⊕ icon to add more organization configurations. **Important** The organizations must belong to different level-1 organizations.

5. Click **Save**.

6.Operations

6.1. Resource operations

6.1.1. Manage application forms

The **Application Form** page displays the application forms that are generated when you perform operations related to management, cloud services, and service catalogs.

Background information

You can view the application forms on the **My Application Forms**, **To Be Approved**, and **All Application Forms** tabs.

- On the **My Application Forms** tab, you can view all application forms created by the current user and the details of the application forms. You can also withdraw and execute application forms.
- On the **To Be Approved** tab, you can view the details of the application forms that require to be approved. You can also approve and transfer application forms and add signatories.
- On the **All Application Forms** tab, you can view all application forms on which you have the management permissions.

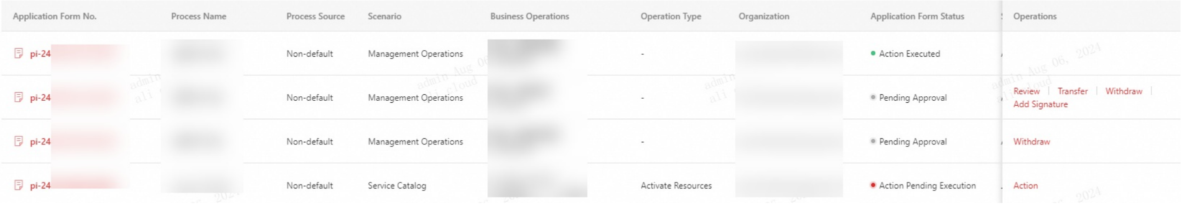
My Application Forms

View application forms

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, click **Application Form**.
4. On the **Application Form** page, click the **My Application Forms** tab.
5. Optional. In the **Advanced Filter** section, configure the **Application Form No.**, **Scenario**, **Application Form Status**, and **Process Name** parameters and click **Search**.

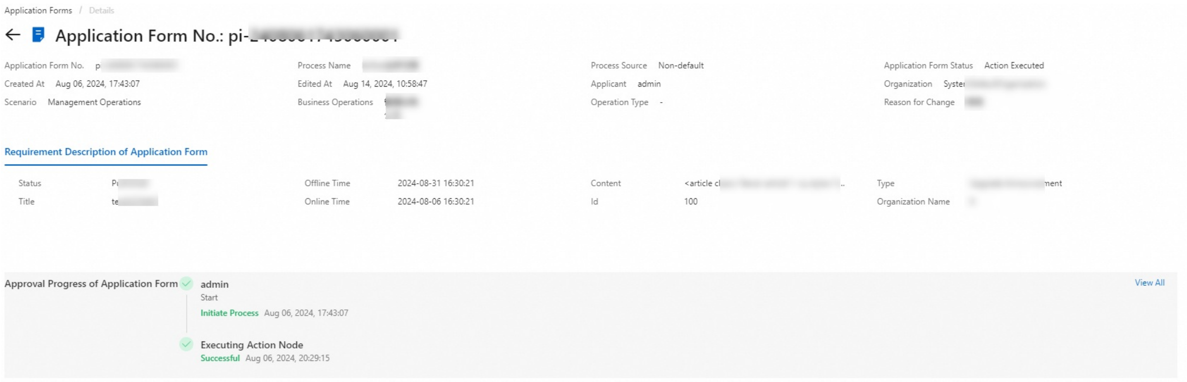
   > ? **Note**
   >
   > - Valid values of the **Scenario** parameter include **Management Operations**, **Cloud Service Operations**, and **Service Catalog**. After you select a specific scenario, you can select a business operation from the corresponding **Management Operations**, **Cloud Service Operations**, or **Service Catalog** filter.
   > - Valid values of the **Application Form Status** parameter include **All Process Status** and **All Action Status**.
   >   - Options of **All Process Status** include **To Be Committed**, **Pending Approval**, **Approval Failed**, and **Process Terminated**.
   >   - Options of **All Action Status** include **Action Pending Execution**, **Executing**, **Action Executed**, **Action Failed**, and **Action Execution Terminated**.

6. In the application form list, view the information about application forms in the following columns: **Application Form No.**, **Process Name**, **Process Source**, **Scenario**, **Business Operations**, **Operation Type**, **Organization**, **Application Form Status**, **Submitted At**, and **Updated At**.



Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Operations
pi-24[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Action Executed	
pi-24[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Pending Approval	Review | Transfer | Withdraw | Add Signature
pi-24[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Pending Approval	Withdraw
pi-24[redacted]	[redacted]	Non-default	Service Catalog	[redacted]	Activate Resources	[redacted]	● Action Pending Execution	Action

7. Find the application form that you want to view and click the **application form number** to go to the **details** page of the application form.



Application Forms / Details

Application Form No.: pi-[redacted]

Application Form No. p[redacted]

Created At Aug 06, 2024, 17:43:07

Scenario Management Operations

Process Name [redacted]

Edited At Aug 14, 2024, 10:58:47

Business Operations [redacted]

Process Source Non-default

Applicant admin

Operation Type -

Application Form Status Action Executed

Organization Syste[redacted]

Reason for Change [redacted]

Requirement Description of Application Form

Status P[redacted]

Title te[redacted]

Offline Time 2024-08-31 16:30:21

Online Time 2024-08-06 16:30:21

Content <article cl[redacted]..

Id 100

Type [redacted]ment

Organization Name [redacted]

Approval Progress of Application Form

admin

Start

Initiate Process Aug 06, 2024, 17:43:07

Executing Action Node

Successful Aug 06, 2024, 20:29:15

View All

> **Note**
>
> - The basic information about the application form is displayed in the upper part of the page.
> - The requirement description of the application form is displayed in the middle part of the page. The description varies based on the business scenario.
> - The progress of the application form is displayed in the lower part of the page. You can click **View All** to view the progress details.

Withdraw an application form

> **Important**
>
> You can withdraw an application form only when the application form is in the **Pending Approval** state.

1. On the **Application Form** page, click the **My Application Forms** tab.
2. In the application form list, find the application form that you want to withdraw and click **Withdraw** in the **Operations** column.
3. In the message that appears, click **OK**.
4. The status of the application form changes to **Process Terminated**.

Execute an application form

> **Important**

> - After an application form is approved, you can manually execute the application form.
> - You can execute an application form only when the application form is in the **Action Pending Execution** or **Action Failed** state.

1. On the **Application Form** page, click the **My Application Forms** tab.
2. In the application form list, find the application form that you want to execute and click **Execute** in the **Operations** column.
3. In the message that appears, click **OK**.

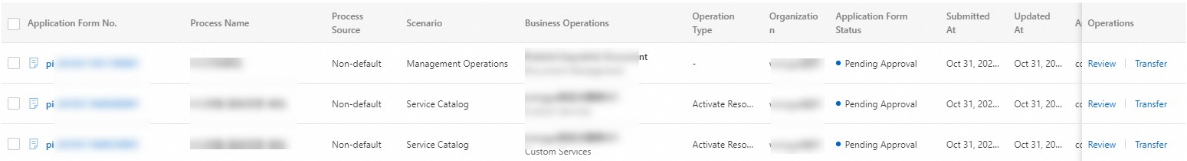
To Be Approved

View application forms to be approved

1. On the **Application Form** page, click the **To Be Approved** tab.
2. Optional. In the **Advanced Filter** section, configure the **Application Form No.**, **Process Name**, **Scenario**, **Application Form Status**, **Query Type**, **Applicant Organization**, and **Include Subordinate Organizations** parameters and click **Search**.

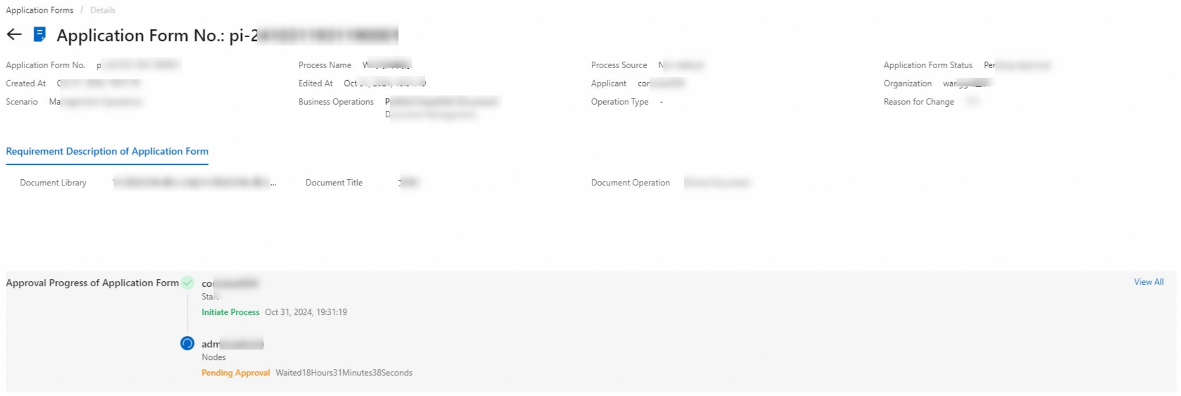
   > **Note**
   >
   > Valid values of the **Scenario** parameter include **Management Operations**, **Cloud Service Operations**, and **Service Catalog**. After you select a specific scenario, you can select a business operation from the corresponding **Management Operations**, **Cloud Service Operations**, or **Service Catalog** filter.

3. In the application form list, view the information about the application forms to be approved in the following columns: **Application Form No.**, **Process Name**, **Process Source**, **Scenario**, **Business Operations**, **Operation Type**, **Organization**, **Application Form Status**, **Submitted At**, **Updated At**, and **Applicant**.



□ Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Submitted At	Updated At	A	Operations
□ pi[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Pending Approval	Oct 31, 202...	Oct 31, 20...	co	Review | Transfer
□ pi[redacted]	[redacted]	Non-default	Service Catalog	[redacted]	Activate Reso...	[redacted]	● Pending Approval	Oct 31, 202...	Oct 31, 20...	co	Review | Transfer
□ pi[redacted]	[redacted]	Non-default	Service Catalog	[redacted] Custom Services	Activate Reso...	[redacted]	● Pending Approval	Oct 31, 202...	Oct 31, 20...	co	Review | Transfer

4. Find the application form that you want to view and click the application form number to go to the details page of the application form.



Application Forms / Details

← Application Form No.: pi-2[redacted]

Application Form No.	p[redacted]	Process Name	W[redacted]	Process Source	N[redacted]	Application Form Status	Per[redacted]
Created At	C[redacted]	Edited At	Oct [redacted]	Applicant	cor[redacted]	Organization	war[redacted]
Scenario	Ma[redacted]	Business Operations	P[redacted] D[redacted]	Operation Type	-	Reason for Change	[redacted]

Requirement Description of Application Form

Document Library [redacted] ... Document Title [redacted] Document Operation [redacted]

Approval Progress of Application Form ✓ co[redacted] Sta[redacted] Initiate Process Oct 31, 2024, 19:31:19

adm[redacted] Nodes Pending Approval Waited18Hours31Minutes38Seconds

View All

> **Note**
>
> - The basic information about the application form is displayed in the upper part of the page.
> - The requirement description of the application form is displayed in the middle part of the page. The description varies based on the business scenario.
> - The progress of the application form is displayed in the lower part of the page. You can click **View All** to view the progress details.

Review an application form

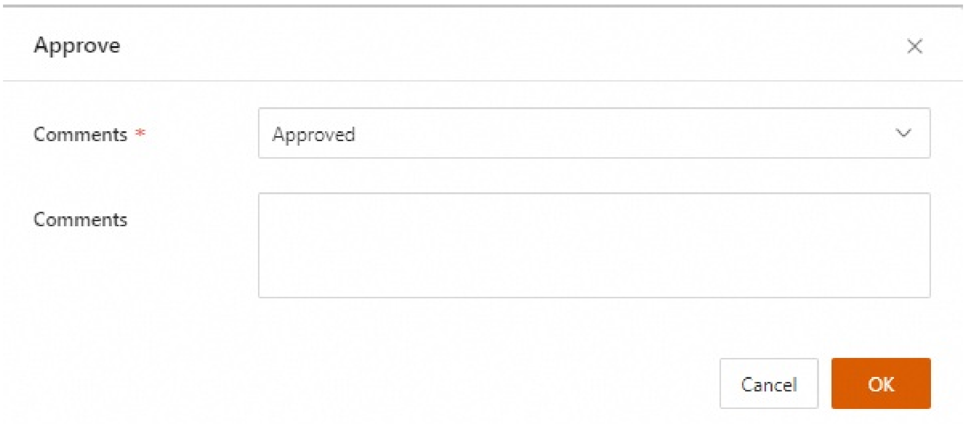
You can receive notifications about application forms pending approval by using emails, internal messages, and DingTalk chatbots.

1. On the **Application Form** page, click the **To Be Approved** tab.

> **Note**
>
> If the application form that you want to approve is also displayed on the **All Application Forms** or **My Application Forms** tab, you can also perform the following operations on the corresponding tab to approve the application form.

2. In the application form list, find the application form that you want to approve and click **Review** in the **Operations** column.
3. In the **Review** dialog box, configure the **Comments** parameter and enter a **description**.

> **Note**
>
> You can set the **Comments** parameter to **Passed** or **Failed**.



Approve

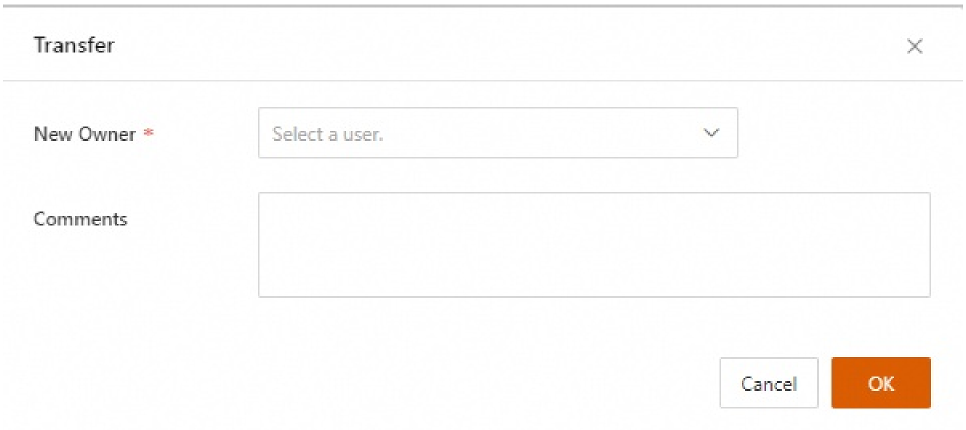
Comments * Approved

Comments

4. Click **OK**.

Transfer an application form

1. On the **Application Form** page, click the **To Be Approved** tab.
2. In the application form list, find the application form that you want to transfer and click **Transfer** in the **Operations** column.
3. In the **Transfer** dialog box, configure the **New Owner** and **Comments** parameters.

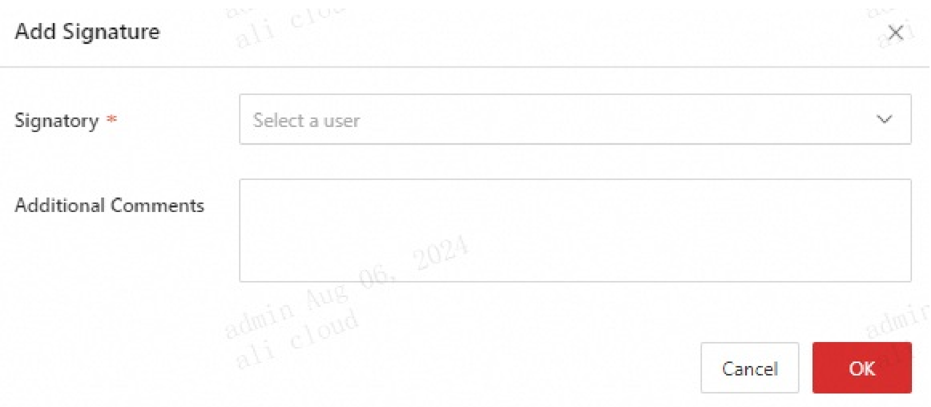


4. Click **OK**.

Add a signer to an application form

> **Important**
>
> - You can add a signer to an application form for which **Allow the approver to specify additional signatories** is selected during the approval node configuration of the process.
> - You can add only one additional signer to an application form. After you add a signer, an approval node is added before the current node for approval. The signer can receive the same message notification as the approver.

1. On the **Application Form** page, click the **To Be Approved** tab.
2. In the application form list, find the application form that you want to manage and click **Add Signature** in the **Operations** column.
3. In the **Add Signature** dialog box, configure the **Signatory** and **Additional Comments** parameters.



4. Click **OK**.

All Application Forms

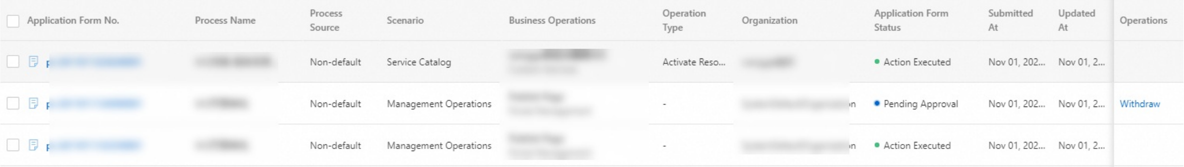
View all application forms

> **Note**
>
> Operations administrators can view all application forms in the platform, whereas organization administrators can view only application forms in the current organization.

1. On the **Application Form** page, click the **All Application Forms** tab.
2. Optional. In the **Advanced Filter** section, configure the **Application Form No.**, **Process Name**, **Scenario**, **Application Form Status**, **Query Type**, **Applicant Organization**, and **Include Subordinate Organizations** parameters and click **Search**.

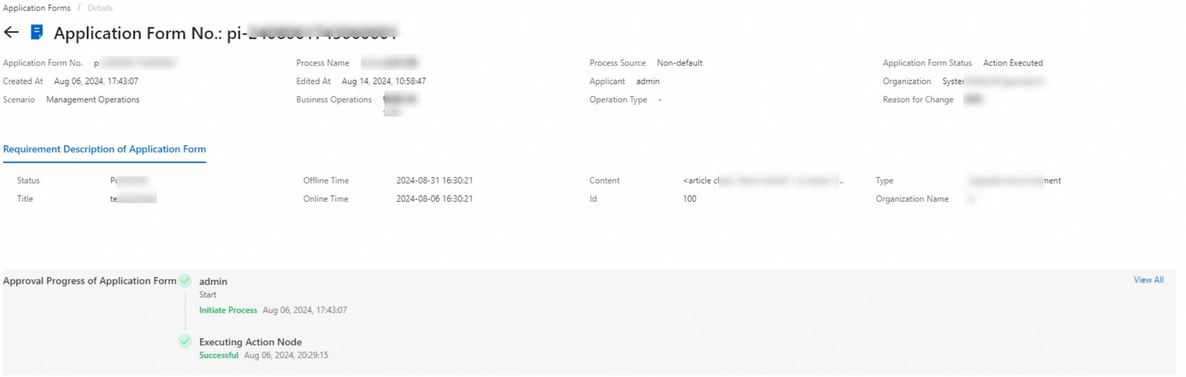
   > **Note**
   >
   > Valid values of the **Scenario** parameter include **Management Operations**, **Cloud Service Operations**, and **Service Catalog**. After you select a specific scenario, you can select a business operation from the corresponding **Management Operations**, **Cloud Service Operations**, or **Service Catalog** filter.

3. In the application form list, view the information about all application forms in the following columns: **Application Form No.**, **Process Name**, **Process Source**, **Scenario**, **Business Operations**, **Operation Type**, **Organization**, **Application Form Status**, **Submitted At**, **Updated At**, and **Applicant**.



□	Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Submitted At	Updated At	Operations
□	[redacted]	[redacted]	Non-default	Service Catalog	[redacted]	Activate Reso...	[redacted]	● Action Executed	Nov 01, 202...	Nov 01, 2...	
□	[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Pending Approval	Nov 01, 202...	Nov 01, 2...	Withdraw
□	[redacted]	[redacted]	Non-default	Management Operations	[redacted]	-	[redacted]	● Action Executed	Nov 01, 202...	Nov 01, 2...	

4. Find the application form that you want to view and click the application form number to go to the details page of the application form.



Application Forms / Details

← Application Form No.: pi-[redacted]

Application Form No. [redacted]
Created At Aug 06, 2024, 17:43:07
Scenario Management Operations

Process Name [redacted]
Edited At Aug 14, 2024, 10:58:47
Business Operations [redacted]

Process Source Non-default
Applicant admin
Operation Type -

Application Form Status Action Executed
Organization [redacted]
Reason for Change [redacted]

Requirement Description of Application Form

Status [redacted]
Title [redacted]

Offline Time 2024-08-31 16:30:21
Online Time 2024-08-06 16:30:21

Content <article [redacted]
Id 100

Type [redacted]
Organization Name [redacted]

Approval Progress of Application Form

✓ admin
Start
Initiate Process Aug 06, 2024, 17:43:07

✓ Executing Action Node
Successful Aug 06, 2024, 20:29:15

> **Note**
>
> - The basic information about the application form is displayed in the upper part of the page.
> - The requirement description of the application form is displayed in the middle part of the page. The description varies based on the business scenario.
> - The progress of the application form is displayed in the lower part of the page. You can click **View All** to view the progress details.

6.1.2. Approval processes

6.1.2.1. Process management

You can create process definitions to define approval procedures based on the requirements of different organizations and products.

Background information

Process management is implemented at the operation control layer of the Apsara Uni-manager Management Console to control whether user operations are allowed to be performed. This way, user operations can be approved in a fine-grained manner. The process management feature is used to approve operations performed by users, such as creating resources. You may perform high-risk operations in the Apsara Uni-manager Management Console. Before you perform high-risk operations, a role with higher or centralized permissions must approve the operations. This prevents accidental operations or unauthorized access and ensures the security, stability, and compliance of the system.

- If you associate a process with all organizations, all users or specific roles in all organizations can initiate the process. If you associate a process with a specific organization, all users or specific roles in the specified organization can initiate the process.
- When you create a process, you can specify multiple optional approvers or required approvers.
  - Optional approver: If one of the approvers for the approval node approves a process, the process is approved.
  - Required approver: A process is approved only if all the approvers for the approval node approve the process.
- After a process is created, you can modify, publish, disable, or delete the process.
  - If a process changes, you can modify the process.
  - You can publish processes that are in the Initialization or Disabled state. After a process is published, it can be associated with management operations, cloud service operations, or service catalogs.
  - You can disable a published process.
  - You can delete a process if you no longer need it.

Create a process

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Management**.
4. On the **Process Management** page, click **Create Process**.
5. In the **Create Process** wizard, configure the parameters in the **Basic Information** and **Process Configuration** steps.

i. The following table describes the parameters in the Basic Information step. After you configure the parameters, click **Next**.

Parameter	Description
Process Name	The name of the process.
Process Description	The description of the process.
Applicable Personnel	The organization with which the process can be associated. You can select **All Organizations** or **Select Organization**. - **All Organizations**: The process can be associated with all organizations. - **Select Organization**: The process can be associated only with the selected organization.
Select Organization	This parameter is displayed only if the **Applicable Personnel** parameter is set to **Select Organization**. Select an organization from the **Select Organization** drop-down list. You can select only one organization within a tenant. The process can be associated only with the selected organization.
Bind Sub-organization	This parameter is displayed only if the **Applicable Personnel** parameter is set to **Select Organization**. Specifies whether the process can be associated with the sub-organizations of the selected organization. If a sub-organization is associated with another process, the configuration does not take effect. After you select an organization from the **Select Organization** drop-down list, you can enable or disable this feature. - ●: The process can be associated with the sub-organizations of the selected organization. - ○: The process cannot be associated with the sub-organizations of the selected organization.
Select Initiator	Select **All Users** or **Specified Role**. If you set the **Applicable Personnel** parameter to **Select Organization** and turn on **Bind Sub-organization**, **all users** or **specified roles** in the selected organization and its sub-organizations can initiate the process.
Select Role	The roles that can initiate the process. This parameter is displayed only if the **Select Initiator** parameter is set to **Specified Role**. You can select one or more roles from the **Select Role** drop-down list. All users that assume the selected roles can initiate the process.

ii. Perform the following steps to configure the parameters in the **Process Configuration** step and click **Submit**:

a. Optional. Click the **Start** card. In the **Initiator Settings** panel, select or clear **Allow Initiator to Add CC Recipient**.

   - Select **Allow Initiator to Add CC Recipient**: allows the initiator to add CC recipients.

     > ⓘ **Note**
     >
     > If you select **Allow Initiator to Add CC Recipient**, the initiator can select only available users as CC recipients.

   - Clear **Allow Initiator to Add CC Recipient**: does not allow the initiator to add CC recipients.

b. Click the ⊕ icon on the canvas and click **Add Approval** to add an approval node.

> ⓘ **Note**
>
> After an approval node is added, you can click the ... icon in the upper-right corner of the approval node and click **Delete** to remove the approval node.

c. Click the **Approved By** card. In the **Approval Node Settings** panel, configure the approval node. When the applicant and the approver of the approval node are the same person, the approver automatically approves the process. If multiple approvers are involved, the other approvers review the process as normal.

Parameter	Description
	Type: the type of the approver. Valid values: **Specific Personnel**, **Specified Role**, **Supervisor**, and **Continuous Multi-level Supervisor**. ▪ If you set the **Type** parameter to **Specific Personnel**, select one or more users from the **Specific Personnel** drop-down list to specify the users as the approvers of the approval node. ▪ If you set the **Type** parameter to **Specified Role**, select a role from the **Select Role** drop-down list. You can select only one role. ⓘ **Note** You can specify whether to allow only the roles in the organization to which the initiator belongs to approve the process. If you select the check box, only the roles in the organization to which the initiator belongs can approve the process. If you do not select the check box, all users assigned the selected role in the level-1 organization can approve the process.

Approved By	- If you set the **Type** parameter to **Supervisor**, select a value from the **Initiator** drop-down list to specify the level of the supervisor. Only a supervisor of the selected level is involved as the approver of the approval node. The valid values of the **Initiator** parameter are **Direct Supervisor**, **Second Level Supervisor**, **Third Level Supervisor**, **Fourth Level Supervisor**, and **Fifth Level Supervisor**. You can select only one level of the supervisor as the approver. **Note** - A member that assumes the organization administrator role in each level of the organization hierarchy is the supervisor. If you select **Direct Supervisor**, the approver is the organization administrator of the organization to which the initiator belongs. If you select **Second Level Supervisor**, the approver is the organization administrator of the parent organization to which the initiator belongs. You can select a supervisor of up to the fifth level. - If no supervisor can be found, the process is automatically approved. After you configure continuous multi-level supervisors, the supervisors at different levels can approve the process in turn. - If you set the **Type** parameter to **Continuous Multi-level Supervisor**, select a value from the **Approval Endpoint** drop-down list to specify the level of the supervisor as the final approver. The process is approved based on the organization hierarchy from the lowest level to the highest level. Supervisors of multiple levels may be involved as the approvers of the approval node. The valid values of the **Approval Endpoint** parameter are **Direct Supervisor**, **Second Level Supervisor**, **Third Level Supervisor**, **Fourth Level Supervisor**, and **Fifth Level Supervisor**. You can select only one level of the supervisor as the final approver. **Note** - If you select **Direct Supervisor**, the final approver is the organization administrator of the organization to which the initiator belongs. If you select **Second Level Supervisor**, the final approver is the organization administrator of the parent organization to which the initiator belongs. You can select a supervisor of up to the fifth level. - If no supervisor can be found, the process is automatically approved. After you configure continuous multi-level supervisors, the supervisors at different levels can approve the process in turn.

Approval Method	▪ **When multiple approvers are specified**: You can select **Parallel Signature(Requires Approval by One)** or **Sequential Signature(Requires Approval by All)**. ▪ **When the approver is not specified**: You can select **Automatically Approved**, **This parameter is required**, or **Handled by Specific Personnel**. **Note** ▪ This parameter is displayed only if the **Type** parameter is set to **Supervisor** or **Continuous Multi-level Supervisor**. ▪ If the **When the approver is not specified** parameter is set to **This parameter is required**, you must specify an approver. Otherwise, the process configuration is invalid and cannot be submitted. ▪ If the **When the approver is not specified** parameter is set to **Handled by Specific Personnel**, you must configure the **Specific Personnel** parameter. You can select one or more users from the **Specific Personnel** drop-down list. ▪ **Allow the approver to specify additional signatories**: specifies whether the approver can add signatories. ▪ Select **Allow the approver to specify additional signatories**: allows the approver to add signatories. **Note** Only the current approver can add signatories. Multiple signatories can be specified. ▪ Clear **Allow the approver to specify additional signatories**: does not allow the approver to add signatories.
Add CC Recipient	The CC recipients. You can select one or more users from the**Specific Personnel** drop-down list.

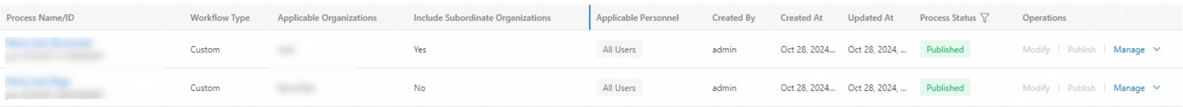
d. Optional. Click the **End** card. In the **End Node Settings** panel, specify the users who are notified of the end of the process. After the process ends, the approval results are automatically sent to the specified users.

   You can select one or more users from the **Specific Personnel** drop-down list. The selected users must be visible to the process creator.

View processes

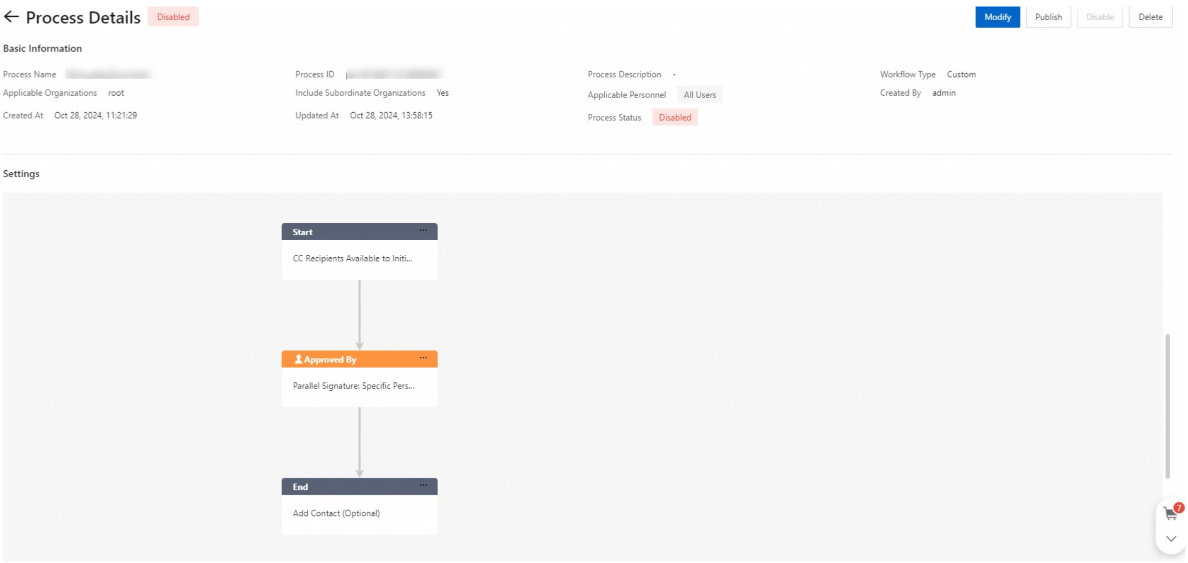
1. On the **Process Management** page, click **Advanced Filter** to search for a process.
2. In the process list, view the information displayed in the following columns: **Process Name/ID**, **Workflow Type**, **Applicable Organizations**, **Include Subordinate Organizations**, **Applicable Personnel**, **Created By**, **Created At**, **Updated At**, and **Process Status**.

> **Note**
>
> A process can be in the **Initialization**, **Published**, or **Disabled** state. You can click the ▽ icon in the **Process Status** column to filter processes by status.



Process Name/ID	Workflow Type	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Created By	Created At	Updated At	Process Status ▽	Operations
[redacted]	Custom	[redacted]	Yes	All Users	admin	Oct 28, 2024...	Oct 28, 2024, ...	Published	Modify | Publish | Manage
[redacted]	Custom	[redacted]	No	All Users	admin	Oct 28, 2024...	Oct 28, 2024, ...	Published	Modify | Publish | Manage

3. Click the process name to go to the **Process Details** page.



Basic Information

Process Name [redacted]

Applicable Organizations root

Created At Oct 28, 2024, 11:21:29

Process ID [redacted]

Include Subordinate Organizations Yes

Updated At Oct 28, 2024, 13:58:15

Process Description -

Applicable Personnel All Users

Process Status Disabled

Workflow Type Custom

Created By admin

Settings

Start
CC Recipients Available to Initi...
Approved By
Parallel Signature: Specific Pers...
End
Add Contact (Optional)

> **Note**
>
> Click the information card in the **Settings** section to view the detailed configuration of each process node.

Modify a process

> **Important**
>
> Only processes that are in the **Initialization** or **Disabled** state can be modified.

1. On the **Process Management** page, find the process that you want to modify and click **Modify** in the **Operations** column.
2. In the **Edit Process** wizard, configure the process based on your business requirements. For more information, see the Create a process section of this topic.

Publish a process

> **Important**
>
> Only processes that are in the **Initialization** or **Disabled** state can be published.

1. On the **Process Management** page, find the process that you want to publish and click **Publish** in the **Operations** column.

2. In the message that appears, click **OK**.

   After the process is published, the status of the process changes to **Published**.

Disable a process

> ⓘ **Important**
>
> Only processes that are in the **Published** state can be disabled.

1. On the **Process Management** page, find the process that you want to disable and choose **Manage** > **Disable** in the **Operations** column.
2. In the message that appears, click **OK**.

   After the process is disabled, the status of the process changes to **Disabled**.

Delete a process

> ⓘ **Important**
>
> Before you delete a process, disassociate the process from the associated business scenarios. Otherwise, the process associations with business scenarios are also deleted after the process is deleted.

1. On the **Process Management** page, find the process that you want to delete and choose **Manage** > **Delete** in the **Operations** column.
2. In the message that appears, click **OK**.

6.1.2.2. Process binding

You can configure the mappings between processes and operation items to meet the business requirements in different scenarios.

Background information

- You can associate a process with a business scenario based on your business requirements and process configurations. This way, the operations in the business scenario can be performed only after the process is approved. This helps you better control the operations in business scenarios and ensures the compliance and accuracy of business activities.
- You can create, modify, and delete process associations.

Create a process association

> ⓘ **Important**
>
> Before you associate a process with a business scenario, make sure that the process is created and is in the **Published** state.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Binding**.
4. In the upper part of the page, click **Process Binding**.
5. On the **Process Binding** page, configure the parameters that are described in the following table.

Parameter	Description
Process Name	The name of the process that you want to associate. Select a process from the Process Name drop-down list. You can select only a process in the **Published** state.
Scenario	The business scenario with which the process is associated. Valid values: **Management Operations**, **Cloud Service Operations**, and **Service Catalog**. You can select only one value.
Management Operations	This parameter is displayed only if the **Scenario** parameter is set to **Management Operations**. In this business scenario, process approval is required before specific management operations are performed, such as managing organizations and resource sets.
Cloud Service Operations	This parameter is displayed only if the **Scenario** parameter is set to **Cloud Service Operations**. In this business scenario, process approval is required before specific cloud service operations are performed, such as starting and stopping Elastic Compute Service (ECS) instances.
Service Catalog	This parameter is displayed only if the **Scenario** parameter is set to **Service Catalog**. After you select a service type, the corresponding service catalogs are displayed. In the service catalog list, select operations in the **Operations** column. For example, you can select Create and Change.

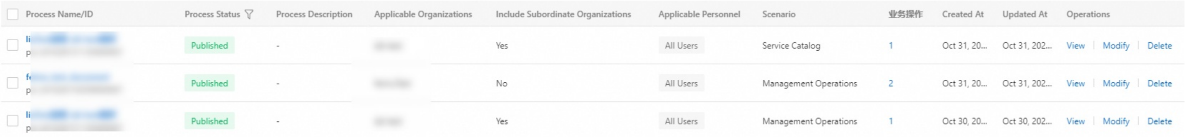
6. Click **Submit**.

> **Note**
>
> If you select **No permissions are required for the initiator** , the initiator can initiate a process without the need to obtain the permissions to perform the operations in the process.

View process associations

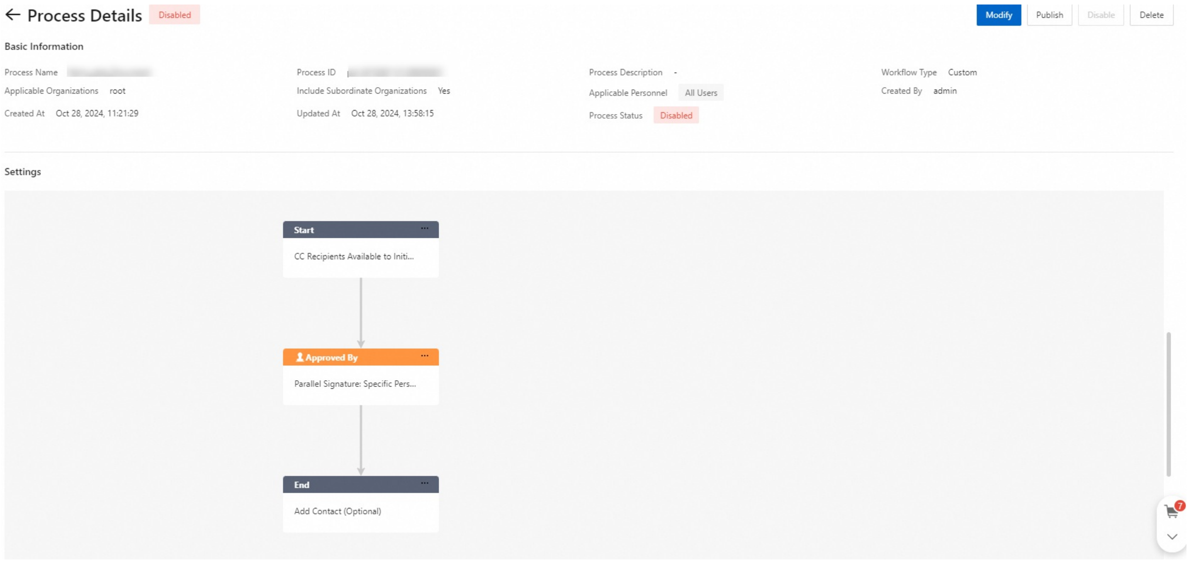
1. On the **Process Binding** page, click **Advanced Filter**. Configure the **Process Name**, **Applicable Personnel**, and **Scenario** filter conditions to search for a process.
2. In the process association list, view the information displayed in the following columns: **Process Name/ID**, **Process Status**, **Process Description**, **Applicable Organizations**, **Include Subordinate Organizations**, **Applicable Personnel**, **Scenario**, **Business Operations**, **Created At**, and **Updated At**.

> **Note**
>
> Valid values of the **Scenario** parameter include **Management Operations**, **Cloud Service Operations**, and **Service Catalog**. After you select a specific scenario, you can select a business operation from the corresponding **Management Operations**, **Cloud Service Operations**, or **Service Catalog** filter.



Process Name/ID	Process Status	Process Description	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Scenario	业务操作	Created At	Updated At	Operations
[redacted]	Published	-	[redacted]	Yes	All Users	Service Catalog	1	Oct 31, 20...	Oct 31, 202...	View | Modify | Delete
[redacted]	Published	-	[redacted]	No	All Users	Management Operations	2	Oct 31, 20...	Oct 31, 202...	View | Modify | Delete
[redacted]	Published	-	[redacted]	Yes	All Users	Management Operations	1	Oct 30, 20...	Oct 30, 202...	View | Modify | Delete

3. Click the process name or click **View** in the **Actions** column to go to the details page of the process.



Basic Information

Process Name [redacted]
Process ID [redacted]
Process Description -
Workflow Type Custom
Applicable Organizations root
Include Subordinate Organizations Yes
Applicable Personnel All Users
Created By admin
Created At Oct 28, 2024, 11:21:29
Updated At Oct 28, 2024, 13:58:15
Process Status Disabled

Settings

Start
CC Recipients Available to Initi...
Approved By
Parallel Signature: Specific Pers...
End
Add Contact (Optional)

> **Note**
>
> Click the information card in the **Settings** section to view the detailed configuration of each process node.

Modify a process association

> **Note**
>
> When you modify a process association, you can modify only the specific management operations, cloud service operations, or service catalogs. Other configurations cannot be modified.

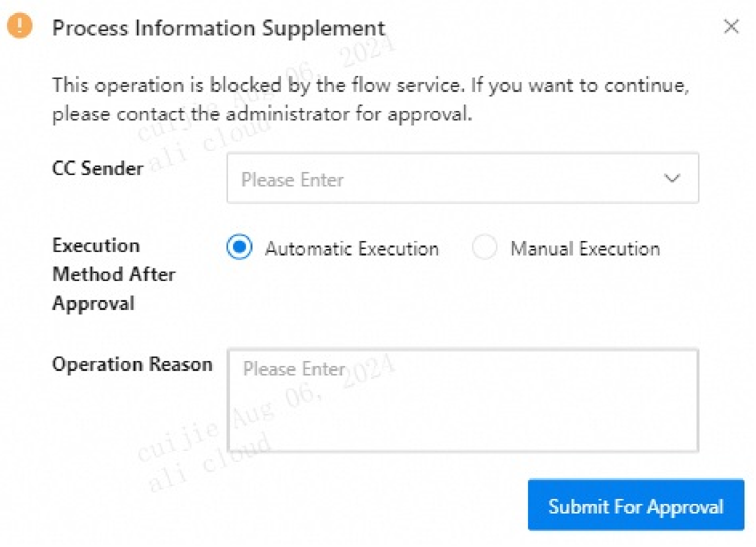
1. On the **Process Binding** page, click **Advanced Filter** to search for the process that is bound to your business.
2. In the process association list, find the process association that you want to modify and click **Modify** in the **Operations** column.
3. Modify the operations based on your business requirements.

Delete a process association

1. On the **Process Binding** page, click **Advanced Filter** to search for the process that is bound to your business.
2. In the process association list, find the process association that you want to delete and click **Delete** in the **Operations** column.
3. Click **OK**.

Provide supplementary information

After a process is associated with a business scenario, the related operations are reviewed by using the process management feature before the operations can be performed. Before you initiate a process, you must provide supplementary information.



Process Information Supplement

This operation is blocked by the flow service. If you want to continue, please contact the administrator for approval.

CC Sender: Please Enter

Execution Method After Approval: ● Automatic Execution ○ Manual Execution

Operation Reason: Please Enter

> **Note**
>
> The initiator can add CC recipients only if Allow Initiator to Add CC Recipient is selected during process configuration. The initiator can select only available users as CC recipients.

6.1.3. Quota management

6.1.3.1. Overview

The organization administrator and users of an organization can create resources within the quota of the cloud services. When the quota of a service in an organization is exhausted, resources of the service can no longer be created. You must increase the quota of the service in the organization before you can create resources again. If no quotas are set, an unlimited amount of resources can be created.

> **Note**
>
> Quotas for resources such as disks, memory, and storage capacity are measured in **GB**, and the quantities are integers. Decimals are rounded to their nearest integer. For example, 0.8 GB is rounded up to 1 GB, and 0.2 GB is rounded down to 0 GB.

6.1.3.1.1. Elastic computing

6.1.3.1.1.1. ROS

This topic describes the quotas that you can configure for Resource Orchestration Service (ROS), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
Stacks(Units)	The total number of stacks that can be created for ROS.

Calculation methods of quota usage

Quota usage of ROS = Number of stacks that are created

> **Note**
>
> The quota usage of ROS is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.1.2. ECS

This topic describes the quotas that you can configure for Elastic Compute Service (ECS), calculation method of quota usage, and inventory source.

Quotas

Quota	Description
CPU Quota(Cores)	The total number of CPU cores that you can configure for ECS.
GPU Quota(GPUs)	The total number of GPU cores that you can configure for ECS.
Memory Quota(G)	The total memory size that you can configure for ECS.
SSD(GB)	The total capacity of SSDs that you can configure for ECS.
Ultra Disk(GB)	The total capacity of ultra disks that you can configure for ECS.
Premium Performance Disk(GB)	The total capacity of high-performance disks that you can configure for ECS.

Standard Performance Disk(GB)	The total capacity of standard performance disks that you can configure for ECS.

Calculation method of quota usage

The usage of CPU cores, memory, GPUs, and disk capacity of a single ECS instance is calculated based on the following formulas:

- CPU core usage = instanceTypeId.cpu
- Memory usage = instanceTypeId.mem
- GPU usage = instanceTypeId.gpu
- Disk capacity usage= ∑ (System disks and attached disks)

> **Note**
>
> - - instanceTypeId.cpu indicates the number of CPU cores defined in the selected instance type.
>   - instanceTypeId.mem indicates the memory size defined in the selected instance type.
>   - instanceTypeId.gpu indicates the number of GPUs defined in the selected instance type.
> - You can calculate the disk capacity usage of an instance by accumulating the size of the system disks and the size of the attached disks.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

> **Important**
>
> Some Elastic Block Storage (EBS) clusters can share disks of multiple types. When you configure the logical inventory, make sure that the sum of the logical inventories of the quota items of multiple disks cannot be greater than the physical inventory. For example, if an I/O15 cluster has a physical inventory of 1,000 GB and can share premium performance disks and SSDs, the physical inventory of both premium performance disks and SSDs is increased by 1,000 GB. When you configure the logical inventory, you need to check whether disk sharing is enabled for the EBS cluster and make sure that logical inventory cannot be greater than 1,000 GB.

6.1.3.1.1.3. Auto Scaling

This topic describes the quotas that you can configure for Auto Scaling, the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
Scaling Group(Units)	The total number of scaling groups that can be created for Auto Scaling.

Calculation methods of quota usage

Quota usage of Auto Scaling = Number of scaling groups that are created

> ? **Note**
>
> The quota usage of Auto Scaling is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.1.4. DDH

This topic describes the quotas that you can configure for Dedicated Host (DDH), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
DDH Quota(Units)	The total number of dedicated hosts that can be created for DDH.

Calculation methods of quota usage

Quota usage of DDH = Number of dedicated hosts that are created

> ? **Note**
>
> The quota usage of DDH is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.1.5. BMS

This topic describes the quotas that you can configure for Bare-metal Management Service (BMS), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
Bare Metal Instances(Units)	The total number of bare metal instances that can be managed by BMS.
In-band Instance(Sets)	The total number of in-band instances that can be created for BMS.

Out-of-band Instance(Sets)	The total number of out-of-band instances that can be created for BMS.

Calculation methods of quota usage

- Bare metal instance quota usage = Number of bare metal instances that are managed by BMS
- In-band instance quota usage = Number of in-band instances that are created for BMS
- Out-of-band instance quota usage = Number of out-of-band instances that are created for BMS

> **Note**
>
> The quota usage of BMS is calculated based on the number of resource instances.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.1.6. ACK

This topic describes the quotas that you can configure for Container Service for Kubernetes (ACK), calculation method of quota usage, and inventory source.

Quota

Quota	Description
Cluster(Units)	The total number of clusters that can be created for ACK.

Calculation method of quota usage

ACK quota usage = Number of clusters that are created for ACK

> **Note**
>
> The quota usage of ACK is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.1.7. OOS

This topic describes the quotas that you can configure for CloudOps Orchestration Service (OOS), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
OOS Custom Template(Units)	The total number of custom templates that can be created for OOS.

Calculation methods of quota usage

Quota usage of OOS = Number of custom templates that are created

> ? **Note**
>
> The quota usage of OOS is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.1.8. Container Registry Standard Edition

This topic describes the quotas that you can configure for Container Registry Standard Edition, calculation method of quota usage, and inventory source.

Quota

Quota	Description
Image Repository Quota	The number of image repositories that can be created for Container Registry Standard Edition.

Calculation method of quota usage

Quota usage of Container Registry Standard Edition = Number of image repositories that are created for Container Registry Standard Edition

> ? **Note**
>
> The quota usage of Container Registry Standard Edition is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.2. Storage

6.1.3.1.2.1. NAS

This topic describes the quotas that you can configure for File Storage NAS (NAS) and Cloud Parallel File Storage (CPFS), calculation method of quota usage, and inventory source.

Quotas

Quota	Description
NAS Quota(GB)	The total storage capacity of NAS.
NAS Usage(GB)	This quota is of the weak verification type. You can configure this quota to specify the maximum storage capacity of NAS that can be used. If the actual used storage capacity of NAS exceeds the value that you specify for this quota, you cannot create new NAS file systems. However, the existing NAS file systems are not affected.
Performance Disk Capacity(GB)	The storage capacity of a Performance CPFS file system.
Capacity Disk Capacity(GB)	The storage capacity of a Capacity CPFS file system.

Calculation method of quota usage

Quota usage of a single NAS or CPFS file system = Quota usage of the NAS or CPFS file system that you select

> ⓘ **Note**
>
> - The maximum capacity that can be pre-allocated to a NAS file system is equal to the total capacity of the NAS file system.
> - The actual capacity usage of a NAS file system is included in the NAS Usage quota.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.2.2. OSS

This topic describes the quotas that you can configure for Object Storage Service (OSS), calculation method of quota usage, and inventory source.

Quotas

Quota	Description
Bucket Quota(GB)	The total capacity of OSS buckets.
Bucket Usage(GB)	The maximum capacity of the OSS buckets that can be used. Weak verification is performed on the quota. If the actual used capacity of OSS buckets exceeds the value that you specify for this quota, you cannot create new buckets, but the existing buckets are not affected.

Calculation method of quota usage

Capacity quota of a single bucket = Capacity of the selected bucket

> **Note**
>
> - The total capacity of a bucket is equal to the maximum capacity that can be pre-allocated to the bucket.
> - The resource usage details of a bucket are included in the Bucket Usage quota.
> - The total capacity of an OSS bucket whose capacity is unlimited is calculated as 0.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.2.3. Tablestore

This topic describes the quotas that you can configure for Tablestore, calculation method of quota usage, and inventory source.

Quota

Quota	Description
Instances(Units)	The maximum number of Tablestore instances that can be created.

Calculation method of quota usage

Tablestore quota usage = Number of Tablestore instances that are created

> **Note**
>
> The quota usage of Tablestore is calculated based on the number of Tablestore instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.2.4. APFS File System

This topic describes the quota that you can configure for APFS file systems, calculation method of quota usage, and inventory source.

Quotas

Quota	Description
Performance Disk Capacity(GB)	The storage capacity of a Performance APFS file system.

Calculation method of quota usage

Quota usage of a Performance APFS file system = Storage capacity of the Performance APFS file system

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.3. Networking

6.1.3.1.3.1. EIP

This topic describes the quotas that you can configure for Elastic IP Address (EIP), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
EIP Quota(Units)	The total number of EIPs that can be created.

Calculation methods of quota usage

Quota usage of EIP = Number of EIPs that are created

> ? **Note**
>
> The quota usage of EIP is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.2. SLB

This topic describes the quotas that you can configure for Server Load Balancer (SLB), calculation methods of quota usage, and inventory source.

Quotas

Quota	Description
Internal IP Quota - Classic Network(Units)	The total number of IP addresses that can be created for SLB in the classic network.
Internal IP Quota - VPC(Units)	The total number of IP addresses that can be created for SLB in a virtual private cloud (VPC).
Public IP Address Quota(Units)	The total number of public IP addresses that can be created for SLB.

CA Certificate(Units)	The total number of certificate authority (CA) certificates that can be created for SLB.
Server Certificate(Units)	The total number of server certificates that can be created for SLB.

Calculation methods of quota usage

- Usage of private IP addresses that are created in the classic network = Number of IP addresses that are created for SLB in the classic network
- Usage of private IP addresses that are created in a VPC = Number of IP addresses that are created for SLB in the VPC
- Public IP address usage = Number of public IP address that are created for SLB
- CA certificate usage = Number of CA certificate instances
- Server certificate usage = Number of server certificate instances

> ? **Note**
>
> The quota usage of SLB is calculated based on the number of corresponding resource instances.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.3.3. HAVIP

This topic describes the quotas that you can configure for high-availability virtual IP address (HAVIP), calculation method of quota usage, and inventory source.

Quota

Quota	Description
HAVIP Quota(Units)	The maximum number of HAVIPs that can be created.

Calculation method of quota usage

HAVIP usage = Number of HAVIPs that are created

> ? **Note**
>
> The quota usage of HAVIP is calculated based on the number of HAVIPs that are created.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.4. VPC

This topic describes the quotas that you can configure for Virtual Private Cloud (VPC), the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
VPC Quota(Units)	The total number of VPCs that can be created.

Calculation methods of quota usage

Quota usage of VPC = Number of VPCs that are created

> **Note**
> The quota usage of VPC is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.5. Express Connect

This topic describes the quotas that you can configure for Express Connect, calculation method of quota usage, and inventory source.

Quota

Quota	Description
Connections(Units)	The total number of VBR-to-VPC connections that can be created for Express Connect.

Calculation method of quota usage

Quota usage of Express Connect =Total number of VBR-to-VPC connections that are created for Express Connect

> **Note**
> The quota usage of Express Connect is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.6. NAT Gateway

This topic describes the quotas that you can configure for NAT Gateway, calculation method of quota usage, and inventory source.

Quota

Quota	Description
Instances(Units)	The number of NAT gateways that can be created for NAT Gateway.

Calculation method of quota usage

Quota usage of NAT Gateway = Number of NAT gateways that are created for NAT Gateway

> **Note**
> The quota usage of NAT Gateway is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.7. VPN Gateway

This topic describes the quotas that you can configure for VPN Gateway, calculation method of quota usage, and inventory source.

Quota

Quota	Description
Instances(Units)	The total number of VPN gateways that can be created for VPN Gateway.

Calculation method of quota usage

Quota usage of VPN Gateway = Number of VPN gateways that are created for VPN Gateway

> **Note**
> The quota usage of VPN Gateway is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.3.8. DNS

This topic describes the quotas that you can configure for Apsara Stack DNS (DNS), calculation method of quota usage, and inventory source.

Quota

Quota	Description
Private Line(Units)	The number of private lines that can be created for DNS.

Calculation method of quota usage

Private line usage = Number of private lines that are created for DNS.

> ? **Note**
> The quota usage of DNS is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.4. Database services

6.1.3.1.4.1. ApsaraDB for MongoDB

This topic describes the quotas that you can configure for ApsaraDB for MongoDB, the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
CPU Quota(Cores)	The total number of CPU cores that can be configured for ApsaraDB for MongoDB.
Memory Quota(GB)	The total memory capacity that can be configured for ApsaraDB for MongoDB.
Disk Quota(GB)	The total storage capacity that can be configured for ApsaraDB for MongoDB.

Calculation methods of quota usage

- **Replica set instance**
  - CPU quota usage = DBInstanceClass.cpu × Number of primary and secondary nodes
  - Memory quota usage = DBInstanceClass.mem × Number of primary and secondary nodes
  - Disk quota usage = DBInstanceStorage × Number of primary and secondary nodes

> **Note**
>
> The quota usage is calculated based on the instance specifications and the number of primary and secondary nodes.
>
> - DBInstanceClass.cpu: the number of CPU cores of the selected instance specifications.
> - DBInstanceClass.mem: the memory capacity of the selected instance specifications.
> - DBInstanceStorage: the storage capacity of the selected instance specifications.
> - By default, the number of primary and secondary nodes is 3.

- **Sharded cluster instance**
  - CPU quota usage = mongosSpec.cpu × mongosCount + shardSpec.cpu × shardCount × Number of replicas + configserverSpec.cpu × configserverCount × Number of replicas
  - Memory quota usage = mongosSpec.mem × mongosCount + shardSpec.mem × shardCount × Number of replicas + configserverSpec.mem × configserverCount × Number of replicas
  - Disk quota usage = shardStorage × shardCount × Number of replicas + configserverStorage × configserverCount × Number of replicas

> **Note**
>
> The quota usage of mongos nodes, shard nodes, and Configserver nodes is calculated.
>
> - The quota usage of mongos nodes is calculated based on the node specifications and the number of mongos nodes.
>   - mongosSpec.cpu: the number of CPU cores of the selected mongos node specifications.
>   - mongosCount: the number of mongos nodes.
> - The quota usage of shard nodes is calculated based on the node specifications, the number of shard nodes, and the number of replicas.
>   - shardSpec.cpu: the number of CPU cores of the selected shard node specifications.
>   - shardSpec.mem: the memory capacity of the selected shard node specifications.
>   - shardStorage: the storage capacity of the selected shard node specifications.
>   - shardCount: the number of shard nodes.
>   - By default, the number of replicas is 3.
> - The quota usage of Configserver nodes is calculated based on the node specifications, the number of Configserver nodes, and the number of replicas.
>   - configserverSpec.cpu: the number of CPU cores of the selected Configserver node specifications.
>   - configserverSpec.mem: the memory capacity of the selected Configserver node specifications.
>   - configserverStorage: the storage capacity of the selected Configserver node specifications.
>   - configserverCount: the number of Configserver nodes.
>   - By default, the number of replicas is 3.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

> **Note**
>
> Sharded ApsaraDB for MongoDB instances share physical resources with each other without being limited by the physical inventory. The shared physical resources include the memory capacity and CPU cores. Therefore, the physical inventory of the memory capacity and CPU cores may not indicate the saleable memory capacity and CPU cores. The saleable memory capacity and CPU cores may be greater than the physical inventory.

6.1.3.1.4.2. PolarDB-X 1.0

This topic describes the quotas that you can configure for PolarDB-X 1.0, calculation method of quota usage, and inventory source.

Quota

Quota	Description
CPU Quota(Cores)	The total number of CPU cores that can be configured for PolarDB-X 1.0.

Calculation method of quota usage

CPU core usage = drdsSpec.cpu

> ? **Note**
>
> drdsSpec.cpu indicates the number of CPU cores of the selected instance type.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.4.3. ApsaraDB RDS

This topic describes the quotas that you can configure for ApsaraDB RDS, the calculation methods of quota usage, and the inventory source.

Database engines

ApsaraDB RDS supports the following database engines: MySQL, PostgreSQL, PolarDB, and SQL Server. You can configure quotas for different database engines.

Quotas

Quota	Description
CPU Quota(Cores)	The total number of CPU cores that can be configured for ApsaraDB RDS.
Memory Quota(GB)	The total memory capacity that can be configured for ApsaraDB RDS.
Disk Quota(GB)	The total storage capacity that can be configured for ApsaraDB RDS.

Calculation methods of quota usage

- **High-availability Edition**
  - CPU quota usage = dbInstanceClass.cpu × Number of nodes
  - Memory quota usage = dbInstanceClass.mem × Number of nodes
  - Disk quota usage = DBInstanceStorage × Number of nodes

> **Note**
>
> The quota usage is calculated based on the instance specifications and the number of nodes.
>
> - dbInstanceClass.cpu: the number of CPU cores of the selected instance specifications.
> - dbInstanceClass.mem: the memory capacity of the selected instance specifications.
> - DBInstanceStorage: the storage capacity of the selected instance specifications.
> - By default, the number of nodes is 2.

- **Enterprise Edition**
  - CPU quota usage = dbInstanceClass.cpu × Number of regular nodes + Fixed CPU overhead of replica nodes
  - Memory quota usage = dbInstanceClass.mem × Number of regular nodes + Fixed memory overhead of replica nodes
  - Disk quota usage = DBInstanceStorage × Number of regular nodes + Fixed storage overhead of replica nodes

> **Note**
>
> - The CPU quota usage is calculated based on the instance specifications, the number of regular nodes, and the fixed resource overhead of replica nodes.
>   - dbInstanceClass.cpu: the number of CPU cores of the selected instance specifications.
>   - By default, the number of regular nodes is 2.
>   - The CPU overhead of replica nodes is fixed to 2 GB.
> - The memory quota usage is calculated based on the instance specifications, the number of regular nodes, and the fixed resource overhead of replica nodes.
>   - dbInstanceClass.mem: the memory capacity of the selected instance specifications.
>   - By default, the number of regular nodes is 2.
>   - The memory overhead of replica nodes is fixed to 4 GB.
> - The disk quota usage is calculated based on the instance specifications, the number of regular nodes, and the fixed resource overhead of replica nodes.
>   - DBInstanceStorage: the storage capacity of the selected instance specifications.
>   - By default, the number of regular nodes is 2.
>   - The storage overhead of replica nodes is fixed to 50 GB.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

> **Note**
>
> - ApsaraDB RDS for MySQL instances and PolarDB for MySQL clusters that use local disks share the inventory.
> - Shared ApsaraDB RDS instances share physical resources with each other without being limited by the physical inventory. The shared physical resources include the memory capacity and CPU cores. Therefore, the physical inventory of the memory capacity and CPU cores may not indicate the saleable memory capacity and CPU cores. The saleable memory capacity and CPU cores may be greater than the physical inventory.

6.1.3.1.4.4. KVStore for Redis

This topic describes the quotas that you can configure for KVStore for Redis, calculation method of quota usage, and inventory source.

Quotas

Quota	Description
Memory Quota(GB)	The total size of memory that can be configured for KVStore for Redis.

Calculation method of quota usage

- **Standard (Master-replica) Edition**

  Memory usage = instanceClass.mem × Number of replicas

  > **Note**
  >
  > The preceding formula is used to calculate the memory usage of a standard instance.
  >
  > - instanceClass.mem indicates the memory size that is defined in the instance type.
  > - The number of replicas is fixed as 2.

- **Cluster Edition**

  Memory usage = instanceClass.mem × Number of replicas + Proxy node overhead + CS node overhead

> **Note**
>
> The preceding formula is used to calculate the memory usage of a cluster instance.
>
> - instanceClass.mem indicates the memory size that is defined in the instance type.
> - The number of replicas is fixed as 2.
> - You can calculate the corresponding proxy node overhead based on the number of proxy nodes. You can obtain the number of proxy nodes by checking the number before "proxy" in the InstanceClass field. For example, if an instance is of the redis.logic.sharding.8g.8db.0rodb.8proxy.default class, the number of proxy nodes of the instance is 8.
> - The CS node overhead is fixed as 1GB.

- **Read/write Splitting**

  Memory usage = instanceClass.mem × (1 + Number of read-only nodes) + Proxy node overhead

> **Note**
>
> The preceding formula is used to calculate the memory usage of a read/write splitting instance.
>
> - instanceClass.mem indicates the memory size that is defined in the instance type.
> - You can select one or three read-only nodes when you select a node type.
> - You can calculate the corresponding proxy node overhead based on the number of proxy nodes. You can obtain the number of proxy nodes by checking the number before "proxy" in the InstanceClass field. For example, if an instance is of the redis.logic.sharding.8g.8db.0rodb.8proxy.default class, the number of proxy nodes of the instance is 8.

The following table describes the relationships between the number of proxy nodes and the proxy node overhead.

Number of proxy nodes	Proxy node overhead
4	20 GB
6	30 GB
8	40 GB
12	40 GB
16	60 GB

24	80 GB
32	120 GB
48	180 GB
64	240 GB
96	320 GB
128	480 GB
192	480 GB
256	480 GB
384	960 GB
512	1,280 GB
768	1,920 GB
1024	2,560 GB

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

> **Note**
>
> The memory of a shared Redis instance can be shared. The shared Redis instance shares physical resources with other shared Redis instances without being limited by the physical inventory. Therefore, the physical inventory data of the memory size may not be equal to the exact saleable memory size. The saleable memory size may be greater than the physical inventory.

6.1.3.1.4.5. PolarDB

This topic describes the quotas that you can configure for PolarDB, calculation method of quota usage, and inventory source.

Quotas

Quota	Description
CPU Quota(Cores)	The total number of CPU cores that you can configure for PolarDB.
Memory Quota(G)	The total size of memory that you can configure for PolarDB.
Disk Quota(GB)	The total storage capacity that you can configure for PolarDB.

Calculation method of quota usage

- CPU core usage = DBNodeClass.cpu × DBNodeNum + CPU overhead of hot standby storage cluster + CPU overheads of PolarProxy.
- Memory usage = DBNodeClass.mem × DBNodeNum + Memory overhead of hot standby storage cluster + Memory overhead of PolarProxy.
- Disk capacity usage = StorageSpace + Disk overhead of hot standby storage cluster.

> ⓘ **Note**
>
> - DBNodeClass.cpu indicates the number of CPU cores defined in the selected node specifications.
> - DBNodeNum indicates the number of selected nodes. If you select **1 read/write node and 1 read-only node**, the number of nodes is 2. If you select **1 read/write node**, the number of nodes is 1.
> - DBNodeClass.mem indicates the memory size defined in the selected node specifications.
> - StorageSpace indicates the storage space of the selected disk.
> - You can disable the hot standby storage cluster feature to eliminate the CPU overhead of hot standby storage cluster.
>   - If the hot standby storage cluster feature is disabled, the CPU overhead of hot standby storage cluster is 0.
>   - If the hot standby storage cluster feature is enabled, the CPU overhead is equal to the number of CPU cores defined in the selected node specifications.
> - You can disable the PolarProxy feature to eliminate the CPU overhead of PolarProxy.
>   - If the PolarProxy feature is disabled, the CPU overhead of PolarProxy is 0.
>   - If the PolarProxy feature is enabled, the CPU overhead is calculated based on the following formulas:
>   - MySQL and PostgreSQL: CPU overhead of PolarProxy = Number of CPU cores defined in the selected cluster specifications.
>   - Oracle: CPU overhead of PolarProxy = Number of CPU cores defined in the selected cluster specifications × 2. By default, two replicas are used.
> - You can disable the hot standby storage cluster feature to eliminate the memory overhead of hot standby storage cluster.

> - If the hot standby storage cluster feature is disabled, the memory overhead of hot standby storage cluster is 0.
>   - If the hot standby storage cluster feature is enabled, the memory overhead is equal to the number of CPU cores defined in the selected node specifications.
> - You can disable the PolarProxy feature to eliminate the memory overhead of PolarProxy.
>   - If the PolarProxy feature is disabled, the memory overhead of PolarProxy is 0.
>   - If the PolarProxy feature is enabled, the memory overhead is calculated based on the following formulas:
>   - MySQL and PostgreSQL: Memory overhead of PolarProxy = 4 GB. This is a fixed value.
>   - Oracle: Memory overhead of PolarProxy = Number of memory size defined in the selected cluster specifications × 2. By default, two replicas are used.
> - You can disable the hot standby storage cluster feature to eliminate the disk overhead of hot standby storage cluster.
>   - If the hot standby storage cluster feature is disabled, the disk overhead of hot standby storage cluster is 0.
>   - If the hot standby storage cluster feature is enabled, the disk overhead is equal to the storage space of the selected disk.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.4.6. DTS

This topic describes the quotas that you can configure for Data Transmission Service (DTS), calculation method of quota usage, and inventory source.

Quotas

Quota	Description
Migration Task(Units)	The total number of migration tasks that can be created for DTS.
Synchronization Tasks(Units)	The total number of synchronization tasks that can be created for DTS.
Subscription Tasks(Units)	The total number of change tracking tasks that can be created for DTS.

Calculation method of quota usage

- Migration task usage = Number of migration tasks that are created for DTS
- Synchronization task usage = Number of synchronization tasks that are created for DTS

- Change tracking task usage = Number of change tracking tasks that are created for DTS

> ⓘ **Note**
>
> The quota usage of DTS is calculated based on the number of corresponding resource instances.

Inventory source

No inventory is connected. By default, the inventory is unlimited.

6.1.3.1.5. Big data

6.1.3.1.5.1. MaxCompute

This topic describes the quotas that you can configure for MaxCompute, the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
CU Quota(Units)	The total number of compute units (CUs) that can be configured for MaxCompute.
Disk Quota(GB)	The total capacity of disks that can be configured for MaxCompute.

Calculation methods of quota usage

- CU quota usage = Number of CUs that are configured for the current instance
- Disk quota usage = Used disk capacity of the current instance

> ⓘ **Note**
>
> - The CU quota usage of the current instance is equal to the number of CUs that are configured for the current instance.
> - The disk quota usage of the current instance is calculated based on the requested disk size.

Inventory source

The data is collected by the Capacity module of the Apsara Uni-manager Operations Console.

6.1.3.1.6. Security

6.1.3.1.6.1. PAM

This topic describes the quotas that you can configure for Privileged Access Management (PAM), calculation method of quota usage, and inventory source.

Quota

Quota	Description
Instances(Units)	The maximum number of PAM instances that can be created.

Calculation method of quota usage

Quota usage of PAM = Number of PAM instances that are created

> ⓘ **Note**
>
> The quota usage of PAM is calculated based on the number of PAM instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.6.2. KMS

This topic describes the quotas that you can configure for Key Management Service (KMS), calculation method of quota usage, and inventory source.

Quota

Quota	Description
Instances(Units)	The total number of instances that can be created for KMS.

Calculation method of quota usage

KMS quota usage = Number of KMS instances that are created

> ⓘ **Note**
>
> The quota usage of KMS is calculated based on the number of instances of the corresponding resource.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.7. Middleware

6.1.3.1.7.1. ApsaraMQ

This topic describes the quotas that you can configure for ApsaraMQ, the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
Message Queue Instances(Units)	The total number of ApsaraMQ instances that can be created for ApsaraMQ.
Tiangong Message Queue Instances(Units)	The total number of Tiangong ApsaraMQ instances that can be created for ApsaraMQ.

Calculation methods of quota usage

- ApsaraMQ instance quota usage = Number of ApsaraMQ instances that are created
- Tiangong ApsaraMQ instance quota usage = Number of Tiangong ApsaraMQ instances that are created

> **Note**
> The quota usage of ApsaraMQ is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.1.8. Application services

6.1.3.1.8.1. API Gateway

This topic describes the quotas that you can configure for API Gateway, the calculation methods of quota usage, and the inventory source.

Quotas

Quota	Description
API Groups(Units)	The total number of API groups that can be created for API Gateway.
Extensions(Units)	The total number of extensions that can be created for API Gateway.
Applications(Units)	The total number of applications that can be created for API Gateway.

Calculation methods of quota usage

- API group quota usage = Number of API groups that are created
- Extension quota usage = Number of extensions that are created
- Application quota usage = Number of applications that are created

> ⓘ **Note**
>
> The quota usage of API Gateway is calculated based on the number of resource instances.

Inventory source

No inventory is involved. By default, the inventory is unlimited.

6.1.3.2. Manage quotas

The amount of resources on the cloud platform is limited. Therefore, you must limit the amount of resources available for each organization based on the scope of its responsibilities. You can use the quota management feature to create, modify, and clear quotas for cloud services in each organization and each resource set.

Background information

Quota management in the Apsara Uni-manager Management Console involves the following concepts: physical inventory, quota, allocated resources, used resources, and remaining resources.

- Physical inventory: the physical inventory of a specific type of resource that is available for an organization or a resource set. The physical inventory can be used to create resource sets for the current organization or its sub-organizations.
- Quota: the total amount of a specific type of resource available for a cloud service.
- Allocated resources: the amount of a specific type of resource that an organization allocates to its sub-organizations. The resources that each organization receives are allocated by its parent organization.
- Used resources: the amount of a specific type of resource that has been used in an organization or a resource set, including the resources used by the sub-organizations and resource sets of an organization.
- Remaining resources: the amount of a specific type of resource that is available in an organization or a resource set, which equals the result of the physical inventory minus used resources. Resources can be used to create instances only if the amount of required resources is less than the amount of remaining resources.

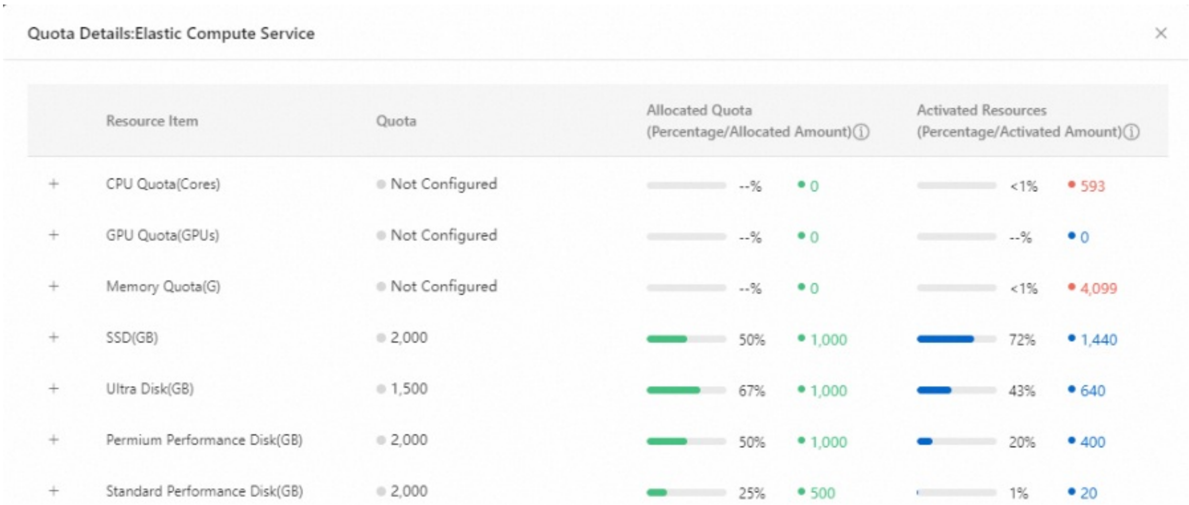
Limits

- Before you configure quotas for an organization, make sure that a platform administrator or the super user has configured a resource pool. For more information, see Configure resource pools.
- You must configure quotas for a parent organization before you can configure quotas for its sub-organizations. You cannot configure quotas for a sub-organization before you configure quotas for its parent organization.

Create or modify quotas

1. Log on to the Apsara Uni-manager Management Console as an operations administrator or an organization administrator of the current organization.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quotas**.
4. In the navigation tree on the **Quotas** page, find an organization or a resource set and click the name of the organization or resource set.

5. Select a region from the region drop-down list above the cloud service list. On the right side of the region drop-down list, select **Only View Cloud Services That Trigger Alerts** to display only the cloud services that trigger alerts.
6. In the cloud service list, click a cloud service. The Quota Details panel appears. In this example, Elastic Compute Service (ECS) is used. For more information about the resource quotas of each cloud service, see Overview.



Quota Details:Elastic Compute Service

	Resource Item	Quota	Allocated Quota (Percentage/Allocated Amount)ⓘ	Activated Resources (Percentage/Activated Amount)ⓘ
+	CPU Quota(Cores)	● Not Configured	--% ● 0	<1% ● 593
+	GPU Quota(GPUs)	● Not Configured	--% ● 0	--% ● 0
+	Memory Quota(G)	● Not Configured	--% ● 0	<1% ● 4,099
+	SSD(GB)	● 2,000	50% ● 1,000	72% ● 1,440
+	Ultra Disk(GB)	● 1,500	67% ● 1,000	43% ● 640
+	Permium Performance Disk(GB)	● 2,000	50% ● 1,000	20% ● 400
+	Standard Performance Disk(GB)	● 2,000	25% ● 500	1% ● 20

7. In the Quota Details panel, click **Create Quotas** or **Modify Quota**. Configure the resource quotas for ECS and click **Save**.

> **Important**
>
> - When you configure the quota of a resource item of a cloud service for an organization, if the organization has a parent organization other than the root organization, the quota of the resource item that you can configure for the organization is calculated based on the following formula: Quota of the resource item that can be configured for the organization = Quota of the resource item for the parent organization - Allocated quota of the resource item.
> - If you do not specify a quota for a resource item, no quota is configured for the resource item by default. The system does not limit the overhead of the corresponding resources in the current organization or resource set. The quotas of the parent organization to which the current organization or resource set belongs are used for verification and calculation.

Create alert rules for quota items

After you configure quotas for cloud resources, click **Create Quota Alert** to create alert rules for cloud resources. For more information about the configuration items of an alert rule, see Create an alert rule for a quota item.

Clear quotas

After you configure quotas for a cloud service, you can clear quotas based on your business requirements.

> **Important**
>
> - After you clear quotas for a cloud service, the system does not limit the corresponding resource quotas in the current organization or resource set. The quotas of the parent organization to which the current organization or resource set belongs are used for verification and calculation.

> - Before you clear quotas for an organization, make sure that all sub-organizations and resource sets of the organization do not have quotas.

1. In the cloud service list, click a cloud service. In the Quota Details panel, click **Clear Quota**.
2. In the **Reset Quota** message, click **OK**.

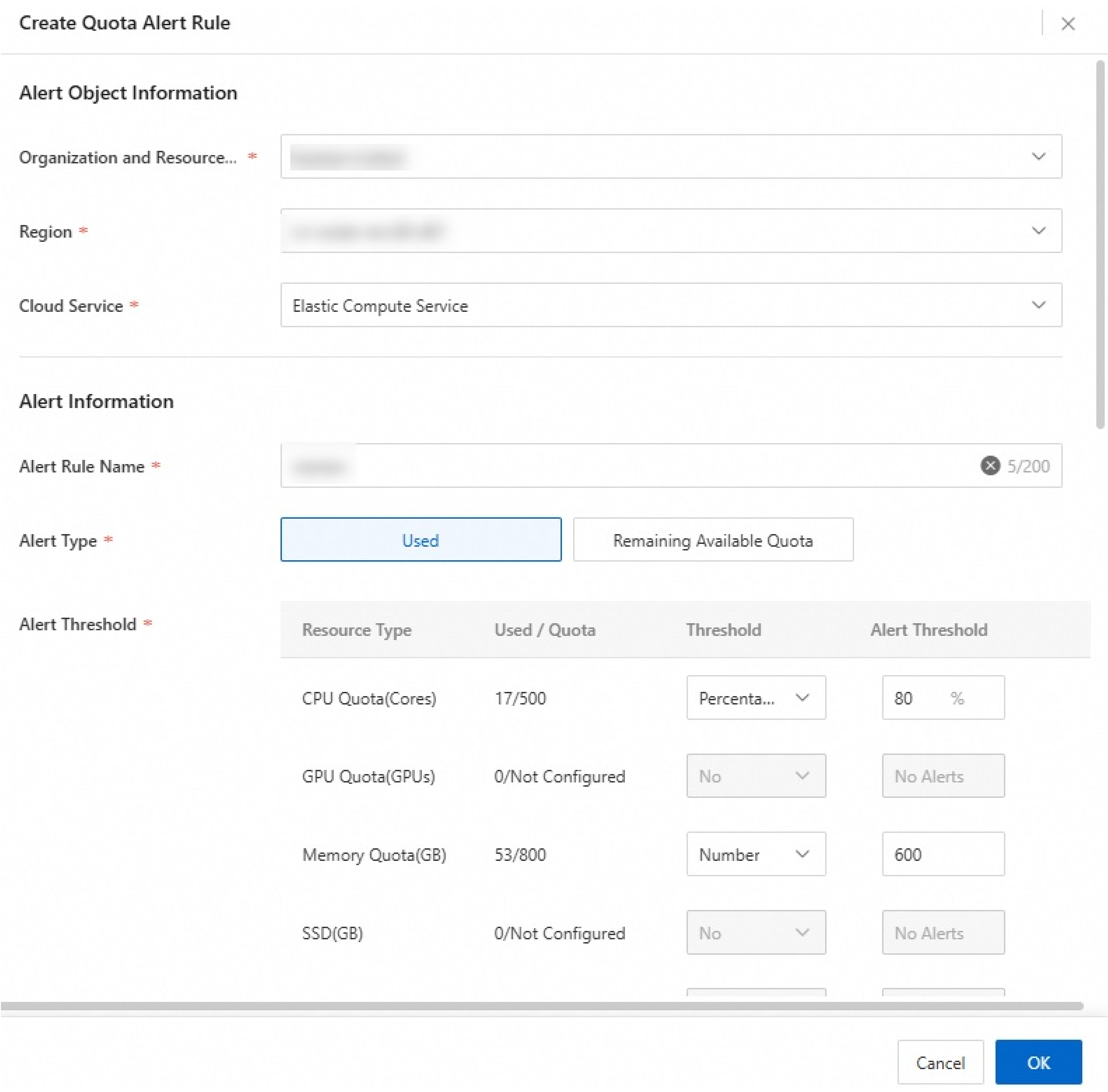
6.1.3.3. Quota alert management

6.1.3.3.1. Create an alert rule for quotas

You can create quota alert rules for cloud services that have quotas in organizations and resource sets. When the usage of a quota reaches the preset threshold, an alert is generated and an alert notification is sent. In this case, you can submit an application to increase the quota in advance.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quota Alerts**.
4. On the **Quota Alerts** page, click **Create Alert Rule**.
5. In the **Create Quota Alert Rule** dialog box, configure the parameters that are described in the following table.



Create Quota Alert Rule

Alert Object Information

Organization and Resource... *: [redacted]

Region *: [redacted]

Cloud Service *: Elastic Compute Service

Alert Information

Alert Rule Name *: [redacted] 5/200

Alert Type *: Used | Remaining Available Quota

Alert Threshold *

Resource Type	Used / Quota	Threshold	Alert Threshold
CPU Quota(Cores)	17/500	Percenta...	80 %
GPU Quota(GPUs)	0/Not Configured	No	No Alerts
Memory Quota(GB)	53/800	Number	600
SSD(GB)	0/Not Configured	No	No Alerts

Section	Parameter	Description
Alert Object Information	Organization /Resource Set	The organization or resource set that contains the quota for which you want to create the alert rule.
	Region	The region in which the quota for which you want to create the alert rule resides.
	Cloud Service	The cloud service for which you want to create the quota alert rule. **Important** Only the cloud services for which quotas are configured in the organization are available.

Alert Information	Alert Rule Name	The name of the quota alert rule. The name can contain letters, digits, hyphens (-), and underscores (_).
	Alert Type	◦ The criteria based on which an alert is generated. Valid values: **Used**: An alert is generated when the quota used by the organization and its sub-organizations exceeds the configured alert threshold. ◦ **Remaining Available Quota**: An alert is generated when the remaining available quota of the organization and its sub-organizations is less than the configured alert threshold.
	Alert Threshold	◦ **Resource Type**: The default value is the value of the Cloud Service Category parameter. ◦ **Used / Quota** or **Remaining Available Quota / Quota**: The default value is the used quota or remaining available quota and the configured quota of the cloud service in the organization and resource set to which the alert object belongs. ◦ **Threshold**: You can set the alert threshold to a percentage value or a numeric value. ◦ **Alert Threshold**: the threshold based on which the alert rule is triggered. If the used quota exceeds the alert threshold or the remaining available quota is less than the alert threshold, an alert is generated.

6. Click **OK**.

6.1.3.3.2. Manage quota alert rules

If the quotas of an organization are changed, you can modify or delete existing quota alert rules. Generated alerts are recorded. Operations staff can analyze the alert history to learn about the resource usage of organizations. This way, they can optimize the quota allocation and create quota alert rules.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quota Alerts**.
4. Optional. Click **Advanced Filter**. Configure the **Alert Rule Name**, **Organization/Resource Set**, **Region**, and **Cloud Service** parameters, and then click **Search**.
5. Perform the operations described in the following table to manage alert rules for quotas.

Operation	Description
View a quota alert rule	Find the alert rule that you want to view and click its name. In the**View Quota Alert Rule** panel, view the configurations of the alert rule.

Modify a quota alert rule	i. Find the alert rule that you want to modify and click**Edit** in the **Actions** column. ii. In the Modify Quota Alert Rule dialog box, modify the**Alert Rule Name**, **Alert Type**, and **Alert Threshold** parameters. iii. Click **OK**.
View the history of an alert rule	i. Find the alert rule whose history you want to view and click**View Alert History** in the **Actions** column. You are redirected to the**Quota Alert History** page. ii. On the **Quota Alert History** page, view the history of the alert rule. **Note** The quota alert history is updated every two hours.
Delete a quota alert rule	i. Find the alert rule that you want to delete and click**Delete** in the **Actions** column. ii. In the **Delete Quota Alert** message, click **OK**.

6.1.3.4. View the quota alert history

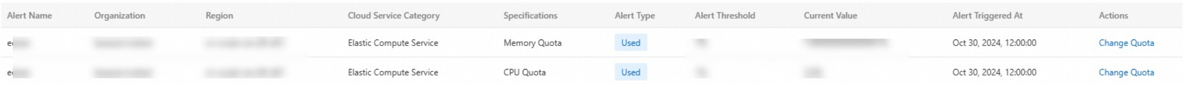
If a quota reaches the specified alert threshold, alerts are generated. You can view the alerts to understand the resource quota usage and identify exceptions at the earliest opportunity.

Prerequisites

A quota alert rule is created. For more information, see Quota alert management.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quota Alert History**.
4. Optional. Click **Advanced Filter**. Configure the **Alert Triggered At**, **Alert Rule Name**, **Organization/Resource Set**, **Region**, and **Cloud Service** parameters, and then click **Search**.
5. In the alert list, view the information about alerts in the following columns: **Alert Rule Name**, **Organization/Resource Set**, **Region**, **Cloud Service**, **Specifications**, **Alert Type**, **Alert Threshold**, **Current Value**, and **Alert Triggered At**.

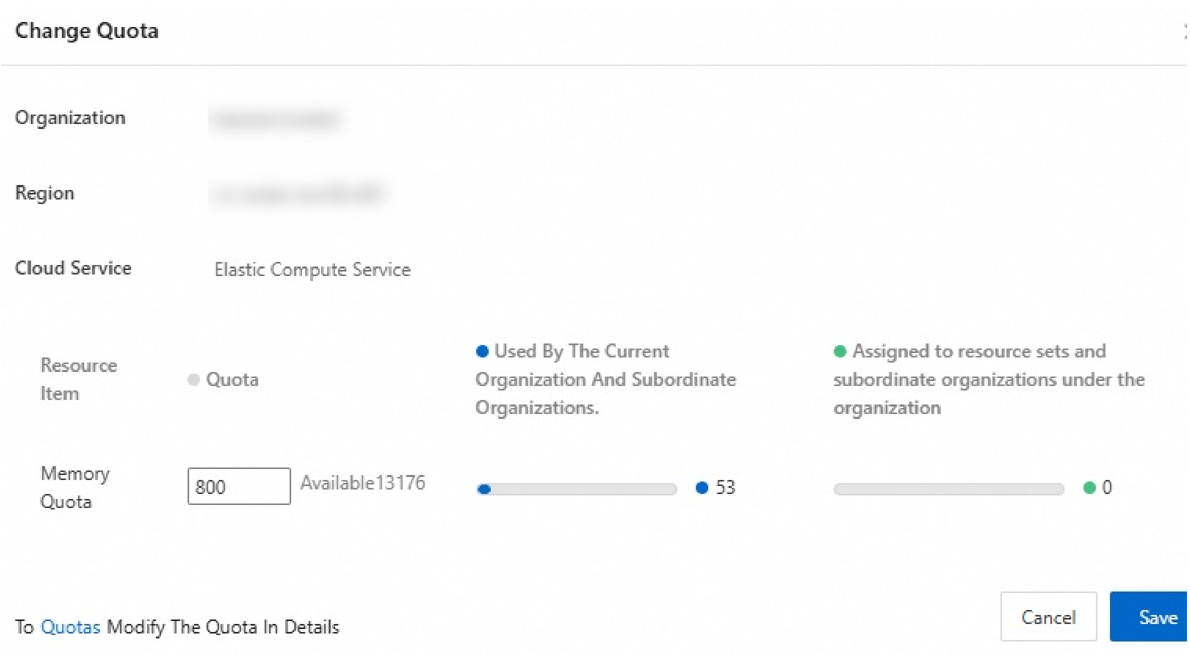


Alert Name	Organization	Region	Cloud Service Category	Specifications	Alert Type	Alert Threshold	Current Value	Alert Triggered At	Actions
e[redacted]	[redacted]	[redacted]	Elastic Compute Service	Memory Quota	Used	[redacted]	[redacted]	Oct 30, 2024, 12:00:00	Change Quota
e[redacted]	[redacted]	[redacted]	Elastic Compute Service	CPU Quota	Used	[redacted]	[redacted]	Oct 30, 2024, 12:00:00	Change Quota

Note

The quota alert history is updated every two hours.

6. Optional. Find an alert that you want to manage and click **Change Quota** in the **Actions** column. In the **Change Quota** dialog box, modify the allocated resource quota.



Change Quota

Organization [redacted]

Region [redacted]

Cloud Service Elastic Compute Service

Resource Item	● Quota		● Used By The Current Organization And Subordinate Organizations.	● Assigned to resource sets and subordinate organizations under the organization
Memory Quota	800	Available13176	● 53	● 0

To Quotas Modify The Quota In Details

6.1.3.5. Configure network specification quotas

You can configure the specification quotas for an instance to restrict the specifications that can be enabled or configured for the instance.

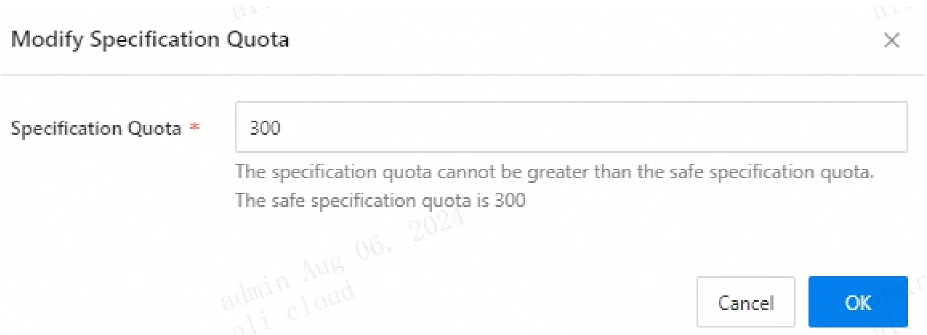
Prerequisites

You have logged on to the Apsara Uni-manager Management Console as an operations administrator.

Procedure

> **Important**
>
> - You can configure network specification quotas only for level-1 organizations.
> - The security quota threshold varies based on the specification and cloud service. The specified specification quota cannot be greater than the security quota threshold.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Network Specification Quota**.
4. Optional. Select an organization, region, cloud service, and specification name to efficiently filter specifications.
5. Find the specification that you want to manage and click **Modify** in the **Operations** column.
6. In the **Modify Specification Quota** dialog box, modify the specification quota and click **OK**.


Modify Specification Quota

Specification Quota * 300

The specification quota cannot be greater than the safe specification quota.
The safe specification quota is 300

6.1.4. Manage tags

Tags are used to classify and manage resources based on different dimensions. You can add tags to cloud resources and manage the resources in a finer-grained and more intelligent manner.

Background information

- Each tag consists of a tag key and a tag value.
  - A tag key is the core identification part of a tag. It is used to define the resource category or describe resource attributes. In most cases, the tag key is a short and descriptive string. Each tag key added to a resource must be unique.
  - A tag value refers to the specific content that is associated with a tag key and provides more detailed data about a resource.
- Administrators can define various types of tags based on business requirements and add multiple tag keys and corresponding tag values to cloud resources. This way, you can classify and retrieve resources based on different dimensions. This helps you quickly find the resources that you require from a large amount of resources and improves the management efficiency of cloud resources.

Limits

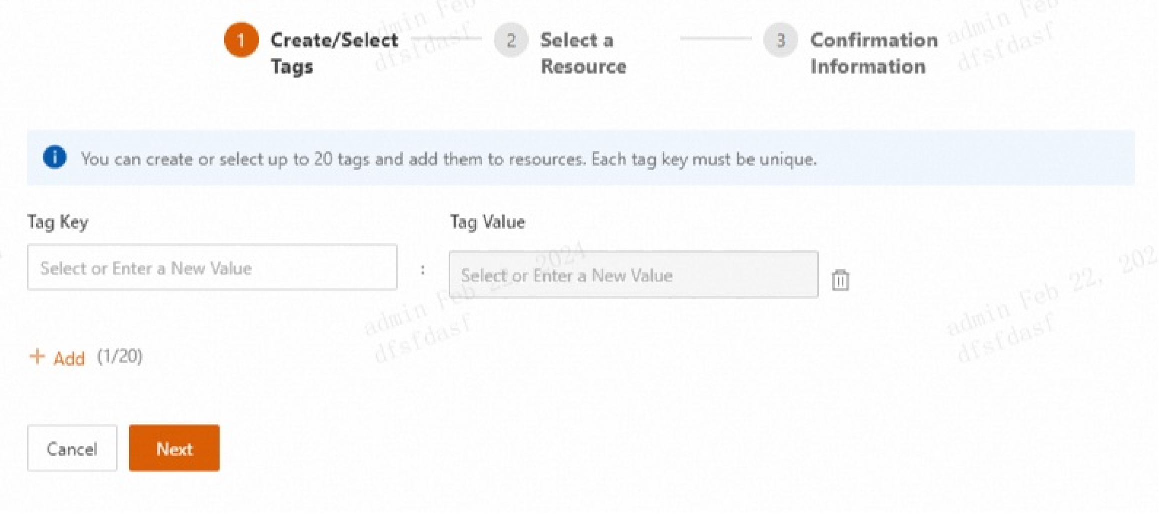
- You can create up to 20 tags at a time and add the tags to resources.
- You can select up to 50 resource instances at a time when you add tags to resources.

Create or select tags and add the tags to resources

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, click **Tags**.
4. On the **Tags** page, click **Create/Select Tags & Add to Resources**.
5. In the **Create/Select Tags & Add to Resources** dialog box, perform the following steps as prompted:

i. Create or select tags.

Select an existing tag key or create a tag key, enter a tag value in the **Tag Value** field, and then click **Next**.



You can create or select up to 20 tags and add them to resources. Each tag key must be unique.

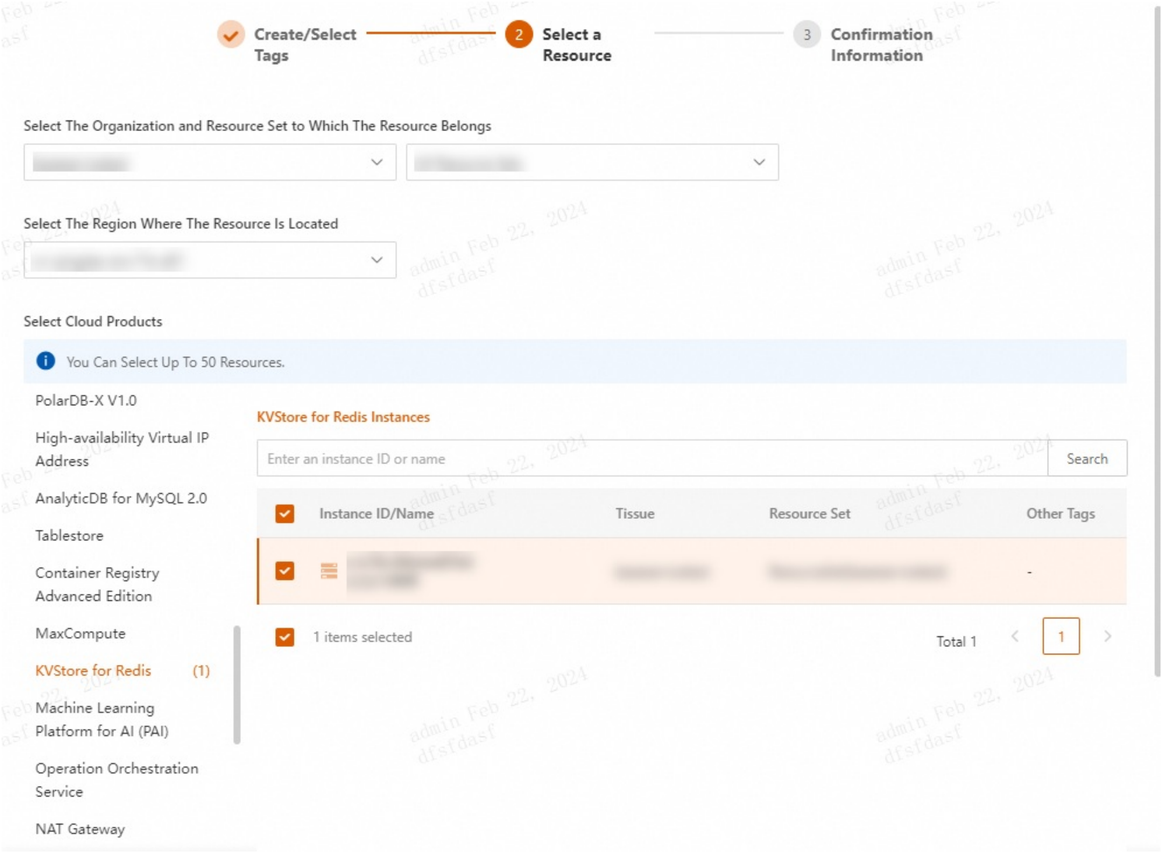
Tag Key: Select or Enter a New Value

Tag Value: Select or Enter a New Value

> **Note**
>
> In the **Create/Select Tags** step, you can create multiple tags at a time.
>
> - Click **Add** to create or select more tags.
> - Click the 🗑 icon to delete a tag.

ii. Select resources.

Select the organization and resource set to which resources belong, select the region in which resources reside, and then select a cloud service. Select the resources to which you want to add tags and click **Next**.



Create/Select Tags
2 Select a Resource
3 Confirmation Information

Select The Organization and Resource Set to Which The Resource Belongs

Select The Region Where The Resource Is Located

Select Cloud Products

You Can Select Up To 50 Resources.

PolarDB-X V1.0
High-availability Virtual IP Address
AnalyticDB for MySQL 2.0
Tablestore
Container Registry Advanced Edition
MaxCompute
KVStore for Redis (1)
Machine Learning Platform for AI (PAI)
Operation Orchestration Service
NAT Gateway

KVStore for Redis Instances

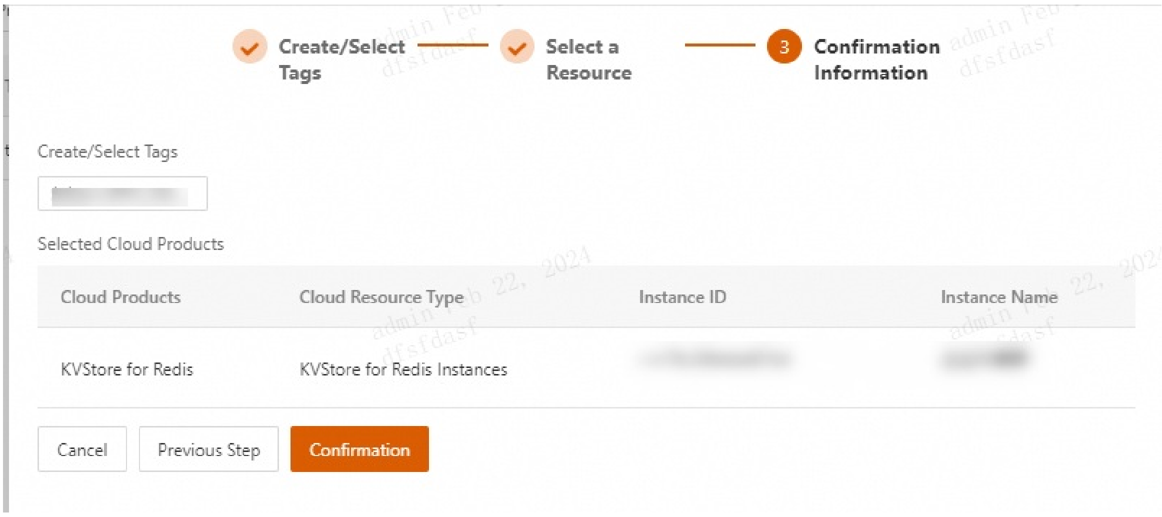
Enter an instance ID or name
Search

☑	Instance ID/Name	Tissue	Resource Set	Other Tags
☑				-

☑ 1 items selected

iii. Confirm the information.

Confirm the information about the tags and resources, and click **Confirmation**.



Create/Select Tags

Selected Cloud Products

Cloud Products	Cloud Resource Type	Instance ID	Instance Name
KVStore for Redis	KVStore for Redis Instances		

View the resources to which tags are added

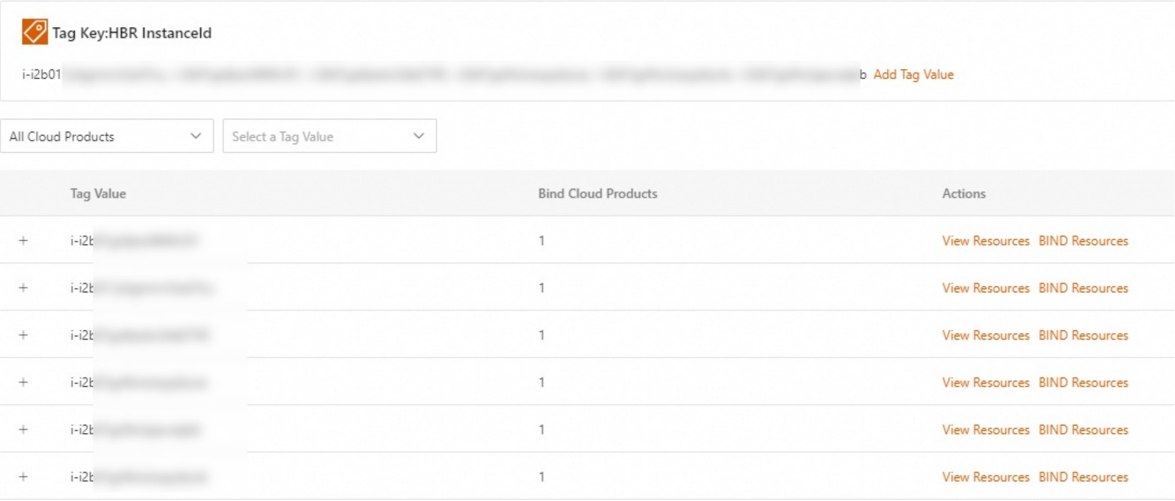
1. In the left-side **Tag Key** pane of the **Tags** page, find the tag key that you want to manage.

You can click the ▽ icon next to **Tag Key** to specify filter conditions, including the **organization** and **resource set** to which resources belong, the **region** in which resources reside, and **keyword**.

> **Note**
>
> - The number next to **Tag Key** indicates the total number of tag keys.
> - In the tag key list, the number next to each tag key indicates the number of tag values that correspond to the tag key.

2. Click a tag key. In the right-side **Tag Key** section, view the tag values that correspond to the tag key and the cloud services to which the tags are added.

> **Note**
>
> - In the right-side Tag Key section, click **Add Tag Value** to add one or more tag values to the tag key.
> - In the tag value list, view the number of cloud services to which each tag is added.



Tag Key:HBR InstanceId

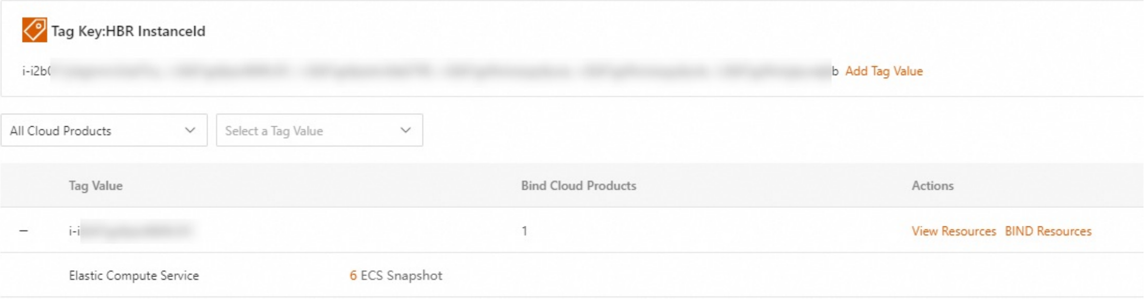
i-i2b01[redacted]b Add Tag Value

All Cloud Products ⌄ Select a Tag Value ⌄

	Tag Value	Bind Cloud Products	Actions
+	i-i2b[redacted]	1	View Resources BIND Resources
+	i-i2b[redacted]	1	View Resources BIND Resources
+	i-i2b[redacted]	1	View Resources BIND Resources
+	i-i2b[redacted]	1	View Resources BIND Resources
+	i-i2b[redacted]	1	View Resources BIND Resources
+	i-i2b[redacted]	1	View Resources BIND Resources

3. View the resources to which a tag is added.

   i. Click the + icon next to a tag value in the **Tag Value** column to view the cloud services to which the tag is added.



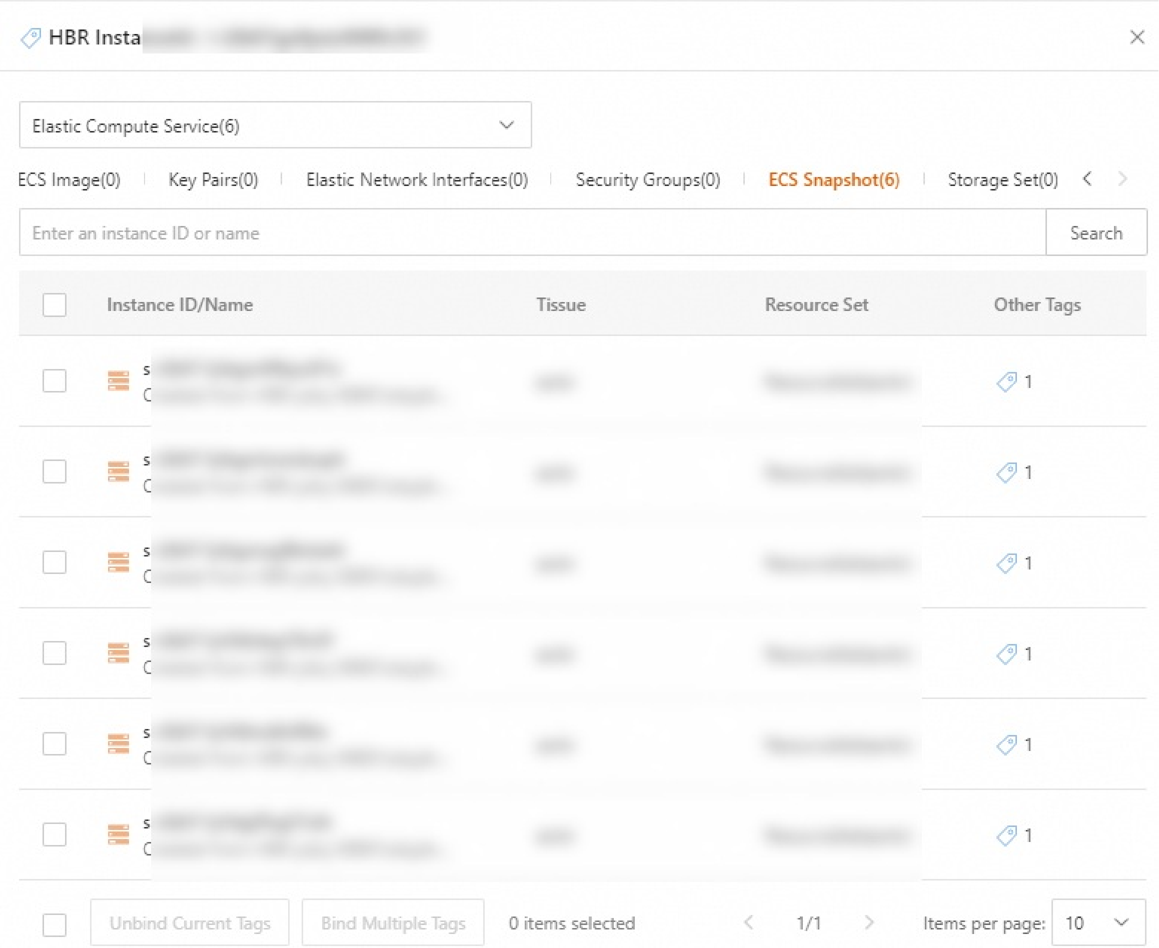
Tag Key:HBR InstanceId

i-i2b[redacted]b Add Tag Value

All Cloud Products ⌄ Select a Tag Value ⌄

	Tag Value		Bind Cloud Products	Actions
−	i-i[redacted]		1	View Resources BIND Resources
	Elastic Compute Service	6 ECS Snapshot		

ii. Click the number next to a displayed cloud service resource type to view the specific resources to which the tag is added. You can also click **View Resources** in the **Actions** column. In the panel that appears, select a specific cloud service to view the specific resources to which the tag is added.



HBR Insta[redacted]

Elastic Compute Service(6)

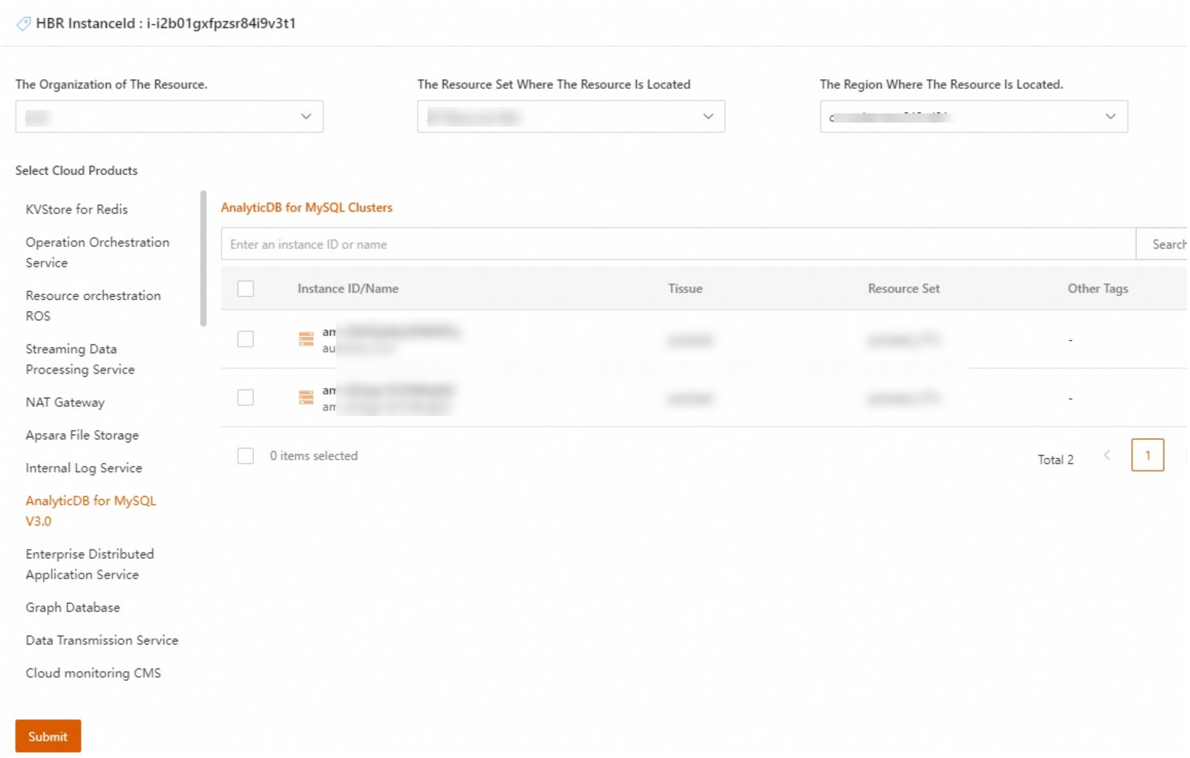
ECS Image(0) | Key Pairs(0) | Elastic Network Interfaces(0) | Security Groups(0) | ECS Snapshot(6) | Storage Set(0)

Enter an instance ID or name | Search

□	Instance ID/Name	Tissue	Resource Set	Other Tags
□	s[redacted] C[redacted]	[redacted]	[redacted]	1
□	s[redacted] C[redacted]	[redacted]	[redacted]	1
□	s[redacted] C[redacted]	[redacted]	[redacted]	1
□	s[redacted] C[redacted]	[redacted]	[redacted]	1
□	s[redacted] C[redacted]	[redacted]	[redacted]	1
□	s[redacted] C[redacted]	[redacted]	[redacted]	1

□ Unbind Current Tags | Bind Multiple Tags | 0 items selected | 1/1 | Items per page: 10

4. Optional. In the tag value list, find a tag value and click **BIND Resources** in the **Actions** column. In the panel that appears, select the resources to which you want to add the tag and click **Submit**.



HBR InstanceId : i-i2b01gxfpzsr84i9v3t1

The Organization of The Resource.

The Resource Set Where The Resource Is Located

The Region Where The Resource Is Located.

Select Cloud Products

- KVStore for Redis
- Operation Orchestration Service
- Resource orchestration ROS
- Streaming Data Processing Service
- NAT Gateway
- Apsara File Storage
- Internal Log Service
- AnalyticDB for MySQL V3.0
- Enterprise Distributed Application Service
- Graph Database
- Data Transmission Service
- Cloud monitoring CMS

AnalyticDB for MySQL Clusters

Enter an instance ID or name | Search

□	Instance ID/Name	Tissue	Resource Set	Other Tags
□	an au			-
□	an an			-

□ 0 items selected

Total 2 < 1

Submit

6.1.5. Manage usage statistics

You can view the resource usage statistics. Information of instances and metering changes are recorded at a granularity of one hour or one second.

Supported cloud services

The following table describes the cloud services or resources whose usage statistics you can view.

Category	Cloud service or resource

Elastic computing	• Container Service for Kubernetes (ACK)
	• Bare-metal Management Service (BMS)
	• Container Registry (ACR)
	  ◦ Image repository
	  ◦ Image repository (Apsara Stack Advanced Edition)
	  ◦ Namespace
	  ◦ Namespace (Apsara Stack Advanced Edition)
	• Elastic Compute Service (ECS)
	  ◦ ECS instance
	  ◦ Elastic Block Storage (EBS)
	  ◦ Dedicated Host (DDH)
	  ◦ ECS snapshot
	• Intelligent Computing LINGJUN node
	• Auto Scaling

Network	• Server Load Balancer (SLB) • Virtual Private Cloud (VPC) ◦ Virtual private cloud (VPC) ◦ Elastic IP address (EIP) ◦ High-availability virtual IP address (HAVIP) ◦ IPv6 gateway ◦ NAT gateway • Express Connect • VPN Gateway • Apsara Stack DNS ◦ Internal domain name of tenants
Database	• ApsaraDB RDS ◦ ApsaraDB RDS for MySQL ◦ PolarDB ◦ ApsaraDB RDS for PostgreSQL ◦ ApsaraDB RDS for SQL Server • PolarDB • ApsaraDB for Redis • ApsaraDB for MongoDB • Data Transmission Service (DTS) • Data Management (DMS) • PolarDB-X 2.0 • PolarDB-X 1.0

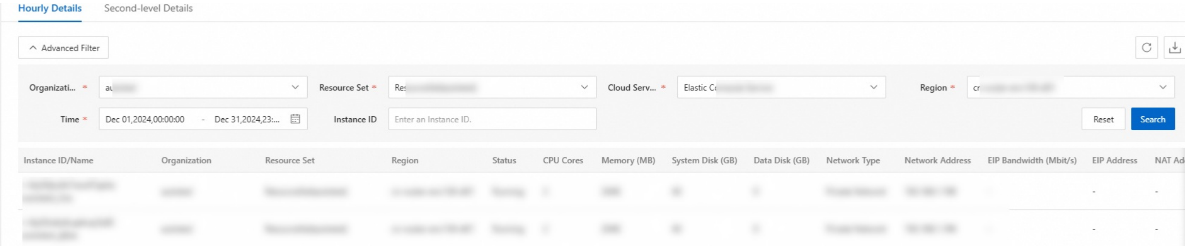
Storage	- File Storage NAS (NAS) - Object Storage Service (OSS) - Tablestore - Simple Log Service (SLS) - Cloud Parallel File Storage (CPFS)
Middleware	- ApsaraMQ - ApsaraMQ for RocketMQ
Big Data	- Realtime Compute for Apache Flink - DataHub - DataWorks - MaxCompute ◦ Project
Application services	- API Gateway
Disaster recovery	- Apsara Stack Resilience for Backup and Recovery (ASR-BR)

Security	• Server Guard • Security Center ◦ Threat Detection Service (TDS) ◦ Security Operations Center (SOC) ◦ Cloud Security Scanner • Bastionhost ◦ Bastionhost (previous version) • Key Management Service (KMS) • Web Application Firewall (WAF) • Network Detection and Response ◦ Traffic security monitoring ◦ Network detection and response

Hourly Details

On the **Hourly Details** tab, you can view the resource usage statistics that are recorded at a granularity of one hour.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, click **Metering Management**.
4. On the **Hourly Details** tab, click **Advanced Filter**. Configure the following filter conditions to query resource usage statistics: **Organization**, **Resource Set**, **Cloud Service**, **Region**, **Time**, and **Instance ID**.



Organizati... * au[redacted]
Resource Set * Res[redacted]
Cloud Serv... * Elastic C[redacted]
Region * cr[redacted]
Time * Dec 01,2024,00:00:00 - Dec 31,2024,23:...
Instance ID Enter an Instance ID.

Instance ID/Name	Organization	Resource Set	Region	Status	CPU Cores	Memory (MB)	System Disk (GB)	Data Disk (GB)	Network Type	Network Address	EIP Bandwidth (Mbit/s)	EIP Address	NAT Ad
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-	-
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-	-

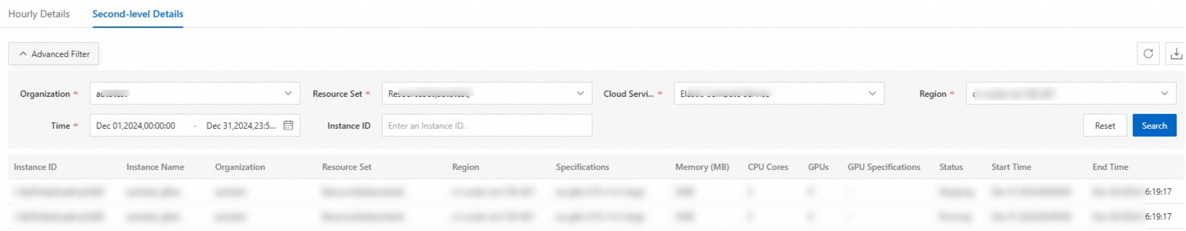
5. Click the ⤓ icon in the upper-right corner to export the usage statistics to your computer as a **.xlsx** file.

> **Note**
>
> You can view or export up to 1,000 entries of usage statistics in the console. If you want to view or export more usage statistics, you can call the MeteringQuery operation.

Second-level Details

On the **Second-level Details** tab, you can view the resource usage statistics that are recorded at a granularity of one second.

1. On the **Second-level Details** tab, click **Advanced Filter**. Configure the following filter conditions to query resource usage statistics: **Organization**, **Resource Set**, **Cloud Service**, **Region**, **Time**, and **Instance ID**.



Organization * a[redacted]

Resource Set * Re[redacted]

Cloud Servi... * El[redacted]

Region * [redacted]

Time * Dec 01,2024,00:00:00 - Dec 31,2024,23:5...

Instance ID Enter an Instance ID.

Instance ID	Instance Name	Organization	Resource Set	Region	Specifications	Memory (MB)	CPU Cores	GPUs	GPU Specifications	Status	Start Time	End Time
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] 6:19:17
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] 6:19:17

2. Click the ⤓ icon in the upper-right corner to export the usage statistics to your computer as a **.xlsx** file.

> **Note**
>
> You can view or export up to 1,000 entries of usage statistics in the console. If you want to view or export more usage statistics, you can call the MeteringQuery operation.

6.1.6. Examples

6.1.6.1. Example: Manage the memory quota of ECS

This topic describes how to manage the memory quota of Elastic Compute Service (ECS).

Prerequisites

- You are an operations administrator or organization administrator.
- Quotas are configured for the parent organization.

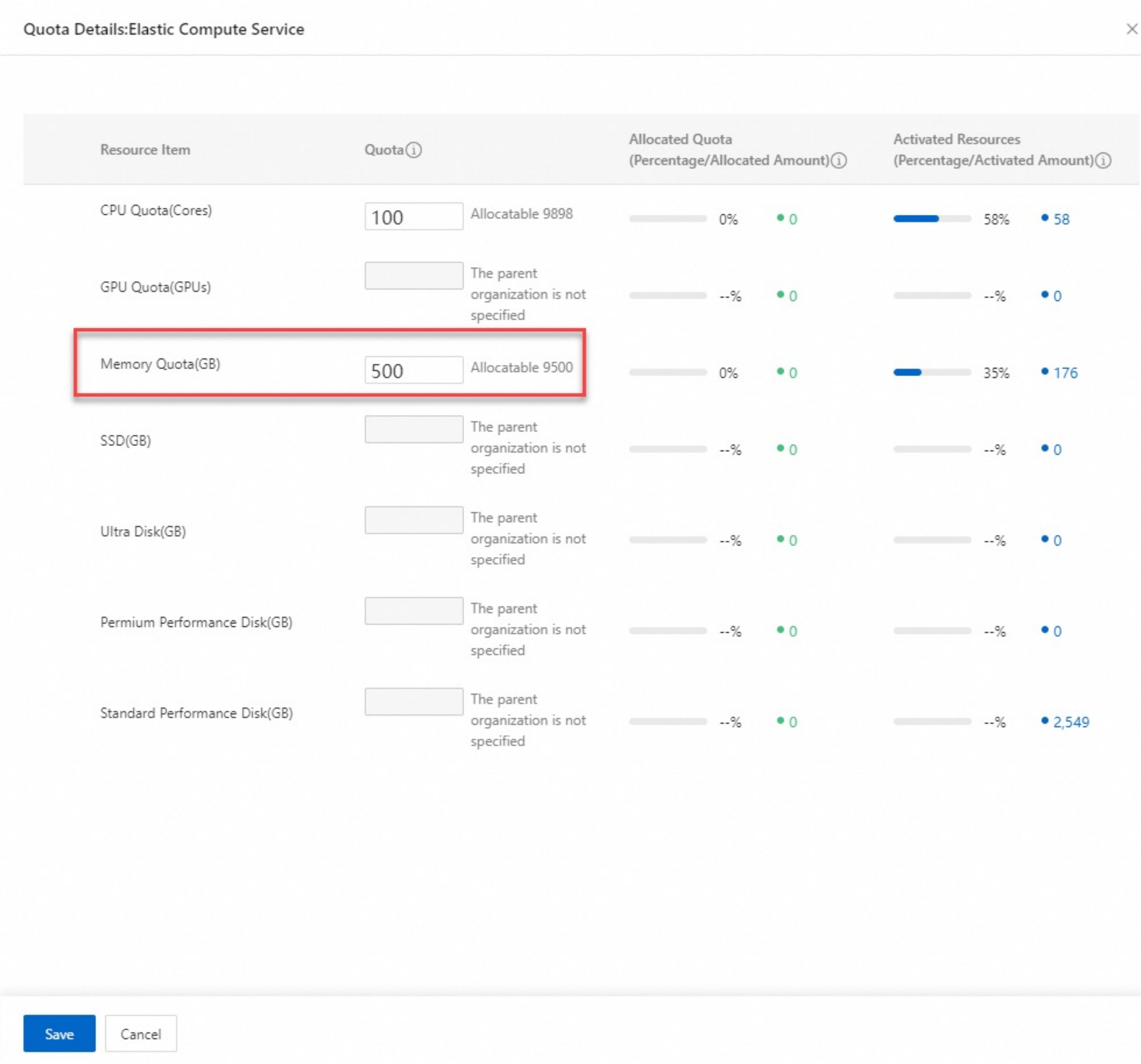
Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the main menu, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quotas**.
4. In the left-side organizational structure of the Quotas page, select the organization or resource set whose resources you want to manage.
5. In the upper-right corner of the page, select a region.
6. Click the **Elastic Compute Service** card to view the quota details.
7. In the **Quota Details** panel, view the resource items, quotas, amount and percentage of allocated quotas, and amount and percentage of activated resources.

Note

- **Quota**: If you do not specify a quota for a resource item, no quota is configured for the resource item. The system does not limit the usage of the corresponding resources.
- **Allocated Quota (Percentage/Allocated Amount)**: displays the quotas that are allocated to each resource item in the specified organization and its sub-organizations. You can view the amount and percentage of allocated quotas.
- **Activated Resources (Percentage/Activated Amount)**: displays the resources that are activated in the specified organization and its sub-organizations. You can view the amount and percentage of the activated resources.

8. In the lower part of the **Quota Details** panel, click **Create Quotas** or **Modify Quota**.
9. In the **Quota** column of the **Memory Quota(GB)** field, enter the quota that you want to set. Example: 500.



Quota Details:Elastic Compute Service

Resource Item	Quota		Allocated Quota (Percentage/Allocated Amount)		Activated Resources (Percentage/Activated Amount)	
CPU Quota(Cores)	100	Allocatable 9898	0%	● 0	58%	● 58
GPU Quota(GPUs)		The parent organization is not specified	--%	● 0	--%	● 0
Memory Quota(GB)	500	Allocatable 9500	0%	● 0	35%	● 176
SSD(GB)		The parent organization is not specified	--%	● 0	--%	● 0
Ultra Disk(GB)		The parent organization is not specified	--%	● 0	--%	● 0
Permium Performance Disk(GB)		The parent organization is not specified	--%	● 0	--%	● 0
Standard Performance Disk(GB)		The parent organization is not specified	--%	● 0	--%	● 2,549

0. Click **Save**.

6.1.6.2. Create an alert rule for the memory quota of ECS

This topic describes how to create an alert rule for the memory quota of Elastic Compute Service (ECS).

Prerequisites

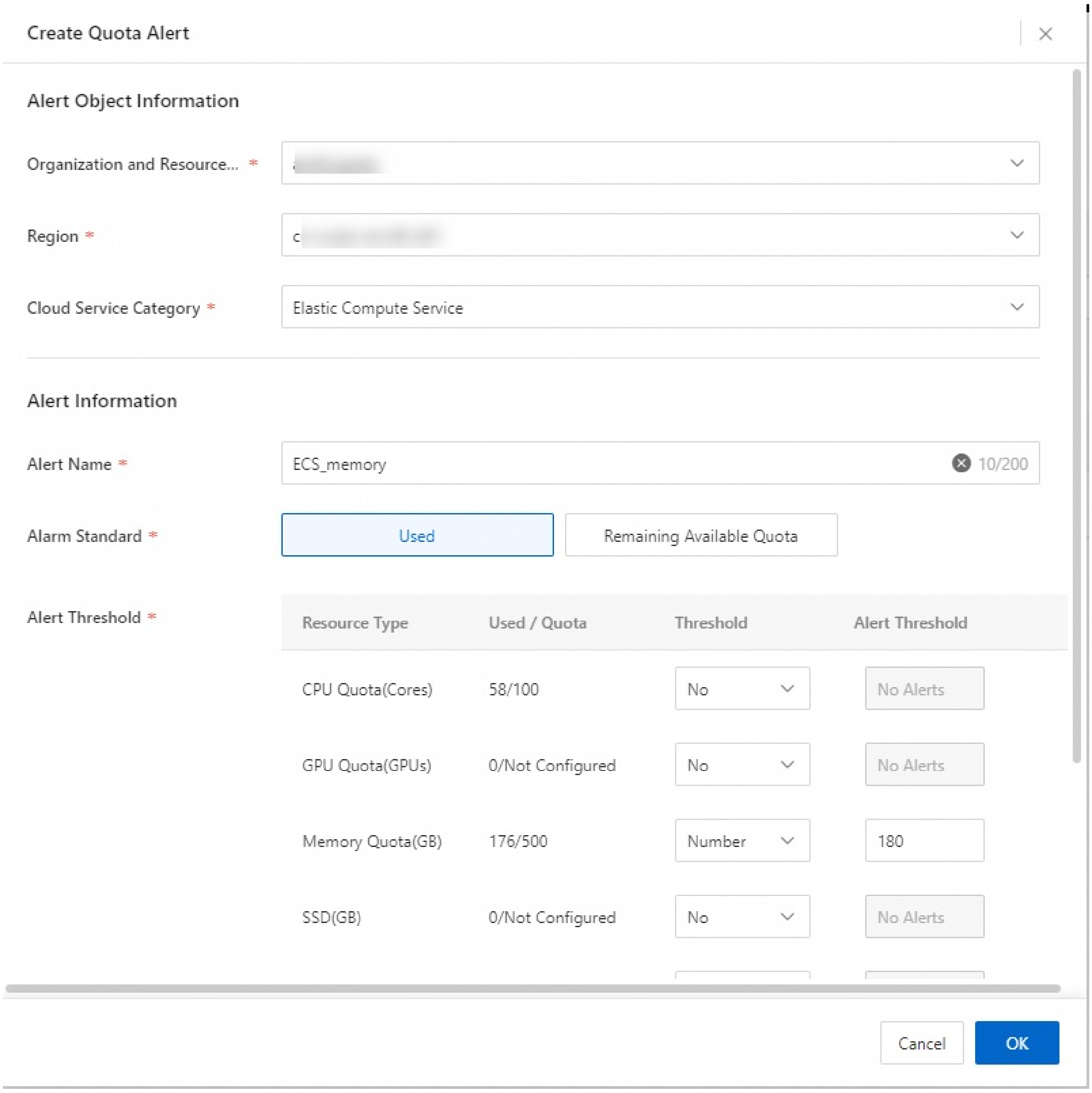
- You are an operations administrator or organization administrator.
- The memory quota of ECS is configured.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the main menu, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Quotas** > **Quota Alerts**.
4. On the Quota Alerts page, click **Create Alert**.
5. In the **Create Quota Alert** dialog box, configure the parameters in the Alert Object Information and Alert Information sections.

   In the Alert Object Information section, select an organization or a resource set and a region. Select **Elastic Compute Service** from the Cloud Service Category drop-down list.

   In the Alert Information section, configure the Alert Name, Alarm Standard, and Alert Threshold parameters. For example, you can set the name of the alert rule to ECS_memory, select Used for the Alarm Standard parameter, select Number from the drop-down list in the Threshold column of the Memory Quota(GB) field, and set the threshold to 180. This way, an alert is triggered when the used memory of ECS exceeds 180 GB in size.



Create Quota Alert

Alert Object Information

Organization and Resource... *	[redacted]
Region *	c[redacted]
Cloud Service Category *	Elastic Compute Service

Alert Information

Alert Name *	ECS_memory 10/200
Alarm Standard *	Used / Remaining Available Quota

Alert Threshold *

Resource Type	Used / Quota	Threshold	Alert Threshold
CPU Quota(Cores)	58/100	No	No Alerts
GPU Quota(GPUs)	0/Not Configured	No	No Alerts
Memory Quota(GB)	176/500	Number	180
SSD(GB)	0/Not Configured	No	No Alerts

6. Click **OK**.

6.1.6.3. Example: Create and publish a process

This topic provides an example on how to create and publish a process.

Prerequisites

You are an operations administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Management**.
4. On the **Process Management** page, click **Create Process**.
5. Configure the basic information and click **Next**.

- **Process Name**: Enter a name for the process. Example: Process for baseservicetest.
- **Process Description**: Enter a description for the process. Example: The process is used for the baseservicetest organization.
- **Applicable Personnel**: Select **All Organizations** or **Select Organization**. Example: Select **Select Organization** and select baseservicetest from the **Select Organization** drop-down list.

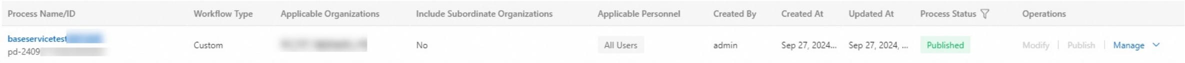
  > **Note**
  >
  > If you turn off **Bind Sub-organization**, the process cannot be associated with the sub-organizations of the selected organization. If you need to associate sub-organizations with the process, turn on **Bind Sub-organization**.

- **Select Initiator**: Select **All Users** or **Specified Role**. Example: Select **All Users**.

6. In the **Process Configuration** step, configure the process nodes, including the start, approver, and end information. After the configuration is complete, click **Submit**.
   - **Start**: Click the **Start** card. In the **Initiator Settings** panel, select or clear **Allow Initiator to Add CC Recipient**. Example: Clear **Allow Initiator to Add CC Recipient**. In this case, the initiator is not allowed to add CC recipients.
   - **Approved By**: Click the ⊕ icon. In the **Approval Node Settings** panel, configure the approval node.
     - **Approved By**: specify the approver type. Example: Set the **Type** parameter to **Specific Personnel** and select **admin(admin)** from the **Specific Personnel** drop-down list.
     - **Approval Method**: Select **Parallel Signature(Requires Approval by One)** or **Sequential Signature(Requires Approval by All)** for **When multiple approvers are specified**. You have specified admin as the approver. Keep the default setting. Select or clear **Allow the approver to specify additional signatories** . Only the current approver can add signatories. Multiple signatories can be specified. Example: Select **Allow the approver to specify additional signatories** . In this case, the admin user is allowed to add signatories.
     - **Add CC Recipient**: You can select CC recipients from the **Specific Personnel** drop-down list. Example: Leave the **Specific Personnel** parameter empty.
   - **End**: Click the **End** card. In the **End Node Settings** panel, you can specify the users who are notified of the end of the process. After the process ends, the approval results are automatically sent to the specified users. Example: Leave the **Specific Personnel** parameter empty.

     > **Note**
     >
     > If you need to notify other users, select the users from the **Specific Personnel** drop-down list. The selected users must be visible to the process creator.

7. After the process is created, view the process in the process list.



Process Name/ID	Workflow Type	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Created By	Created At	Updated At	Process Status	Operations
baseservicetest[redacted] pd-2409[redacted]	Custom	[redacted]	No	All Users	admin	Sep 27, 2024...	Sep 27, 2024, ...	Published	Modify | Publish | Manage

8. Click **Publish** in the **Operations** column of the process. After the process is published, the status of the process changes to **Published**. You can associate a process with a business scenario only when the process is in the **Published** state.

6.1.6.4. Example: Associate a process with management operations

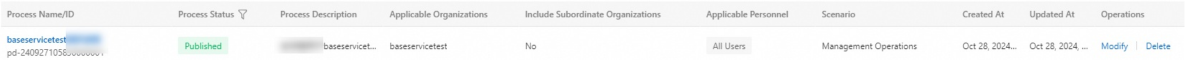
This topic provides an example on how to associate a process with management operations (creating and deleting organizations).

Prerequisites

- A process is created and published. For more information, see Example: Create and publish a process.
- You are an operations administrator.

Procedure

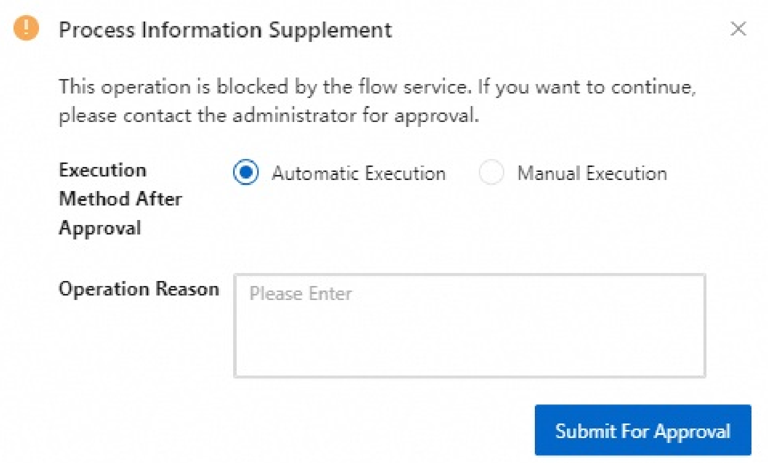
1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Binding**.
4. On the **Process Binding** page, click **Process Binding**.
5. Configure the parameters for process association and click **Submit**.
   - **Process Name**: For example, select the process created and published in Example: Create and publish a process.
   - **Scenario**: For example, select **Management Operations**.
   - **Management Operations**: For example, find and click Organization Management in the left-side pane and then select **Create and delete organizations**.
6. After you submit the process association, the process association is displayed in the process list.



Process Name/ID	Process Status	Process Description	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Scenario	Created At	Updated At	Operations
baseservicetest[redacted] pd-2409271058[redacted]	Published	[redacted]baseservicet...	baseservicetest	No	All Users	Management Operations	Oct 28, 2024...	Oct 28, 2024, ...	Modify | Delete

Impacts

When a user in the baseservicetest organization attempts to create or delete an organization, the operation is reviewed by using the process management feature before the operation can be performed. Before you initiate a process, you must provide supplementary information.



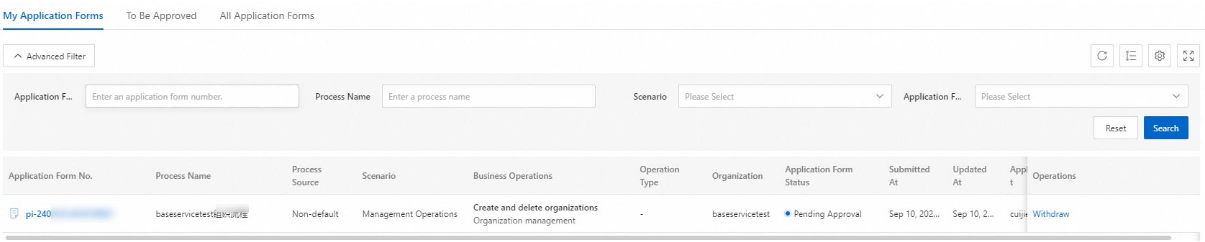
Process Information Supplement

This operation is blocked by the flow service. If you want to continue, please contact the administrator for approval.

Execution Method After Approval: ● Automatic Execution ○ Manual Execution

Operation Reason: Please Enter

After the application is submitted for approval, a process application form is generated. You can create or delete an organization only after the approver approves the application.



Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Submitted At	Updated At	Appl t	Operations
pi-240[redacted]	baseservicetest[redacted]	Non-default	Management Operations	Create and delete organizations Organization management	-	baseservicetest	● Pending Approval	Sep 10, 202...	Sep 10, 2...	cuiji	Withdraw

6.1.6.5. Example: Associate a process with cloud service operations

This topic provides an example on how to associate a process with the operation of modifying virtual private clouds (VPCs).

Prerequisites

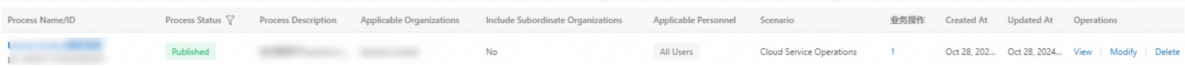
- A process is created and published. For more information, see Example: Create and publish a process.
- You are an operations administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Binding**.
4. On the **Process Binding** page, click **Process Binding**.
5. Configure the parameters for process association and click **Submit**.
   - **Process Name**: For example, select the process created and published in Example: Create and publish a process.
   - **Scenario**: For example, select **Cloud Service Operations**.
   - **Cloud Service Operations**: For example, find and click **VPC** in the left-side pane. In the **Instance** section, select **Modify VPC**.

   > **Note**
   >
   > If an operation is dimmed and cannot be selected, it means that the operation is associated with a process configured by the parent organization.

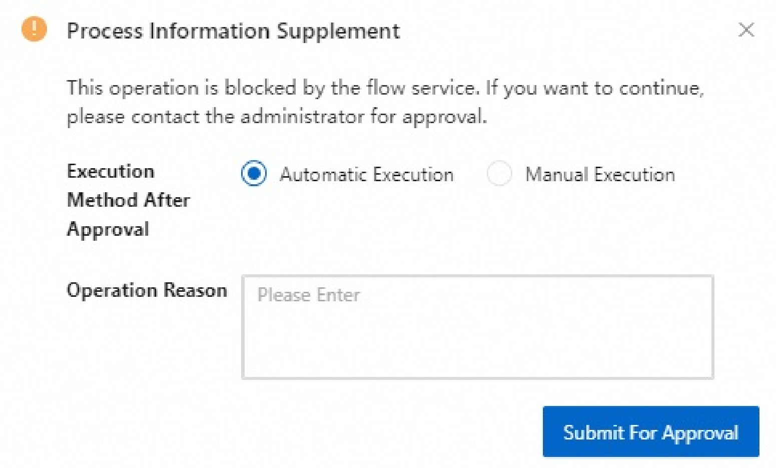
6. After you submit the process association, the process association is displayed in the process list.



Process Name/ID	Process Status	Process Description	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Scenario	业务操作	Created At	Updated At	Operations
[redacted]	Published	[redacted]	[redacted]	No	All Users	Cloud Service Operations	1	Oct 28, 202...	Oct 28, 2024...	View | Modify | Delete

Impacts

When a user in the baseservicetest organization attempts to modify a VPC, the operation is reviewed by using the process management feature before the operation can be performed. Before you initiate a process, you must provide supplementary information.



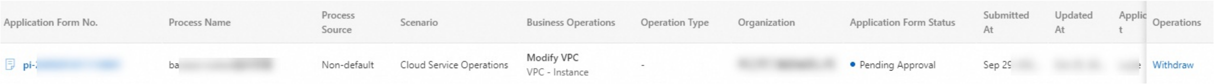
Process Information Supplement

This operation is blocked by the flow service. If you want to continue, please contact the administrator for approval.

Execution Method After Approval: ● Automatic Execution ○ Manual Execution

Operation Reason: Please Enter

After the application is submitted for approval, a process application form is generated. You can modify a VPC only after the approver approves the application.



Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Submitted At	Updated At	Applic t	Operations
pi-[redacted]	ba[redacted]	Non-default	Cloud Service Operations	Modify VPC VPC - Instance	-	[redacted]	● Pending Approval	Sep 29[redacted]	[redacted]	[redacted]	Withdraw

6.1.6.6. Example: Associate a process with service catalogs

This topic provides an example on how to associate a process with service catalogs.

Prerequisites

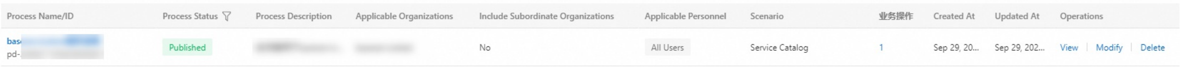
- A process is created and published. For more information, see Example: Create and publish a process.
- You are an operations administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Resource Operations**.
3. In the left-side navigation pane, choose **Process Management** > **Process Binding**.
4. On the **Process Binding** page, click **Process Binding**.
5. Configure the parameters for process association and click **Submit**.
   - **Process Name**: For example, select the process created and published in Example: Create and publish a process.
   - **Scenario**: For example, select **Service Catalog**.
   - **Service Catalog**: For example, select Elastic Compute Service (ECS) and ECS instances. Find the provisioned basic services of ECS instances and select **Create** in the **Operations** column.

   > **Note**
   >
   > If an operation is dimmed and cannot be selected, it means that the operation is associated with a process configured by the parent organization.

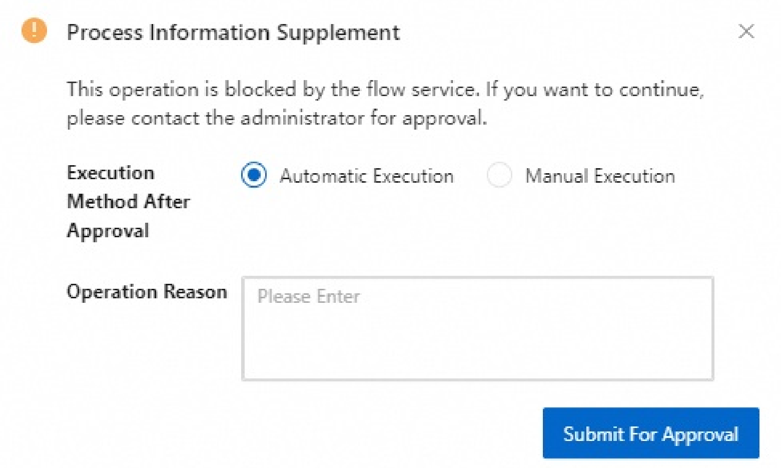
6. After you submit the process association, the process association is displayed in the process list.



Process Name/ID	Process Status	Process Description	Applicable Organizations	Include Subordinate Organizations	Applicable Personnel	Scenario	业务操作	Created At	Updated At	Operations
bas[redacted] pd-[redacted]	Published	[redacted]	[redacted]	No	All Users	Service Catalog	1	Sep 29, 20...	Sep 29, 202...	View | Modify | Delete

Impacts

When a user in the baseservicetest organization attempts to create resources by using the provisioned basic services of ECS instances, the operation is reviewed by using the process management feature before the operation can be performed. Before you initiate a process, you must provide supplementary information.



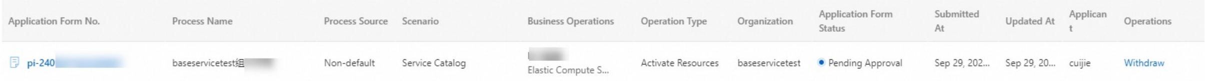
Process Information Supplement

This operation is blocked by the flow service. If you want to continue, please contact the administrator for approval.

Execution Method After Approval: ● Automatic Execution ○ Manual Execution

Operation Reason: Please Enter

After the application is submitted for approval, a process application form is generated. You can create ECS instances only after the approver approves the application.



Application Form No.	Process Name	Process Source	Scenario	Business Operations	Operation Type	Organization	Application Form Status	Submitted At	Updated At	Applicant	Operations
pi-240[redacted]	baseservicetest组[redacted]	Non-default	Service Catalog	[redacted] Elastic Compute S...	Activate Resources	baseservicetest	● Pending Approval	Sep 29, 202...	Sep 29, 20...	cuijie	Withdraw

6.2. Data analysis

6.2.1. Custom analysis

6.2.1.1. Analyze service data

The data analysis feature allows you to analyze data of a specific service including the resource details and resource quotas of the service. You can also export the service data.

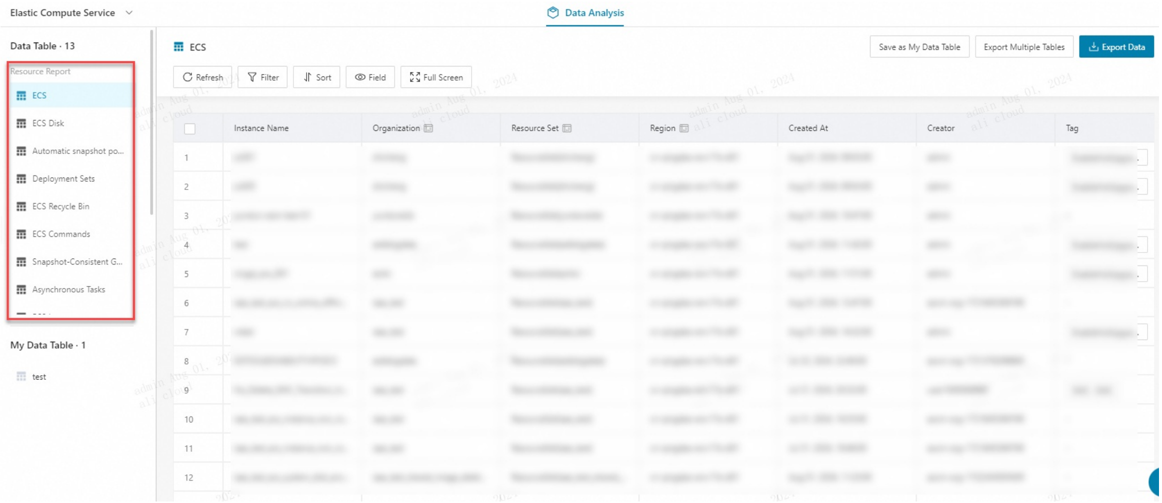
Background information

- You can view the resource reports and quota report of a service on the Product Data Analysis page.
  - Resource Report: displays detailed information about all resources and instances of the cloud service on the platform.
  - Quota Report: displays the resource quota allocation and usage of the cloud service on the platform.
- You can set filter conditions by adding entries to search for and filter data.
- You can save resource and quota reports as custom reports.

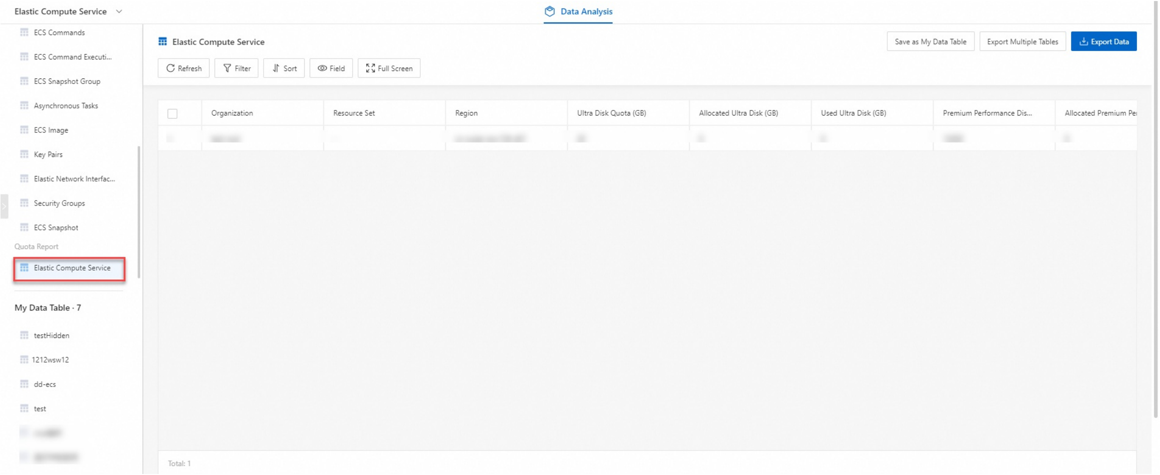
- You can export data as an **.xlsx** file to your computer.

View data tables

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Custom Analysis** > **Product Data Analysis**.
4. Select a cloud service from the drop-down list in the upper-left corner and view the data tables.
   - **View a resource report**: Select a resource type in the **Resource Report** section and view the resource report in the **Data Analysis** section.



   - **View a quota report**: Select a resource type in the **Quota Report** section and view the quota report in the **Data Analysis** section.



5. Optional. Click **Refresh** above the table to update the data in the table.
6. Optional. Click **Filter** above the table and set filter conditions by adding entries to find the data that you require.

> **Note**
>
> - If you filter reports by organization, you can select whether to filter reports in the specified organization and its sub-organizations or filter reports only in the specified organization.
> - If you filter reports by resource sets, you can select multiple resource sets.
> - You can also click Export Data to export data that meets the specified filter conditions. The fields vary based on the service. When you export reports of multiple cloud services at a time, only the following filter conditions are used: organization, resource set, region, creation time, and tag. Other fields are cleared.

7. Optional. Click **Sort** above the table, and set a sorting condition by adding an entry to sort data in ascending or descending order. You can set only one sorting condition at a time.
8. Optional. Click **Field** above the table and select or clear fields to display or hide fields and data.

> **Note**
>
> You can also click Export Data to export the data of the displayed fields.

9. Optional. Click **Full Screen** above the table to enable the full-screen mode.

Customize a chart

1. Move the pointer over the **Organization**, **Resource Set**, or **Region** column.
2. Click the ⌄ icon and select a scenario to customize the corresponding chart.
3. Click **Data Configuration** and configure data on the right side of the page based on your business requirements.

Parameter	Description
X Axis	The field that you want to display on the X axis. You can drag only one field from the Field Details section.
Y Axis	The field that you want to display on the Y axis. You can drag only one field from the Field Details section.
Data Filtering	The field that you want to use to filter data. You can drag multiple fields from the Field Details section.
Filter Chart Fields	The field that you want to display in the chart. You can drag multiple fields from the Field Details section.

4. Click the 📊 or ▭ icon to display data in a chart or table.

> **Note**
>
> After you click the 📊 icon to display data in a chart, you can click the 📊 or ◔ icon to display data in a column chart or pie chart.

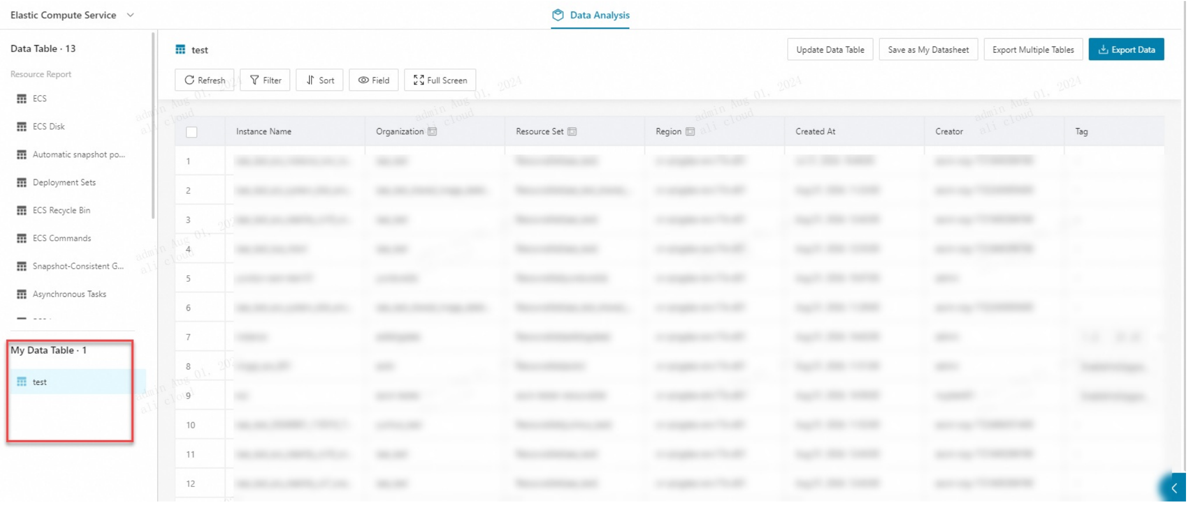
5. View the custom chart based on the data configuration and the selected display type.

> **Note**
>
> - Click **Refresh** to update the data.
> - Click **Full Screen** to enable the full-screen mode.
> - Click the 📷 icon in the upper-right corner of the graph section to capture a snapshot of the chart and save it to your computer in the PNG format.

Save data as a table

1. Click **Save as My Data Table** above the table.
2. In the dialog box that appears, enter a new name in the **New Name** field and click **OK**.
3. View the data table in the left-side **My Data Table** section.

> **Note**
>
> - Move the pointer over the name of the custom data table and click the 🗑 icon to delete the custom data table.
> - Click the name of a custom data table. In the Data Analysis section, you can specify the filter conditions, sorting condition, and fields to find the data that you require. You can also click **Update Data Table** to update the data table.



Export multiple tables

1. Click **Export Multiple Tables** above the table.
2. In the Export Multiple Tables dialog box, configure the **Task Name**, **Report Type**, and **Report** parameters.

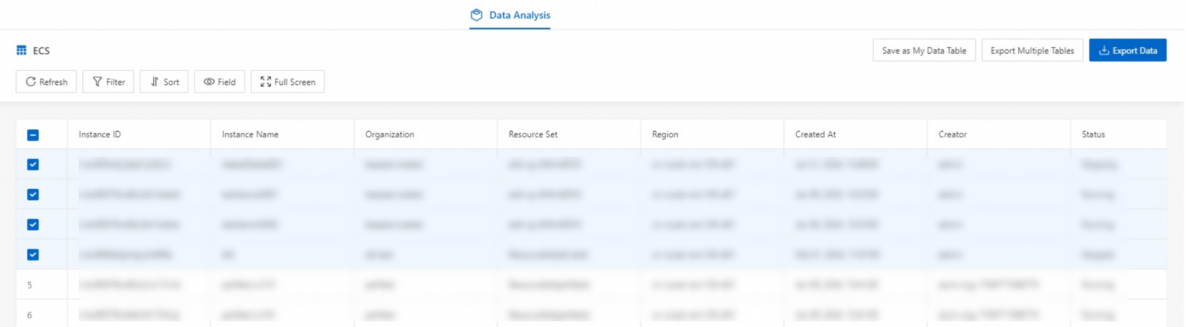
> **Note**
>
> - When you export multiple tables, a report download task is created. The fields vary based on the service. When you export reports of multiple cloud services at a time, only the following filter conditions are used: organization, resource set, region, creation time, and tag. Other fields are cleared.
> - After the report export task is created, you can go to the **Download Report** page to view the report export task.

3. Click **OK**.

Export data

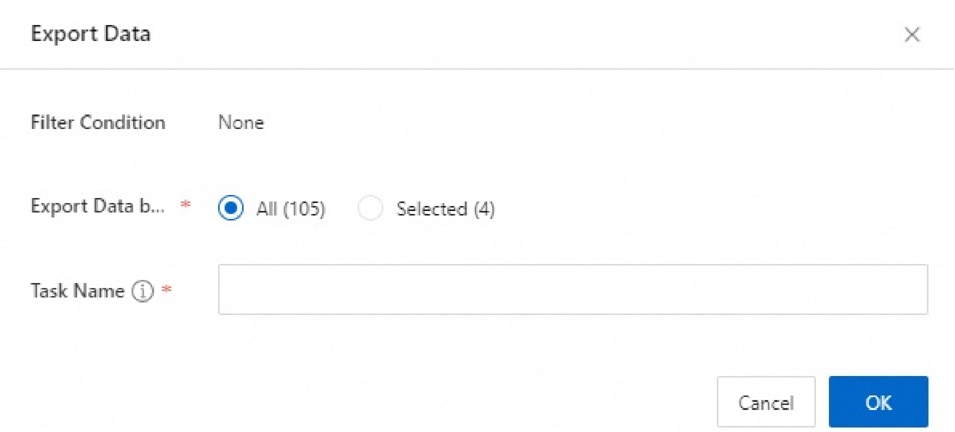
Export selected data

1. In the **Data Analysis** section, select the data that you want to export and click **Export Data**.



2. In the **Export Data** dialog box, configure the **Export Data by Scope** and **Task Name** parameters and click **OK**.

> **Note**
>
> - You can set the Export Data by Scope parameter to **All** or **Selected** based on your business requirements.
> - The data is exported as an **.xlsx** file to your computer.



Export Data

Filter Condition None

Export Data b... * ● All (105) ○ Selected (4)

Task Name ⓘ *

Export all data

1. In the **Data Analysis** section, click **Export Data**. By default, all data is exported.

2. In the **Export Data** dialog box, configure the **Task Name** parameter and click **OK**.

> **Note**
>
> - By default, the **Export Data by Scope** parameter is set to **All**.
> - After the report export task is created, you can go to the **Download Report** page to view the report export task.

6.2.1.2. Analyze organizational data

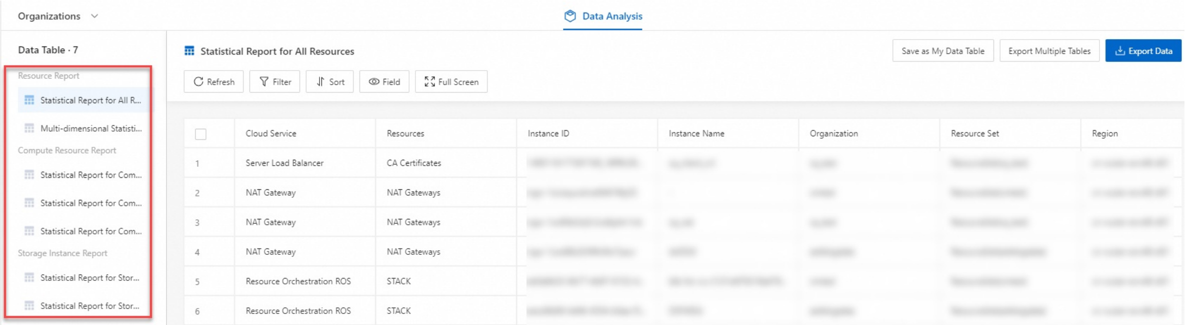
The organizational data analysis feature allows you to analyze data of a specific organization or resource set. The data includes the resource details, resource usage, and resource quotas. You can also export the organizational data.

Background information

- You can view the resource reports, computing resource reports, and storage reports on the Organization Data Analysis page.
  - Resource reports: include full resource reports and multi-dimensional resource statistical reports.
  - Computing resource reports: include computing instance reports, organization-based computing resource statistical reports, and resource set-based computing resource statistical reports.
  - Storage reports: include organization-based storage resource statistical reports and resource set-based storage resource statistical reports.
- You can set filter conditions by adding entries to search for and filter data.
- You can save data reports as custom reports.
- You can export data as an **.xlsx** file to your computer.

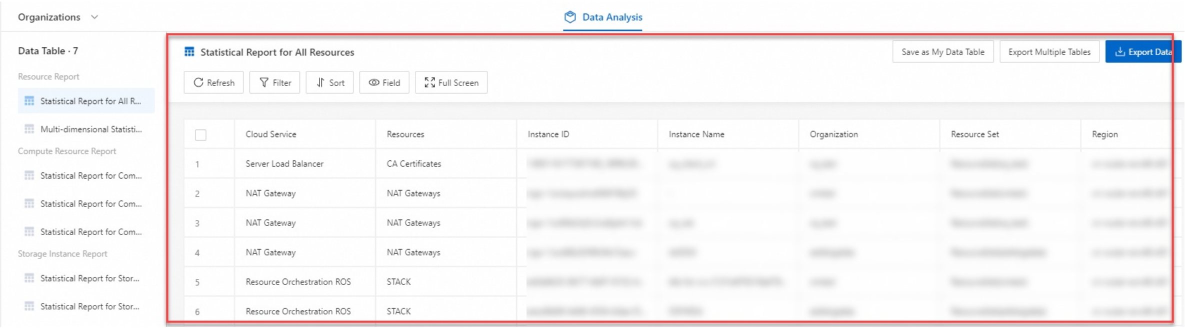
View data reports

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Custom Analysis** > **Organization Data Analysis**.
4. In the **Data Table** section on the left side of the Organization Data Analysis page, select a type of data report that you want to view.


Organizations
Data Analysis
Data Table · 7
Resource Report
Statistical Report for All R...
Multi-dimensional Statisti...
Compute Resource Report
Statistical Report for Com...
Statistical Report for Com...
Statistical Report for Com...
Storage Instance Report
Statistical Report for Stor...
Statistical Report for Stor...
Statistical Report for All Resources
Save as My Data Table
Export Multiple Tables
Export Data
Refresh
Filter
Sort
Field
Full Screen

□	Cloud Service	Resources	Instance ID	Instance Name	Organization	Resource Set	Region
1	Server Load Balancer	CA Certificates	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	NAT Gateway	NAT Gateways	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3	NAT Gateway	NAT Gateways	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4	NAT Gateway	NAT Gateways	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
5	Resource Orchestration ROS	STACK	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6	Resource Orchestration ROS	STACK	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

5. View the report data in the Data Analysis section.



Data Table · 7

Resource Report

- Statistical Report for All R...
- Multi-dimensional Statisti...

Compute Resource Report

- Statistical Report for Com...
- Statistical Report for Com...
- Statistical Report for Com...

Storage Instance Report

- Statistical Report for Stor...
- Statistical Report for Stor...

Statistical Report for All Resources

□	Cloud Service	Resources	Instance ID	Instance Name	Organization	Resource Set	Region
1	Server Load Balancer	CA Certificates	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	NAT Gateway	NAT Gateways	[redacted]	-	[redacted]	[redacted]	[redacted]
3	NAT Gateway	NAT Gateways	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4	NAT Gateway	NAT Gateways	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
5	Resource Orchestration ROS	STACK	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6	Resource Orchestration ROS	STACK	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

6. Optional. Click **Refresh** above the table to update the data in the table.
7. Optional. Click **Filter** above the table and set filter conditions by adding entries to find the data that you require. If you filter data by resource set, you can enter keywords in the search box to search for resource sets.

> **Note**
>
> - If you filter reports by organization, you can select whether to filter reports in the specified organization and its sub-organizations or filter reports only in the specified organization.
> - If you filter reports by resource sets, you can select multiple resource sets.
> - You can also click Export Data to export data that meets the specified filter conditions. The fields vary based on the service. When you export reports of multiple cloud services at a time, only the following filter conditions are used: organization, resource set, region, creation time, and tag. Other fields are cleared.

8. Optional. Click **Sort** above the table, and set a sorting condition by adding an entry to sort data in ascending or descending order. You can set only one sorting condition at a time.
9. Optional. Click **Field** above the table and select or clear fields to display or hide fields and data. You can also click Export Data to export the data of the fields that meet the specified filter conditions.

0. Optional. Click **Full Screen** above the table to enable the full-screen mode.

Save data as a table

1. Click **Save as My Data Table** above the table.
2. In the dialog box that appears, enter a new name in the **New Name** field and click **OK**.
3. View the data table in the left-side **My Data Table** section.

> **Note**
>
> - Move the pointer over the name of the custom data table and click the 🗑 icon to delete the custom data table.
> - Click the name of a custom data table. In the Data Analysis section, you can specify the filter conditions, sorting condition, and fields to find the data that you require. You can also click **Update Data Table** to update the data table.

Export multiple tables

1. Click **Export Multiple Tables** above the table.

2. In the Export Multiple Tables dialog box, configure the **Task Name**, **Report Type**, and **Report** parameters.

   > **Note**
   >
   > - When you export multiple tables, a report download task is created. The fields vary based on the service. When you export reports of multiple cloud services at a time, only the following filter conditions are used: organization, resource set, region, creation time, and tag. Other fields are cleared.
   > - After the report export task is created, you can go to the **Download Report** page to view the report export task.

3. Click **OK**.

Export all data

1. In the **Data Analysis** section, click **Export Data**. By default, all data is exported.
2. In the **Export Data** dialog box, configure the **Task Name** parameter and click **OK**.

   > **Note**
   >
   > - By default, the **Export Data by Scope** parameter is set to **All**.
   > - After the report export task is created, you can go to the **Download Report** page to view the report export task.

6.2.2. Report management

6.2.2.1. Manage push rules of daily operations reports

The Apsara Uni-manager Management Console provides the report subscription feature that allows you to configure push rules of daily operations reports. You can specify the scheduled time to send reports and the desired content of reports. The system automatically generates operations reports and sends them to your email address based on the rules that you configure. This helps you keep track of the resource usage and facilitates monitoring and alerting.

Background information

You can configure up to ten push rules for each of your role. The system generates report files in the .xlsx format based on the content settings that you configure in a rule and sends the report files to your email address based on the scheduled time that you specify. The reports contain enterprise, operations, and cloud service statistics, which can be accessed by the role corresponding to the rule.

Create a push rule of daily operations reports

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Reports** > **Daily Operations Report Delivery**.
4. On the **Daily Operations Report Delivery** page, click **Create Rule**.

Step	Parameter	Description
Basic Settings	**Rule Name**	The name of the rule. The name must be 2 to 64 characters in length and can contain letters, digits, hyphens (-), and underscores (_).
	Rule Description	The description of the rule.
	Report Name	The name of the generated reports, which are attached in the emails sent to your email address.
	Push At	The interval at which a report is generated and sent. Valid values: **Every Day** and **Every Week**.
	Scheduled Time	The point of time at which reports are generated. **Note** If you set the Push At parameter to Every Week, you must configure the **Days** parameter to specify the days of the week on which reports are generated and sent.
Content Settings		In this step, you can specify the following content of the reports: ◦ Enterprise statistics: the numbers of and changes in users, roles, organizations, and resource sets. ◦ Operation statistics: the usage and alerting of quotas. ◦ Cloud service statistics: the changes in the numbers of resources and alerts. **Note** The reports contain only data of the resources that can be accessed by the current role.
Push Preview		In this step, you can preview a demo report. The report is generated based on the content settings that you configure in the previous step.

5. Preview the report and click **Create**. The system sends reports to your email address based on the scheduled time that you specify.

6. Optional. After you create a push rule of daily operations reports, you can manage the rule on the Daily Operations Report Delivery page.

   - Click **Details** in the Actions column to view the details and push history of the rule. You can also modify the report content settings on the rule details page.

> **Note**
>
> - On the rule details page, click **Edit** in the Rule Content section to modify the report content settings.
> - On the rule details page, find the push task that you want to download in the Push History section and click **Download** in the Actions column to save the report pushed by the push task as a **.xlsx** file to your local device.

- Click **Modify Attributes** in the Actions column to modify the configurations of the rule such as rule name, rule description, report name, push cycle, and scheduled time. You can modify the report content settings only on the rule details page.
- Click **Enable** or **Disable** in the Actions column to enable or disable the rule. If the rule is disabled, no push task is triggered.

> **Note**
>
> A disabled rule is still counted as one rule. If the number of rules created for one role reaches 10, you cannot create new rules for the role.

- Move the pointer over the More icon in the Actions column and select **Push History** to view the push tasks that were triggered by the rule. You can also download historical reports.
- Move the pointer over the More icon in the Actions column and select **Delete** to delete the push rule. If the number of existing push rules reaches the upper limit, you can delete the rules that you no longer need.

6.2.2.2. Download reports

The report download feature allows you to download existing resource and quota reports. You can also create download tasks to export reports that contain specified data.

Background information

- Reports are downloaded in the **.xlsx** format. You can find the downloaded reports in the download directory of your browser.
- Reports of the following types are supported: metering report, resource report, quota report, organization report, resource set report, access policy report, user report, user group report, user role report, and detailed billing report.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Reports** > **Download Report**.
4. Optional. Configure the **Report Name**, **Report Type**, **Cloud Service**, **Status**, and **Start And End Time** parameters and click **Search** to filter reports.
5. On the **Download Report** page, perform the operations that are described in the following table.

Operation	Procedure

Create a download task	i. Click **Create Download Task**. ii. In the **Create Download Task** dialog box, configure the following parameters: ▪ **Report Name**: the name of the report. ▪ **Report Type**: the type of the report. **Note** If you set the Report Type parameter to**Organization Report**, **Resource Set Report**, **Access Policy Report**, **User Report**, **User Group Report**, or **User Role Report**, you need to only enter the report name to create a download task. ▪ **Service**: the cloud service whose report you want to download. **Note** You can click **Select All** to select all the listed cloud services. ▪ **Start And End Time**: the time range of the report. **Note** This parameter is displayed only if the Report Type parameter is set to **Metering Report** or **Detailed Billing Report**. ▪ **Organizations and Resource Sets**: the organization and resource set to which the report belongs. ▪ **Region**: the region in which the report resides. ▪ **Account Period**: the accounting period of the report. **Note** This parameter is displayed only if the Report Type parameter is set to **Detailed Billing Report**. ▪ **Sending User**: Select **Send Email After Completion** and select one or more users to whom you want to send the report. iii. Click **OK**.
Download a report	Find a report that you want to download and click**Download Report** in the **Actions** column. **Note** If the report is in the **Failed** or **Canceled** state, click **Retry** to retry the download task. If the state of the report changes to **Completed**, you can click **Download Report** in the Actions column to download the report.

Delete a report	◦ Delete a single report a. Find a report that you want to delete and click**Delete** in the **Actions** column. b. In the **Delete Task** message, click **OK**. ◦ Delete multiple reports at a time a. Select the reports that you want to delete. b. Click **Delete** in the lower-left corner. In the Delete Task message, click **OK**.

6.2.3. Cloud resource optimization

6.2.3.1. Analyze health

The health analysis feature allows you to analyze the health status of cloud resources based on core metrics such as resource usage efficiency and security. This helps you understand the health status of resources, continuously improve overall resource governance, and optimize resource allocation policies.

Background information

- The Apsara Uni-manager Management Console displays health analysis data by organization, resource set, and resource.
  - Health analysis on organizations: collects the health status of all resource sets of each organization. By default, the health status of sub-organizations is not included. You can select Aggregate Sub-organizations to calculate the average health score of an organization and its sub-organizations.
  - Health analysis on resource sets: collects the health status of all resources of each resource set and displays the scoring details of all resources in each resource set.
  - Health analysis on resources: collects the data metrics that are related to the utilization and security of each resource and displays the scoring details of each resource.
- You can view the distribution of health data by the day, week, or month based on your business requirements.

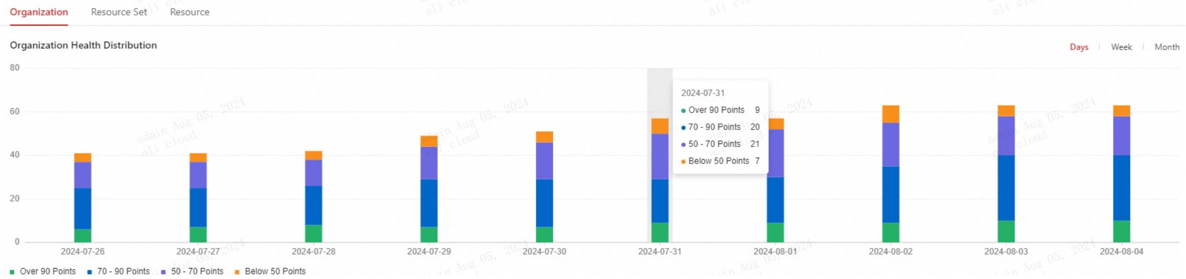
  > **Note**
  >
  > Different colors represent different health scores.
  >
  > - 🟩: excellent, with a health score greater than 90.
  > - 🟦: health, with a health score in the range of 70 to 90.
  > - 🟪: general, with a health score in the range of 50 to 70.
  > - 🟧: poor, with a health score less than 50.

- You can view the health details based on metrics such as the usage rate score and security score. You can also view the algorithm rules, scoring reasons, and optimization suggestions.

View the health analysis data of organizations

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Cloud Resource Optimization** > **Overall Health Score**.
4. On the **Overall Health Score** page, click the **Organization** tab.
5. View the distribution of organizations with different health scores.

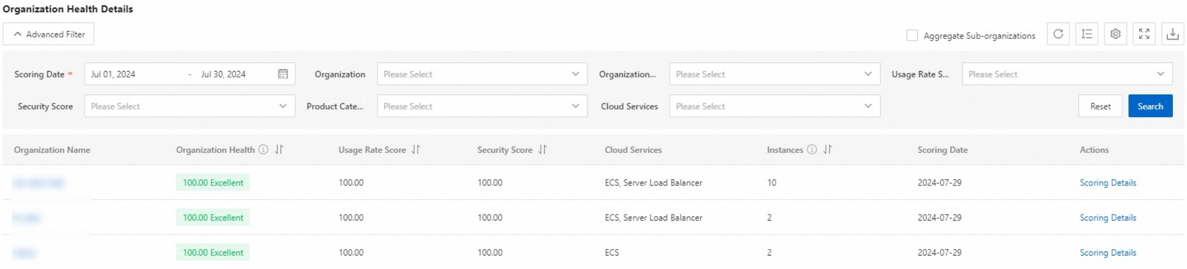
   In the **Organization Health Distribution** section, you can view the distribution of organizations with different health scores by the day, week, or month. You can move the pointer over a column in the chart to view the number of organizations with different health scores.



6. View the health details of organizations.

   In the Organization Health Details section, you can view the details of the health status of organizations. You can configure the **Scoring Date**, **Organization**, **Organization Health**, **Usage Rate Score**, **Security Score**, **Product Categories**, and **Cloud Services** parameters to filter data.

   > **Note**
   >
   > - Select **Aggregate Sub-organizations** to calculate the average health score of an organization and its sub-organizations.
   > - Click the icon to export and save the data to your computer.



Organization Health Details

Advanced Filter

□ Aggregate Sub-organizations

Scoring Date * Jul 01, 2024 - Jul 30, 2024

Organization: Please Select

Organization...: Please Select

Usage Rate S...: Please Select

Security Score: Please Select

Product Cate...: Please Select

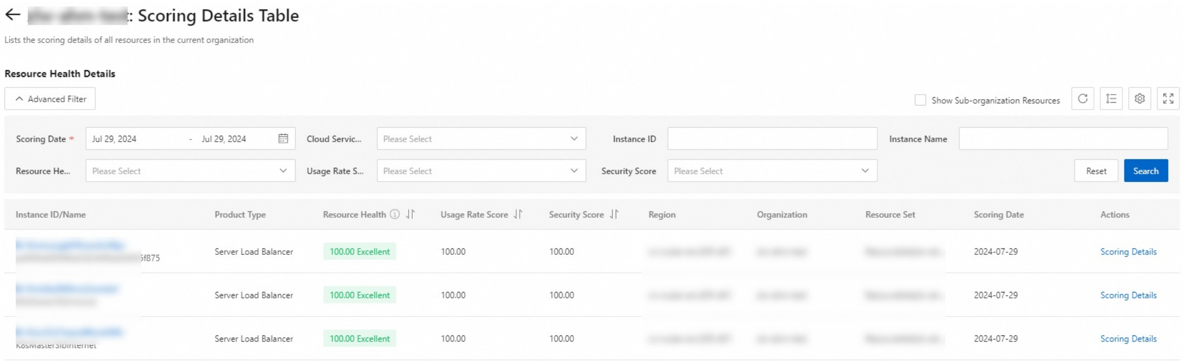
Cloud Services: Please Select

Reset Search

Organization Name	Organization Health	Usage Rate Score	Security Score	Cloud Services	Instances	Scoring Date	Actions
[redacted]	100.00 Excellent	100.00	100.00	ECS, Server Load Balancer	10	2024-07-29	Scoring Details
[redacted]	100.00 Excellent	100.00	100.00	ECS, Server Load Balancer	2	2024-07-29	Scoring Details
[redacted]	100.00 Excellent	100.00	100.00	ECS	2	2024-07-29	Scoring Details

7. Optional. In the Organization Health Details section, find an organization and click **Scoring Details** in the **Actions** column. On the Scoring Details Table page, view the scoring details of all resources in the organization.

   > **Note**
   >
   > Select **Show Sub-organization Resources** in the upper-right corner of the Scoring Details Table page to view the health details of resources in sub-organizations.



[redacted]: Scoring Details Table

Lists the scoring details of all resources in the current organization

Resource Health Details

Advanced Filter

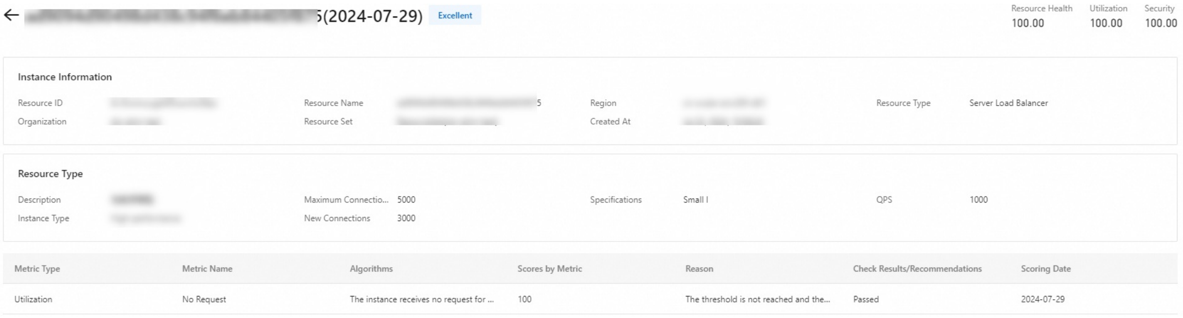
□ Show Sub-organization Resources

Scoring Date * Jul 29, 2024 - Jul 29, 2024 | Cloud Servic... Please Select | Instance ID | Instance Name

Resource He... Please Select | Usage Rate S... Please Select | Security Score Please Select | Reset | Search

Instance ID/Name	Product Type	Resource Health	Usage Rate Score	Security Score	Region	Organization	Resource Set	Scoring Date	Actions
[redacted]5f875	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details
[redacted] KosMasterSlbInternet	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details

8. Optional. On the **Scoring Details Table** page, find the resource whose health details you want to view and click **Scoring Details** in the **Actions** column.



[redacted]5(2024-07-29) Excellent

Resource Health 100.00 | Utilization 100.00 | Security 100.00

Instance Information

Resource ID	[redacted]	Resource Name	[redacted]5	Region	[redacted]	Resource Type	Server Load Balancer
Organization	[redacted]	Resource Set	[redacted]	Created At	[redacted]		

Resource Type

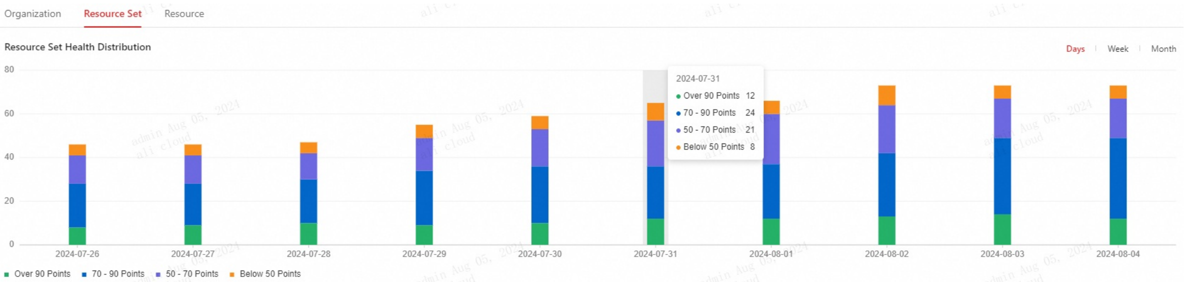
Description	[redacted]	Maximum Connectio...	5000	Specifications	Small I	QPS	1000
Instance Type	[redacted]	New Connections	3000				

Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Utilization	No Request	The instance receives no request for ...	100	The threshold is not reached and the...	Passed	2024-07-29

View the health analysis data of resource sets

1. On the **Overall Health Score** page, click the **Resource Set** tab.
2. View the distribution of resource sets with different health scores.

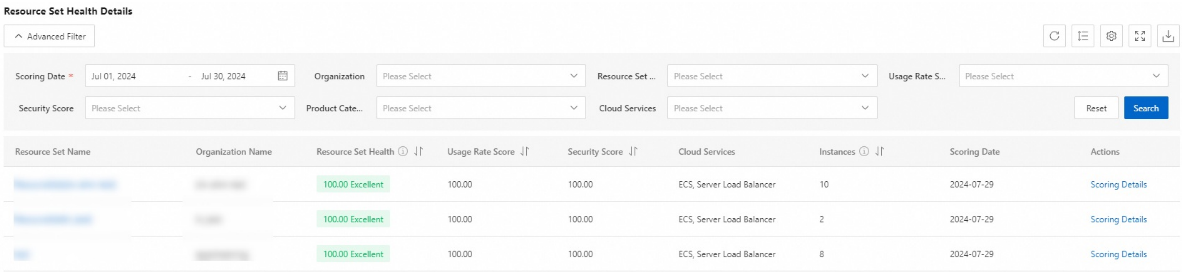
   In the **Resource Set Health Distribution** section, you can view the distribution of resource sets with different health scores by the day, week, or month. You can move the pointer over a column in the chart to view the number of resource sets with different health scores.



3. View the health details of resource sets**.**

   In the Resource Set Health Details section, you can view the details of the health status of resource sets. You can configure the **Scoring Date**, **Organization**, **Resource Set Health**, **Usage Rate Score**, **Security Score**, **Product Categories**, and **Cloud Services** parameters to filter data.

> **Note**
>
> Click the ⤓ icon to export and save the data to your computer.



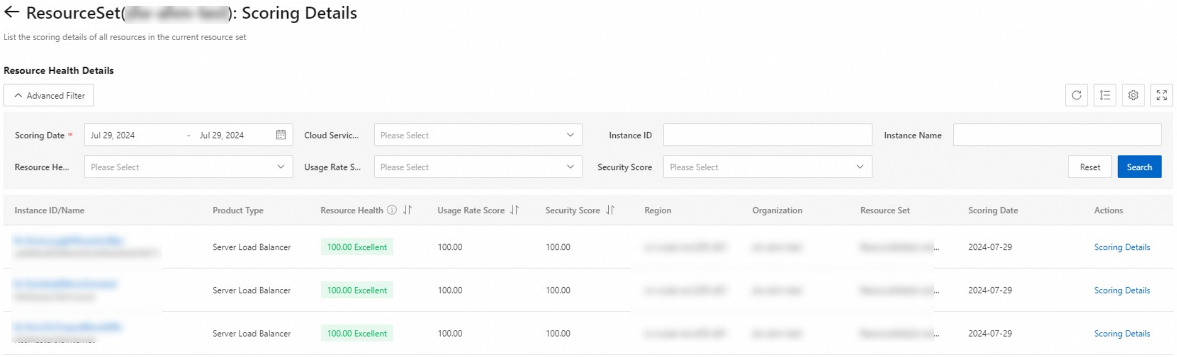
Resource Set Health Details

Advanced Filter

Scoring Date * Jul 01, 2024 - Jul 30, 2024 | Organization Please Select | Resource Set ... Please Select | Usage Rate S... Please Select
Security Score Please Select | Product Cate... Please Select | Cloud Services Please Select | Reset | Search

Resource Set Name	Organization Name	Resource Set Health	Usage Rate Score	Security Score	Cloud Services	Instances	Scoring Date	Actions
[redacted]	[redacted]	100.00 Excellent	100.00	100.00	ECS, Server Load Balancer	10	2024-07-29	Scoring Details
[redacted]	[redacted]	100.00 Excellent	100.00	100.00	ECS, Server Load Balancer	2	2024-07-29	Scoring Details
[redacted]	[redacted]	100.00 Excellent	100.00	100.00	ECS, Server Load Balancer	8	2024-07-29	Scoring Details

4. Optional. In the Resource Set Health Details section, find a resource set and click **Scoring Details** in the **Actions** column. On the Scoring Details page, view the scoring details of all resources in the resource set.



ResourceSet([redacted]): Scoring Details

List the scoring details of all resources in the current resource set

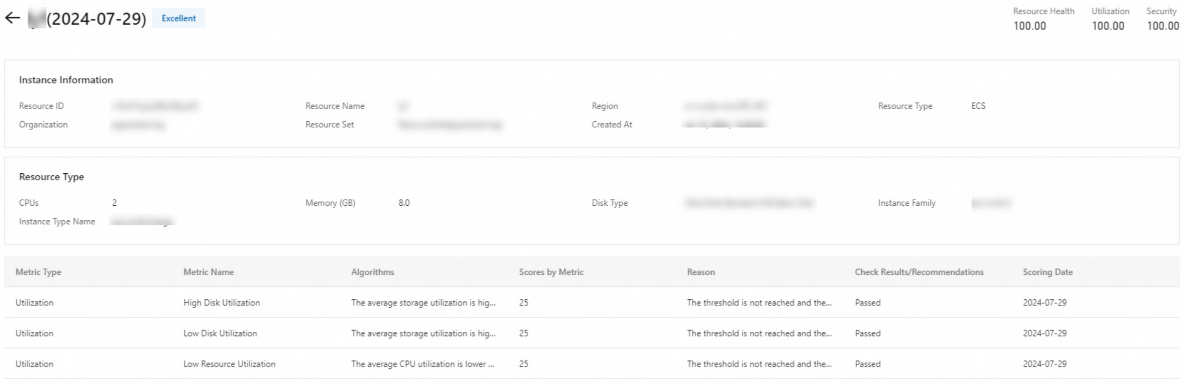
Resource Health Details

Advanced Filter

Scoring Date * Jul 29, 2024 - Jul 29, 2024 | Cloud Servic... Please Select | Instance ID | Instance Name
Resource He... Please Select | Usage Rate S... Please Select | Security Score Please Select | Reset | Search

Instance ID/Name	Product Type	Resource Health	Usage Rate Score	Security Score	Region	Organization	Resource Set	Scoring Date	Actions
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]	2024-07-29	Scoring Details

5. Optional. On the **Scoring Details** page, find the resource whose health details you want to view and click **Scoring Details** in the **Actions** column.



[redacted](2024-07-29) Excellent

Resource Health 100.00 | Utilization 100.00 | Security 100.00

Instance Information

Resource ID [redacted] | Resource Name [redacted] | Region [redacted] | Resource Type ECS
Organization [redacted] | Resource Set [redacted] | Created At [redacted]

Resource Type

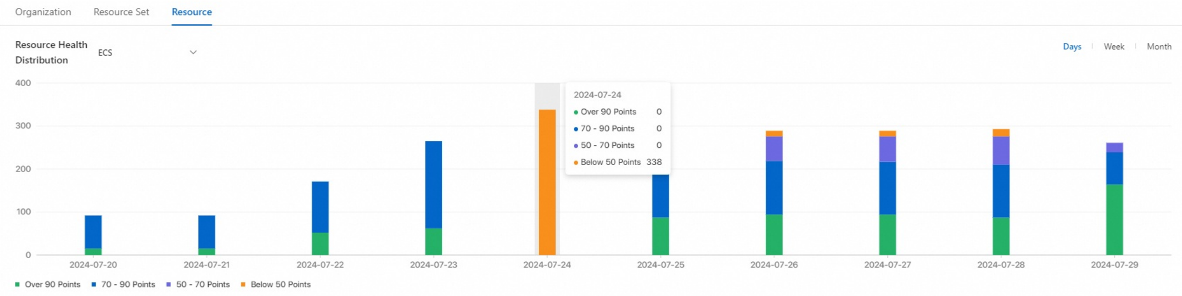
CPUs 2 | Memory (GB) 8.0 | Disk Type [redacted] | Instance Family [redacted]
Instance Type Name [redacted]

Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Utilization	High Disk Utilization	The average storage utilization is hig...	25	The threshold is not reached and the...	Passed	2024-07-29
Utilization	Low Disk Utilization	The average storage utilization is hig...	25	The threshold is not reached and the...	Passed	2024-07-29
Utilization	Low Resource Utilization	The average CPU utilization is lower ...	25	The threshold is not reached and the...	Passed	2024-07-29

View the health analysis data of resources

1. On the **Overall Health Score** page, click the **Resource** tab.
2. View the distribution of resources with different health scores.

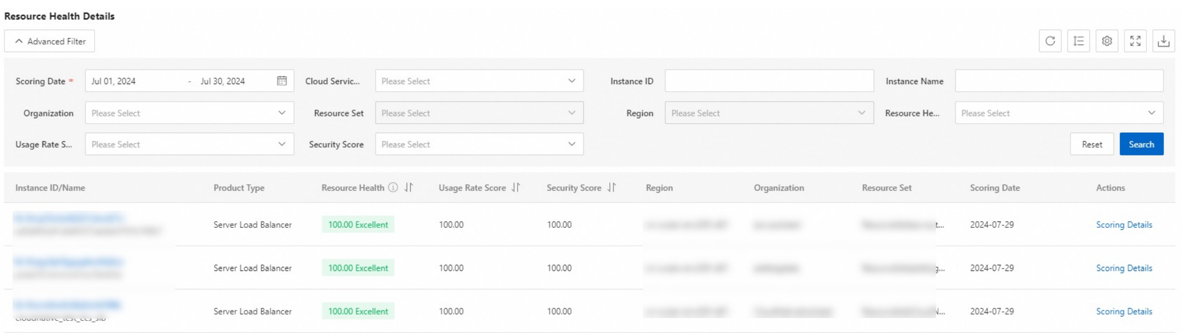
   In the **Resource Health Distribution** section, you can view the distribution of resources with different health scores by the day, week, or month. You can move the pointer over a column in the chart to view the number of resources with different health scores.



3. View the health details of resources.

   In the Resource Health Details section, you can view the details of the health status of resources. You can configure the **Scoring Date**, **Cloud Service Type**, **Instance ID**, **Instance Name**, **Organization**, **Resource Set**, **Region**, **Resource Health**, **Usage Rate Score**, and **Security Score** parameters to filter data.

   > **Note**
   >
   > Click the icon to export and save the data to your computer.

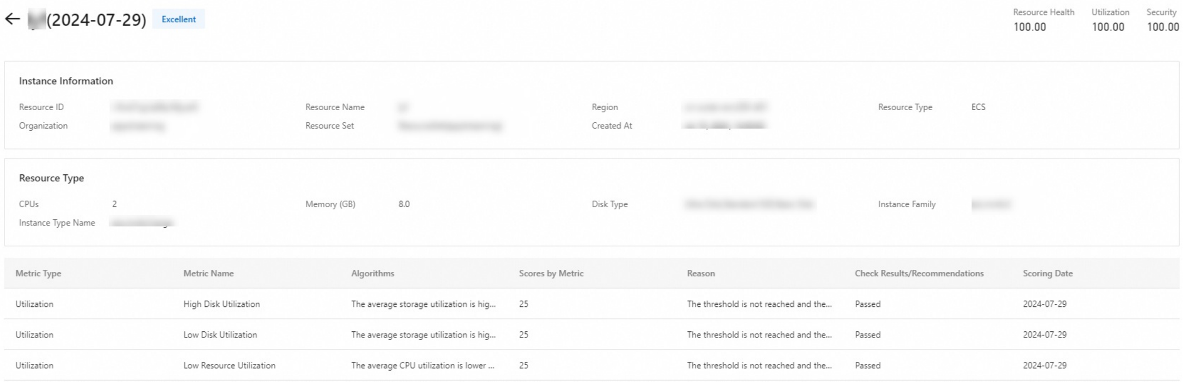


Resource Health Details

Scoring Date *: Jul 01, 2024 - Jul 30, 2024
Cloud Servic...: Please Select
Instance ID:
Instance Name:
Organization: Please Select
Resource Set: Please Select
Region: Please Select
Resource He...: Please Select
Usage Rate S...: Please Select
Security Score: Please Select

Instance ID/Name	Product Type	Resource Health	Usage Rate Score	Security Score	Region	Organization	Resource Set	Scoring Date	Actions
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]t...	2024-07-29	Scoring Details
[redacted]	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]g...	2024-07-29	Scoring Details
[redacted] cloudnative_test_ces_slb	Server Load Balancer	100.00 Excellent	100.00	100.00	[redacted]	[redacted]	[redacted]N...	2024-07-29	Scoring Details

4. In the Resource Health Details section, find the resource whose health details you want to view and click **Scoring Details** in the **Actions** column. On the page that appears, view the scoring details of the resource.



[redacted](2024-07-29) Excellent

Resource Health 100.00
Utilization 100.00
Security 100.00

Instance Information

Resource ID: [redacted]
Organization: [redacted]
Resource Name: [redacted]
Resource Set: [redacted]
Region: [redacted]
Created At: [redacted]
Resource Type: ECS

Resource Type

CPUs: 2
Instance Type Name: [redacted]
Memory (GB): 8.0
Disk Type: [redacted]
Instance Family: [redacted]

Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Utilization	High Disk Utilization	The average storage utilization is hig...	25	The threshold is not reached and the...	Passed	2024-07-29
Utilization	Low Disk Utilization	The average storage utilization is hig...	25	The threshold is not reached and the...	Passed	2024-07-29
Utilization	Low Resource Utilization	The average CPU utilization is lower ...	25	The threshold is not reached and the...	Passed	2024-07-29

6.2.3.2. Idle resource analysis

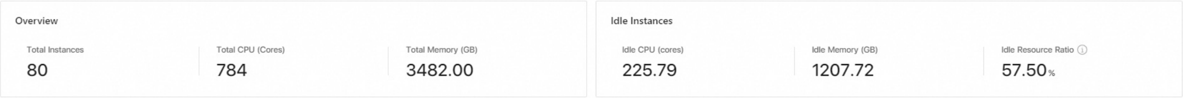
The idle resource analysis feature allows you to analyze the resource usage efficiency based on the CPU and memory metrics. This helps you understand resource utilization, improve overall resource governance, and optimize resource allocation policies.

Background information

- The idle resource analysis feature supports only Elastic Compute Service (ECS), ApsaraDB RDS, and ApsaraDB for Redis.
- You can view data in the trend charts in the Organization Idle Resource Trend section by day, week, or month.
- The idle resource analysis feature collects data of idle CPU cores and memory resources and displays the data of idle resources by organization, resource set, and resource.
- If the data of idle resources is displayed by organization, you can export the data as an **.xlsx** file to your computer.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Cloud Resource Optimization** > **Idle Resource Analysis**.
4. In the upper part of the **Idle Resource Analysis** page, view the overview of idle resources.



Overview

Total Instances 80

Total CPU (Cores) 784

Total Memory (GB) 3482.00

Idle Instances

Idle CPU (cores) 225.79

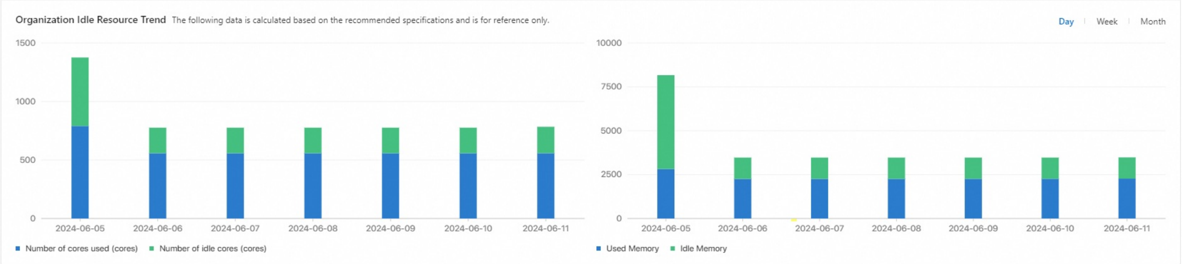
Idle Memory (GB) 1207.72

Idle Resource Ratio 57.50%

   - **Overview**: displays the **total number of instances**, **total number of CPU cores**, and **total memory capacity** measured in GB on the current platform.
   - **Idle Instances**: displays the **number of idle CPU cores**, **idle memory capacity** measured in GB, and **idle resource ratio** on the current platform.

5. In the middle section of the page, view the trend charts of the total number of idle resources of the organization. You can view data by the **day**, **week**, or **month**. When you move the pointer over a column chart, you can view the total number of CPU cores and idle CPU cores or the total memory capacity and idle memory capacity.

> **Note**
>
> The data in the trend charts of the total number of idle resources of an organization is calculated based on the recommended specifications. The data displayed in this topic is for reference only.
>
> - **Used Cores**: the total number of CPU cores of all supported service instances in all organizations.
> - **Idle Cores**: the total number of idle CPU cores of all supported service instances in all organizations.
> - **Used Memory**: the total memory capacity of all supported service instances in all organizations.
> - **Idle Memory**: the total idle memory capacity of all supported service instances in all organizations.

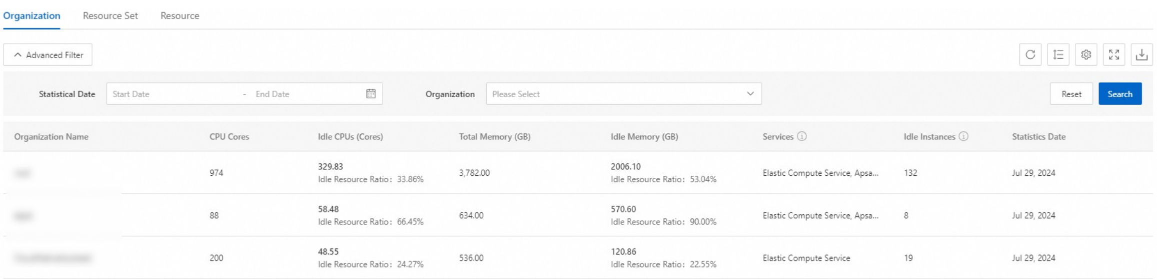


Organization Idle Resource Trend The following data is calculated based on the recommended specifications and is for reference only.

6. In the lower part of the page, view the data of idle resources by **organization**, **resource set**, and **resource**.
   - View data of idle resources by organization

     On the **Organization** tab, specify parameters such as **Statistical Date** and **Organization** to filter data.

> **Note**
> Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.

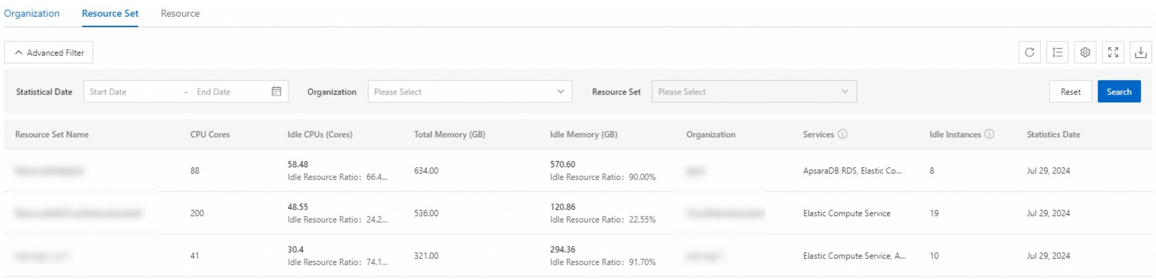


Organization Name	CPU Cores	Idle CPUs (Cores)	Total Memory (GB)	Idle Memory (GB)	Services	Idle Instances	Statistics Date
[redacted]	974	329.83 Idle Resource Ratio：33.86%	3,782.00	2006.10 Idle Resource Ratio：53.04%	Elastic Compute Service, Apsa...	132	Jul 29, 2024
[redacted]	88	58.48 Idle Resource Ratio：66.45%	634.00	570.60 Idle Resource Ratio：90.00%	Elastic Compute Service, Apsa...	8	Jul 29, 2024
[redacted]	200	48.55 Idle Resource Ratio：24.27%	536.00	120.86 Idle Resource Ratio：22.55%	Elastic Compute Service	19	Jul 29, 2024

- View data of idle resources by resource set

  On the **Resource Set** tab, specify parameters such as **Statistical Date**, **Organization**, and **Resource Set** to filter data.

> **Note**
> Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.

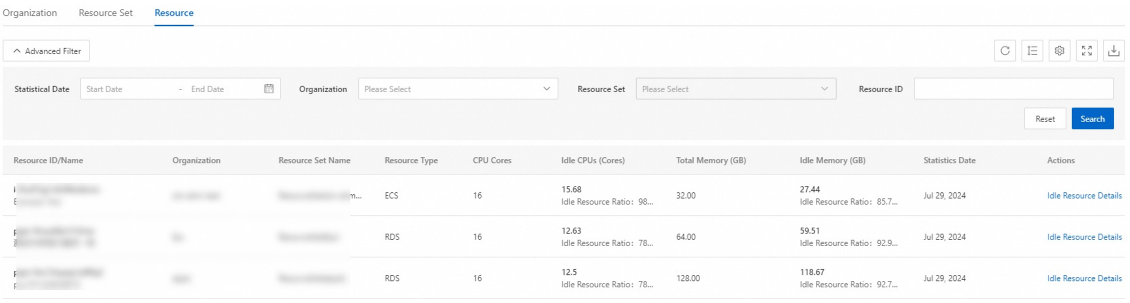


Resource Set Name	CPU Cores	Idle CPUs (Cores)	Total Memory (GB)	Idle Memory (GB)	Organization	Services	Idle Instances	Statistics Date
[redacted]	88	58.48 Idle Resource Ratio：66.4...	634.00	570.60 Idle Resource Ratio：90.00%	[redacted]	ApsaraDB RDS, Elastic Co...	8	Jul 29, 2024
[redacted]	200	48.55 Idle Resource Ratio：24.2...	536.00	120.86 Idle Resource Ratio：22.55%	[redacted]	Elastic Compute Service	19	Jul 29, 2024
[redacted]	41	30.4 Idle Resource Ratio：74.1...	321.00	294.36 Idle Resource Ratio：91.70%	[redacted]	Elastic Compute Service, A...	10	Jul 29, 2024

- View data of idle resources by resource

  a. On the **Resource** tab, specify parameters such as **Statistical Date**, **Organization**, **Resource Set**, and **Resource ID** to filter data.

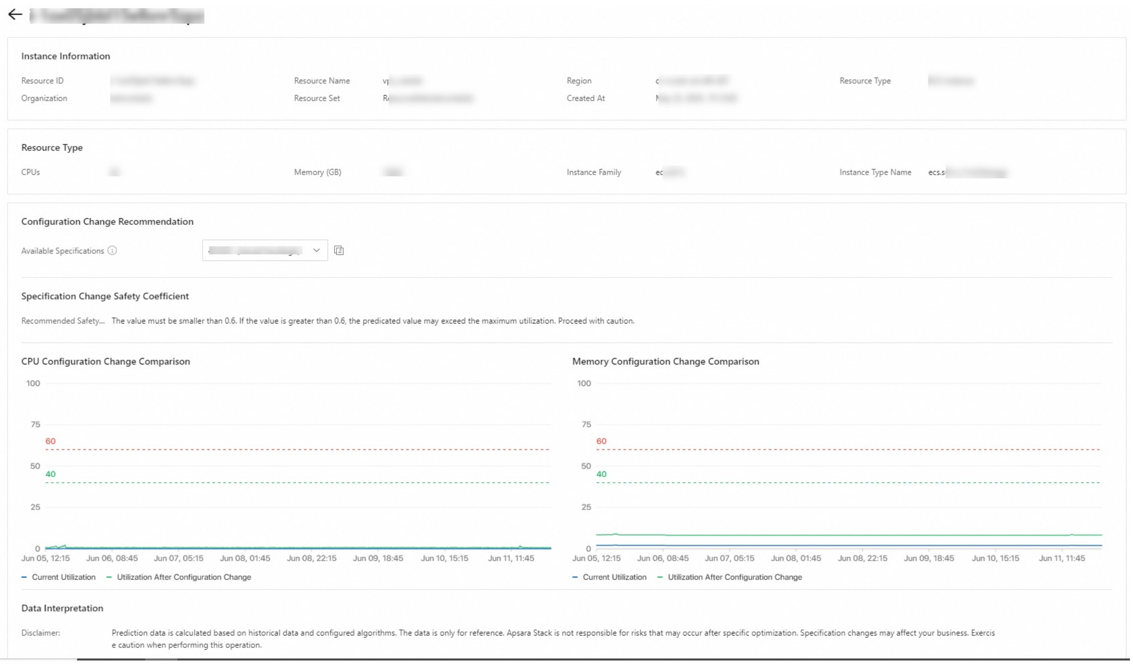
> **Note**
> Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.



Resource ID/Name	Organization	Resource Set Name	Resource Type	CPU Cores	Idle CPUs (Cores)	Total Memory (GB)	Idle Memory (GB)	Statistics Date	Actions
[redacted]	[redacted]	[redacted]	ECS	16	15.68 Idle Resource Ratio：98...	32.00	27.44 Idle Resource Ratio：85.7...	Jul 29, 2024	Idle Resource Details
[redacted]	[redacted]	[redacted]	RDS	16	12.63 Idle Resource Ratio：78...	64.00	59.51 Idle Resource Ratio：92.9...	Jul 29, 2024	Idle Resource Details
[redacted]	[redacted]	[redacted]	RDS	16	12.5 Idle Resource Ratio：78...	128.00	118.67 Idle Resource Ratio：92.7...	Jul 29, 2024	Idle Resource Details

b. Find the idle resource that you want to view and click **Idle Resource Details** in the **Actions** column to go to the details page of the resource. On the details page, you can view the information in the following sections: **Instance Information**, **Resource Type**, **Configuration Change Recommendation**, **Specification Change Safety Coefficient**, **CPU Configuration Change Comparison**, and **Memory Configuration Change Comparison**.

> **Important**
>
> Data of idle specifications prediction is generated by performing calculations and simulations based on data performance and user-configured algorithms. The data is used for reference only and cannot be relied upon as the sole basis for business decisions. Apsara Stack is not responsible for risks that may occur when you optimize resources based on the data. Specification changes may affect your business. Exercise caution when you change specifications.



← [redacted]

Instance Information

Resource ID [redacted]
Resource Name [redacted]
Region [redacted]
Resource Type [redacted]
Organization [redacted]
Resource Set [redacted]
Created At [redacted]

Resource Type

CPUs [redacted]
Memory (GB) [redacted]
Instance Family [redacted]
Instance Type Name [redacted]

Configuration Change Recommendation

Available Specifications [redacted]

Specification Change Safety Coefficient

Recommended Safety... The value must be smaller than 0.6. If the value is greater than 0.6, the predicated value may exceed the maximum utilization. Proceed with caution.

CPU Configuration Change Comparison

Memory Configuration Change Comparison

Data Interpretation

Disclaimer: Prediction data is calculated based on historical data and configured algorithms. The data is only for reference. Apsara Stack is not responsible for risks that may occur after specific optimization. Specification changes may affect your business. Exercise caution when performing this operation.

6.2.3.3. Analyze bottlenecks

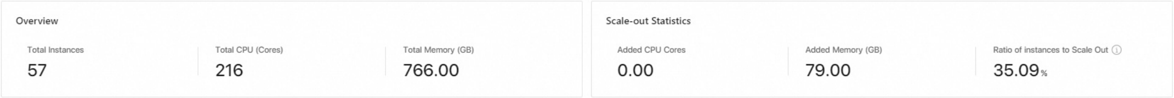
The bottleneck analysis feature focuses on resource utilization and provides scale-up analysis based on the CPU and memory metrics.

Background information

- The bottleneck analysis feature is applicable only to Elastic Compute Service (ECS) and ApsaraDB RDS.
- You can view the trend charts in the Added Cores of Organization section by day, week, or month.
- The scale-up analysis is performed based on the number of CPU cores, number of required additional CPU cores, total memory capacity measured in GB, and required additional memory capacity measured in GB. The statistics are displayed on the Organization, Resource Set, and Resource tabs.
- If the statistics are displayed by organization, you can export the data as an **.xlsx** file to your computer.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Cloud Resource Optimization** > **Bottleneck Analysis**.
4. In the upper part of the **Bottleneck Analysis** page, view the overview information and scale-up statistics about instances.



Overview

Total Instances 57

Total CPU (Cores) 216

Total Memory (GB) 766.00

Scale-out Statistics

Added CPU Cores 0.00

Added Memory (GB) 79.00

Ratio of instances to Scale Out 35.09%

   - **Overview**: displays the **total number of instances**, **total number of CPU cores**, and **total memory capacity** measured in GB on the current platform.
   - **Scale-out Statistics**: displays the **number of required CPU cores**, **required memory capacity** measured in GB, and **percentage of instances that need to be scaled out** on the current platform.

   > **Note**
   >
   > The percentage of instances that need to be scaled up is calculated based on the following formula: Total number of instances that need to be scaled up/Total number of instances.

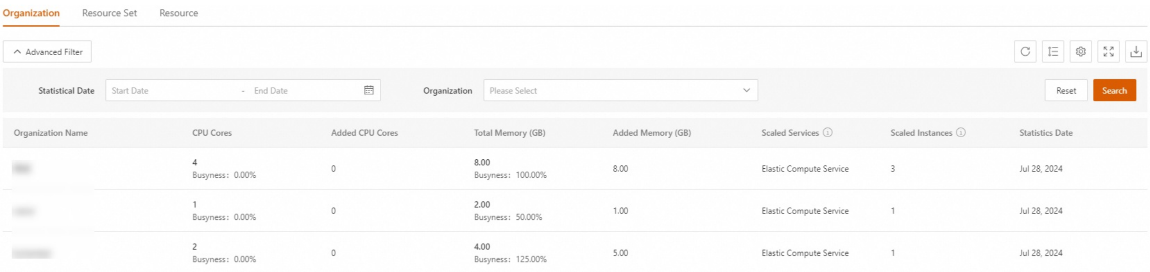
5. In the middle part of the page, view the trend charts in the **Added Cores of Organization** section. You can view the trend charts by **day**, **week**, or **month**. After you move the pointer over a column, you can view the total number of CPU cores and number of required additional CPU cores or the total memory capacity and required additional memory capacity.

   > **Note**
   >
   > The data in the trend charts is calculated based on recommended specifications and is for reference only.

6. In the lower part of the page, view the statistics of the resources that need to be scaled up in organizations on the **Organization**, **Resource Set**, and **Resource** tabs.
   - View statistics by organization

     On the **Organization** tab, configure the **Statistical Date** and **Organization** parameters to filter data.

     > **Note**
     >
     > Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.

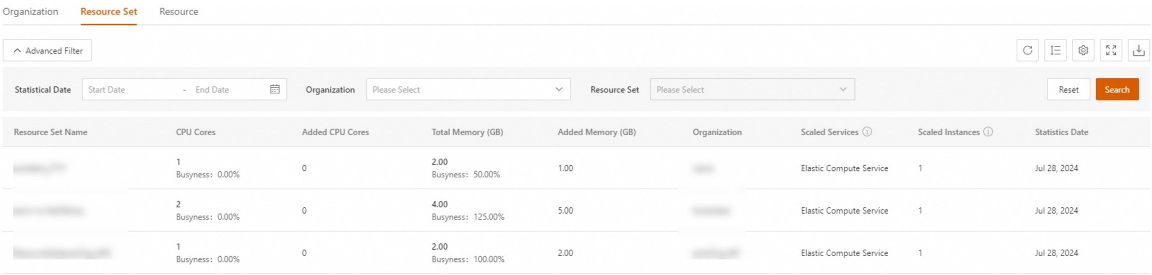


Organization Name	CPU Cores	Added CPU Cores	Total Memory (GB)	Added Memory (GB)	Scaled Services	Scaled Instances	Statistics Date
[redacted]	4 Busyness：0.00%	0	8.00 Busyness：100.00%	8.00	Elastic Compute Service	3	Jul 28, 2024
[redacted]	1 Busyness：0.00%	0	2.00 Busyness：50.00%	1.00	Elastic Compute Service	1	Jul 28, 2024
[redacted]	2 Busyness：0.00%	0	4.00 Busyness：125.00%	5.00	Elastic Compute Service	1	Jul 28, 2024

- View statistics by resource set

  On the **Resource Set** tab, configure the **Statistical Date**, **Organization**, and **Resource Set** parameters to filter data.

  > **Note**
  >
  > Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.

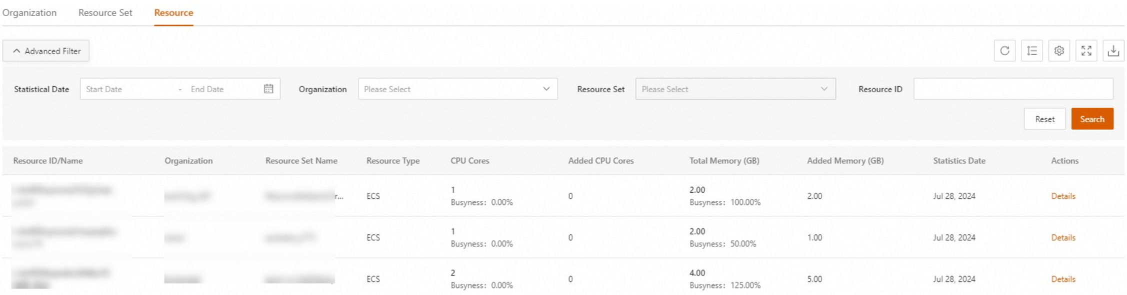


Resource Set Name	CPU Cores	Added CPU Cores	Total Memory (GB)	Added Memory (GB)	Organization	Scaled Services	Scaled Instances	Statistics Date
[redacted]	1 Busyness：0.00%	0	2.00 Busyness：50.00%	1.00	[redacted]	Elastic Compute Service	1	Jul 28, 2024
[redacted]	2 Busyness：0.00%	0	4.00 Busyness：125.00%	5.00	[redacted]	Elastic Compute Service	1	Jul 28, 2024
[redacted]	1 Busyness：0.00%	0	2.00 Busyness：100.00%	2.00	[redacted]	Elastic Compute Service	1	Jul 28, 2024

- View statistics by resource

  a. On the **Resource** tab, configure the **Statistical Date**, **Organization**, **Resource Set**, and **Resource ID** parameters to filter data.

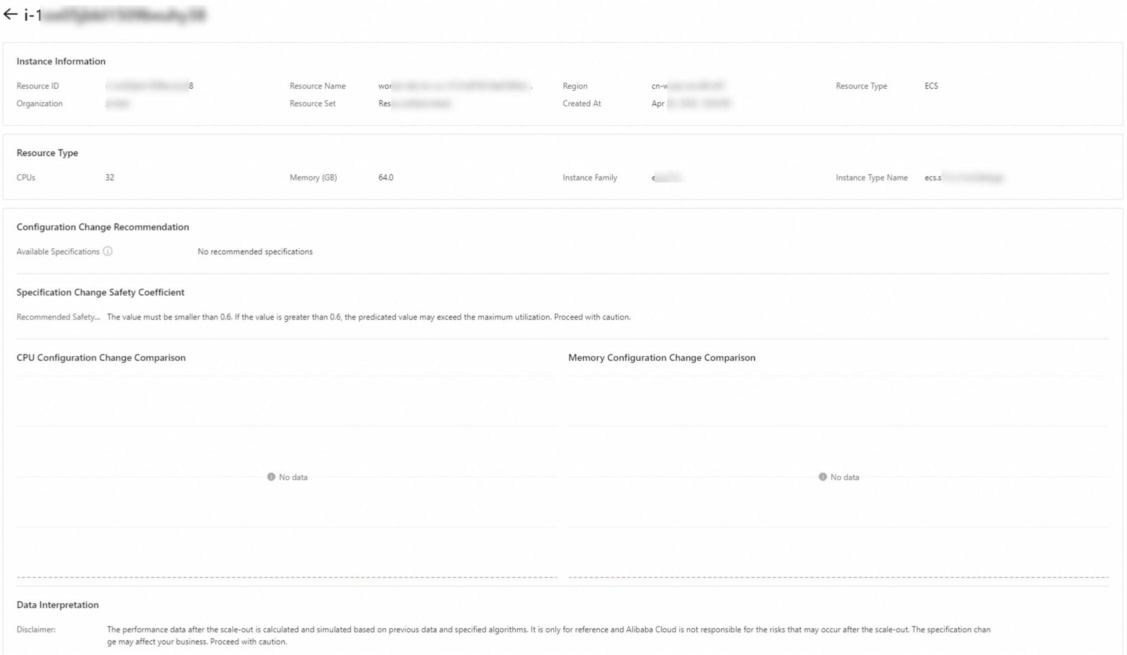
  > **Note**
  >
  > Click the ⤓ icon above the list. In the dialog box that appears, select a date to export the data as an **.xlsx** file to your computer.



Resource ID/Name	Organization	Resource Set Name	Resource Type	CPU Cores	Added CPU Cores	Total Memory (GB)	Added Memory (GB)	Statistics Date	Actions
[redacted]	[redacted]	[redacted]	ECS	1 Busyness：0.00%	0	2.00 Busyness：100.00%	2.00	Jul 28, 2024	Details
[redacted]	[redacted]	[redacted]	ECS	1 Busyness：0.00%	0	2.00 Busyness：50.00%	1.00	Jul 28, 2024	Details
[redacted]	[redacted]	[redacted]	ECS	2 Busyness：0.00%	0	4.00 Busyness：125.00%	5.00	Jul 28, 2024	Details

b. Find the resource that you want to manage and click **Details** in the **Actions** column to go to the resource details page. On the details page, you can view the information in the following sections: **Instance Information**, **Resource Type**, **Configuration Change Recommendation**, **Specification Change Safety Coefficient**, **CPU Configuration Change Comparison**, and **Memory Configuration Change Comparison**.

> **Important**
>
> Data of specification scale-up prediction is generated by performing calculations and simulations based on data performance and user-configured algorithms. The data is used for reference only and cannot be relied upon as the sole basis for business decisions. Apsara Stack is not responsible for risks that may occur when you optimize resources based on the data. Specification changes may affect your business. Proceed with caution.



← i-1[redacted]

Instance Information

Resource ID	[redacted]8	Resource Name	wor[redacted]	Region	cn-w[redacted]	Resource Type	ECS
Organization	[redacted]	Resource Set	Res[redacted]	Created At	Apr [redacted]		

Resource Type

CPUs	32	Memory (GB)	64.0	Instance Family	e[redacted]	Instance Type Name	ecs.s[redacted]

Configuration Change Recommendation

Available Specifications ⓘ No recommended specifications

Specification Change Safety Coefficient

Recommended Safety... The value must be smaller than 0.6. If the value is greater than 0.6, the predicated value may exceed the maximum utilization. Proceed with caution.

CPU Configuration Change Comparison

No data

Memory Configuration Change Comparison

No data

Data Interpretation

Disclaimer: The performance data after the scale-out is calculated and simulated based on previous data and specified algorithms. It is only for reference and Alibaba Cloud is not responsible for the risks that may occur after the scale-out. The specification change may affect your business. Proceed with caution.

6.2.3.4. Security compliance analysis

The security compliance analysis feature allows you to analyze the overall resource security based on resource security metrics, This helps you identify potential security risks and non-compliant configurations.

Background information

- The Apsara Uni-manager Management Console displays security compliance data by organization, resource set, and resource.
    - Security compliance analysis on organizations: collects the security compliance data of all resource sets of each organization. By default, the security compliance data of sub-organizations is not included. You can select Aggregate Sub-organizations to calculate the average security scores of an organization and its sub-organizations.
    - Security compliance analysis on resource sets: collects the security compliance data of all resources of each resource set and displays the scoring details of all resources in each resource set.

  - Security compliance analysis on resources: collects the data metrics that are related to the security of each resource and displays the scoring details of each resource.

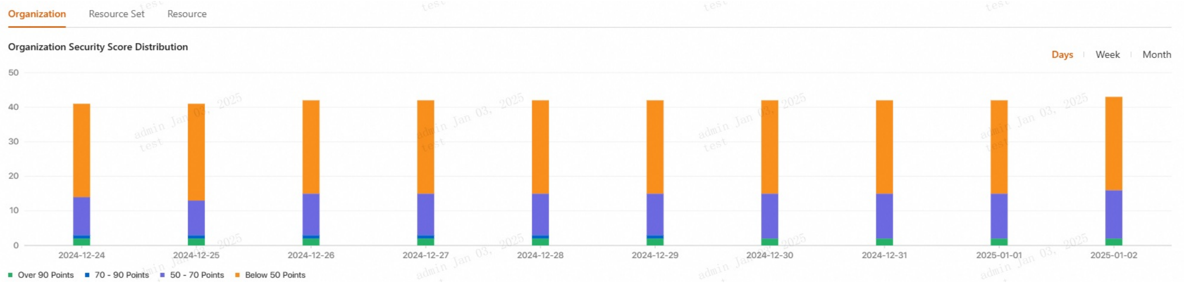
- You can view the distribution of security compliance data by day, week, or month based on your business requirements.

> **Note**
>
> Different colors represent different security scores.
>
> - 🟩: excellent, with a security score greater than or equal to 90.
> - 🟦: healthy, with a security score greater than or equal to 70 but smaller than 90.
> - 🟪: general, with a security score greater than or equal to 50 but smaller than 70.
> - 🟧: poor, with a security score smaller than 50.

View the security compliance analysis data of organizations

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Cloud Resource Optimization** > **Security Compliance Analytics**.
4. On the **Security Compliance Analytics** page, click the **Organization** tab.
5. View the security score distribution of organizations.

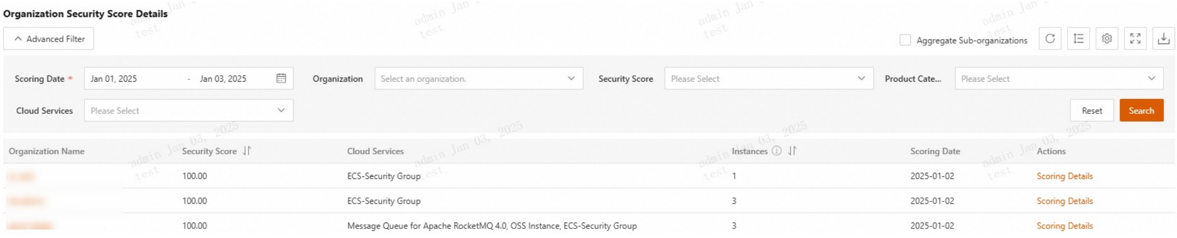
   In the Organization Security Score Distribution section, you can view the distribution of organizations with different security scores by day, week, or month. You can move the pointer over a column in the chart to view the number of organizations with different security scores.



6. View the scoring details of organizations.

   In the Organization Security Score Details section, you can view the details of the security scores of organizations. You can configure the **Scoring Date**, **Organization**, **Security Score**, **Product Categories**, and **Cloud Services** parameters to filter data.

> **Note**
>
> - Select **Aggregate Sub-organizations** to calculate the average security scores of an organization and its sub-organizations.
> - Click the ⤓ icon to export and save the data to your computer.



Organization Security Score Details

Scoring Date * Jan 01, 2025 - Jan 03, 2025

Organization: Select an organization.

Security Score: Please Select

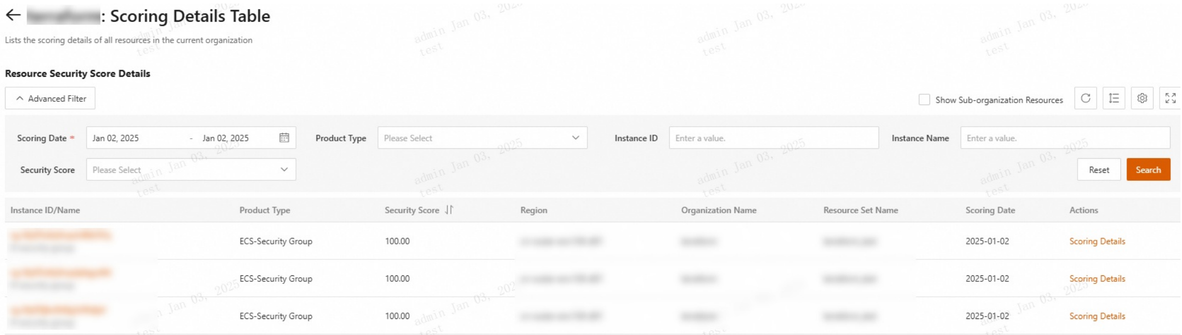
Product Cate...: Please Select

Cloud Services: Please Select

Organization Name	Security Score	Cloud Services	Instances	Scoring Date	Actions
[redacted]	100.00	ECS-Security Group	1	2025-01-02	Scoring Details
[redacted]	100.00	ECS-Security Group	3	2025-01-02	Scoring Details
[redacted]	100.00	Message Queue for Apache RocketMQ 4.0, OSS Instance, ECS-Security Group	3	2025-01-02	Scoring Details

7. Optional. In the Organization Security Score Details section, find an organization and click **Scoring Details** in the **Actions** column. On the **Scoring Details Table** page, view the scoring details of all resources in the organization.

   > **Note**
   >
   > Select **Show Sub-organization Resources** in the upper-right corner of the Scoring Details Table page to view the scoring details of resources in sub-organizations.



[redacted]: Scoring Details Table

Lists the scoring details of all resources in the current organization

Resource Security Score Details

Scoring Date * Jan 02, 2025 - Jan 02, 2025

Product Type: Please Select

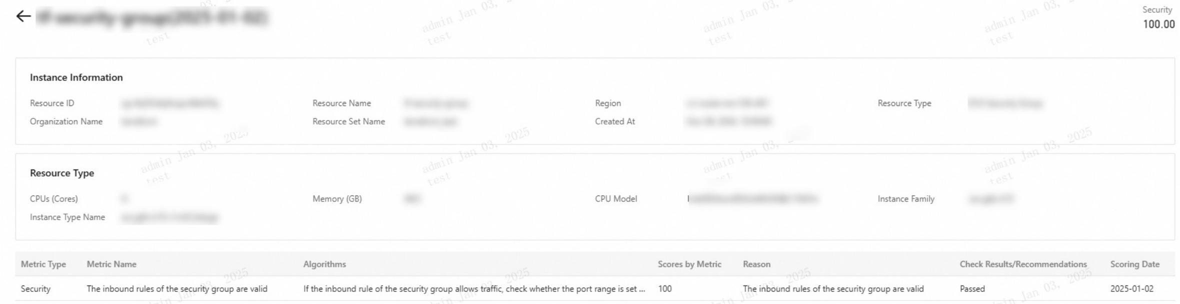
Instance ID: Enter a value.

Instance Name: Enter a value.

Security Score: Please Select

Instance ID/Name	Product Type	Security Score	Region	Organization Name	Resource Set Name	Scoring Date	Actions
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details

8. Optional. On the **Scoring Details Table** page, find the resource whose scoring details you want to view and click **Scoring Details** in the **Actions** column.



[redacted]

Security 100.00

Instance Information

Resource ID	[redacted]	Resource Name	[redacted]	Region	[redacted]	Resource Type	[redacted]
Organization Name	[redacted]	Resource Set Name	[redacted]	Created At	[redacted]		

Resource Type

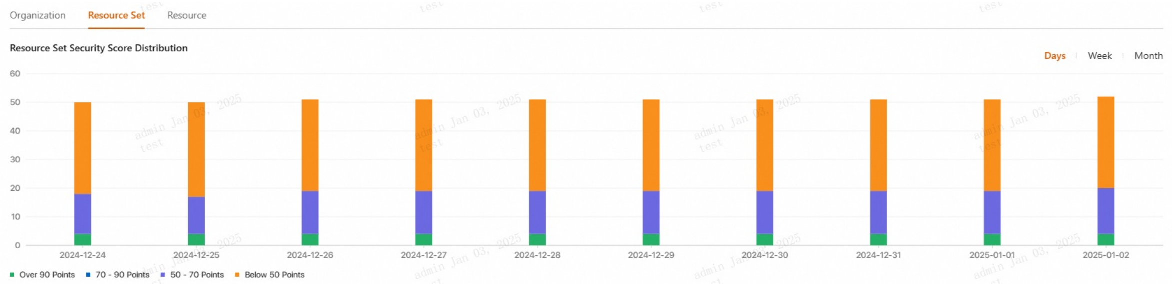
CPUs (Cores)	[redacted]	Memory (GB)	[redacted]	CPU Model	[redacted]	Instance Family	[redacted]
Instance Type Name	[redacted]						

Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Security	The inbound rules of the security group are valid	If the inbound rule of the security group allows traffic, check whether the port range is set ...	100	The inbound rules of the security group are valid	Passed	2025-01-02

View the security compliance analysis data of resource sets

1. On the **Security Compliance Analytics** page, click the **Resource Set** tab.
2. View the security score distribution of resource sets.

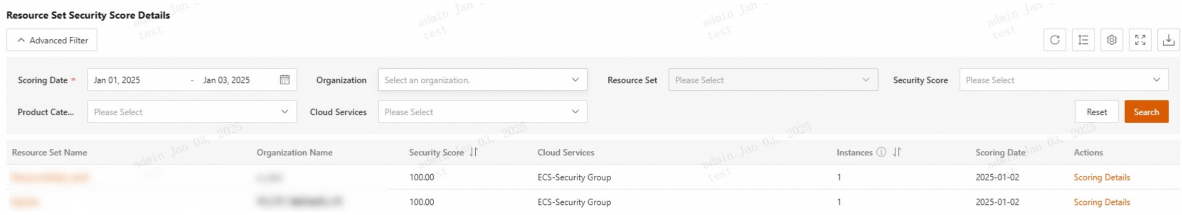
   In the Resource Set Security Score Distribution section, you can view the distribution of resource sets with different security scores by day, week, or month. You can move the pointer over a column in the chart to view the number of resource sets with different security scores.



3. View the scoring details of resource sets.

   In the Resource Set Security Score Details section, you can view the details of the security scores of resource sets. You can configure the **Scoring Date**, **Organization**, **Resource Set**, **Security Score**, **Product Categories**, and **Cloud Services** parameters to filter data.

   > **Note**
   >
   > Click the ⤓ icon to export and save the data to your computer.



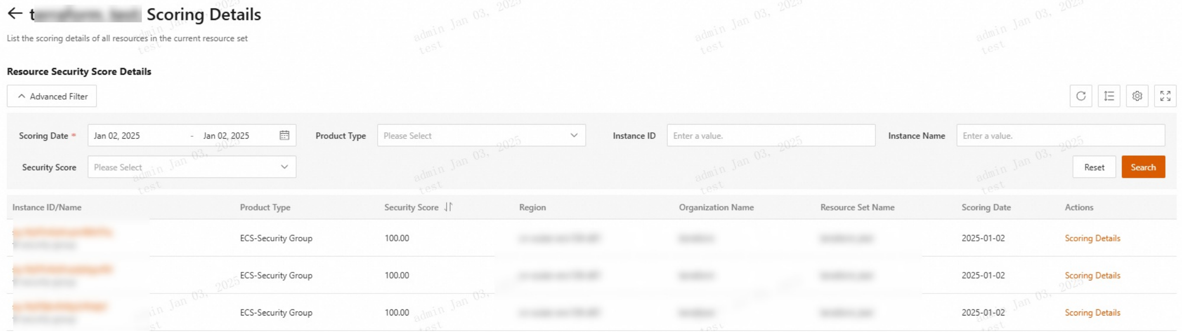
Resource Set Security Score Details

Scoring Date * Jan 01, 2025 - Jan 03, 2025 | Organization: Select an organization. | Resource Set: Please Select | Security Score: Please Select

Product Cate...: Please Select | Cloud Services: Please Select

Resource Set Name	Organization Name	Security Score	Cloud Services	Instances	Scoring Date	Actions
[redacted]	[redacted]	100.00	ECS-Security Group	1	2025-01-02	Scoring Details
[redacted]	[redacted]	100.00	ECS-Security Group	1	2025-01-02	Scoring Details

4. Optional. In the Resource Set Security Score Details section, find a resource set and click **Scoring Details** in the **Actions** column. On the Scoring Details page, view the scoring details of all resources in the resource set.



← [redacted] Scoring Details

List the scoring details of all resources in the current resource set

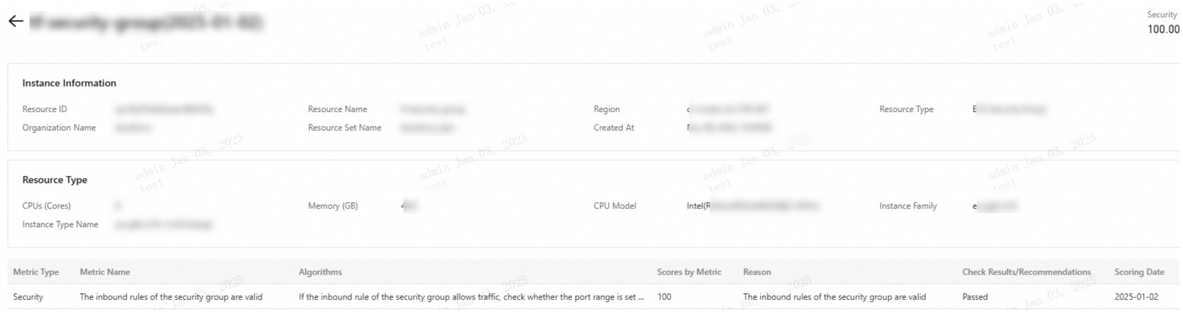
Resource Security Score Details

Scoring Date * Jan 02, 2025 - Jan 02, 2025 | Product Type: Please Select | Instance ID: Enter a value. | Instance Name: Enter a value.

Security Score: Please Select

Instance ID/Name	Product Type	Security Score	Region	Organization Name	Resource Set Name	Scoring Date	Actions
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details

5. Optional. On the Scoring Details page, find the resource whose scoring details you want to view and click **Scoring Details** in the **Actions** column.



← [redacted]

Security
100.00

Instance Information

Resource ID	[redacted]	Resource Name	[redacted]	Region	[redacted]	Resource Type	[redacted]
Organization Name	[redacted]	Resource Set Name	[redacted]	Created At	[redacted]		

Resource Type

CPUs (Cores)	[redacted]	Memory (GB)	[redacted]	CPU Model	[redacted]	Instance Family	[redacted]
Instance Type Name	[redacted]						

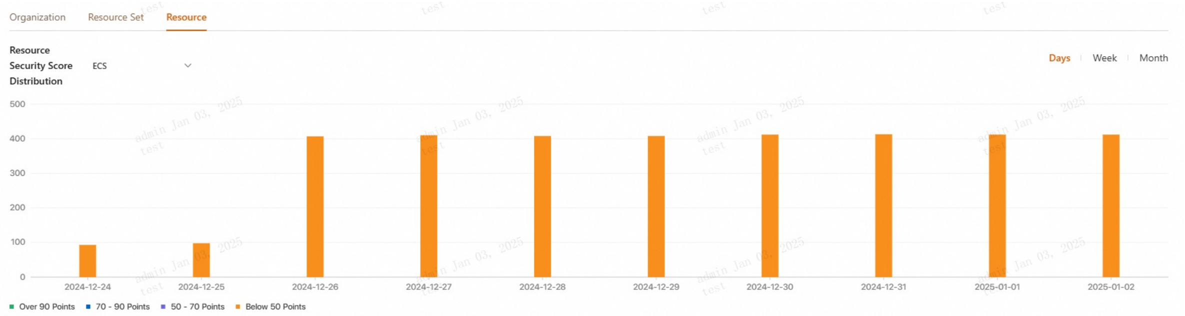
Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Security	The inbound rules of the security group are valid	If the inbound rule of the security group allows traffic, check whether the port range is set ...	100	The inbound rules of the security group are valid	Passed	2025-01-02

View the security compliance analysis data of resources

1. On the **Security Compliance Analytics** page, click the **Resource** tab.

2. View the security score distribution of resources.

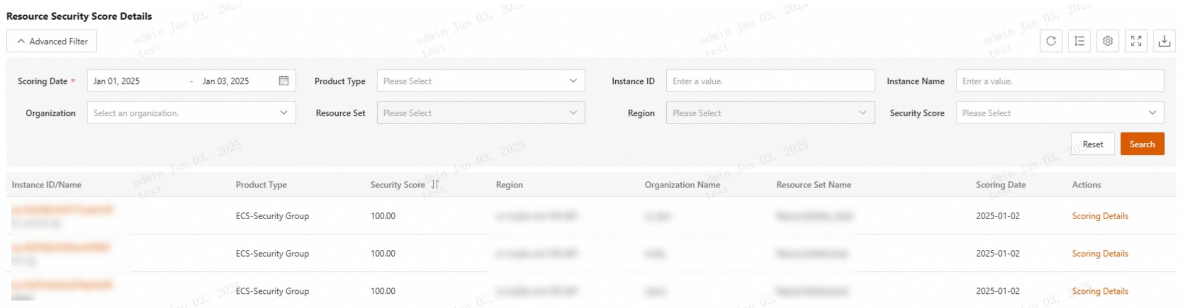
   In the Resource Security Score Distribution section, you can view the distribution of resources with different security scores by day, week, or month. You can move the pointer over a column in the chart to view the number of resources with different security scores.



3. View the scoring details of resources.

   In the Resource Security Score Details section, you can view the details of the security scores of resources. You can configure the**Scoring Date**, **Product Type**, **Instance ID**, **Instance Name**, **Organization**, **Resource Set**, **Region**, and **Security Score** parameters to filter data.

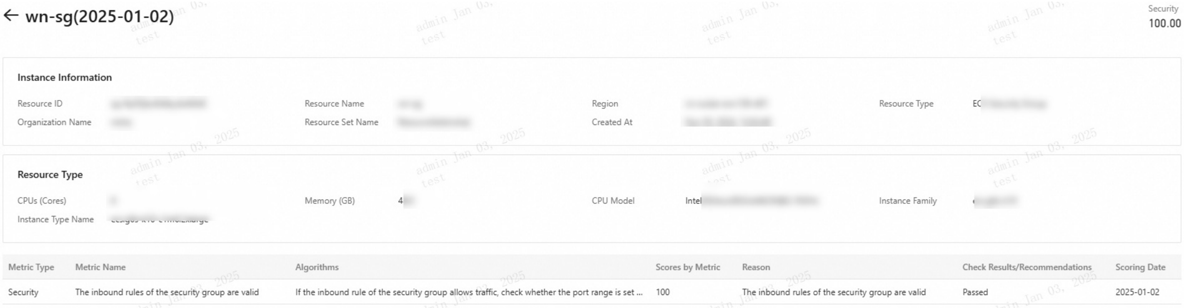
> **Note**
>
> Click the ⤓ icon to export and save the data to your computer.


Resource Security Score Details

Scoring Date * Jan 01, 2025 - Jan 03, 2025
Product Type Please Select
Instance ID Enter a value.
Instance Name Enter a value.
Organization Select an organization.
Resource Set Please Select
Region Please Select
Security Score Please Select

Instance ID/Name	Product Type	Security Score	Region	Organization Name	Resource Set Name	Scoring Date	Actions
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details
[redacted]	ECS-Security Group	100.00	[redacted]	[redacted]	[redacted]	2025-01-02	Scoring Details

4. In the Resource Security Score Details section, find the resource whose scoring details you want to view and click **Scoring Details** in the **Actions** column. On the page that appears, view the scoring details of the resource.


← wn-sg(2025-01-02)

Security 100.00

Instance Information

Resource ID [redacted]
Resource Name [redacted]
Region [redacted]
Resource Type EC[redacted]
Organization Name [redacted]
Resource Set Name [redacted]
Created At [redacted]

Resource Type

CPUs (Cores) [redacted]
Memory (GB) 4[redacted]
CPU Model Intel[redacted]
Instance Family [redacted]
Instance Type Name [redacted]

Metric Type	Metric Name	Algorithms	Scores by Metric	Reason	Check Results/Recommendations	Scoring Date
Security	The inbound rules of the security group are valid	If the inbound rule of the security group allows traffic, check whether the port range is set ...	100	The inbound rules of the security group are valid	Passed	2025-01-02

6.2.3.5. Resource optimization settings

You can configure policies that are used for idle resource analysis, optimization plans, and health analysis. You can modify existing policies.

Background information

The following table describes the cloud services for which you can configure resource optimization settings, the type of the resources that can be optimized, and the names of the resource optimization settings.

Cloud service category	Cloud service	Type of resources that can be optimized	Resource optimization setting
Elastic computing	Elastic Compute Service (ECS)	Idle resource	• ECS downtime • Idle storage
		Resource to be optimized	• Low disk utilization • High disk utilization • High resource utilization • Low resource utilization
	Elastic Block Storage (EBS)	Idle resource	• Unbound EBS
Storage	Objective Storage Service (OSS)	Idle resource	• Idle storage
		Resource to be optimized	• High disk utilization
	File Storage NAS (NAS)	Idle resource	• No read/write traffic
Networking	EIP	Idle resource	• Unbound EIP
	Server Load Balancer (SLB)	Idle resource	• No requests
		Non-compliant resource	• SLB port
		Idle resource	• No new connection

Database services	ApsaraDB RDS	Resource to be optimized	• Low resource utilization • High disk utilization • High resource utilization
	Tair (Redis OSS-compatible)	Resource to be optimized	• High resource utilization • Low resource utilization
	AnalyticDB for PostgreSQL	Resource to be optimized	• Low resource utilization • High resource utilization
	ApsaraDB for MongoDB	Resource to be optimized	• Low resource utilization • High resource utilization
	AnalyticDB for MySQL V3.0	Resource to be optimized	• Low disk utilization • High disk utilization
	PolarDB-X	Resource to be optimized	• High resource utilization • Low resource utilization
Big data	Hologres	Resource to be optimized	• High resource utilization • Low resource utilization
Middleware	ApsaraMQ	Idle resource	• Congested messages

Modify a resource optimization setting

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Data Analysis**.
3. In the left-side navigation pane, choose **Cloud Resource Optimization > Resource Optimization Settings**.
4. Optional. Specify the **configuration name**, **category**, or **cloud service** to filter data.
5. Find a resource optimization setting that you want to modify and click **Edit** in the **Actions** column. On the Alert Configuration Details page, modify the parameters in the sections such as **Description**, **Time Range**, **Valid value**, **Set Threshold**, and **Suggestions**. The following table describes the parameters.

> **Note**
>
> The parameters that can be modified vary based on the type of optimization settings.

Parameter		Description
Basic Information	**Name**	The setting name. You cannot modify the parameter.
	Classification	The type of the resource to be optimized. You cannot modify the parameter.
	Description	The description of the resource optimization setting. The description must be 1 to 300 characters in length.
	Resource Type	The cloud service to which the resource belongs. You cannot modify the parameter.
Time Range	**Duration**	The duration of the resource optimization. Valid values:**1 Day**, **1 Week**, **2 Weeks**, and 30 Days.
Valid value	**Hourly Usage**	The hourly usage of the service. Valid values:**Average**, **Maximum Value**, and **Minimum Value**.
	Daily Usage	The daily usage of the service. Valid values:**All** and **Duration**. **Note** If you select **Duration**, you must add new entries to configure the **Time Range** and **Weight** parameters. You can add multiple entries.
Set Threshold	**Idle Rules**	Configure a threshold for the idle rules of the setting.
Suggestions	**Suggestions**	The suggestions for fixing the optimization setting. The suggestions must be 0 to 300 characters in length.

6. Click **Submit**.

6.3. Service operations

6.3.1. Shopping cart

You can add the cloud services for which you want to apply to the shopping cart and apply for multiple cloud services of different types at a time on the Shopping Cart page.

Background information

You can add multiple cloud services for which you want to apply to the shopping cart, confirm the information on the Shopping Cart page, and then submit multiple applications at a time. This improves your efficiency.

You can add a service to the shopping cart on the service configuration page. After a service is added to the shopping cart, you can remove and modify the configurations of the service on the Shopping Cart page. After an application is submitted, a service order is generated.

Add a service to the shopping cart

In this example, Virtual Private Cloud (VPC) is used.

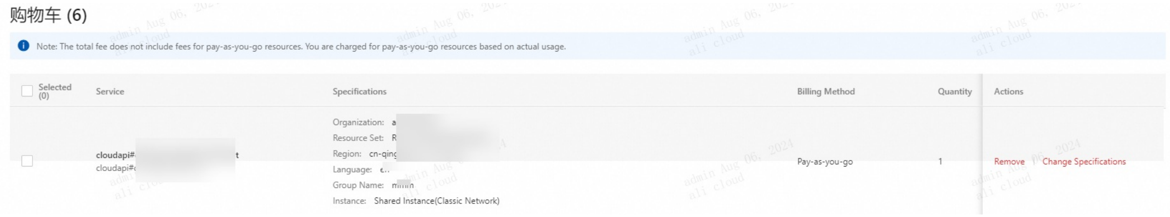
1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Networking** > **Cloud Network** > **Virtual Private Cloud**.
3. In the left-side navigation pane, click **Virtual Private Clouds**.
4. On the Virtual Private Clouds page, click **Create VPC**.
5. On the Create VPC page, configure the parameters. For more information, see the user guide of VPC.
6. After you configure the parameters, click **Add to Cart** in the lower part of the page

View services in the shopping cart

1. In the lower-right corner of the console, click the ‹ icon to show the floating menu and click the 🛒6 icon to go to the Shopping Cart page.

   > **Note**
   > - After you add a service to the shopping cart on the service configuration page, you are automatically navigated to the Shopping Cart page.
   > - The number in the upper-right corner of the Shopping Cart icon indicates the number of services added to the shopping cart.

2. On the Shopping Cart page, view the information about cloud services that are added to the shopping cart in the following columns: **Service**, **Specifications**, **Billing Method**, and **Quantity**.



购物车 (6)

Note: The total fee does not include fees for pay-as-you-go resources. You are charged for pay-as-you-go resources based on actual usage.

□ Selected (0)	Service	Specifications	Billing Method	Quantity	Actions
□	cloudapi# [redacted] t cloudapi#	Organization: a [redacted] Resource Set: R Region: cn-qing Language: e.. Group Name: m[redacted]n Instance: Shared Instance(Classic Network)	Pay-as-you-go	1	Remove | Change Specifications

Remove one or more services from the shopping cart

- **Remove a single service**

  i. On the Shopping Cart page, find the service that you want to remove and click **Remove** in the **Actions** column.

ii. In the message that appears, click **OK**. After the service is removed, it is no longer displayed in the shopping cart.

- **Remove multiple services at a time**

  i. On the Shopping Cart page, select the services that you want to remove.

  ii. Click **Batch Remove** in the lower part of the page.

  iii. In the message that appears, click **OK**.

Modify service configurations in the shopping cart

1. On the Shopping Cart page, find the service that you want to manage and click **Change Specifications** in the **Actions** column.
2. Modify the configurations based on your business requirements by referring to the user guide of the cloud service.

Submit service applications

1. On the Shopping Cart page, select the services for which you want to apply.
2. In the lower part of the page, click **Apply Now**.
3. On the **Confirm Order** page, click **Create Now**.

6.3.2. Service catalog

6.3.2.1. Services

The Services page displays all available services and allows you to quickly create resources by activating services.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose Service Catalog > **Services**.
4. In the left-side navigation pane, click **Service Catalogs**. Find the service in the right window.

   > **Note**
   >
   > You can use the search box at the top of the page to quickly find the service.

5. Find the service and click **Activate Service**. On the page that appears, create a resource.

6.3.2.2. Manage services

The Service Management page displays all services that you can manage. You can create custom services, publish services, and authorize specific users to access services.

Background information

The service management feature is used to manage and control the specific specifications of services within an enterprise or organization. For example, enterprises or organizations require employees to go through an approval process before the employees purchase Elastic Compute Service (ECS) instances with high specifications, or authorize only a specific user or users in a specific organization to purchase high-specification ECS instances. In this case, enterprises or organizations can configure the specifications and specify users by using the service management feature. After a service is published, the authorized users or organizations can select only the specifications that they are authorized to access. If they create resources with high specifications, they must go through an approval process. This way, enterprises or organizations can impose limits on resource users and manage specifications in a fine-grained manner.

- **Cloud Product Services**: displays the services of cloud products. They can be system-preset ones and custom ones. You cannot modify, authorize, or delete system-preset services. By default, you can define basic information, form parameter configurations, and pricing configurations for cloud product services.
- **Custom Services**: displays custom services. They can be system-preset ones and custom ones. You cannot modify, authorize, or delete system-preset services. For custom services, you can define custom configurations, specified URLs, and cloud product links. Cloud product links are preset by the system. You cannot modify them.

Supported cloud products and resource items

Cloud Products	Resource item
Elastic Compute Service (ECS)	• High performance computing (HPC) cluster • Elastic network interface (ENI) • Dedicated host • ECS disk • Deployment set • Security group • Dedicated host cluster • ECS instance
Container Registry	• Image repository (Apsara Stack Advanced Edition) • Namespace (Apsara Stack Advanced Edition) • Image repository • Namespace
Bare Metal Computing Platform (BMCP)	• Bare Metal - Easy AI cluster • EVCP • ACK - Easy AI cluster
Bare-metal Management Service (BMS)	• Bare Metal instance • Bare Metal instance (unified computing)

File Storage NAS (NAS)	• Unified namespace • File system • Permission group • Cloud Parallel File Storage (CPFS) file system
Tablestore	• Tablestore instance
DataHub	• DataHub project
MaxCompute	• Project • Quota group
Key Management Service (KMS)	• AccessKey pair
API Gateway (Old)	• API application • API group • API plug-in
ApsaraMQ for RocketMQ	• ApsaraMQ for RocketMQ instance
Virtual Private Cloud (VPC)	• VPN connection • IPv6 gateway • Network access control list (ACL) • High-availability virtual IP address (HAVIP) • Customer gateway • NAT gateway • VPN gateway • SSL client • SSL server • Route table • vSwitch • VPC
Express Connect	• Router interface (VPC-to-VPC) • Express Connect circuit • Router interface (VBR-to-VPC) • Router interface
SLB	• SLB instance

Elastic IP Address (EIP)	• EIP
ApsaraDB for Redis	• ApsaraDB for Redis instance
ApsaraDB RDS	• ApsaraDB RDS instance
PolarDB	• PolarDB for PostgreSQL (Compatible with Oracle) Shared Storage Edition cluster
PolarDB-X 1.0	• PolarDB-X instance
PolarDB-X 2.0	• PolarDB-X 2.0 instance
ApsaraDB for MongoDB	• ApsaraDB for MongoDB instance

Cloud product services

Create a cloud product service

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Service Catalog** > **Manage Services**.
4. On the **Cloud Product Services** tab, click **Create Service**. In the Create Service dialog box, perform the Basic Information, Form Parameter Configuration, and pricing Configuration steps.

    i. In the **Basic Information** step, you can specify the users and approval processes of the service.

Parameter		Description
Service Type	**Service Type**	By default, the value of this parameter is **Cloud Product Service**.
	Cloud Products	The cloud products whose resources you want to restrict.
Service Information	**Service Name**	The name of the service. The name must be 3 to 25 characters in length. The name must be unique.
	Service Description	The description of the service. The service description must be 2 to 100 characters in length. The description is displayed in service catalogs.

Service Authorization	**Authorization Type**	The authorization type. Valid values: - **Global**: allows all users in all organizations to access the service. - **Specified Organization**: allows all users in the specified organization to access the service. - **Specified Users**: allows specified users to access the service.
	Authorized Organization	The organizations in which users can access the service. If you set the Authorization Type parameter to **Specified Organization**, you must select one or more organizations.
	Authorized User	The users who can access the service. If you set the Authorization type parameter to **Specified User**, you must add one or more users. Click **Add User**. In the Add User dialog box, select an organization and users. After a user is added, you can click **Delete** in the Operation column to remove the user from the authorized user list.
Request Configuration	**Configuration Details**	The types of applications that can be submitted for the service. Valid values: New Purchase (Create), Configuration Change, and Unsubscription (Release). **Note** - The supported application types vary based on the cloud product and resource item. The application types displayed in the console prevail. - To configure an approval process, create a process and associate the process with the service by using the process management feature after you create the service.

ii. In the **Form Parameter Configuration** step, you can configure optional information and prompt information for form items.

- Form attributes

  Click **Select Attribute Fields**. In the panel that appears, select the fields that you want to specify. The fields that you have selected are displayed as the parameters. Configure the parameters.

  > **Note**
  >
  > - The fields for the selected service type are displayed. The fields are organized in a tree chart.
  > - When you purchase, change, or release resources in the Apsara Uni-manager Management Console, you must provide the detailed information about organizations and resource sets. Therefore, the Organization and Resource Set fields are dimmed and you do not need to select these two fields.

- Specification pools
  - Add: You can create specification pools that are used to group multiple organizations and resource sets. You can click **Add** to add multiple specification pools.

    > **Note**
    >
    > - Move the pointer over the name of a specification pool and click the ✎ icon to modify the specification pool name. You cannot modify the name of the default specification pool.
    > - Move the pointer over the name of a specification pool and click the 🗑 icon to delete the specification pool. You cannot delete the default specification pool.

  - Preview Complete Form: You can view all the configuration items that are required to create the corresponding cloud resource.

iii. In the **Pricing Configuration** step, you can view the pricing configurations of the service.

> **Note**
>
> You can click **View Details** to go to the billing configuration details page.

5. Click **Submit**. The service is created. All created services are displayed as Custom.

View cloud product services

1. In the navigation tree of the **Service Management** page, select a service category based on your business requirements.

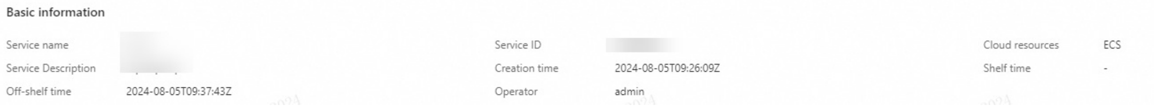
> **Note**
>
> On the Cloud Product Services tab, only the system-preset cloud products are displayed in the following categories: computing, storage, networking, security, middleware, database services, big data computing, and development tools. You can click a category to show and hide the products in this category, or click All to select all products.

2. In the service list, view the information in the following columns: **Service ID/Name**, **Cloud Products**, **Cloud Resources**, **Source**, **Status**, **Authorization Type**, **Authorized Organization/User**, **Operator**, and **Update Time**.

> **Note**
>
> - Click the ⏷ icon next to the **Source** column to filter services based on the source. You can view services grouped by custom services and cloud product services.
> - Click the ⏷ icon next to the **Status** column to filter services based on the status. You can view services grouped by the **Published**, **Unpublished**, and **To Be Published** state.

3. Find the service and click its ID to go to the service details page.

   - **Basic Information**: displays the service name, service ID, cloud resource, service description, creation time, publication time, unpublication time, and operator of the service.

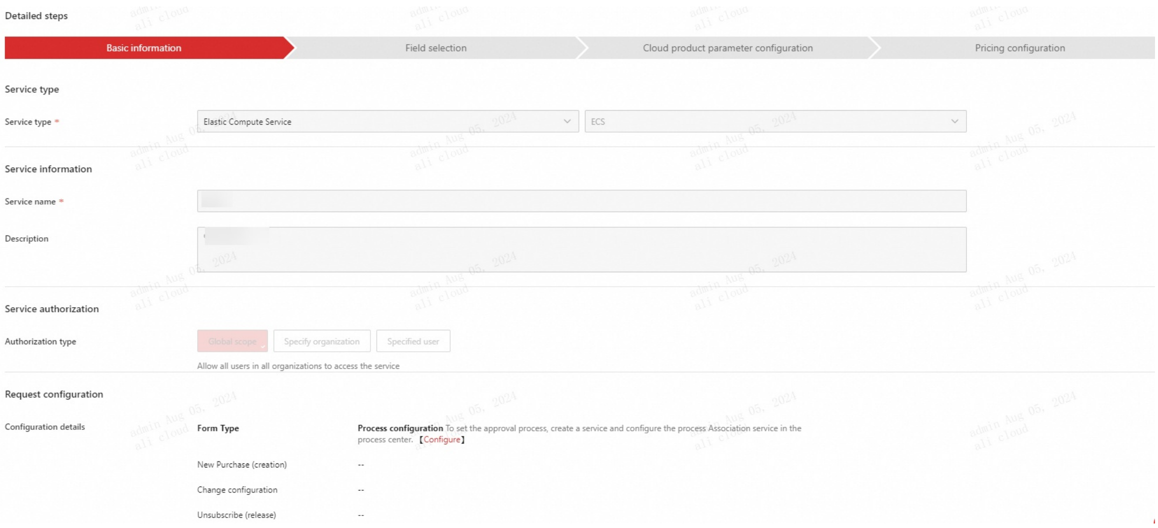


Basic information

Service name		Service ID		Cloud resources	ECS
Service Description		Creation time	2024-08-05T09:26:09Z	Shelf time	-
Off-shelf time	2024-08-05T09:37:43Z	Operator	admin		

   - **Detailed Steps**: displays information of the service in the **Basic Information**, **Form Parameter Configuration**, and **Pricing Configuration** steps.

> **Note**
>
> You can click a step to view the detailed configurations.



Detailed steps

Basic information > Field selection > Cloud product parameter configuration > Pricing configuration

Service type

Service type *: Elastic Compute Service | ECS

Service information

Service name *:

Description:

Service authorization

Authorization type: Global scope | Specify organization | Specified user

Allow all users in all organizations to access the service

Request configuration

Configuration details

Form Type	Process configuration To set the approval process, create a service and configure the process Association service in the process center. 【Configure】
New Purchase (creation)	--
Change configuration	--
Unsubscribe (release)	--

Modify a cloud product service

> **Important**
>
> - You can modify services only in the **To Be Published** or **Unpublished** state and with the Custom source.
> - When you modify a service, the Service type parameter cannot be modified.

1. On the **Cloud Product Services** tab, find the service and click **Edit** in the **Actions** column.
2. On the **Edit Service** page, modify the service information. For more information, see Create a service.

Publish a cloud product service

> **Important**
>
> You can publish services only in the **To Be Published** or **Unpublished** state.

1. On the **Cloud Product Services** tab, find the service and click **Publish** in the **Actions** column.
2. Click **OK**. After the service is published, the service changes to the **Published** state.

Unpublish a cloud product service

> **Important**
>
> You can unpublish services only in the **Published** state.

1. On the **Cloud Product Services** tab, find the service and click **Unpublish** in the **Actions** column.
2. Click **OK**. After the service is unpublished, the service changes to the **Unpublished** state.

Copy a cloud product service

1. On the **Cloud Product Services** tab, find the service and click **Copy** in the **Actions** column.
2. Click **OK**.

Authorize a cloud product service

> **Important**
>
> You can authorize services only with the Custom source to specify their organizations and users again.

1. On the **Cloud Product Services** tab, find the service, click the ··· icon in the **Actions** column, and then select **Authorize**.
2. In the dialog box that appears, change the authorization type based on your business requirements and specify the organizations or users.
3. Click **OK**.

Delete a cloud product service

> ⓘ **Important**
>
> You can delete services only in the **To Be Published** or **Unpublished** state and with the Custom source.

1. On the **Cloud Product Services** tab, find the service, click the ... icon in the **Actions** column, and then select **Delete**.
2. Click **OK**.

Custom services

Create a custom service category

Two service category levels are supported. The Custom Services tab displays all service categories, including those preset by the system. You cannot perform any operations on the system-preset service categories.

1. On the **Custom Services** tab, click the + icon next to **Service Categories** to create a level-1 service category. When you create a level-1 service category, a level-2 service category is also created by default.

   To create a level-2 service category, click the ... icon next to the level-1 service category and select **Create Sub-category**.
2. In the dialog box that appears, enter a category name and click **OK**.

   > ⓘ **Note**
   >
   > - The service category name must be unique. It can be up to 30 characters in length.
   > - If you add a space at the end of the service category name, it will be automatically removed.

Rename a custom service category

1. On the **Custom Services** tab, click the ... icon next to a custom service category and select **Rename**.
2. In the dialog box that appears, change the category name and click **OK**.

Move a custom service category

1. On the **Custom Services** tab, click the ... icon next to a custom service category and select **Move**.
2. In the dialog box that appears, set **Select Location** and **Move To**, and then click **OK**.

   > ⓘ **Important**
   >
   > - You can move a custom service category to another place at the same level.
   >   - When you move a level-1 custom service category, you can only select another level-1 service category to move it before and after the category you select.

> - When you move a level-2 custom service category, you can only select another level-2 service category of the same level-1 custom service category to move it before and after the category you select.
>
> - You cannot move system-preset service categories.

Delete a custom service category

> **Important**
>
> If a custom service category contains services, you must delete the services before you can delete the custom service category.

1. On the **Custom Services** tab, click the ... icon next to a custom service category and select **Delete**.
2. Click **OK**.

Create a custom service

1. On the **Custom Services** tab, click **Create Custom Service**. Perform the Basic Information, Form Parameter Configuration, and Pricing Configuration steps.

   i. In the **Basic Information** step, you can specify the users and approval processes of the service.

Parameter		Description
Service Type	**Service Type**	By default, the value of this parameter is **Custom Service**.
Service Information	**Service Name**	The name of the service. The name must be 3 to 25 characters in length. The name must be unique.
	Service Category	Select the level-1 and level-2 categories to which the service belongs. You can select system-preset service categories or custom service categories.
	Service Provider	The service provider. It must be 3 to 25 characters in length.
	Service Description	The description of the service. The service description must be 2 to 100 characters in length. The description is displayed in service catalogs.
	Service Configuration Method	Select **Custom Configuration** or **Specify URL**. ▪ Custom Configuration: allows you to configure the application form. ▪ Specified URL: Select this option for products with third-party activation pages.

Configuration Method	**Delivery Role**	This parameter is required if you set the Service Configuration Method parameter to **Custom Configuration**. The delivery role of the service. You can select multiple roles. Users with the corresponding delivery role can complete order delivery.
	Activation URL	This parameter is required if you set the Service Configuration Method parameter to **Specify URL**. The URL that is used to activate the service.
Service Authorization	**Authorization Type**	The authorization type. Valid values: ▪ **Global**: allows all users in all organizations to access the service. ▪ **Specified Organization**: allows all users in the specified organization to access the service. ▪ **Specified Users**: allows specified users to access the service.
	Authorized Organization	The organizations in which users can access the service. If you set the Authorization Type parameter to **Specified Organization**, you must select one or more organizations.
	Authorized User	The users who can access the service. If you set the Authorization type parameter to **Specified User**, you must add one or more users. Click **Add User**. In the Add User dialog box, select an organization and users. After a user is added, you can click **Delete** in the Operation column to remove the user from the authorized user list.
Request Configuration	**Configuration Details**	This parameter is required if you set the **Service Configuration Method** parameter to **Custom Configuration**. The types of applications that can be submitted for the service. For example, new purchase (create), unsubscription. **Note** To configure an approval process, create a process and associate the process with the service by using the process management feature after you create the service.

ii. In the **Form Configuration** step, you can configure optional information and prompt information for form items. Drag groups and components from the left list to the middle list. Then, configure the groups and components in the right list. Components are divided into five categories: container, input, selection, time, and others.

> ⓘ **Important**
>
> This step is displayed if you set the **Service Configuration Method** parameter to **Custom Configuration**.

Category	Component
Container	Includes groups. You can drag components to a group.
Input	Includes input box, number input, multi-line input, password.
Selection	Includes drop-down list, radio button, and check box.
Time	Includes date, year, month, and time.
Others	Includes organization, resource set, region, and zone.

iii. In the **Pricing Configuration** step, you can view the pricing configurations of the service.

> ⓘ **Important**
>
> This step is displayed if you set the **Service Configuration Method** parameter to **Custom Configuration**.

2. Click **Submit**.

View custom services

1. In the navigation tree of the **Service Management** page, select a service category based on your business requirements.

> ⓘ **Note**
>
> - The Custom Services tab displays all service categories, including those preset by the system. You cannot perform any operations on the system-preset service categories. You can click a category to show and hide the products in this category, or click All to select all products.
> - System-preset service categories: computing, storage, networking, security, middleware, database service, big data computing, AI and machine learning, development tools, IoT, disaster recovery and backup, migration and O&M management, applications, and others.

2. In the service list, view the information in the following columns: **Service ID/Name**, **Source**, **Status**, **Authorization Type**, **Authorized Organization/User**, **Operator**, and **Update Time**.

> **Note**
>
> - Click the ▽ icon next to the **Source** column to filter services based on the source. You can view services grouped by custom services and cloud product services.
> - Click the ▽ icon next to the **Status** column to filter services based on the status. You can view services grouped by the **Published**, **Unpublished**, and **To Be Published** state.

3. Find the service and click its ID to go to the service details page.

   - **Basic Information**: displays the service name, service ID, service description, creation time, publication time, unpublication time, and operator of the service.
   - **Detailed Steps**: displays information of the service in the **Basic Information**, **Form Configuration**, and **Pricing Configuration** steps.

   > **Note**
   >
   > - You can click a step to view the detailed configurations.
   > - The step information varies with the service configuration methods.
   >   - Steps for Custom Configuration: Basic Information, Form Configuration, and Pricing Configuration.
   >   - Steps for Specified URL and Cloud Product Link: Basic Information and Pricing Configuration. Form Configuration is not supported. The system-preset custom services are all linked to cloud products, and the link URLs in the service configuration method are the same as the menu URLs of the cloud products.

Modify a custom service

> **Important**
>
> - You can modify services only in the **To Be Published** or **Unpublished** state and with the Custom source.
> - When you modify a service, the Service type parameter cannot be modified.

1. On the **Cloud Product Services** tab, find the service and click **Edit** in the **Actions** column.
2. On the **Edit Service** page, modify the service information. For more information, see the Create a custom service section of this topic.

Publish a custom service

> **Important**
>
> You can publish services only in the **To Be Published** or **Unpublished** state.

1. On the **Custom Services** tab, find the service and click **Publish** in the **Actions** column.
2. Click **OK**. After the service is published, the service changes to the **Published** state.

Unpublish a custom service

> **Important**
>
> You can unpublish services only in the **Published** state.

1. On the **Custom Services** tab, find the service and click **Unpublish** in the **Actions** column.
2. Click **OK**. After the service is unpublished, the service changes to the **Unpublished** state.

Copy a custom service

1. On the **Custom Services** tab, find the service and click **Copy** in the **Actions** column.
2. Click **OK**.

Authorize a custom service

> **Important**
>
> You can authorize services only with the Custom source to specify their organizations and users again.

1. On the **Custom Services** tab, find the service, click the ... icon in the **Actions** column, and then select **Authorize**.
2. In the dialog box that appears, change the authorization type based on your business requirements and specify the organizations or users.
3. Click **OK**.

Delete a custom service

> **Important**
>
> You can delete services only in the **To Be Published** or **Unpublished** state and with the Custom source.

1. On the **Custom Services** tab, find the service, click the ... icon in the **Actions** column, and then select **Delete**.
2. Click **OK**.

FAQ

How many specification pools can I configure for a service?

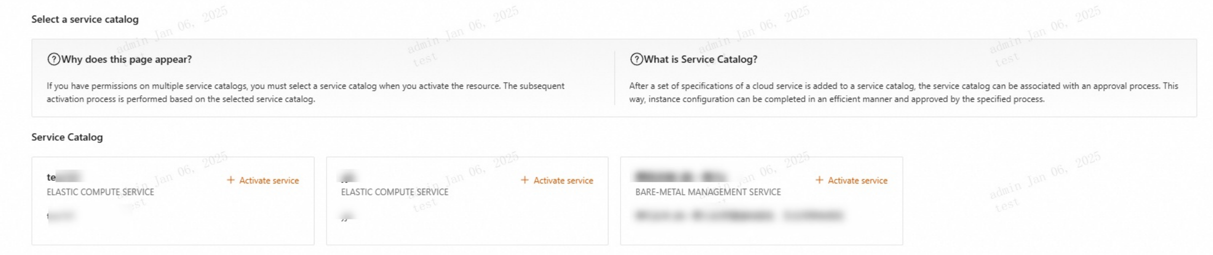
The number of specification pools that can be configured for a service is unlimited. You can configure multiple specification pools for a service based on your business requirements.

How do I specify the effective scope of a service?

A service can be effective for users or organizations. You can select specific users or organizations to authorize multiple users to access a service. After authorization, only the authorized users can access the service.

What happens if a user is authorized to access multiple services of the same service type?

If a user is authorized to access multiple services of the same service type, the user is required to select a service when the user creates a resource of this service type. The following figure shows an example.



Select a service catalog

Why does this page appear?

If you have permissions on multiple service catalogs, you must select a service catalog when you activate the resource. The subsequent activation process is performed based on the selected service catalog.

What is Service Catalog?

After a set of specifications of a cloud service is added to a service catalog, the service catalog can be associated with an approval process. This way, instance configuration can be completed in an efficient manner and approved by the specified process.

Service Catalog

te[redacted]
ELASTIC COMPUTE SERVICE
[redacted]
+ Activate service

[redacted]
ELASTIC COMPUTE SERVICE
[redacted]
+ Activate service

[redacted]
BARE-METAL MANAGEMENT SERVICE
[redacted]
+ Activate service

6.3.2.3. Operation examples

6.3.2.3.1. Example: Create an ECS instance service

This topic describes how to create an ECS instance service.

Prerequisites

You are an operations administrator or organization administrator.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Service Catalog** > **Services**.
4. On the **Cloud Product Services** tab, click **Create Service**.
5. In the Basic Information step, configure the parameters and click **Next**.
   - **Service Type**

     Select **Elastic Compute Service** of the **Computing** category from the first drop-down list and **ECS Instance** from the second drop-down list.
   - **Service Information**
     - **Service Name**: the name for the service. For example, you can enter ECS instance service.
     - **Service Description**: the description for the service. For example, when you create an ECS instance for all users in the baseservietest organization, disks, you can specify the specifications, disks and the number of ECS instances.
   - **Service Authorization**

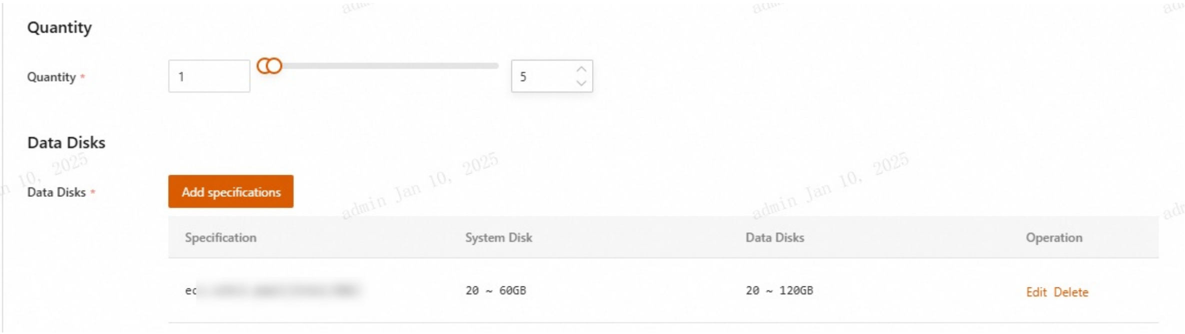
     Specifies which users of which organizations can access the service. For example, if you select **Specified Organization** and select the baseservietest organization from the **Authorized Organization** drop-down list, only users of this organization can access the service.
   - **Request Configuration**

This section displays the configuration details of the new purchase (create), configuration change, and unsubscription (release) of the service. If you want to configure an approval process, you can configure a process associated service in the process center after the service is created.

6. In the Form Parameter Configuration step, select attribute fields, configure their values, and then click **Next**.

   Examples:

   - In the Select Attribute Fields section, select **Specification** of the **Instance** category, **System Disk** and **Data Disks** in the **Storage** category, and **Quantity** in the **Basic Information** category.
   - In the **Data Disks** section, specify the specifications, system disk type and capacity, and data disk type and capacity.
   - If you set **Quantity** to 1 to 5, you can create a maximum of 5 ECS instances at a time.



Quantity

Quantity * 1 – 5

Data Disks

Data Disks *

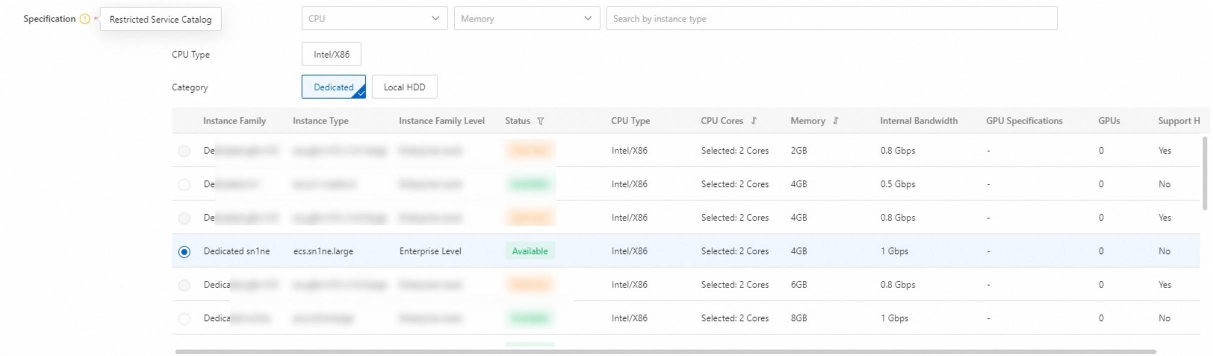
Specification	System Disk	Data Disks	Operation
ec[redacted]	20 ~ 60GB	20 ~ 120GB	Edit Delete

7. In the Pricing Configuration step, confirm the pricing rules and click **Submit**.
8. In the service list, find the service and click **Publish** in the Actions column to publish the service.

Impacts

If a user in the baseservietest organization select the preceding service catalog when he creates ECS instances, the ECS instances are subject to the service catalog restrictions.

Restrictions on specifications

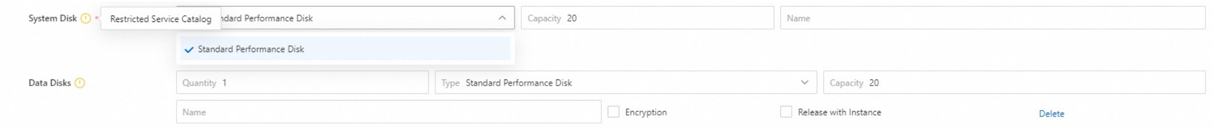


CPU Type: Intel/X86

Category: Dedicated (selected), Local HDD

	Instance Family	Instance Type	Instance Family Level	Status	CPU Type	CPU Cores	Memory	Internal Bandwidth	GPU Specifications	GPUs	Support H
○	De[redacted]	[redacted]	[redacted]	[redacted]	Intel/X86	Selected: 2 Cores	2GB	0.8 Gbps	-	0	Yes
○	De[redacted]	[redacted]	[redacted]	[redacted]	Intel/X86	Selected: 2 Cores	4GB	0.5 Gbps	-	0	No
○	De[redacted]	[redacted]	[redacted]	[redacted]	Intel/X86	Selected: 2 Cores	4GB	0.8 Gbps	-	0	Yes
●	Dedicated sn1ne	ecs.sn1ne.large	Enterprise Level	Available	Intel/X86	Selected: 2 Cores	4GB	1 Gbps	-	0	No
○	Dedica[redacted]	[redacted]	[redacted]	[redacted]	Intel/X86	Selected: 2 Cores	6GB	0.8 Gbps	-	0	Yes
○	Dedica[redacted]	[redacted]	[redacted]	[redacted]	Intel/X86	Selected: 2 Cores	8GB	1 Gbps	-	0	No

Restrictions on system disk type and capacity and data disk type and capacity

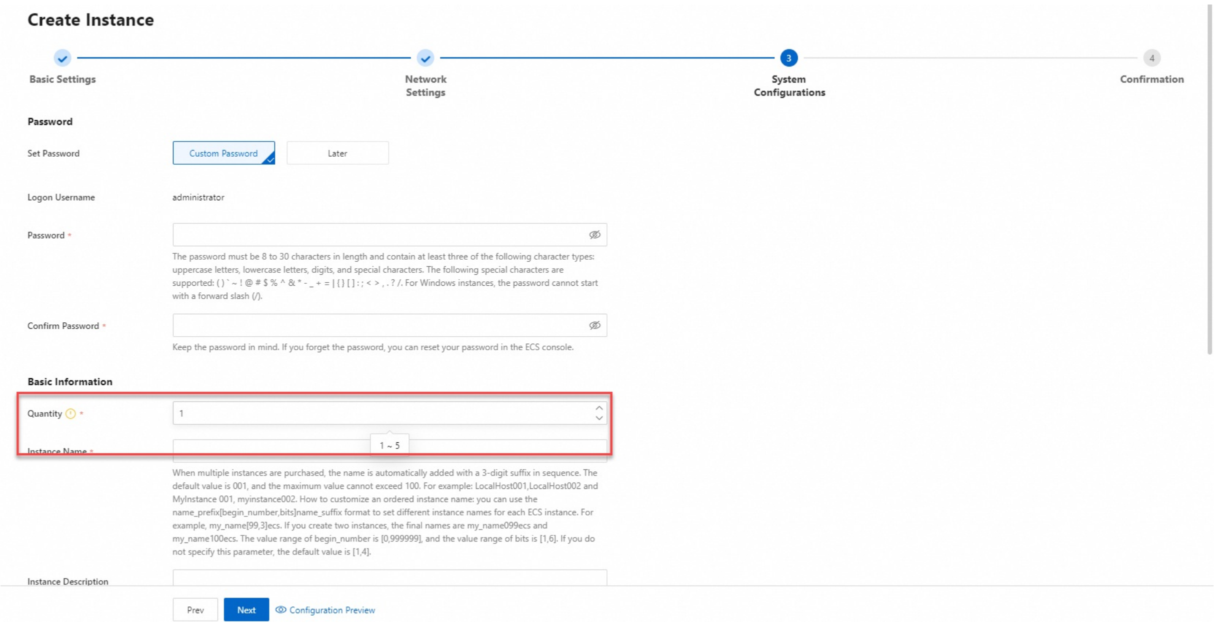


System Disk * Restricted Service Catalog: ndard Performance Disk; Capacity 20; Name

✓ Standard Performance Disk

Data Disks: Quantity 1; Type Standard Performance Disk; Capacity 20; Name; □ Encryption; □ Release with Instance

Restrictions on the number of ECS instances



Password

Set Password: Custom Password

Logon Username: administrator

Password *

The password must be 8 to 30 characters in length and contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The following special characters are supported: ( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; < > , . ? /. For Windows instances, the password cannot start with a forward slash (/).

Confirm Password *

Keep the password in mind. If you forget the password, you can reset your password in the ECS console.

Basic Information

Quantity * 1

Instance Name *

When multiple instances are purchased, the name is automatically added with a 3-digit suffix in sequence. The default value is 001, and the maximum value cannot exceed 100. For example: LocalHost001,LocalHost002 and MyInstance 001, myinstance002. How to customize an ordered instance name: you can use the name_prefix[begin_number,bits]name_suffix format to set different instance names for each ECS instance. For example, my_name[99,3]ecs. If you create two instances, the final names are my_name099ecs and my_name100ecs. The value range of begin_number is [0,999999], and the value range of bits is [1,6]. If you do not specify this parameter, the default value is [1,4].

Instance Description

6.3.3. Order management

6.3.3.1. Orders

On the Order List page, you can view the order history, including order status, date, and cost information, and track the progress of the order.

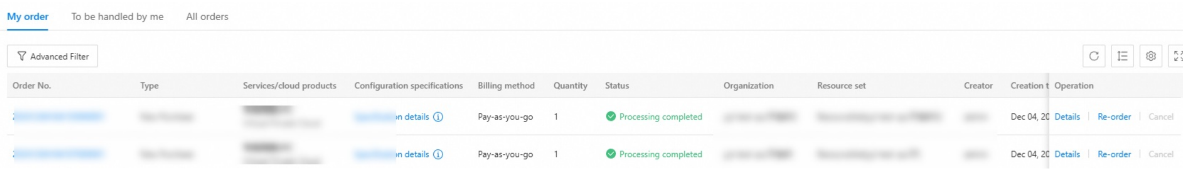
Background information

- Orders are generated in the following three scenarios:
  - Service activation: If you activate a cloud service for the first time, an instance is created in the corresponding console.
  - Configuration change: You can scale in, scale out, upgrade, or downgrade cloud service resources.
  - Unsubscription: You can unsubscribe from cloud services and release resources.
- A main order is generated for a cloud service, and a sub-order is generated for each cloud resource. If a service does not correspond to any cloud product, a main order is generated for it. By default, the sub-order information is not displayed in the main order details. The sub-order information is displayed as instance information.

My orders

The My Orders page displays only the orders created by you. You can place again and cancel orders.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Order Management** > **Orders**.
4. On the Orders page, click the **My Orders** tab.
5. In the order list, view all your historical orders and current orders.



Order No.	Type	Services/cloud products	Configuration specifications	Billing method	Quantity	Status	Organization	Resource set	Creator	Creation t	Operation
[redacted]	[redacted]	[redacted]	[redacted]n details ⓘ	Pay-as-you-go	1	✓ Processing completed	[redacted]	[redacted]	[redacted]	Dec 04, 20	Details | Re-order | Cancel
[redacted]	[redacted]	[redacted]	[redacted]n details ⓘ	Pay-as-you-go	1	✓ Processing completed	[redacted]	[redacted]	[redacted]	Dec 04, 20	Details | Re-order | Cancel

> **Note**
>
> Move the pointer over the ⓘ in the Specification Details column to view the specification details.

- **View order details**: Click an order number or click **Details** in the **Actions** column.

Parameter	Description
Basic Information	Displays the organization, resource set, region, creator, creation time, order type, and billing method of the order.
Service Information	Displays the service configuration information and instance activation details of the order. The service information is the sub-order information. The status of the main order is displayed based on the instance activation status of the sub-order. ▪ **Service Configuration**: displays the name, specifications, and billing method of the service. ▪ **Instance Details**: displays the details of the instances associated with the order. The instance snapshot information when the order is completed is displayed here. If the instance changes, the snapshot information remains unchanged. ▪ Overall service activation: ▪ Total: the total number of resources in the order. ▪ Completed: the number of created resources. ▪ Failed: the number of failed resources. For failed resources, you can click **Re-execute** or **Cancel** on the page. ▪ Canceled: the number of canceled resources. ▪ Update Time: the time of the last update, including the operation triggered in re-execution or cancellation. ▪ Instance Details list: displays the details of the ordered instances.
Implementation Progress	Displays the overall progress of the order.

- **Place again an order**: Click **Re-order** in the Actions column of the order to go to the Create Order page. When you place a new order, the original order information is carried.

> **Note**
>
> You can place again the **Purchase** orders.

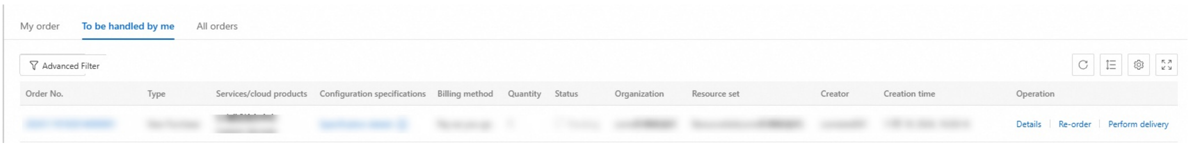
- **Cancel an order**: Click **Cancel** in the Actions column. After the order is canceled, the order is in the Canceled state.

  > **Note**
  >
  > You can cancel only the orders in the **Rejected** or **Being Approved** state.

Orders to be handled

The list displays all orders that are to be delivered by you.

- On the Orders page, click the **Orders to Be Handled** tab.
- In the order list, view all the orders to be handled by you.



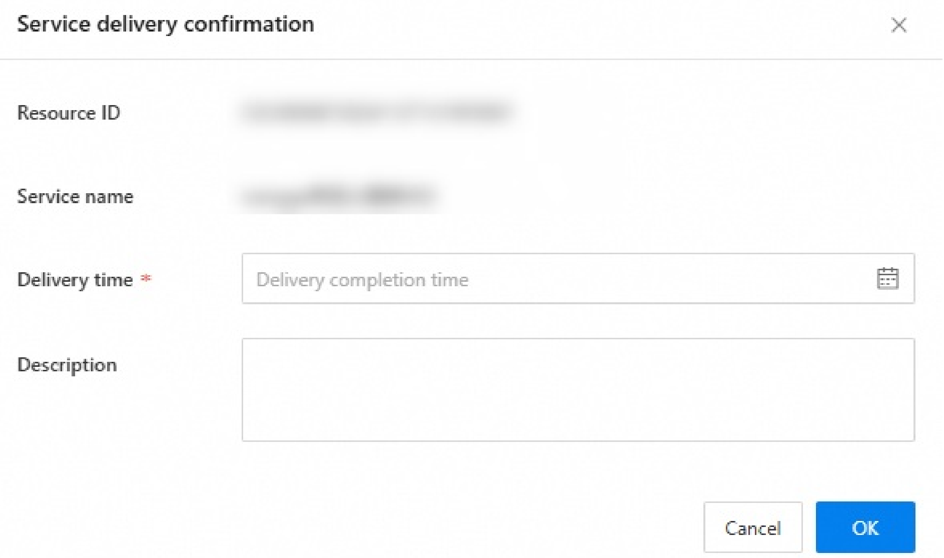
Order No.	Type	Services/cloud products	Configuration specifications	Billing method	Quantity	Status	Organization	Resource set	Creator	Creation time	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Details | Re-order | Perform delivery

> **Note**
>
> Move the pointer over the ⓘ in the Specification Details column to view the specification details.

- **View order details**: Click an order number or click **Details** in the **Actions** column.

Parameter	Description
Basic Information	Displays the organization, resource set, region, creator, creation time, order type, and billing method of the order.
Service Information	Displays the service configuration information and instance activation details of the order. The service information is the sub-order information. The status of the main order is displayed based on the instance activation status of the sub-order. ▪ **Service Configuration**: displays the name, specifications, and billing method of the service. ▪ **Instance Details**: displays the details of the instances associated with the order. The instance snapshot information when the order is completed is displayed here. If the instance changes, the snapshot information remains unchanged. ▪ Overall service activation: ▪ Total: the total number of resources in the order. ▪ Completed: the number of created resources. ▪ Failed: the number of failed resources. For failed resources, you can click **Re-execute** or **Cancel** on the page. ▪ Canceled: the number of canceled resources. ▪ Update Time: the time of the last update, including the operation triggered in re-execution or cancellation. ▪ Instance Details list: displays the details of the ordered instances.
Implementation Progress	Displays the overall progress of the order.

- **Deliver**: Click **Deliver** in the **Actions** column of the order. In the dialog box that appears, specify **Delivery Time** and **Description**, and then click **OK**.



Service delivery confirmation

Resource ID [redacted]

Service name [redacted]

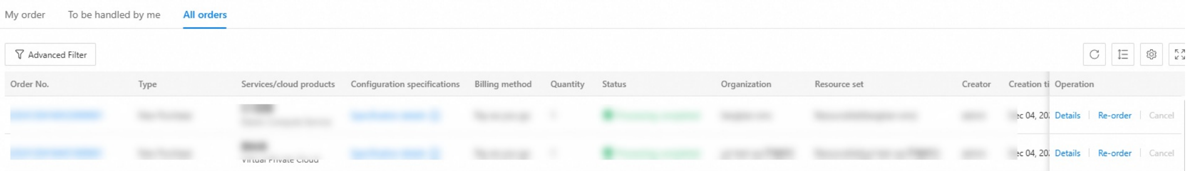
Delivery time * Delivery completion time

Description

All orders

The All Orders tab displays all orders on which you have the management permissions. The orders include global orders, the orders of the organization to which you belong and those of its sub-organizations, and the orders of the resource sets that you can manage. You can view all orders on which you have management permissions, but you can only place again and cancel orders that you create.

1. On the Orders page, click the **All Orders** tab.
2. In the order list, view all the orders on which you has the management permissions.



Order No.	Type	Services/cloud products	Configuration specifications	Billing method	Quantity	Status	Organization	Resource set	Creator	Creation ti	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ːc 04, 20ː	Details | Re-order | Cancel
[redacted]	[redacted]	[redacted] Virtual Private Cloud	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ːc 04, 20ː	Details | Re-order | Cancel

> **Note**
>
> Move the pointer over the ⓘ in the Specification Details column to view the specification details.

- **View order details**: Click an order number or click **Details** in the **Actions** column.

Parameter	Description
Basic Information	Displays the organization, resource set, region, creator, creation time, order type, and billing method of the order.
Service Information	Displays the service configuration information and instance activation details of the order. The service information is the sub-order information. The status of the main order is displayed based on the instance activation status of the sub-order. ▪ **Service Configuration**: displays the name, specifications, and billing method of the service. ▪ **Instance Details**: displays the details of the instances associated with the order. The instance snapshot information when the order is completed is displayed here. If the instance changes, the snapshot information remains unchanged. ▪ Overall service activation: ▪ Total: the total number of resources in the order. ▪ Completed: the number of created resources. ▪ Failed: the number of failed resources. For failed resources, you can click **Re-execute** or **Cancel** on the page. ▪ Canceled: the number of canceled resources. ▪ Update Time: the time of the last update, including the operation triggered in re-execution or cancellation. ▪ Instance Details list: displays the details of the ordered instances.

Implementation Progress	Displays the overall progress of the order.

- **Place again an order**: Click **Re-order** in the Actions column of the order to go to the Create Order page. When you place a new order, the original order information is carried.

  > **Note**
  >
  > You can place again the **Purchase** orders.

- **Cancel an order**: Click **Cancel** in the Actions column. After the order is canceled, the order is in the Canceled state.

  > **Note**
  >
  > You can cancel only the orders in the **Rejected** or **Being Approved** state.

6.3.4. Bill management

6.3.4.1. View the overview of service bills

The Product Billing Overview page displays the overview of monthly bills by service.

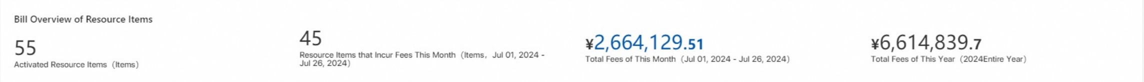
Background information

On the Product Billing Overview page, you can view the overview of bills and monthly bills by service.

- Bill Overview: allows you to select an accounting period and view the bill overview of resource items, resource item consumption trend, top 5 or top 10 resource items for which the most fees are charged, and consumption details of all resource items within the selected accounting period.
- Monthly Billing Overview: allows you select an accounting period and view all the bills of resource items within the selected accounting period. You can also view bill details by month or transaction. You can also export the bill data as a **.csv** file to your computer.

View the bill overview

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Bill Management** > **Product Billing Overview** to go to the **Product Billing Overview** page.
4. On the **Bill Overview** tab, select an accounting period from the **Accounting Period** drop-down list.
   - **Bill Overview of Resource Items**: displays the **number of activated resource items**, **number of resource items for which fees are charged in the selected month**, **total fees in the selected month**, and **total fees of the year**.



Bill Overview of Resource Items

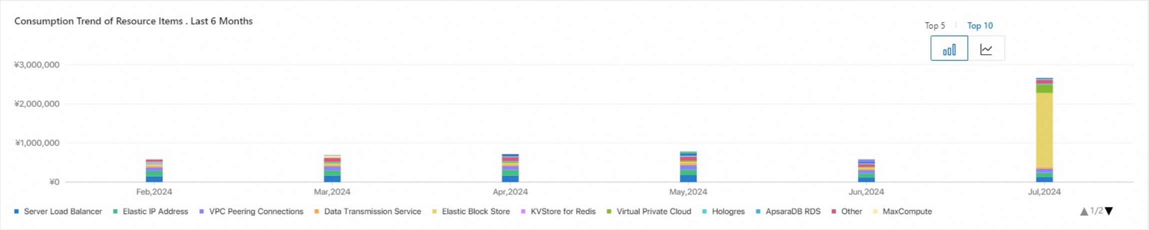
55
Activated Resource Items（Items）

45
Resource Items that Incur Fees This Month（Items，Jul 01, 2024 - Jul 26, 2024）

¥2,664,129.51
Total Fees of This Month（Jul 01, 2024 - Jul 26, 2024）

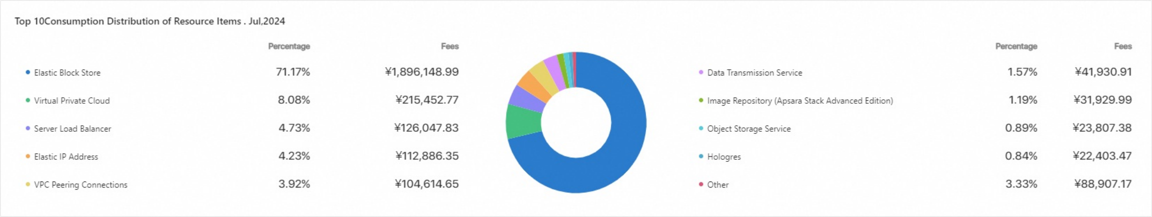
¥6,614,839.7
Total Fees of This Year（2024Entire Year）

- **Consumption Trend of Resource Items . Last 6 Months** : displays the consumption trend of each resource item in the selected month and the previous five months.



  - Click **Top 5** or **Top 10** in the upper-right corner to display the top 5 or top 10 resource items for which the most fees are charged each month.
  - Click the 📊 or 📈 icon to display the consumption trend of resource items in a column chart or a line chart.

- **Top 5 or Top 10 Consumption Distribution of Resource Items** : displays the fees and percentage of the fees that are charged for the top 5 or top 10 resource items in the selected month.



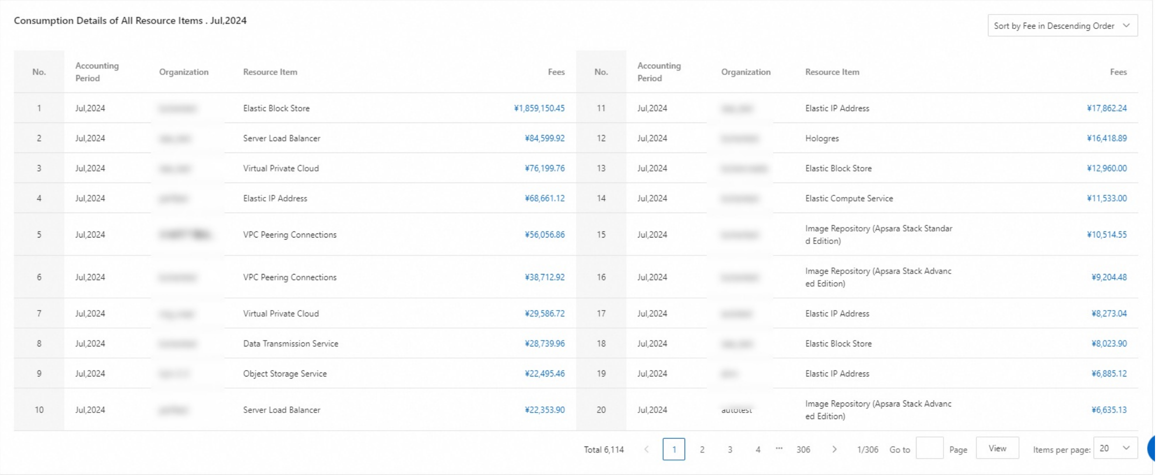
Top 10Consumption Distribution of Resource Items . Jul,2024

	Percentage	Fees
Elastic Block Store	71.17%	¥1,896,148.99
Virtual Private Cloud	8.08%	¥215,452.77
Server Load Balancer	4.73%	¥126,047.83
Elastic IP Address	4.23%	¥112,886.35
VPC Peering Connections	3.92%	¥104,614.65

	Percentage	Fees
Data Transmission Service	1.57%	¥41,930.91
Image Repository (Apsara Stack Advanced Edition)	1.19%	¥31,929.99
Object Storage Service	0.89%	¥23,807.38
Hologres	0.84%	¥22,403.47
Other	3.33%	¥88,907.17

- **Consumption Details of All Resource Items**: displays the fees that are charged for all resource items in each organization in the selected month.

  In the upper-right corner of the section, you can select **Sort by Fee in Descending Order** or **Sort by Fee in Ascending Order** .



Consumption Details of All Resource Items . Jul,2024

Sort by Fee in Descending Order

No.	Accounting Period	Organization	Resource Item	Fees	No.	Accounting Period	Organization	Resource Item	Fees
1	Jul,2024	[redacted]	Elastic Block Store	¥1,859,150.45	11	Jul,2024	[redacted]	Elastic IP Address	¥17,862.24
2	Jul,2024	[redacted]	Server Load Balancer	¥84,599.92	12	Jul,2024	[redacted]	Hologres	¥16,418.89
3	Jul,2024	[redacted]	Virtual Private Cloud	¥76,199.76	13	Jul,2024	[redacted]	Elastic Block Store	¥12,960.00
4	Jul,2024	[redacted]	Elastic IP Address	¥68,661.12	14	Jul,2024	[redacted]	Elastic Compute Service	¥11,533.00
5	Jul,2024	[redacted]	VPC Peering Connections	¥56,056.86	15	Jul,2024	[redacted]	Image Repository (Apsara Stack Standard Edition)	¥10,514.55
6	Jul,2024	[redacted]	VPC Peering Connections	¥38,712.92	16	Jul,2024	[redacted]	Image Repository (Apsara Stack Advanced Edition)	¥9,204.48
7	Jul,2024	[redacted]	Virtual Private Cloud	¥29,586.72	17	Jul,2024	[redacted]	Elastic IP Address	¥8,273.04
8	Jul,2024	[redacted]	Data Transmission Service	¥28,739.96	18	Jul,2024	[redacted]	Elastic Block Store	¥8,023.90
9	Jul,2024	[redacted]	Object Storage Service	¥22,495.46	19	Jul,2024	[redacted]	Elastic IP Address	¥6,885.12
10	Jul,2024	[redacted]	Server Load Balancer	¥22,353.90	20	Jul,2024	[redacted]	Image Repository (Apsara Stack Advanced Edition)	¥6,635.13

Total 6,114 ‹ 1 2 3 4 ··· 306 › 1/306 Go to Page View Items per page: 20

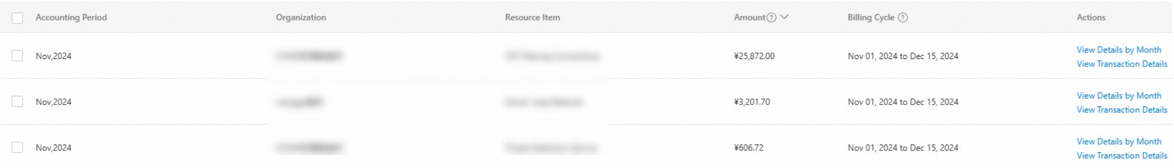
View the overview of monthly bills

1. On the **Product Billing Overview** page, click the **Monthly Billing Overview** tab.
2. Optional. Select an accounting period, resource item, and organization based on your business requirements, and click **Search**.

> **Note**
>
> You can enter the name of the resource item in the search box to efficiently search for the resource item.

3. In the bill list, view the bill information including the accounting period, organization, resource item, amount, and billing cycle.

   > **Note**
   >
   > - Find the bill that you want to view and click **View Details by Month** in the **Actions** column to go to the **Monthly Details** tab of the **Billing Details** page.
   > - Find the bill that you want to view and click **View flow details** in the **Actions** column to go to the **Flow Details** tab of the **Billing Details** page.



□	Accounting Period	Organization	Resource Item	Amount	Billing Cycle	Actions
□	Nov,2024	[redacted]	[redacted]	¥25,872.00	Nov 01, 2024 to Dec 15, 2024	View Details by Month View Transaction Details
□	Nov,2024	[redacted]	[redacted]	¥3,201.70	Nov 01, 2024 to Dec 15, 2024	View Details by Month View Transaction Details
□	Nov,2024	[redacted]	[redacted]	¥606.72	Nov 01, 2024 to Dec 15, 2024	View Details by Month View Transaction Details

4. Optional. Export the bill data as a **.csv** file to your computer.
   - Click **Export All Bills** to export all the queried bills.
   - Select the bills that you want to export and click **Export Selected Bills** to export the selected bills.

6.3.4.2. View the overview of organization bills

The Organization Bill Overview page displays the overview of monthly bills by organization and resource set.

Background information

On the Organization Bill Overview page, you can view the overview of bills and monthly bills by organization and resource set.

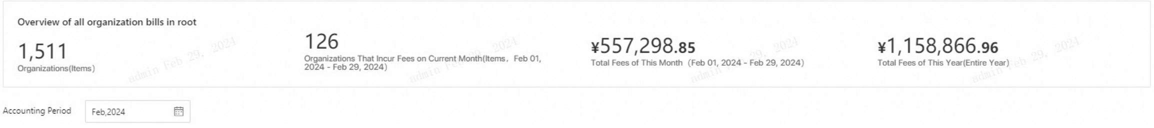
- Bill Overview: allows you to view the bill overview, organization consumption trend, top 5 or top 10 resource sets that generate the most fees, and consumption details of the organizations that you have the permissions to view within the selected accounting period.
- Monthly Billing Overview: allows you select an accounting period and view all the bills of organizations and resource sets within the selected accounting period. You can also view bill details by month or transaction. You can also export the bill data as a **.csv** file to your computer.

View the bill overview

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Bill Management** > **Organization Bill Overview** to go to the **Organization Bill Overview** page.
4. On the **Bill Overview** tab, select an accounting period from the **Accounting Period** drop-down list.

- **Overview of all organization bills in root**: displays the **number of organizations**, **number of organizations that incur fees in the selected month**, **total fees in the selected month**, and **total fees of the year**.

  > **Note**
  >
  > The operations administrator can view the bill overview of all organizations.

  Overview of all organization bills in root

  1,511
  Organizations(Items)

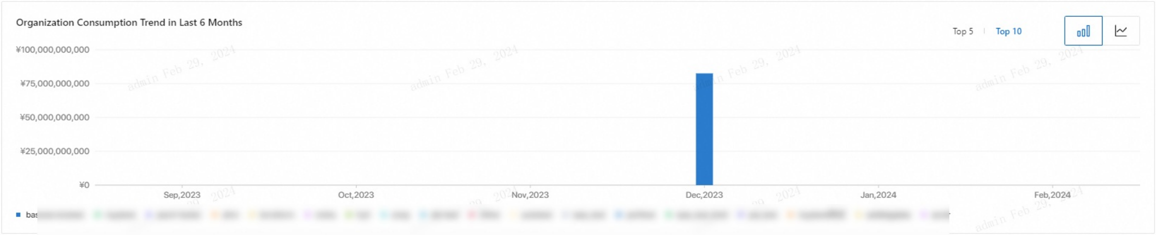
  126
  Organizations That Incur Fees on Current Month(Items, Feb 01, 2024 - Feb 29, 2024)

  ¥557,298.85
  Total Fees of This Month (Feb 01, 2024 - Feb 29, 2024)

  ¥1,158,866.96
  Total Fees of This Year(Entire Year)

  Accounting Period Feb,2024

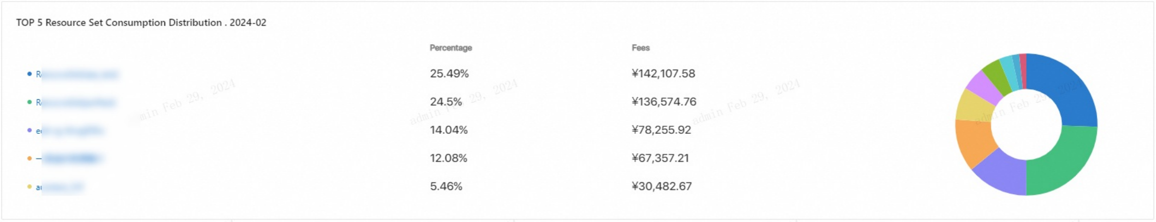
- **Organization Consumption Trends in Last 6 Months**: displays the consumption trend of each organization in the selected month and the previous five months.

  Organization Consumption Trend in Last 6 Months

  - Click **Top 5** or **Top 10** in the upper-right corner to display the top five or ten organizations that incur most fees each month.
  - Click the 📊 or 📈 icon to display the consumption trend of organizations in a column chart or a line chart.

- **Top 5 or Top 10 Resource Set Consumption Distribution**: displays the fees and percentage of the fees incurred by the top five or top ten organizations in the selected month.

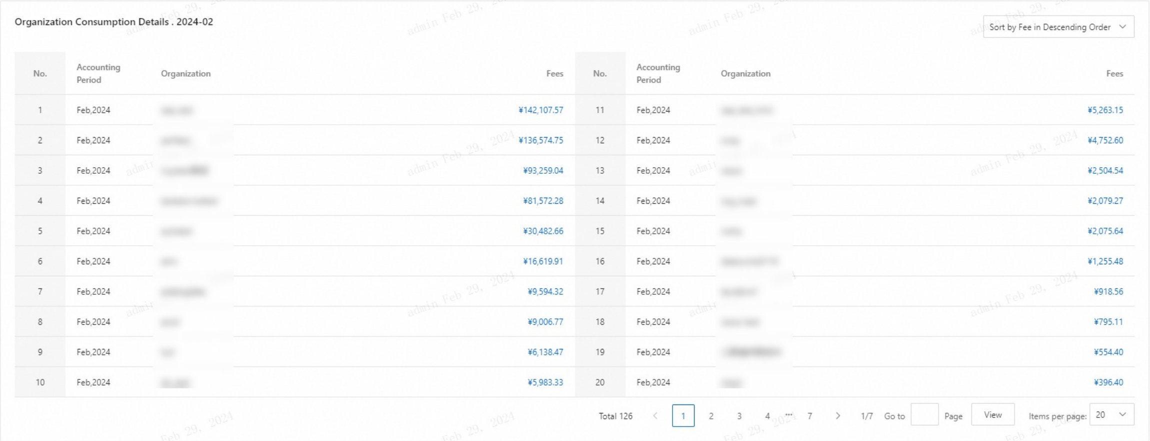
  

  TOP 5 Resource Set Consumption Distribution . 2024-02

	Percentage	Fees
[illegible]	25.49%	¥142,107.58
[illegible]	24.5%	¥136,574.76
[illegible]	14.04%	¥78,255.92
[illegible]	12.08%	¥67,357.21
[illegible]	5.46%	¥30,482.67

- **Organization Consumption Details**: displays the fees incurred by all organizations in the selected month.

  In the upper-right corner of the section, you can select **Sort by Fee in Descending Order** or **Sort by Fee in Ascending Order**.



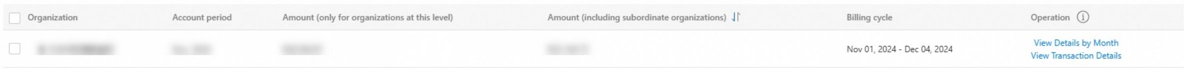
Organization Consumption Details . 2024-02

Sort by Fee in Descending Order

No.	Accounting Period	Organization	Fees	No.	Accounting Period	Organization	Fees
1	Feb,2024	[redacted]	¥142,107.57	11	Feb,2024	[redacted]	¥5,263.15
2	Feb,2024	[redacted]	¥136,574.75	12	Feb,2024	[redacted]	¥4,752.60
3	Feb,2024	[redacted]	¥93,259.04	13	Feb,2024	[redacted]	¥2,504.54
4	Feb,2024	[redacted]	¥81,572.28	14	Feb,2024	[redacted]	¥2,079.27
5	Feb,2024	[redacted]	¥30,482.66	15	Feb,2024	[redacted]	¥2,075.64
6	Feb,2024	[redacted]	¥16,619.91	16	Feb,2024	[redacted]	¥1,255.48
7	Feb,2024	[redacted]	¥9,594.32	17	Feb,2024	[redacted]	¥918.56
8	Feb,2024	[redacted]	¥9,006.77	18	Feb,2024	[redacted]	¥795.11
9	Feb,2024	[redacted]	¥6,138.47	19	Feb,2024	[redacted]	¥554.40
10	Feb,2024	[redacted]	¥5,983.33	20	Feb,2024	[redacted]	¥396.40

View the monthly bill overview of an organization

1. On the **Organization Bill Overview** page, click the **Organization Monthly Bill Overview** tab.
2. (Optional) Click Advanced Filter, select **Accounting Period** and **Organization**, and then click **Search** to filter data.
3. The bill list includes the **Organization**, **Accounting Period**, **Amount (only Current Organization Level)**, **Amount (Including Subordinate Organizations)**, and **Billing Cycle** columns.



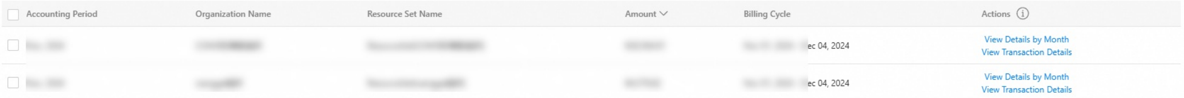
□	Organization	Account period	Amount (only for organizations at this level)	Amount (including subordinate organizations) ↓↑	Billing cycle	Operation ⓘ
□	[redacted]	[redacted]	[redacted]	[redacted]	Nov 01, 2024 - Dec 04, 2024	View Details by Month View Transaction Details

> **Note**
>
> - Click the ↓ icon next to **Amount (Including Subordinate Organizations)** to sort by amount in descending order.
> - Click the ↑ icon next to **Amount (Including Subordinate Organizations)** to sort by amount in ascending order.

- Find the bill that you want to view and click **View Details by Month** in the **Actions** column to go to the **Monthly Details** tab of the **Billing Details** page.
- Find the bill that you want to view and click **View Transaction Details** in the **Actions** column to go to the **Hourly Details** tab of the **Bill Details** page. After you are redirected to the Hourly Details page, the page displays the data of the first product by default due to the storage limits of the underlying layer.
- Click **Export All Bills** to export all the bills that meet the specified search conditions.
- Select the bills that you want to export and click **Export Selected Bills** to export the selected bills.

View the monthly bill overview of a resource set

1. On the **Organization Bill Overview** page, click the **Resource Set Monthly Bill Overview** tab.
2. (Optional) Click Advanced Filter, select **Accounting Period**, **Organization**, and **Resource Set**, and then click **Search** to filter data.
3. The bill list includes the **Accounting Period**, **Organization Name**, **Resource Set Name**, **Amount**, and **Billing Cycle** columns.



□	Accounting Period	Organization Name	Resource Set Name	Amount	Billing Cycle	Actions
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] ec 04, 2024	View Details by Month View Transaction Details
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] ec 04, 2024	View Details by Month View Transaction Details

> **Note**
>
> - Click the ↓ icon next to **Amount (Including Subordinate Organizations)** to sort by amount in descending order.
> - Click the ↑ icon next to **Amount (Including Subordinate Organizations)** to sort by amount in ascending order.

- Find the bill that you want to view and click **View Details by Month** in the **Actions** column to go to the **Monthly Details** tab of the **Billing Details** page.
- Find the bill that you want to view and click **View Transaction Details** in the **Actions** column to go to the **Hourly Details** tab of the **Bill Details** page. After you are redirected to the Hourly Details page, the page displays the data of the first product by default due to the storage limits of the underlying layer.
- Click **Export All Bills** to export all the bills that meet the specified search conditions.
- Select the bills that you want to export and click **Export Selected Bills** to export the selected bills.

6.3.4.3. Bill Details

The Bill Details page displays the bill details by month or hour. This helps you understand the bills within a specific period of time.

Background information

- Monthly Details: displays the bills of cloud instances in all organizations within a specific accounting period. You can view the following information about each bill: accounting period, cloud product, resource item, product type, organization, resource set, instance ID, label, specifications, region, billing cycle, consumption amount, and payable amount. You can also export monthly bills.
- Daily Details: displays the bills of cloud instances in all organizations within a specific accounting period. You can view the following information about each bill: instance ID, billing method, label, product type, cloud product, resource item, organization, resource set, region, consumption amount, discounted amount, payable amount, billing source, and start and end time. You can also export daily bills.
- Hourly Details: displays the bills of cloud instances in all organizations by hour within a specific accounting period. You can view the following information about each bill: instance ID, billing method, label, product type, cloud product, resource item, organization, resource set, region, consumption amount, discounted amount, payable amount, and start and end time. You can also export hourly bills.

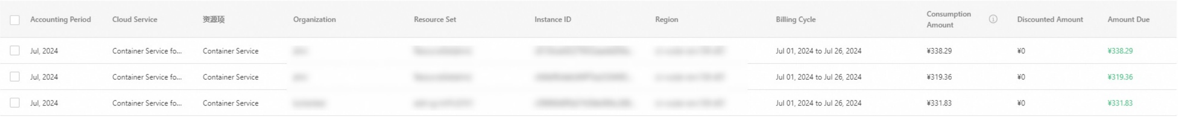
View monthly bill details

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Bill Management** > **Billing Details** to go to the **Billing Details** page.
4. On the **Bill Details** page, click the **Monthly Details** tab.

5. (Optional) Configure the **Accounting Period**, **Cloud Products**, **Resource Item**, **Organization**, **Resource Set**, **Region**, and **Instance ID** parameters and click **Search** to filter data.

> **Note**
>
> You can enter a product name in the search box to search for the product.

6. View monthly details in the list.



□	Accounting Period	Cloud Service	资源项	Organization	Resource Set	Instance ID	Region	Billing Cycle	Consumption Amount ⓘ	Discounted Amount	Amount Due
□	Jul, 2024	Container Service fo...	Container Service	[redacted]	[redacted]	[redacted]	[redacted]	Jul 01, 2024 to Jul 26, 2024	¥338.29	¥0	¥338.29
□	Jul, 2024	Container Service fo...	Container Service	[redacted]	[redacted]	[redacted]	[redacted]	Jul 01, 2024 to Jul 26, 2024	¥319.36	¥0	¥319.36
□	Jul, 2024	Container Service fo...	Container Service	[redacted]	[redacted]	[redacted]	[redacted]	Jul 01, 2024 to Jul 26, 2024	¥331.83	¥0	¥331.83

> **Note**
>
> - A label is set for a cloud instance.
> - Consumption amount = Payable amount - Free amount

- **Export details of all monthly bills**: Click **Export All Details**. In the **Create Report Export Task** dialog box, configure the **Report Name**, **Accounting Period**, **Organization**, **Resource Set**, **Cloud Products**, **Resource Item**, and **Region** parameters, and click **OK**. After the report export task is created, you can go to the **Download Report** page to view the task. The report type of the task is displayed as **Monthly Bill Report**.
- **Export details of selected bills**: Select the bills whose details you want to export and click **Export Selected Details** to export the selected bill details to your local device.

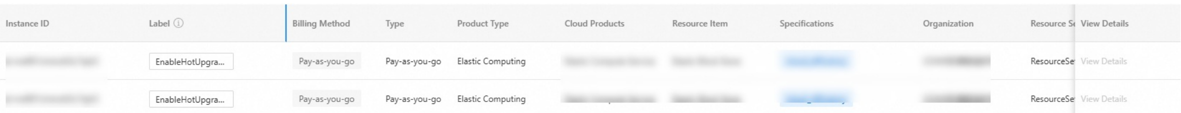
View daily bill details

1. On the **Bill Details** page, click the **Daily Details** tab.
2. (Optional) Configure the **Instance ID**, **Organization**, **Resource Set**, **Cloud Products**, **Resource Item**, **Region**, **Accounting Period**, **Start and End Time**, and **Billing Source** parameters and click **Search** to filter data.

> **Note**
>
> Bills can be generated by the system or manually reconciled.

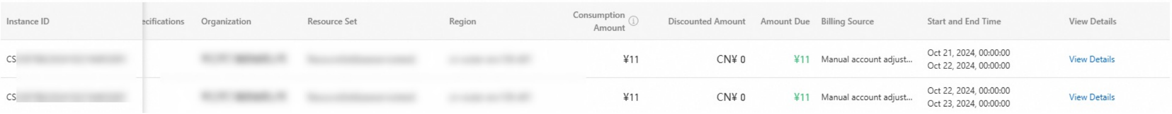
3. View daily details in the list.

System-generated bill details



Instance ID	Label ⓘ	Billing Method	Type	Product Type	Cloud Products	Resource Item	Specifications	Organization	Resource Se	View Details
[redacted]	EnableHotUpgra...	Pay-as-you-go	Pay-as-you-go	Elastic Computing	[redacted]	[redacted]	[redacted]	[redacted]	ResourceSe	View Details
[redacted]	EnableHotUpgra...	Pay-as-you-go	Pay-as-you-go	Elastic Computing	[redacted]	[redacted]	[redacted]	[redacted]	ResourceSe	View Details

Manually reconciled bill details



Instance ID	ecifications	Organization	Resource Set	Region	Consumption Amount ⓘ	Discounted Amount	Amount Due	Billing Source	Start and End Time	View Details
CS[redacted]		[redacted]	[redacted]	[redacted]	¥11	CN¥ 0	¥11	Manual account adjust...	Oct 21, 2024, 00:00:00 Oct 22, 2024, 00:00:00	View Details
CS[redacted]		[redacted]	[redacted]	[redacted]	¥11	CN¥ 0	¥11	Manual account adjust...	Oct 22, 2024, 00:00:00 Oct 23, 2024, 00:00:00	View Details

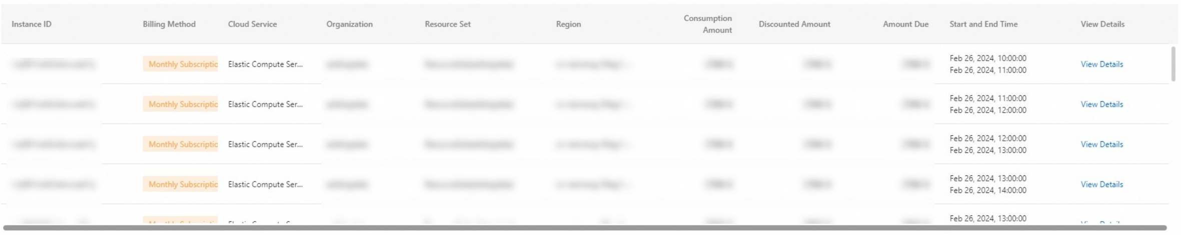
> **Note**
>
> - A label is set for a cloud instance.
> - The consumption amount is the expense incurred by an instance based on billing rules. The consumption amount of the refund type refers to the actual amount that should be refunded.
> - For manually reconciled bills, find a bill that you want to view and click **View Details** in the **Actions** column to view the bill details of the instance.

4. Click **Export Bill Details** in the upper part of the page. In the **Create Report Export Task** dialog box, configure the **Report Name**, **Organization**, **Resource Set**, **Cloud Products**, **Resource Item**, **Region**, and **Accounting Period** parameters, and then click **OK**.

> **Note**
>
> After the report export task is created, you can go to the **Download Report** page to view the task. The report type of the task is displayed as **Detailed Billing Report**.

View hourly bill details

1. On the **Bill Details** page, click the **Hourly Details** tab.
2. (Optional) Configure the **Instance ID**, **Organization**, **Resource Set**, **Cloud Products**, **Resource Item**, **Region**, **Accounting Period**, and **Start and End Time** parameters and click **Search** to filter data.
3. View hourly details in the list.



Instance ID	Billing Method	Cloud Service	Organization	Resource Set	Region	Consumption Amount	Discounted Amount	Amount Due	Start and End Time	View Details
[redacted]	Monthly Subscriptic	Elastic Compute Ser...	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Feb 26, 2024, 10:00:00 Feb 26, 2024, 11:00:00	View Details
[redacted]	Monthly Subscriptic	Elastic Compute Ser...	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Feb 26, 2024, 11:00:00 Feb 26, 2024, 12:00:00	View Details
[redacted]	Monthly Subscriptic	Elastic Compute Ser...	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Feb 26, 2024, 12:00:00 Feb 26, 2024, 13:00:00	View Details
[redacted]	Monthly Subscriptic	Elastic Compute Ser...	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Feb 26, 2024, 13:00:00 Feb 26, 2024, 14:00:00	View Details
[redacted]	[illegible]	[illegible]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Feb 26, 2024, 13:00:00	[illegible]

> **Note**
>
> - A label is set for a cloud instance.
> - The consumption amount is the expense incurred by an instance based on billing rules. The consumption amount of the refund type refers to the actual amount that should be refunded.
> - Find a bill that you want to view and click **View Details** in the **Actions** column to view the bill details of the instance.

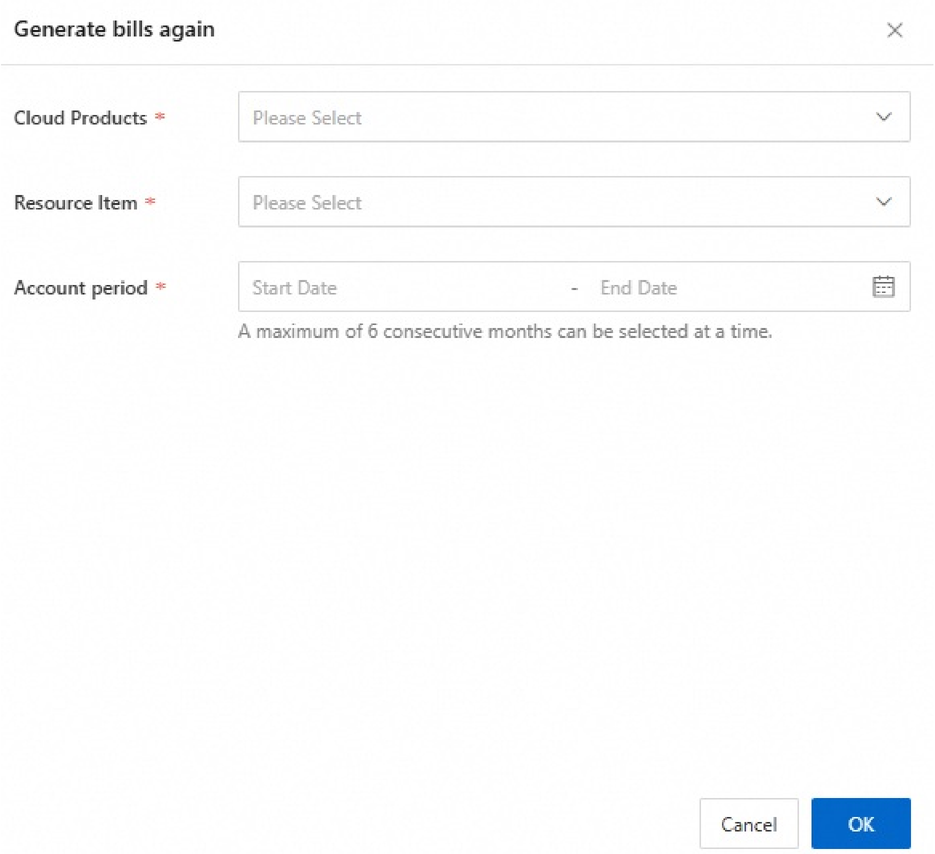
4. Click **Export Bill Details** in the upper part of the page. In the **Create Report Export Task** dialog box, configure the **Report Name**, **Organization**, **Resource Set**, **Cloud Products**, **Resource Item**, **Region**, and **Accounting Period** parameters, and then click **OK**.

> **Note**
>
> After the report export task is created, you can go to the **Download Report** page to view the task. The report type of the task is displayed as **Detailed Billing Report**.

Regenerate bills

> **Important**
>
> When you regenerate bills, the historical records remain unchanged, and only new records are added based on the reconciliation.

1. On the **Bill Details** page, click **Regenerate Bills** in the upper-right corner.
2. In the Regenerate Bills dialog box, configure the **Cloud Products**, **Resource Item**, and **Accounting Period** parameters, and then click **OK**.



Generate bills again

Cloud Products * Please Select

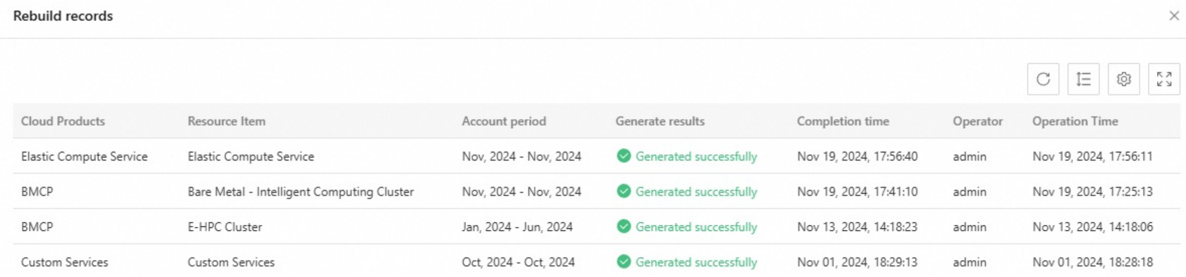
Resource Item * Please Select

Account period * Start Date - End Date

A maximum of 6 consecutive months can be selected at a time.

> **Note**
>
> - You can select values for the Cloud Products and Resource Item parameters.
> - You can select a maximum of six consecutive months for a single accounting period.
> - New bills are generated based on the current billing rules.
>   - Active records are added to the details based on the reconciliation.
>   - Expired records are removed from the details based on the reconciliation history.
>   - After new bills are generated, the monthly bill statistics are updated.

3. After new bills are generated, you can click **Regenerate Records** to view record details.



Rebuild records

Cloud Products	Resource Item	Account period	Generate results	Completion time	Operator	Operation Time
Elastic Compute Service	Elastic Compute Service	Nov, 2024 - Nov, 2024	✓ Generated successfully	Nov 19, 2024, 17:56:40	admin	Nov 19, 2024, 17:56:11
BMCP	Bare Metal - Intelligent Computing Cluster	Nov, 2024 - Nov, 2024	✓ Generated successfully	Nov 19, 2024, 17:41:10	admin	Nov 19, 2024, 17:25:13
BMCP	E-HPC Cluster	Jan, 2024 - Jun, 2024	✓ Generated successfully	Nov 13, 2024, 14:18:23	admin	Nov 13, 2024, 14:18:06
Custom Services	Custom Services	Oct, 2024 - Oct, 2024	✓ Generated successfully	Nov 01, 2024, 18:29:13	admin	Nov 01, 2024, 18:28:18

6.3.4.4. Bill Reconciliation

The Bill Reconciliation feature allows you to increase or decrease bill amounts when they are incorrect to ensure the accuracy of bills.

Background information

When bill amounts are incorrect, you can use the Bill Reconciliation feature to increase or decrease them for each instance. After you add bill reconciliation records, you must regenerate bills to show correct amounts in bills. You can also regenerate historical bills.

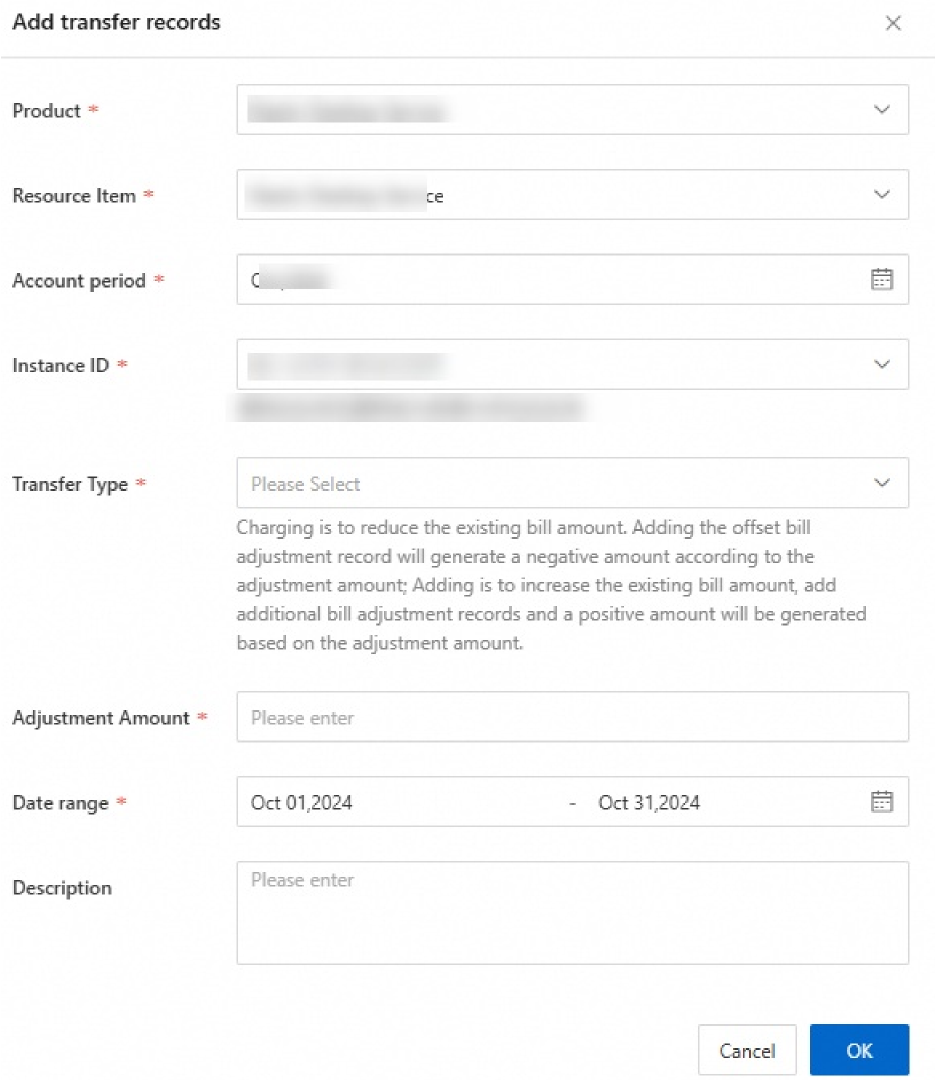
Add a reconciliation record

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Bill Management** > **Bill Reconciliation** to go to the **Bill Reconciliation** page.
4. Click **Add Reconciliation Record** in the upper part of the page.
5. In the **Add Reconciliation Record** dialog box, configure the parameters and click **OK**.

   By default, the new reconciliation record is in the Pending state.

Parameter	Description
Product	The product involved in the reconciliation.
Resource Item	The resource involved in the reconciliation.

Accounting Period	The accounting period involved in the reconciliation.
Instance ID	The instance involved in the reconciliation. **Note** If the instance ownership is changed, new bills are generated based on the current ownership. Modifying prices and pricing plans does not affect the generation of historical reconciliation records.
Reconciliation Type	Reconciliation types include **Decrease** and **Increase**. ◦ Decrease: You add a reconciliation record to decrease the amount of an existing bill, and a negative number is generated. The decreased amount is displayed as a negative number in red. ◦ Increase: You add a reconciliation record to increase the amount of an existing bill, and a positive number is generated. The increased amount is displayed as a positive number in blue.
Amount	The amount to be reconciled.
Date Range	The time range involved in the reconciliation.
Description	The description of the reconciliation.

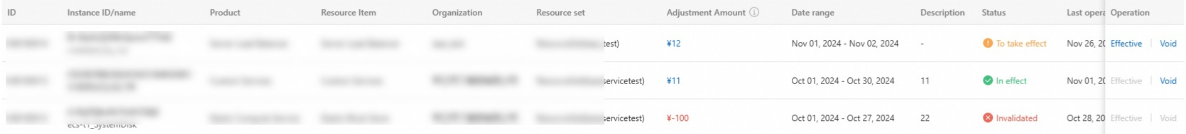


Add transfer records

Product *	[redacted]
Resource Item *	[redacted]ce
Account period *	C[redacted]
Instance ID *	[redacted] [redacted]
Transfer Type *	Please Select Charging is to reduce the existing bill amount. Adding the offset bill adjustment record will generate a negative amount according to the adjustment amount; Adding is to increase the existing bill amount, add additional bill adjustment records and a positive amount will be generated based on the adjustment amount.
Adjustment Amount *	Please enter
Date range *	Oct 01,2024 - Oct 31,2024
Description	Please enter

View reconciliation records

1. On the **Bill Reconciliation** page, click Advanced Filter, specify the ID, Instance ID, Instance Name, Product, Resource Item, Organization, Resource Set, and Status parameters, and then click Search to filter reconciliation records.
2. View reconciliation records in the list.



ID	Instance ID/name	Product	Resource Item	Organization	Resource set	Adjustment Amount ⓘ	Date range	Description	Status	Last opera	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]test)	¥12	Nov 01, 2024 - Nov 02, 2024	-	! To take effect	Nov 26, 20	Effective | Void
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]servicetest)	¥11	Oct 01, 2024 - Oct 30, 2024	11	✓ In effect	Nov 01, 20	Effective | Void
[redacted]	[redacted] ecs-t1_SystemDisk	[redacted]	[redacted]	[redacted]	[redacted]servicetest)	¥-100	Oct 01, 2024 - Oct 27, 2024	22	✕ Invalidated	Oct 28, 20	Effective | Void

Enable a reconciliation record

> **Important**
>
> - You can enable only reconciliation records in the Pending state.
> - After you enable a reconciliation record, you must click Regenerate Bills on the Bill Details page to regenerate bills. Bill details and reconciliation amounts are then added.

1. On the **Bill Reconciliation** page, click Advanced Filter, specify the ID, Instance ID, Instance Name, Product, Resource Item, Organization, Resource Set, and Status parameters, and then click Search to filter reconciliation records.
2. Find the reconciliation record and click **Enable** in the Actions column.
3. In the message that appears, click **OK**. The reconciliation record changes to the Effective state.

Disable a reconciliation record

> ⓘ **Important**
>
> You can disable only reconciliation records in the Pending or Effective state.
>
> - After a reconciliation record in the Pending state is disabled, you do not need to regenerate bills.
> - After you disable a reconciliation record in the Effective state, you must click Regenerate Bills on the Bill Details page to regenerate bills. Bill details related to the historical reconciliation record are then removed.

1. On the **Bill Reconciliation** page, click Advanced Filter, specify the ID, Instance ID, Instance Name, Product, Resource Item, Organization, Resource Set, and Status parameters, and then click Search to filter reconciliation records.
2. Find the reconciliation record and click **Disable** in the Actions column.
3. In the message that appears, click **OK**. The reconciliation record changes to the Ineffective state.

6.3.5. Pricing

6.3.5.1. Rule Overview

On the Rule Overview page, you can view the timeline of each billing configuration in the Apsara Uni-manager Management Console. The timeline displays the period during which the billing configuration takes effect.

Background information

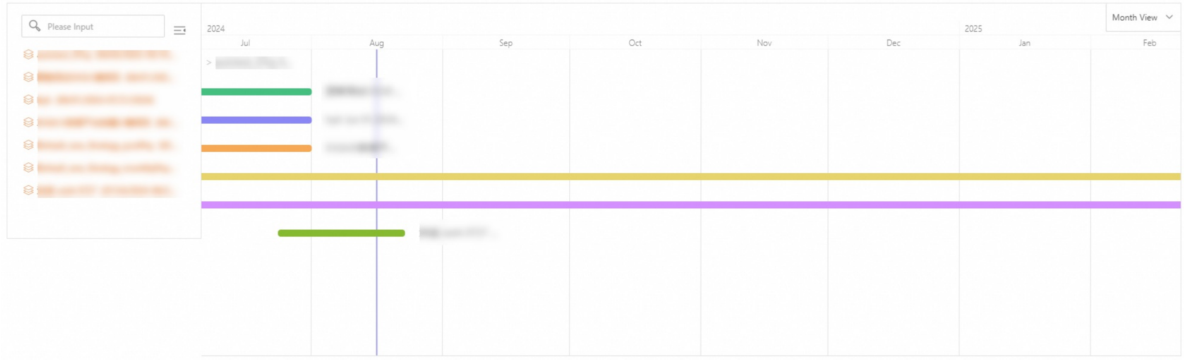
On the Rule Overview page, each billing configuration is displayed in a timeline, which displays the period during which the billing configuration takes effect. This helps you trace the historical billing configuration changes. You can also view billing configurations by day, week, month, quarter, and year. This helps enterprises more clearly and efficiently understand their costs and implement fine-grained operations and cost optimization.

Prerequisites

Billing configurations are created.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operation** > **Service Operations**.
3. In the left-side navigation pane, choose **Pricing** > **Rules**.
4. On the **Rule Overview** page, view the period during which each billing configuration takes effect in the Gantt chart.



> **Note**
>
> By default, billing configurations are displayed by month. The name of a billing configuration contains the time period during which the billing configuration takes effect.

- **Change the time span of the Gantt chart** : In the upper-right corner, select **Day View**, **Week View**, **Month View**, **Quarter View**, or **Year View** from the drop-down list.
- **Search for billing configurations**: In the navigation tree, enter a keyword in the search box above the billing configuration list.
- **View the details of a billing configuration**: In the navigation tree, find the billing configuration that you want to view and click its name. The **Billing Configuration Detail** page appears On the **Billing Configuration Detail** page, view the details of the billing configuration.

6.3.5.2. Manage billing configurations

You can configure the unit prices of cloud products based on the pricing policies or price agreements. The pay-as-you-go billing method is supported.

Background information

- You can configure billing configurations based on an hourly price, a daily price, or a monthly price.
- Billable items: Billable items are definitions of how a cloud service is charged, representing different dimensions of billing.

  For example, you are charged for ApsaraDB RDS based on specifications and storage. In this case, the specifications and storage are two billable items. Each billable item defines the billing method and unit price of a type of service.
- Pricing: The logic for determining the price of a particular feature of a cloud service per unit quantity is categorized into three types: fixed pricing, metered pricing, and tiered pricing.
  - Fixed pricing: Charges for each instance per hour are constant regardless of other variables within the predefined unit quantity.
  - Metered pricing: The pricing of a cloud service is determined based on its specifications and other characteristics. Prices vary based on different types or attribute values.
  - Tiered pricing: Different levels of usage for the same cloud service are associated with different pricing tiers. You can customize one or more numeric ranges and specify the pricing for each range.
- Quantity: Quantity refers to the amount of resource usage or quantity declared for a cloud service within each hour. Quantities are classified into fixed quantity and metered quantity.

- Fixed quantity: The number of instances is fixed in each metered data record. For example, you are charged for Elastic Compute Service (ECS) instances based on specifications, and each metered data record is generated for one instance. In this case, the instance quantity is fixed to 1.
- Metered quantity: The billing module uses the value of a specific numeric field in the metered data as the quantity for billing. For example, the value of the Storage field in the metered data for Object Storage Service (OSS) indicates the storage usage. If you want to charge users for OSS based on the storage usage, you can configure the Storage field as the quantity.

Create a billing configuration

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Pricing** > **Billing Rules**.
4. On the Rule Settings page, click **Create Billing Configuration**.
5. On the Create Billing Configuration page, configure the parameters in the Basic Information step and click **Next: Billing Configuration**. The following table describes the parameters.

Parameter	Description
Billing Configuration Name	The name of the billing configuration. The name must be 1 to 200 characters in length. **Note** Billing configuration names must be unique.
Effective Time	The start and end time of the validity period of the billing configuration. The effective time is accurate to date and excludes the specified end date. For example, if you set the start time to August 13, 2024 and the end time to August 15, 2024, the billing configuration takes effect at 00:00:00 on August 13, 2024 and expires after 00:00:00 on August 15, 2024.
Billing Method	The billing method that is specified for the billing configuration. Set the value to **pay-as-you-go**.
Plan Priority	A unique number that indicates the priority of the billing configuration. **Note** A larger number indicates a higher priority. This priority determines the sequence in which billing configurations are displayed. After a billing configuration is created, its display order is adjusted based on its priority.
Organization	The organization for which the billing configuration takes effect. Only level -1 organizations are supported. If you select root, all organizations are selected.

Remarks	The remarks of the billing configuration. The remarks must be 1 to 256 characters in length.

6. In the upper part of the **Billing Configurations** step, select a cloud service from the **Product Details** drop-down list.
7. Click **Pricing Configuration** in the **Actions** column to configure the billing rules.
   i. Configure the parameters described in the following table and click **Next**.

Parameter	Description
Cloud Service	The name of the cloud service for which you want to configure the billing rules.
Billing Method	The billing method of the cloud service.
Configure Filtering Condition	The filter condition type. Valid values: **Exact Match** and **Conditional Match**. ▪ **Exact Match**: All metered data is included in the billing, which results in the generation of a single bill. ▪ **Conditional Match**: You can select AND or OR. If you select AND, bills are generated if the metered data meets all the specified filter conditions. If you select OR, bills are generated if the metered data meets one of the specified filter conditions. **Note** If you select Conditional Match, you also need to specify filter conditions. A filter condition consists of a filter field and a filter value. You can add one or more filter conditions. If a metered data record has a filter field value that is the same as the predefined filter value, the metered data record meets the filter conditions. In this case, a bill is generated for the metered data record.

Price Type	The unit price that you want to use for the billing configuration. Valid values: **Monthly price**, **Sky-high price**, and **Hourly price**. - If you select **Monthly price**, you can use the following formulas to calculate the **hourly price**, **daily price**, and **annual price**: - Hourly price = Monthly price/30/24 - Daily price = Monthly price/30 - Annual price = Monthly price × 12 - If you select **Sky-high price**, you can use the following formulas to calculate the **hourly price**, **monthly price**, and **annual price**: - Hourly price = Daily price/24 - Monthly price = Daily price × 30 - Annual price = Monthly price × 12 - If you select **Hourly price**, you can use the following formulas to calculate the **daily price**, **monthly price**, and **annual price**. - Daily price = Hourly price × 24 - Monthly price = Daily price × 30 - Annual price = Monthly price × 12 **Note** - If the decimal cannot be completely divided, the amount after the seventh decimal place is automatically rounded off and not included in the unit price. After the hourly price or daily price is calculated, a deviation occurs from the monthly price. We recommend that you use the hourly price for the pay-as-you-go billing method. - 30 indicates the number of days in a calendar month. You need to replace it with the actual number of days in the current month based on the actual situation.

Billing Item Management	You can modify existing billable items or add one or more billable items. ▪ **Billable Item Name**: the name of the billable item. ▪ **Billing Method**: the billing method of the billable item. By default, the billing method is the same as that in the billing configuration. ▪ **Unit Price Settings**: the pricing mode. Valid values: **Fixed Price**, **Quantity-based Price**, and **Stepwise Pricing**. ▪ **Quantity Settings**: the amount of resource usage or quantity declared for the cloud service within each hour. Quantities are classified into fixed quantity and metered quantity. You can add one or more quantity settings. ▪ **Quantity Type**: For metered quantities, the count is based on the usage amount indicated by a specific specification field. For fixed quantities, the count is based on a user-defined value. **Important** If you set the Unit Price Settings parameter to Stepwise Pricing, you can set the Quantity Type parameter only to Quantity. ▪ **Quantity**: If you select Quantity, specify a specification field that is used for metering. If you select Fixed Quantity, specify a number. ▪ **Conversion Factor**: converts the quantity value and unit price into the same unit. **Note** The unit used to measure metered data may not be the same as that used to determine the price. Therefore, when you define a quantity, you need to specify a conversion factor to convert the value of a specific parameter in the metered data to a value in the unit of the price.

ii. In the Price Settings step, configure the parameters described in the following table and click **OK**.

Parameter	Description
Billable Items	The billable items.
Pricing Configuration	The price configuration of each billable item. You can modify the prices.
Unit	The price unit of the billable items.

8. After the billing rules are configured, click **Next: Billing Configuration Verification** .

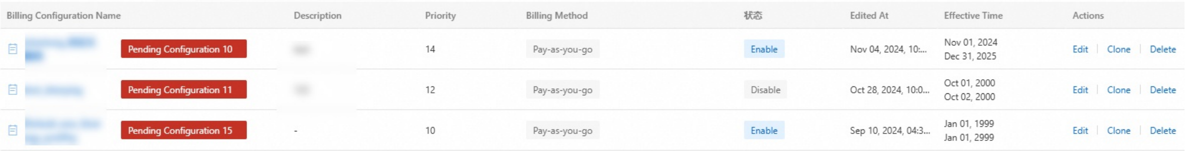
9. In the Billing Configuration Verification step, preview the billing configuration and click **Save**.

Parameter	Description
Cloud Product	The name of the cloud service.
Cloud Product Classification	The category to which the cloud service belongs.
Instance Type Configuration Ratio	The proportion of specifications in the current cloud service whose prices have been set to a number greater than 0.
Price Verification	Indicates whether the configuration ratio is 100%. **Note** If the configuration ratio of a service is smaller than 100%, Rejected is displayed. The parameter value is for reference only. You can create the billing configuration even if the configuration ratios of some services are smaller than 100%.

View a billing configuration

> **Note**
>
> When you create a billing configuration, the service list displays the services and specifications that support and use the billing configuration. If additional services and specifications are added later, **Pending Configuration** is displayed next to the billing configuration names on the Rule Settings page. On the details page of a billing configuration, **New** is displayed in the Product Details column, which prompts you to complete the billing configuration.

1. On the **Rule Settings** page, view the billing configurations that are created.

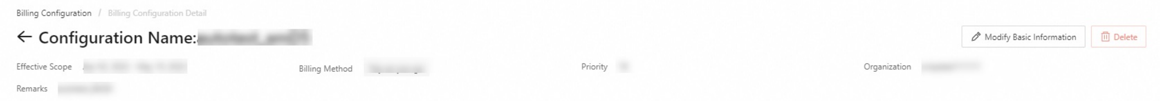


Billing Configuration Name	Description	Priority	Billing Method	状态	Edited At	Effective Time	Actions
[redacted] Pending Configuration 10	[redacted]	14	Pay-as-you-go	Enable	Nov 04, 2024, 10:...	Nov 01, 2024 Dec 31, 2025	Edit | Clone | Delete
[redacted] Pending Configuration 11	[redacted]	12	Pay-as-you-go	Disable	Oct 28, 2024, 10:0...	Oct 01, 2000 Oct 02, 2000	Edit | Clone | Delete
[redacted] Pending Configuration 15	-	10	Pay-as-you-go	Enable	Sep 10, 2024, 04:3...	Jan 01, 1999 Jan 01, 2999	Edit | Clone | Delete

2. Find the billing configuration that you want to manage and click its name. The **Billing Configuration Detail** page appears.

   - **View the basic information**

     In the upper part of the Billing Configuration Detail page, view the basic information about the billing configuration, including the **billing configuration name**, **effective scope**, **billing method**, **priority**, **organization**, and **remarks**.

     Billing Configuration / Billing Configuration Detail

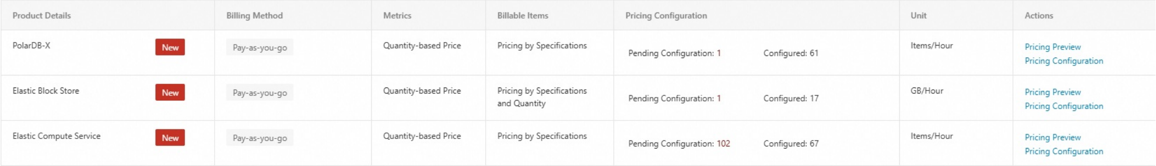
     ← Configuration Name:[redacted]

     Effective Scope [redacted] Billing Method [redacted] Priority [redacted] Organization [redacted]

     Remarks [redacted]

   - **View billing configuration details**

In the table of the Billing Configuration Detail page, view the billing details displayed in the following columns: **Product Details**, **Billing Method**, **Metrics**, **Billable Items**, **Pricing Configuration**, and **Unit**.

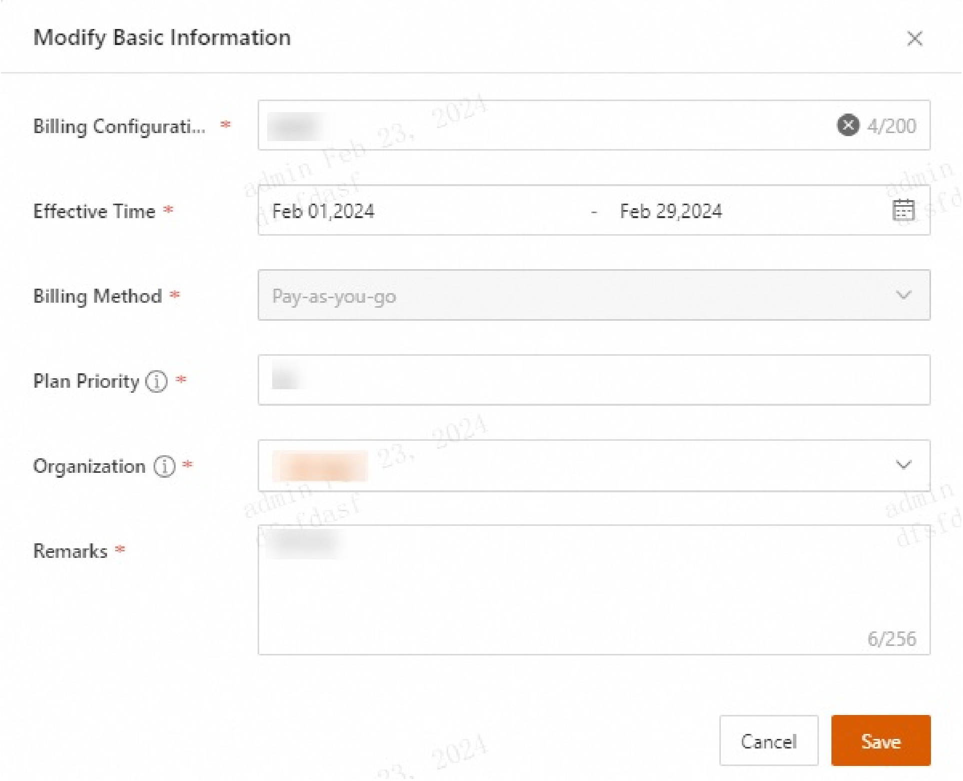


Product Details	Billing Method	Metrics	Billable Items	Pricing Configuration		Unit	Actions
PolarDB-X New	Pay-as-you-go	Quantity-based Price	Pricing by Specifications	Pending Configuration: 1	Configured: 61	Items/Hour	Pricing Preview Pricing Configuration
Elastic Block Store New	Pay-as-you-go	Quantity-based Price	Pricing by Specifications and Quantity	Pending Configuration: 1	Configured: 17	GB/Hour	Pricing Preview Pricing Configuration
Elastic Compute Service New	Pay-as-you-go	Quantity-based Price	Pricing by Specifications	Pending Configuration: 102	Configured: 67	Items/Hour	Pricing Preview Pricing Configuration

Modify the basic information about a billing configuration

If the basic information about a billing configuration changes, you can modify the basic information.

1. On the **Rule Settings** page, find the billing configuration that you want to modify and click **Edit** in the **Actions** column.
2. On the **Billing Configuration Detail** page, click **Modify Basic Information**.
3. In the **Modify Basic Information** dialog box, modify the **Billing Configuration Name**, **Effective Time**, **Plan Priority**, **Organization**, and **Remarks** parameters.



Modify Basic Information

Billing Configurati... * [redacted] 4/200

Effective Time * Feb 01,2024 - Feb 29,2024

Billing Method * Pay-as-you-go

Plan Priority * [redacted]

Organization * [redacted]

Remarks * [redacted] 6/256

4. Click **Save**.

Modify the unit prices or billable items for a billing configuration

If the unit prices or billable items in a billing configuration change, you can modify the unit prices or billable items.

1. On the **Rule Settings** page, find the billing configuration that you want to modify and click **Edit** in the **Actions** column.
2. On the **Billing Configuration Detail** page, view the information about the billing configuration.

3. Find the cloud service whose price configuration you want to modify and click **Pricing Configuration** in the **Actions** column.

> **Note**
>
> You can click **Pricing Preview** in the **Actions** column to preview the price configuration and billable items.

4. In the Pricing Configuration panel, modify the pricing configuration and billable items of the billing configuration based on your business requirements. For more information about the parameters, see the Create a billing configuration section of this topic.

Clone a billing configuration

You can clone an existing billing configuration to create a similar billing configuration.

1. On the **Rule Settings** page, find the billing configuration that you want to clone and click **Clone** in the **Actions** column.
2. On the Clone Billing Configuration page, modify the parameters of the existing billing configuration. For more information about the parameters, see the Create a billing configuration section of this topic.

> **Note**
>
> - Names of billing configurations must be unique. Therefore, you must modify the name.
> - The billing method is the same as that of the original billing configuration and cannot be modified.
> - Priorities of billing configurations must be unique. Therefore, you must modify the priority.

3. Click **Save**.

Enable a billing configuration

You can enable a billing configuration that is in the Disabled state.

1. On the **Rule Settings** page, find the billing configuration that you want to enable and click its name to go to the **Billing Configuration Detail** page.
2. In the upper part of the page, click ○ next to **Enable Configuration**.

> **Note**
>
> If the current billing configuration has products to be configured, configure products before you enable it.

3. Click **OK**. After the billing configuration is enabled, the status of the billing configuration changes to **Enabled**.

Disable a billing configuration

You can disable a billing configuration that is in the Enabled state.

1. On the **Rule Settings** page, find the billing configuration that you want to disable and click its name to go to the **Billing Configuration Detail** page.

2. In the upper part of the page, click next to **Enable Configuration**.

3. Click **OK**. After the billing configuration is disabled, the status of the billing configuration changes to **Disabled**.

Batch upload pricing configurations

You can batch upload pricing configurations only for a billing configuration that is in the Disabled state.

1. On the **Rule Settings** page, find the billing configurations that you want to manage and click its name to go to the **Billing Configuration Detail** page.
2. Click **Download Pricing Template** above the list to download the pricing template to your local computer.
3. In the local pricing template, configure the unit price information.

   > **Important**
   >
   > - The Primary Pricing Factor and Secondary Pricing Factor fields in the pricing template cannot be modified.
   > - By default, the Unit Price field in the pricing template is the price of one main pricing factor, and supports up to 6 decimal places. If an item is free of charge, set it to 0.
   > - If you want to change the pricing factors, modify the corresponding billable items.

4. Click **Batch Upload Pricing Configurations** above the list to upload the pricing template that you have configured.

Export the price list of a billing configuration

You can export the price list of a billing configuration if you want to save the billing configuration to your computer.

1. On the **Rule Settings** page, find the billing configuration that you want to export and click its name to go to the **Billing Configuration Detail** page.
2. In the Product Details drop-down list, select the cloud service whose billing configuration you want to export or select **All**. Then, click **Export Price List**.

> **Note**
>
> The exported price list of the billing configuration is in the **.xls** format. The spreadsheet contains the organization, export time, start and end time of the billing configuration, and the billing details of each service such as the billing method, pricing rule, billable items, billing fields, specifications, prices, counting method, counting field, unit, and conversion factor.

Delete a billing configuration

You can delete a billing configuration if you no longer need the billing configuration.

1. On the **Rule Settings** page, find the billing configuration that you want to delete and click **Delete** in the **Actions** column.

   Alternatively, click the name of the billing configuration that you want to delete. On the **Billing Configuration Detail** page, click **Delete**.

2. In the message that appears, click **OK**.

6.3.5.3. Manage discount rules

You can manage discount rules for specified organizations or products.

Discount rule permissions in different states

> **Note**
>
> Discount rules may be in the following states. Different operations can be performed in different states. In the following table, √ indicates that the operation is supported. × indicates that the operation is not supported.

Status/Operation	Details	Edit	Enable	Disable	Delete	Cancel	Request details
Enable	✓	X	X	✓	X	X	X
Disable	✓	✓	✓	X	✓	X	X
Enable (being approved for disabling)	✓	X	X	X	X	✓	✓
Enable (approval for disabling rejected)	✓	✓	X	✓	X	X	✓
Enable (failed to disable)	✓	✓	X	✓	X	X	X
Disable (being approved for enabling)	✓	X	X	X	X	✓	✓
Disable (approval for enabling rejected)	✓	✓	✓	X	✓	X	✓
Disable (failed to enable)	✓	✓	✓	X	✓	X	X

Prerequisites

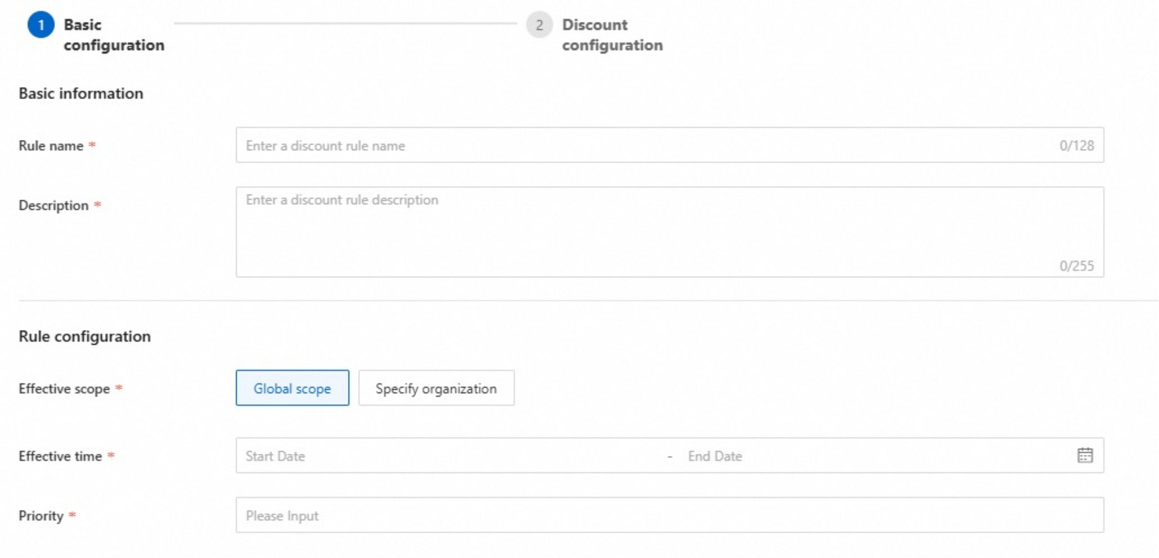
You have logged on to the Apsara Uni-manager Management Console as an operations administrator.

Create a discount rule

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Service Operations**.
3. In the left-side navigation pane, choose **Pricing** > **Discount Management**.
4. On the **Discount Management** page, click **Create Discount Rule**.

5. In the **Create Discount Rule** panel, configure parameters in the **Basic Configuration** and **Discount Configuration** step.

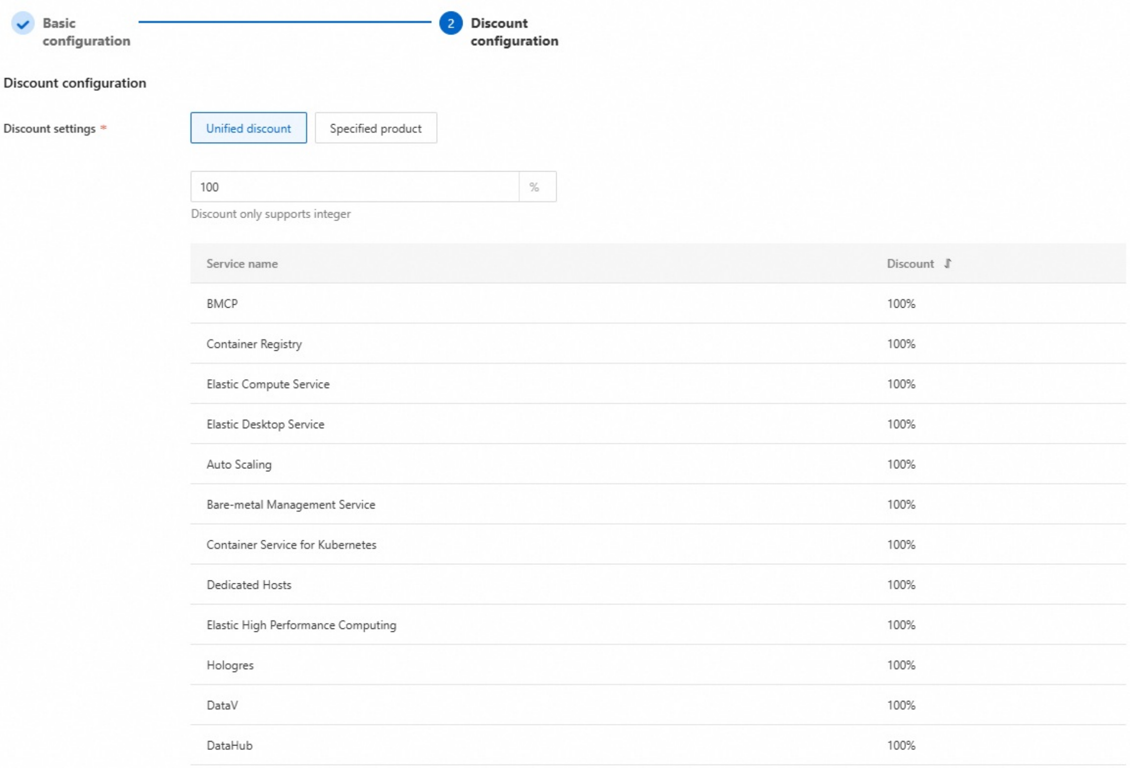
   i. **Basic Configuration**



Parameter		Description
Basic Information	**Rule Name**	The name of the discount rule. The name must be 2 to 128 characters in length. It cannot start or end with a space.
	Description	The description of the discount rule.
Rule Configuration	**Effective Scope**	The organizations for which the discount rule takes effect. Valid values: **Global** and **Specified Organization**.
	Specified Organization	This parameter is displayed only if the **Effective Scope** parameter is set to **Specified Organization**. Select an organization from the drop-down list. You can select multiple organizations.
	Effective Time	The time when the discount rule takes effect.
	Priority	The priority of the discount rule. Valid values: 0 to 99. Click the text box to display the existing priority values. **Note** You must enter a new priority value.

ii. **Discount Configuration**

- **Unified Discount**: By default, a unified discount is applied to all products. Enter a positive integer less than or equal to 1000 in the test box. Unit: %.



Discount configuration

Discount settings *   Unified discount   Specified product

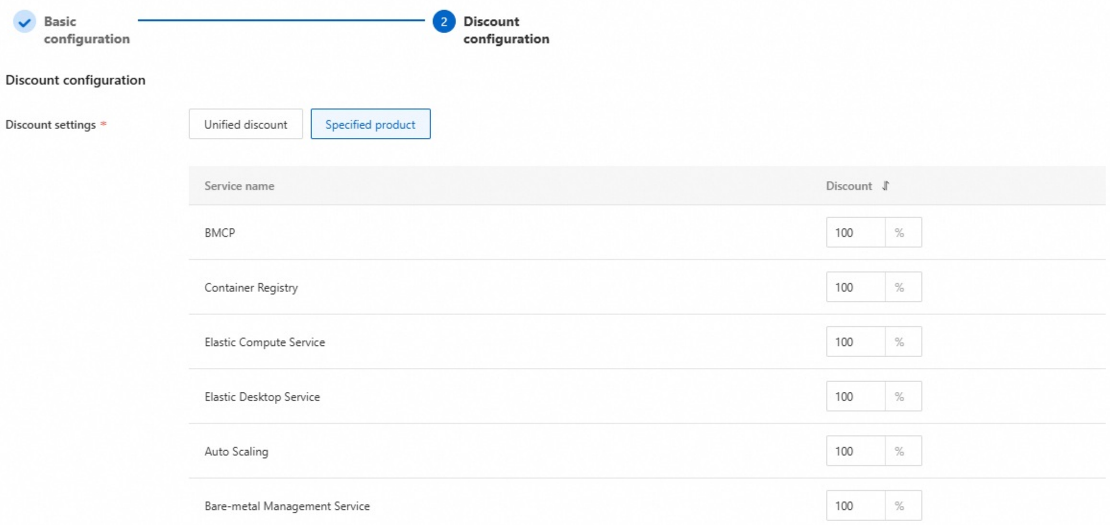
100 %

Discount only supports integer

Service name	Discount
BMCP	100%
Container Registry	100%
Elastic Compute Service	100%
Elastic Desktop Service	100%
Auto Scaling	100%
Bare-metal Management Service	100%
Container Service for Kubernetes	100%
Dedicated Hosts	100%
Elastic High Performance Computing	100%
Hologres	100%
DataV	100%
DataHub	100%

- **Specified Product**: The unified discount text box is not displayed. You must enter a positive integer less than or equal to 1000 (unit: %) next to each product.

> **Note**
>
> If a product is added to the cloud platform, the product is added to the discount rule with the 100% discount by default.



Discount configuration

Discount settings *   Unified discount   Specified product

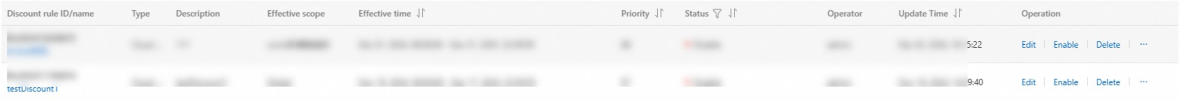
Service name	Discount
BMCP	100 %
Container Registry	100 %
Elastic Compute Service	100 %
Elastic Desktop Service	100 %
Auto Scaling	100 %
Bare-metal Management Service	100 %

iii. Click **Submit**.

View discount rules

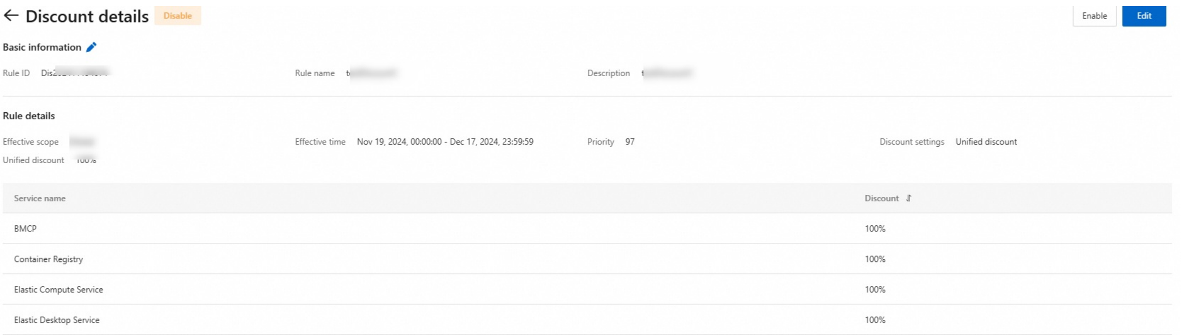
After discount rules are created, you can view them in the list.

1. On the **Discount Management** page, click Advanced Filter and specify **Discount Name** and **Organization** to filter discount rules.
2. The discount rule list contains the following columns: **Discount Rule ID/Name**, **Type**, **Description**, **Effective Scope**, **Effective Time**, **Priority**, **Status**, **Operator**, and **Update Time**.



Discount rule ID/name	Type	Description	Effective scope	Effective time	Priority	Status	Operator	Update Time	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]5:22	Edit | Enable | Delete | ···
[redacted] testDiscount I	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]9:40	Edit | Enable | Delete | ···

3. Click the name of a discount rule in the list. On the **Discount Details** page, you can view information in the **Basic Information** and **Rule Details** sections.



Basic information

Rule ID Dis[redacted]

Rule name t[redacted]

Description t[redacted]

Rule details

Effective scope [redacted]

Effective time Nov 19, 2024, 00:00:00 - Dec 17, 2024, 23:59:59

Priority 97

Discount settings Unified discount

Unified discount 100%

Service name	Discount
BMCP	100%
Container Registry	100%
Elastic Compute Service	100%
Elastic Desktop Service	100%

Edit a discount rule

1. On the **Discount Management** page, find the discount rule and click **Edit** in the **Actions** column.
2. In the **Edit Discount Rule** panel, modify the settings of the discount rule. For more information about the configuration items, see Create a discount rule.

Enable a discount rule

1. On the **Discount Management** page, find the discount rule and click **Enable** in the **Actions** column.
2. In the message that appears, click **OK**.

Disable a discount rule

> **Important**
>
> A discount rule will not be used in cost calculations after it is disabled.

1. On the **Discount Management** page, find the discount rule and click **Enable** in the **Actions** column.
2. In the message that appears, click **OK**.

Delete a discount rule

1. On the **Discount Management** page, find the discount rule and click **Enable** in the **Actions** column.
2. In the message that appears, click **OK**.

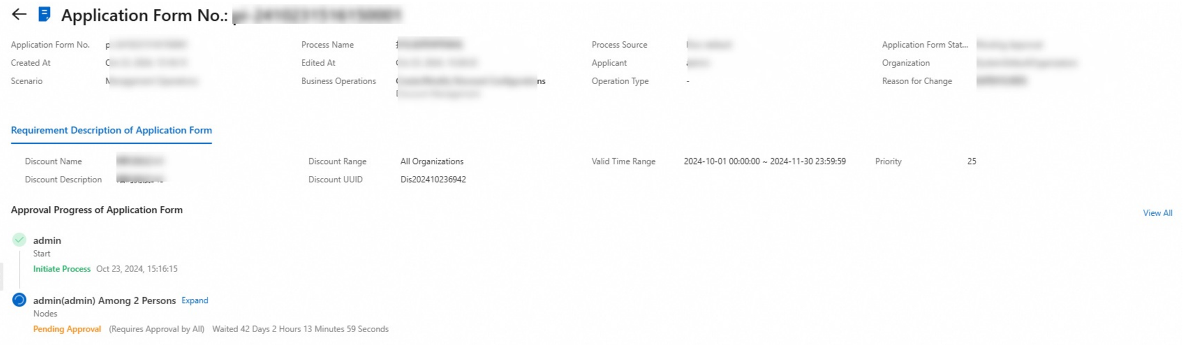
Revoke a discount rule

1. On the **Discount Management** page, find the discount rule, click □ in the **Actions** column, and select **Revoke**.
2. In the message that appears, click **OK**.

View the approval details of a discount rule

> **Important**
>
> Only after approval is enabled, you can view the approval details of the discount rules in the Being Approved or Approval Rejected state. For more information about how to create an approval process and how to bind an approval process to an operation, see Process approval.

1. On the **Discount Management** page, find the discount rule, click □ in the **Actions** column, and select **Approval Details**.
2. On the Approval Details page, view the approval details of the discount rule.



Application Form No.: [redacted]

Application Form No. [redacted]
Created At [redacted]
Scenario [redacted]
Process Name [redacted]
Edited At [redacted]
Business Operations [redacted]
Process Source [redacted]
Applicant [redacted]
Operation Type -
Application Form Stat... [redacted]
Organization [redacted]
Reason for Change [redacted]

Requirement Description of Application Form

Discount Name [redacted]
Discount Description [redacted]
Discount Range All Organizations
Discount UUID Dis202410236942
Valid Time Range 2024-10-01 00:00:00 ~ 2024-11-30 23:59:59
Priority 25

Approval Progress of Application Form

admin
Start
Initiate Process Oct 23, 2024, 15:16:15

admin(admin) Among 2 Persons
Nodes
Pending Approval (Requires Approval by All) Waited 42 Days 2 Hours 13 Minutes 59 Seconds

6.4. Portal management

6.4.1. Manage sites

You can manage all sites on the Sites page, including creating sites, configuring site navigations, publish or unpublish sites, and viewing all pages of sites.

Background information

A site is an independent web portal. An operations administrator can build an independent service portal by using the portal management feature to provide users with an all-in-one web portal to manage cloud services. A site displays multi-aspect information including column navigation and page content. This way, the internal and external organization service information can be managed and published in a centralized manner, the users of a cloud platform can experience the service capabilities and view the operation information about the cloud platform, and the efficiency of information communication is improved.

Procedure

1. Create a site: Configure the domain name and navigation settings of a site when you create the site. This ensures that a page can be directly associated with a site navigation when you create the page.

2. Build pages: Create pages, associate the pages with site navigations, configure the components and uploaded materials and data to complete the page building, and then publish the pages.
3. Publish the site: Check whether the site navigations are associated with pages on the Sites page, preview the display effect of the site, and then publish the site. After the site is published, check the display effect of the site to ensure that the site works as expected.

Prerequisites

You are an operations administrator.

Create a site

Configure the domain name and navigation settings of a site when you create the site. This ensures that a page can be directly associated with a site navigation when you create the page.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Portal Management**.
3. In the left-side navigation pane, click **Sites**.
4. On the **Sites** page, click **Create Site**.
5. In the **Create Site** dialog box, configure the required parameters in the following sections: Basic Information, Theme Color Configuration, Brand Configuration, and Logon Control.

Section and parameter		Description
Basic Information	**Site Name**	The custom name of the site.
	Description	The description of the site.
Theme Color Configuration	**Enable Gray Mode**	Specifies whether to enable the gray mode. The gray mode can be used on days of mourning, including the national mourning days and days on which serious disasters occur. The gray mode takes effect only for service portals. ◦ □: The gray mode is enabled. ◦ □: The gray mode is disabled.
	Recommended Theme Color	The theme color of the site. **Note** This parameter is displayed only if the gray mode is disabled.
	Browser Icon	The icon of the browser. Click **Upload Icon** to upload a browser icon. We recommended that you set the aspect ratio to 1:1 such as 32 × 32 pixels. Format: GIF, PNG, JPG, or JPEG. The image cannot exceed 2 MB in size.

Brand Configuration	**Platform Logo**	The logo of the cloud platform. Click **Upload Logo** to upload a platform logo. The platform logo is displayed in the upper left corner of the site navigations. We recommend that you upload an image of 160 × 36 pixels. Format: GIF, PNG, JPG, or JPEG. The image cannot exceed 2 MB in size.
	Version Information	The information about the site version. The version information is displayed on the footer and must be 1 to 40 characters in length.
	Copyright Declaration	The declaration of the copyright. The copyright declaration is displayed on the footer and must be 1 to 80 characters in length.
	Show Footer	Specifies whether to display the footer on the site pages. ◦ □: The footer is displayed. ◦ □: The footer is hidden.
Logon Control	**Logon**	Specifies whether to enable the logon feature. If you enable the logon feature, users are navigated to the logon page of the console when they visit the site. After they log on to the console, the user information page is displayed. ◦ □: The logon feature is enabled. ◦ □: The logon feature is disabled.
	Console Entry	Specifies whether to display the entry point of the console in the top navigation bar of the site. ◦ □: The entry point is displayed. ◦ □: The entry point is not displayed.

6. Click **OK**. By default, the site that you created is in the **Unpublished** state.

View site details

1. On the Sites page, view all sites created on the platform.
   - Enter a site name above the site list to efficiently filter sites by site name.
   - Click the ▽ icon next to the **Status** field to filter sites by status.

   - Click the ⇅ icon next to the **Publish Time** field to sort sites in ascending or descending order.

2. Click the name of a site to go to the site details page.
3. On the site details page, view the basic information, navigations, and associated pages of the site.
   - **Site Information**: displays the site name, status, description, modification event, publish time, unpublish time, publish and unpublish description, version information, copyright declaration, footer, theme color, browser icon, and platform logo.
   - **Navigation Configuration**: displays the navigation configurations of the site. For more information about how to configure a site navigation, see the Configure a site navigation section of this topic.
   - **Pages**: displays the pages associated with the site. For more information about how to configure a site page, see the Configure a site page section of this topic.

Modify the site information and site homepage

After a site is created, you can modify the site information based on your business requirements.

> **Important**
>
> You cannot modify the information or homepage of a site that is in the **Published** state.

1. On the Sites page, find the site that you want to manage and click **Modify** in the Actions column.
2. In the dialog box that appears, modify the basic site information, theme color configuration, and brand configuration based on your business requirements. For more information about the configuration items, see the Create a site section of this topic.

   > **Note**
   >
   > When you modify a site, you can configure the Site Homepage parameter in the Basic Information section to select a page as the site homepage based on your business requirements. Before you set the homepage, make sure that a page is created.

3. Click **OK**.

Configure a site navigation

1. On the Sites page, find the site that you want to manage and click its name to go to the site details page.
2. On the **Navigation Configuration** tab, click **Add**.
3. In the **Add Navigation** dialog box, configure the parameters described in the following table and click **OK**.

Parameter	Description
Navigation Name	The custom name of the navigation.

Parent Navigation	The parent navigation to which the navigation belongs.
Sorting	The display order of the navigation. A smaller value indicates a higher priority.
Navigation Type	The type of the navigation. Valid values:**Parent Navigation Group**, **Page Navigation**, and **Third-party Link**.
Associated Page	The page with which the navigation is associated. This parameter is displayed only if you set the **Navigation Type** parameter to **Page Navigation**. If no option is available in the drop-down list, create a page first.
Third-party Link	The URL of the third-party page with which the navigation is associated. This parameter is displayed only if you set the **Navigation Type** parameter to **Third-party Link**.
Open With	The method to go to the page with which the navigation is associated. This parameter is displayed only if you set the **Navigation Type** parameter to **Page Navigation**. Valid values: **Open in New Window** or **Open in Current Window**.
Display	Specifies whether to display the navigation and its child navigations. If you set the value to No, the navigation and child navigations are not displayed.

4. Modify or delete the navigation based on your business requirements.
   - Click **Modify** in the Actions column to modify the navigation configurations.
   - Click **Add Child Navigation** in the Actions column to add a child navigation to the current navigation.
   - Click **Delete** in the Actions column to delete the navigation.

Configure a site page

1. On the Sites page, find the site that you want to manage and click its name to go to the site details page.
2. On the **Pages** tab, click **Create Page**.
3. In the **Create Page** dialog box, configure the parameters described in the following table and click **OK**.

Parameter	Description
Page Name	The custom name of the page. The name must be 1 to 30 characters in length. The name must be unique.
Page Type	The type of the page. Set the value to**Low-code Building**.

Site	The site with which the page is associated. The site name is displayed by default.
Description	The description of the page. The description must be 1 to 200 characters in length.

4. Modify, remove, build, and preview the page based on your business requirements.
   - Click **Modify** in the Actions column to modify the basic configurations of the page.
   - Click **View Page** in the Actions column to view the published page.
   - Click **Remove** in the Actions column to remove the page from the associated site. After the page is removed, the page is no longer associated with the site.
   - Click **Build Page** in the Actions column to create and update the layout and content of the page.

Preview a site

After you configure the homepage, navigations, and page settings of a site, preview the site and check the display effect of the site to ensure that the site works as expected.

1. On the Sites page, find the site that you want to manage and click **Preview** in the Actions column.

   Alternatively, go to the site details page and click **Preview** in the upper-right corner.
2. On the page that appears, view the display effect of the site.

Publish a site

Before you publish a site, make sure that all navigations are associated with pages and the associated pages are published. You can preview the display effect of the site to ensure that the site works as expected before it is published.

> **Important**
>
> You can publish only sites in the **Unpublished** state.

1. On the Sites page, find the site that you want to manage, move the pointer over the icon in the Actions column, and then click **Publish**.

   Alternatively, go to the site details page and click **Publish** in the upper-right corner.
2. In the dialog box that appears, enter the description and click **OK**.

Unpublish a site

You can unpublish a site based on your business requirements. After a site is unpublished, users cannot view the site.

> **Important**
>
> You can unpublish only sites in the **Published** state.

1. On the Sites page, find the site that you want to manage, move the pointer over the icon in the Actions column, and then click **Unpublish**.

Alternatively, go to the site details page and click **Unpublish** in the upper-right corner.

2. In the dialog box that appears, enter the description and click **OK**.

Delete a site

You can delete a site if you no longer need it.

> ⓘ **Important**
>
> You can delete only sites in the **Unpublished** state.

1. On the Sites page, find the site that you want to delete and click **Delete** in the Actions column

   Alternatively, go to the site details page and click **Delete** in the upper-right corner.

2. In the message that appears, click **OK**.

Access a site

After a site is published, users can access and view the site content by using the URL of the site. Format: `https://portal.console.con.{rootDomain}/coms/portal/sites/{siteID}/pages/{pageID}` .

> ⓘ **Note**
>
> - https://portal.console.con.{rootDomain}: the domain name of the portal.
>
>   The prefix of a domain name is fixed to https://portal.console.con.. The complete domain name consists of the prefix and the obtained root domain name {rootDomain} such as xxx.shuguang.com.
>
> - /coms/portal/sites/{siteID}/pages/{pageID}: the path of the site homepage. You can view the homepage path on the Sites page.

By default, a platform has a preset site. The URL to access the preset site is `https://portal.console.con.{rootDomain}/coms/portal/sites/1/pages/1` .

6.4.2. Page management

6.4.2.1. Manage pages

During the lifecycle of a site, you can perform operations such as maintaining, updating, and optimizing the content and structure of the site pages based on your business requirements. This ensures the efficiency and accuracy of site information and good user experience.

Background information

Pages are important components of a site. Each page carries specific information or features to provide users with services. You can set a page as the homepage of a site or associate a page with the site navigation based on your business requirements.

Page permissions in different states

Note

Pages may be in the following states. Different operations can be performed in different states. In the following table, √ indicates that the operation is supported. × indicates that the operation is not supported.

Status/Operation	Modify	Preview	Build	Save (with updates)	Publish	Delete	Undo	Approval details
Draft	✓	✓	✓	✓	✓	✓	X	X
To be published as scheduled	X	✓	✓	X	X	X	✓	X
Draft (being approved for publication)	X	✓	✓	X	X	X	✓	✓
Draft (approval rejected)	✓	✓	✓	✓	✓	✓	X	✓
Draft (Publication failed)	✓	✓	✓	✓	✓	✓	X	X
Published	✓	✓	✓	✓	X	✓	X	X
Published (modifications to be published)	✓	✓	✓	✓	✓	✓	X	X
Published (modifications to be published as scheduled)	X	✓	✓	X	X	X	✓	X
Published (being approved for publishing modifications)	X	✓	✓	X	X	X	✓	✓
Published (approval for publishing modifications rejected)	✓	✓	✓	✓	✓	✓	X	✓

Published (failed to publish modifications)	✓	✓	✓	✓	✓	✓	X	X

Prerequisites

You are an operations administrator.

Create a page

You can create a page and configure the basic information about the page.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Portal Management**.
3. In the left-side navigation pane, choose **Page Management** > **Pages**.
4. On the **Pages** page, click **Create Page**.
5. In the **Create Page** dialog box, configure the basic information about the page.

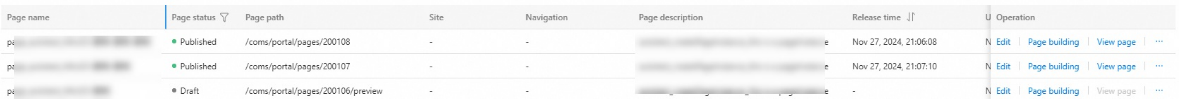
Parameter	Description
Page Name	The custom name of the page. The name must be 1 to 30 characters in length. The name must be unique.
Page Type	The type of the page. Set the value to**Low-code Building**.
Site	The site to which the page belongs. If no option is available in the drop-down list, go to the Sites page to create a site.
Page Description	The description of the page. The description must be 1 to 200 characters in length.

6. Click **OK**.

View the basic information and published content of pages

The Pages page displays all created pages.

1. On the Pages page, view all the created pages.
   - Search for a page by entering the page name or page description.
   - Click the ▽ icon next to the **Page Status** field to filter pages by status.
   - Click the ⇅ icon next to the **Release Time** field to sort pages in ascending or descending order.
2. View page information displayed in the following columns: **Page Name**, **Page Status**, **Page Path**, **Site**, **Navigation**, **Page Description**, **Release Time**, and **Update Time**.



Page name	Page status	Page path	Site	Navigation	Page description	Release time	U	Operation
pa[redacted]	● Published	/coms/portal/pages/200108	-	-	[redacted]e	Nov 27, 2024, 21:06:08	N	Edit | Page building | View page | ···
pa[redacted]	● Published	/coms/portal/pages/200107	-	-	[redacted]e	Nov 27, 2024, 21:07:10	N	Edit | Page building | View page | ···
pa[redacted]	● Draft	/coms/portal/pages/200106/preview	-	-	[redacted]e	-	N	Edit | Page building | View page | ···

Modify a page

You can modify the basic information about a page if the information needs to be updated.

1. On the **Pages** page, find the page and click **Modify** in the Actions column.
2. In the **Modify Page** dialog box, modify the page information based on your business requirements. For more information about the configuration items, see the Create a page section of this topic.

Build a page

You can configure the content and architecture of a page on the Build Page page.

1. On the **Pages** page, find the page and click **Build Page** in the Actions column.
2. On the **Build Page** page, add components and materials based on your business requirements to build the page.
    - Left side: displays the **Outline** and **Component** buttons.
        - Outline: The Outline panel displays the components that have been added to the page. You can move, clone, or delete the added components.
        - Component: The components that you can add to the page are displayed in the following categories: Page Information, Navigation, Card, Image and Text, Display Card, Display Component, and Others. Add components to the page.
    - Middle section: displays the added components. After you add a component, you can move it up or down, clone, and delete it.
    - Right side: displays the settings of the page and components.
        - Page settings: settings of the background color and background image.
            - Background color: You can enter a color code such as #d0021b in the field or click the color picker to select a background color.
            - Background image: You can upload an image or select an image from the image library.
        - Component settings: The configuration items vary based on the component. You can customize the settings based on your business requirements. After you select a component in the middle section, the related settings are displayed on the right. You can configure the component settings based on your business requirements.
3. After the page is built, click **Save** in the upper-right corner.

> **Note**
>
> - Click **Undo** or **Restore** to efficiently modify the page during the page building.
> - Click **Preview** to preview how the built page is displayed.
> - Click **Publish** to publish the built page.
> - Click **View Published Page** to view the content displayed on the published page.

Publish a page

> **Important**

> A page can be published multiple times. Each time a page is published, a version is generated to record the content of the published page.

1. On the **Pages** page, find the page, move the pointer over the icon in the Actions column, and then click **Publish**.

   Alternatively, on the Build Page page, built the page, click Save, and then click **Publish** in the upper-right corner.
2. In the Publish dialog box, set the Publication Time parameter and click **OK**.

   The Publication Time value can be **Now** or **Scheduled**.

   - **Now**: The page is updated in real time after you confirm the publication.
   - **Scheduled**: If you select Scheduled, you must set the time in the lower part of the page. The page content is updated at the specified time. If you want to modify the time when you select Scheduled, you must undo and then redo the republication.

Undo publication

1. On the **Pages** page, find the page, move the pointer over the icon in the Actions column, and then click **Undo**.
2. In the Undo message, click **OK**.

View approval details

> **Important**
>
> Only after approval is enabled, you can view the approval details of the pages in the Being Approved or Approval Rejected state. For more information about how to create an approval process and how to bind an approval process to an operation, see Process approval.

1. On the **Pages** page, find the page, move the pointer over the icon in the Actions column, and then click **View Approval Details**.
2. On the Approval Details page, view the approval details.

View a published page

> **Important**
>
> After a page enters the Published state, the page is published and you can view the published page.

1. On the **Pages** page, find the page and click **View Page** in the Actions column.

   Alternatively, go to the Build Page page and click **View Published Page** in the upper-right corner.
2. On the page that appears, view the display content of the published page.

Manage the versions of a page

1. On the **Pages** page, find the page, move the pointer over the icon in the Actions column, and then click **Version Management**.

2. In the Historical Version panel, view the historical versions of the page.
3. Optional. In the Historical Version panel, find the version and click **View** in the Actions column.
4. Click **Restore** in the Actions column to restore the page to the selected version. After the page is restored, you must publish the page again to make the page take effect.

Copy a page

You can copy a page to quickly add a page of the same content to the site.

1. On the **Pages** page, find the page, move the pointer over the □ icon in the Actions column, and then click **Copy**.
2. In the message that appears, click **OK**.

Delete a page

You can delete a page that you no longer need.

> **Important**
>
> Before you delete a page, disassociate the page from the corresponding site first.

1. On the **Pages** page, find the page, move the pointer over the □ icon in the Actions column, and then click **Delete**.
2. In the message that appears, click **OK**.

6.4.3. Material Center

On the Material Center page, you can upload, modify, and delete site materials based on your business requirements. The site materials include images and videos.

Background information

You can manage the material resources required by your site on the Material Center page. The materials include images and videos. This allows you to search for and use materials in an efficient manner during site management.

Prerequisites

You are an operations administrator.

Upload an image or video

You can upload the images and video materials required by your site to Material Center.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Portal Management**.
3. In the left-side navigation pane, click **Material Center**.
4. On the **Material Center** page, click **Upload Material**.
5. In the **Upload Material** dialog box, configure the **Material Name** and **Material Type** parameters and click **Upload Material** to upload a file.

   > **Important**
   >
   > - An image must meet the following requirements:

> - The image is of the GIF, PNG, JPG, JPEG, or GIF format.
> - The size of the image does not exceed 6 MB.
>
> - A video must meet the following requirements:
>   - The video is of a common video format. We recommend that you use the MP4, MKV, or MOV format.
>   - The resolution of the video must be 360p (640 × 360 pixels) or above.
>   - The size of the video does not exceed 5 GB.

6. Click **OK**.

Preview a material

After a material is uploaded, you can preview the uploaded material.

1. In the upper part of the **Material Center** page, enter a material name and select a material type to search for the material. Valid values of the Material Type parameter: All, Image, and Video.
2. The material card displays the type, format, and latest update time of the material. Move the pointer over the material card and click **Preview** to preview the material.

Update a material

You can update an image or video if the name or content of the material is changed.

> ⓘ **Important**
>
> You cannot modify preset materials.

1. Find the material that you want to modify, move the pointer over the material card, and then click **Edit**.
2. In the **Edit Material** dialog box, you can change the material name or upload a new file.
3. Click **OK**.

Delete a material

You can delete a material if you no longer need it.

> ⓘ **Important**
>
> - You cannot delete preset materials.
> - Before you delete a material, make sure that the material is not used on a site page.

1. Find the material that you want to delete, move the pointer over the material card, and then click **Delete**.
2. In the message that appears, click **OK**.

6.5. Service support

6.5.1. Document management

6.5.1.1. Manage documents

An operations administrator can maintain and update documents such as service manuals and usage specifications to control the query and display of documents.

Background information

As an operations administrator, you can update and maintain knowledge documents related to your cloud platform by using the document management feature. This allows you to manage documents in a centralized manner. Users can query and view knowledge documents and obtain relevant information. For example, users can query the usage specifications and process descriptions of a cloud service on the service portal and help center. This helps users obtain the latest knowledge and information at the earliest opportunity.

- Document list: displays all documents on the cloud platform.
- Document collection: displays the information about document collections. You can create, delete, modify, and move document collections. Document collections are classified into three levels. The first level corresponds to the document category, the second level corresponds to the document group, and the third level corresponds to child document collections.

Operation permissions on directories in different states

> **Note**
>
> Directories may be in the following states. Different operations can be performed in different states. In the following table, ✓ indicates that the operation is supported. × indicates that the operation is not supported.

Status/Operation	Delete	Revoke	View approval details	Launch	Withdraw	Move	Rename
Online	X	X	X	X	✓	X	✓
Online (Offline approval)	X	✓	✓	X	X	X	X
Online (rejected for offline approval)	X	X	✓	X	✓	X	✓
Online (offline failed)	X	X	X	X	✓	X	✓
Downline	✓	X	X	✓	X	✓	✓

Operation permissions on documents in different states

Note

Documents may be in the following states. Different operations can be performed in different states. In the following table, ✓ indicates that the operation is supported. × indicates that the operation is not supported.

States related to the editing and publishing of documents

Status/Operation	Edit	Publish	Copy	Delete	Undo	View approval details	Launch	Withdraw	Move	Rename	Version management
Draft	✓	✓	✓	✓	X	X	X	X	✓	✓	✓
Draft (release approval)	X	X	✓	X	✓	✓	X	X	✓	X	✓
Draft (rejected for release approval)	✓	✓	✓	✓	X	✓	X	X	✓	✓	✓
Draft (failed to publish)	✓	✓	✓	✓	X	✓	X	X	✓	✓	✓
Published	✓	X	✓	✓	X	X	✓	X	✓	✓	✓
Published (modified to be published)	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓
Published (modifying release approval)	X	X	✓	X	✓	✓	X	X	✓	X	✓
Published (modified release approval rejection)	✓	✓	✓	✓	X	✓	✓	X	✓	✓	✓

Published (failed to modify the release)	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓

Approval states of document publishing and unpublishing

Status/Operation	Edit	Publish	Copy	Delete	Revoke	View approval details	Launch	Withdraw	Move	Rename	Version management
Online	✓	✓	✓	X	X	X	X	✓	X	✓	✓
Online (Offline approval)	X	X	✓	X	✓	✓	X	X	X	X	✓
Online (rejected for offline approval)	✓	✓	✓	X	X	✓	X	✓	X	✓	✓
Online (offline failed)	✓	✓	✓	X	X	X	X	✓	X	✓	✓
Downline	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓
Offline (online approval is in progress)	X	X	✓	X	✓	✓	X	X	X	X	✓
Offline (online approval rejected)	✓	✓	✓	✓	X	✓	✓	X	✓	✓	✓
Offline (failed to go online)	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓

Prerequisites

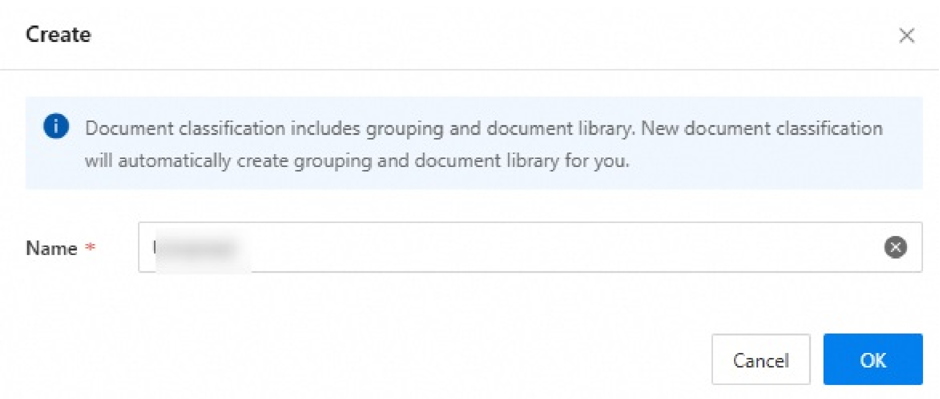
You are an operations administrator.

Manage document collections

Create a document category

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Operations** > **Support**.
3. In the left-side navigation pane, choose **Document Management** > **Documents**.
4. In the **Document Classification** section, click the + icon.
5. In the **Create** dialog box, enter a **name** for the document category and click **OK**.

> **Note**
>
> A document category includes document collections and groups. When you create a document category, a level-2 category and a level-3 category are automatically created in the corresponding directory. The level-2 category is a document group and the level-3 category is a child document collection. By default, a document category is displayed on the top of the corresponding directory tree in the **Document Classification** section after the document category is created.
>
> - The default name of the level-2 category is Default Group ({Document category name}).
> - The default name of the level-3 category is Default Document Collection ({Document category name}).


Create

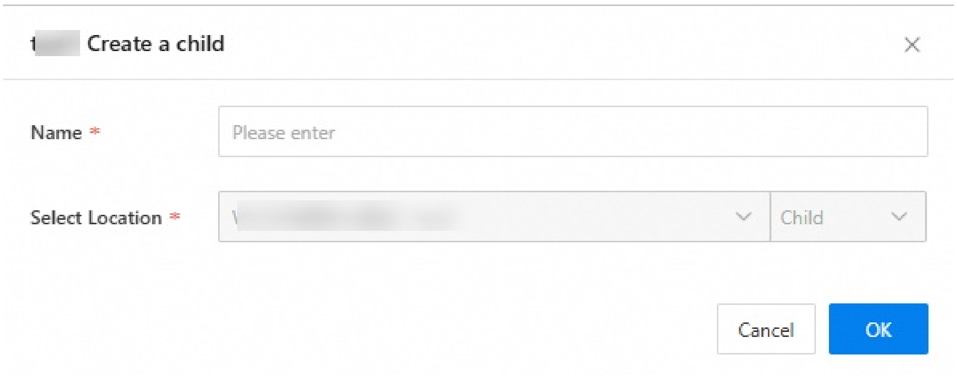
Document classification includes grouping and document library. New document classification will automatically create grouping and document library for you.

Name *

Create a document group

1. In the **Document Classification** section, find the level-1 document collection that you want to manage, move the pointer over the ... icon to the right of its name, and then click **Create a child**.
2. In the dialog box that appears, enter a **name** for the document group and click **OK**.

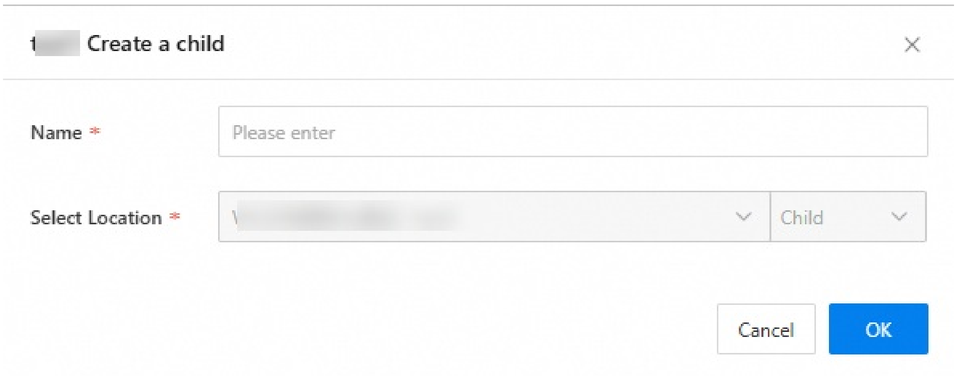
> **Note**
>
> You do not need to configure the **Select Location** parameter. This parameter is dimmed by default and indicates the document collection to which the document group belongs.



Create a child document collection

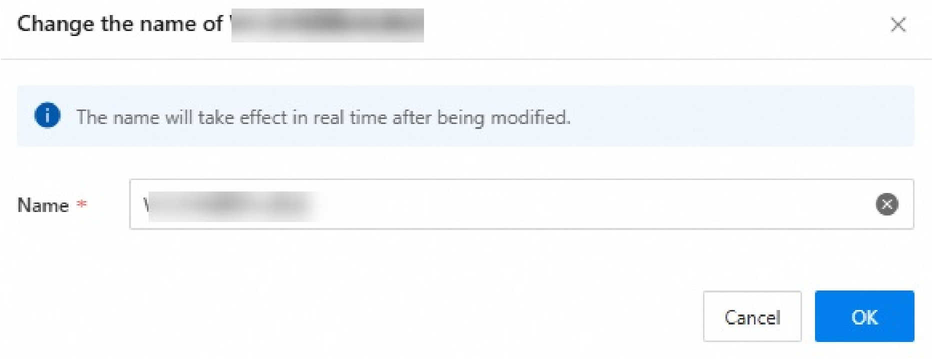
1. In the **Document Classification** section, find the document group that you want to manage, move the pointer over the ... icon to the right of its name, and then click **Create a child**.
2. In the dialog box that appears, enter a **name** for the child document collection and click **OK**.

   > **Note**
   >
   > You do not need to configure the **Select Location** parameter. This parameter is dimmed by default and indicates the document group to which the child document collection belongs.



Rename a document collection or document group

1. In the **Document Classification** section, find the document collection or document group that you want to rename, move the pointer over the ... icon to the right of its name, and then click **Rename**.
2. After you change the **name**, click **OK**.



Change the name of [redacted]

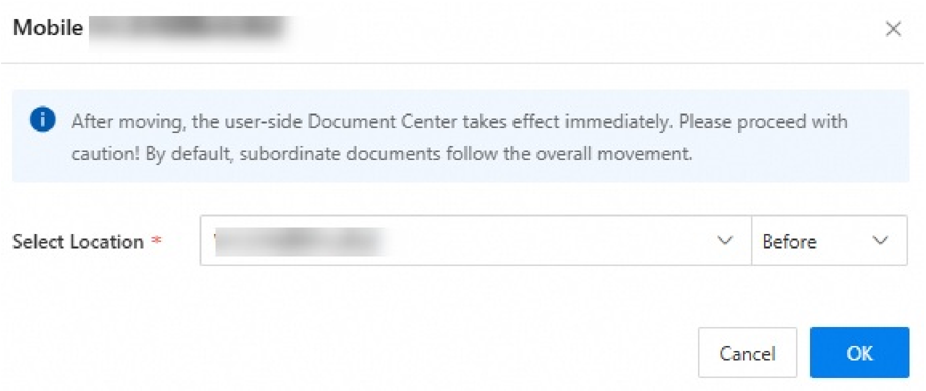
The name will take effect in real time after being modified.

Name * [redacted]

Move a document collection or document group

1. In the **Document Classification** section, find the document collection or document group that you want to move, move the pointer over the ... icon to the right of its name, and then click **Move**.
2. In the dialog box that appears, select the position at which you want the document collection or document group to be displayed and click **OK**.

> **Important**
>
> - You can change the positions of objects of the same level. If you change the position of a document collection, the documents in the document collection are moved accordingly.
> - You can choose to display an object before or after the specified directory.



Mobile [redacted]

After moving, the user-side Document Center takes effect immediately. Please proceed with caution! By default, subordinate documents follow the overall movement.

Select Location * [redacted] Before

Delete a document collection

> **Important**
>
> - After you delete a document category, the documents in the category are also deleted.
> - If a launched document exists in a document collection, the document collection cannot be deleted. You must withdraw the document first.
> - If the documents in a document collection are being approved, the document collection cannot be deleted.

1. In the **Document Classification** section, find the document collection that you want to delete, move the pointer over the ... icon to the right of its name, and then click **Delete**.

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

Manage documents or directories

Create a document or directory

> **Important**
>
> Documents and directories belong to different document categories. Before you create a document or directory, make sure that a document category is created.

1. In the **Document Classification** section, select a child document collection.
2. In the right-side document list section, click **Create**.
3. In the **Create a document** dialog box, configure the parameters and click **OK**.

Parameter	Description
Name	The name of the document or directory.
New type	Specifies whether to create a document or a directory. Valid values: **Document** and **Directory**.
Select Location	Optional. The position of the new document or directory. If you do not configure this parameter, the document or directory is used as the level-1 document or directory.

Rename a document or directory

1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to rename belongs.
2. In the right-side document list section, find the document or directory that you want to rename, move the pointer over the ··· icon in the **Operation** column, and then click **Rename**.

   You can also move the pointer over its name and click the ✎ icon.
3. In the dialog box that appears, enter a new name and click **OK**.

Move a document or directory

> **Important**
>
> - A document that has been launched cannot be moved.
> - A document or child document that is being reviewed for publishing or unpublishing cannot be moved.
> - A document cannot be moved to a directory in which documents or subdirectories are being reviewed for publishing or unpublishing.

1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to manage belongs.

2. In the right-side document list section, find the document or directory that you want to move and click **Mobile** in the **Operation** column.
3. In the dialog box that appears, specify the new position and click **OK**.

Edit the content of a document

1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to manage belongs.
2. In the right-side document list section, find the document that you want to edit, move the pointer over the ··· icon in the **Operation** column, and then click **Edit**.
3. On the **Document Details** page, edit the content of the document and click **Save and exit**.

Publish a document

1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to manage belongs.
2. In the right-side document list section, click the name of the document that you want to publish.
3. On the **Document Details** page, confirm the document content and click **Publish** in the upper-right corner.
4. In the dialog box that appears, enter a description and click **OK**. After the document is published, you can launch it in the document list.

Launch a document or directory

> **Important**
>
> Before a directory can be launched, the directory must contain documents that have been launched. If you launch an operation guide, all parent nodes are launched by default.

1. In the **Document Classification** section, click the child document collection to which the document that you want to launch belongs.
2. In the right-side document list section, find the document or directory that you want to launch and click **Go online** in the **Operation** column.
3. In the dialog box that appears, enter a description and click **Go online**.

Withdraw a document or directory

> **Important**
>
> If you withdraw an operation guide, all child nodes are withdrawn by default.

1. In the **Document Classification** section, click the child document collection to which the document that you want to withdraw belongs.
2. In the right-side document list section, find the document or directory that you want to withdraw and click **Downline** in the **Operation** column.
3. In the dialog box that appears, enter a description and click **Downline**.

Copy a document

1. In the **Document Classification** section, click the child document collection to which the document that you want to copy belongs.
2. In the right-side document list section, find the document that you want to copy, move the pointer over the ··· icon in the **Operation** column, and then click **Copy**.

View the approval details of a document

> **Important**
>
> Only after approval is enabled, you can view the approval details of the documents that are in the Being Approved or Approval Rejected state. For more information about how to create an approval process and how to bind an approval process to an operation, see Process approval.

1. In the **Document Classification** section, click the child document collection to which the document that you want to manage belongs.
2. Move the pointer over the ··· icon in the **Actions** column of a document and select **Approval details**. The **Approval Details** page appears by default.
3. On the **Approval Details** page, view the approval details.

Revoke the publishing, launching, or withdrawal operation performed on a document or directory

> **Important**
>
> If a document or directory is associated with an approval process during a publishing, launching, or withdrawal operation, you can revoke the operation in the corresponding approval state.

1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to manage belongs.
2. In the right-side document list section, find the document or directory that you want to manage, move the pointer over the ··· icon in the **Operation** column, and then click **Revoke**.
3. In the dialog box that appears, click **Revoke**.

Manage the versions of a document

1. In the **Document Classification** section, click the child document collection to which the document that you want to manage belongs.
2. In the right-side document list section, find the document that you want to manage, move the pointer over the ··· icon in the **Operation** column, and then click **Version Management**.
3. On the left side of the Version Management page, view the historical versions of the document.
4. Select a version and click **Restore to current version** in the upper part of the page to restore the document to the selected version. After the document is restored, you must publish the document again to make the document take effect.

Delete a document or directory

> **Important**
>
> - Documents or directories that have been launched or are being approved cannot be deleted.

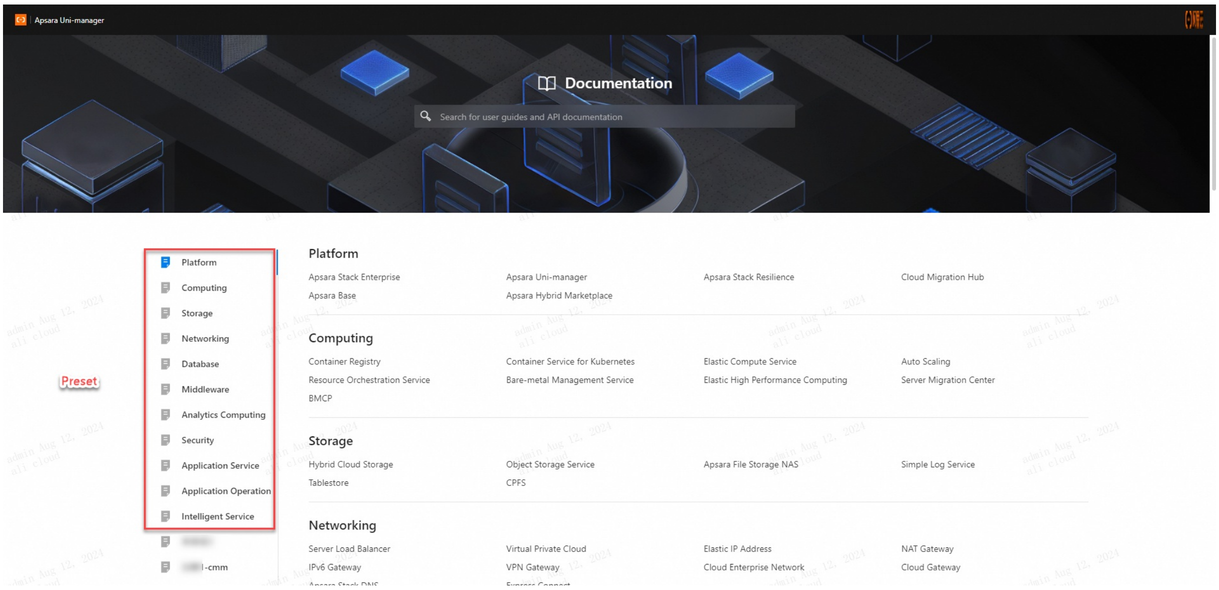
1. In the **Document Classification** section, click the child document collection to which the document or directory that you want to delete belongs.
2. In the right-side document list section, find the document or directory that you want to delete, move the pointer over the ··· icon in the **Operation** column, and then click **Delete**.
3. In the message that appears, click **Delete**.

Access documentation

You can access documentation on the **Documentation** page. On the **Documentation** page, all created level-1 and level-2 document categories are displayed in the preset order.

To go to the **Documentation** page, perform the following operations: Log on to the Apsara Uni-manager Management Console. In the upper-right corner, click the 🕮 icon to go to the **Documentation** page.

> **Important**
>
> A document category is displayed only if **launched** documents exist in the category. If all documents in a document category are **withdrawn**, the category is not displayed.



7.Security

7.1. Overview

The Apsara Uni-manger Management Console uses operations logs, AccessKey pairs, and multi-factor authentication (MFA) to enhance the security when users access systems and resources.

Module	Description
Operation logs	Access and use of resources on the console are recorded in operation logs. • You can filter operation logs by specifying conditions such as the time range, organization, user name, and resource ID. • You can dump logs to Object Storage Service (OSS) and download them to your computer as files.
AccessKey pairs	AccessKey pairs are used by users to access cloud resources. • Users can view their AccessKey pairs. • You can create AccessKey pairs. You can have at most two AccessKey pairs. • You can enable or disable the AccessKey pairs of a personal account. Make sure that at least one AccessKey pair is enabled. • You can delete AccessKey pairs. At least one of the AccessKey pairs must be retained.
MFA	MFA is a method for identity authentication in addition to the username and password of an account. It can be used to improve security. • You can check whether the MFA feature is enabled for a user. If not, you can enable it. However, you cannot disable it after it is enabled. • You can bind or unbind virtual MFA devices. • You can reset MFA keys.

7.2. Operation logs

7.2.1. Query events

On the Event Query page, you can view all the operations that you performed to access and use cloud resources on Apsara Stack. These operations are performed by using the console, calling API operations, and using developer tools.

Background information

- You can search for operations that are performed to create, modify, and delete resources in a precise manner by using filter conditions.
- You can create an event export task to save operation logs to your computer for backup.

Cloud services that support precise query for resource creation, modification, and deletion operations

Product	Resource	Create or modify operation	Delete operation
Realtime Compute for Apache Flink	Namespace	• CreateNamespace • UpdateNamespace	• DeleteNamespace
Container Registry Standard Edition	Image repository	• CreateRepo	• DeleteRepo
	Namespace	• CreateNamespace	• DeleteNamespace
Container Service for Kubernetes (ACK)	ACK cluster	• CreateCluster • UpdateClusterName	• DeleteCluster
PolarDB	PolarDB cluster	• CreateDBCluster • ModifyDBNodesClass • ModifyDBNodeClass • CreateDBNodes • DeleteDBNodes • CreateDBClusterProxy • DeleteDBClusterProxy • ModifyDBClusterProxyClass	• DeleteDBCluster
ApsaraDB RDS	ApsaraDB RDS recycle bin	-	• DestroyDBInstance
	ApsaraDB RDS instance	• CreateDBInstance • CreateReadOnlyDBInstance • CloneDBInstance • CloneDBInstance • CreateDdrInstance • ModifyDBInstanceSpec	• DeleteDBInstance
MaxCompute	Quota group	-	-
	Project	• CreateCalcEngineForAscm	• DeleteCalcEngineForAscm

Tablestore	Tablestore instance	• InsertInstance	• DeleteInstance
Tair (Redis OSS-compatible)	Tair (Redis OSS-compatible) instance	• CreateInstance • CreateInstances • ModifyInstanceSpec	• DeleteInstance
Virtual Private Cloud (VPC)	VPC	• CreateVpc	• DeleteVpc
	Network access control list (ACL)	• CreateNetworkAcl	• DeleteNetworkAcl
	Route table	• CreateRouteTable	• DeleteRouteTable
	vSwitch	• CreateVSwitch	• DeleteVSwitch
Express Connect	Express Connect circuit	• CreatePhysicalConnectionNew	• DeletePhysicalConnection
	Virtual border router (VBR)	• CreateVirtualBorderRouter	• DeleteVirtualBorderRouter
	Router interface	• CreateRouterInterface	• DeleteExpressConnect • DeleteRouterInterface
ApsaraMQ for Kafka	ApsaraMQ for Kafka instance	• CreateInstanceRelation	-
API gateway	API group	• CreateApiGroup	• DeleteApiGroup
	API gateway	• CreateApi • ImportSwagger	• DeleteApi
	API plug-in	• CreatePlugin	• DeletePlugin
	API application	• CreateApp	• DeleteApp
DataHub	DataHub project	• CreateProject	• DeleteProject

Elasticsearch	Elasticsearch cluster	• CreateInstance • UpdateInstance	• DeleteInstance
AnalyticDB for PostgreSQL	AnalyticDB for PostgreSQL instance	• CreateDBInstance • UpgradeDBInstance	• DeleteDBInstance
Container Registry Advanced Edition	Image repository (Apsara Stack Advanced Edition)	• CreateRepository	• DeleteRepository
	Namespace (Apsara Stack Advanced Edition)	• CreateNamespace	• DeleteNamespace
File Storage NAS (NAS)	File System	• CreateFileSystem • ModifyFileSystem	• DeleteFileSystem
	Unified namespace	• CreateNamespace	• DeleteNamespace
	Permission group	• CreateAccessGroup • ModifyAccessGroup	• DeleteAccessGroup
ApsaraMQ	ApsaraMQ instance	• ConsoleInstanceCreate	• ConsoleInstanceDelete
SLB	SLB instance	• CreateLoadBalancer • CreateLoadBalancerPro • ModifyLoadBalancerInstanceSpec • ModifyLoadBalancerInternetSpec	• DeleteLoadBalancer
	Server certificate	• UploadServerCertificate	• DeleteServerCertificate
	Certificate authority (CA) certificate	• UploadCACertificate	• DeleteCACertificate

Object Storage Service (OSS)	OSS bucket	• PutBucket • BucketCreate • SetBucketStorageCapacity	• DeleteBucket
	Single Tunnel	• CreateVpcip	• DeleteVpcip
Simple Log Service	Simple Log Service project	• CreateProject • AnalyzeProductLog • UpdateProject	• DeleteProject
Enterprise Distributed Application Service (EDAS)	Cluster list	-	-
	EDAS application	-	-
CloudMonitor	Alert template	• CreateMetricRuleTemplate • ModifyMetricRuleTemplate • ApplyMetricRuleTemplate	• DeleteMetricRuleTemplate
	Alert rule	• PutResourceMetricRule	• DeleteMetricRules
Key Management Service (KMS)	Key	• CreateKey	-
Auto Scaling	Scheduled task	• CreateScheduledTask	• DeleteScheduledTask
	Scaling group	• CreateScalingGroup	• DeleteScalingGroup
	Event-triggered task	• CreateAlarm	• DeleteAlarm
	ECS image	• CreateImage • ImportImage • CopyImage	• DeleteImage
	Elastic network interface (ENI)	• CreateNetworkInterface	• DeleteNetworkInterface

Elastic Compute Service (ECS)	Storage set	- CreateStorageSet - ModifyStorageSetAttribute	- DeleteStorageSet
	File sending	- SendFile	-
	Asynchronous task	-	-
	Deployment set	- CreateDeploymentSet	- DeleteDeploymentSet
	ECS snapshot	- CreateSnapshot	- DeleteSnapshot
	ECS command	- CreateCommand - RunCommand	- DeleteCommand
	ECS disk	- CreateDisk - ResizeDisk	- DeleteDisk
	ECS recycle bin	-	- DeleteInstances - RestoreSoftDeletedInstances
	Snapshot-consistent group	- CreateSnapshotGroup	- DeleteSnapshotGroup
	Automatic snapshot policy	- CreateAutoSnapshotPolicy	- DeleteAutoSnapshotPolicy
	ECS Instance	- RunInstances - CreateInstance - ModifyInstanceSpec - OpsModifyInstanceVmTypeOnline	- DeleteInstance
	ECS command execution result	- InvokeCommand	-

	Security Group	• CreateSecurityGroup	• DeleteSecurityGroup
	SSH key pair	• CreateKeyPair • ImportKeyPair	• DeleteKeyPairs
PolarDB-X 1.0	PolarDB-X instance	• StartRestore • CreateDrdsInstance • CreateDrdsCrossInstance • UpgradeDrdsInstance	• RemoveDrdsInstance
Resource Orchestration Service (ROS)	Stack	• CreateStack • CreateStacks	• DeleteStack
	Template	• CreateTemplate	• DeleteTemplate
Data Transmission Service (DTS)	Synchronous task	• CreateSynchronizationJob	• DeleteSynchronizationJob
	Subscription task	• CreateSubscriptionInstance	• DeleteSubscriptionInstance
	Data migration task	• CreateMigrationJob	• DeleteMigrationJob
DNS within Cloud	DNS private IP address	• AddPrivateLine • UpdatePrivateLine • UpdatePrivateLinePriority	• DeletePrivateLine
	Internal domain name of tenants	• AddPrivateZone • UpdatePrivateZoneRemark • BindZoneVpc • AddPrivateZoneRecord • DeletePrivateZoneRecord • DeleteZoneVpc	• DeletePrivateZone
	Forwarding domain name of tenants	• AddPrivateForwardZone	• DeletePrivateForwardZone

	Default forwarding configuration of tenants	• AddPrivateDefaultForwardZone	• DeletePrivateDefaultForwardZone
ApsaraDB for MongoDB	ApsaraDB for MongoDB instance	• CreateDBInstance • CreateShardingDBInstance • ModifyDBInstanceSpec	• DeleteDBInstance

Event query

Query events

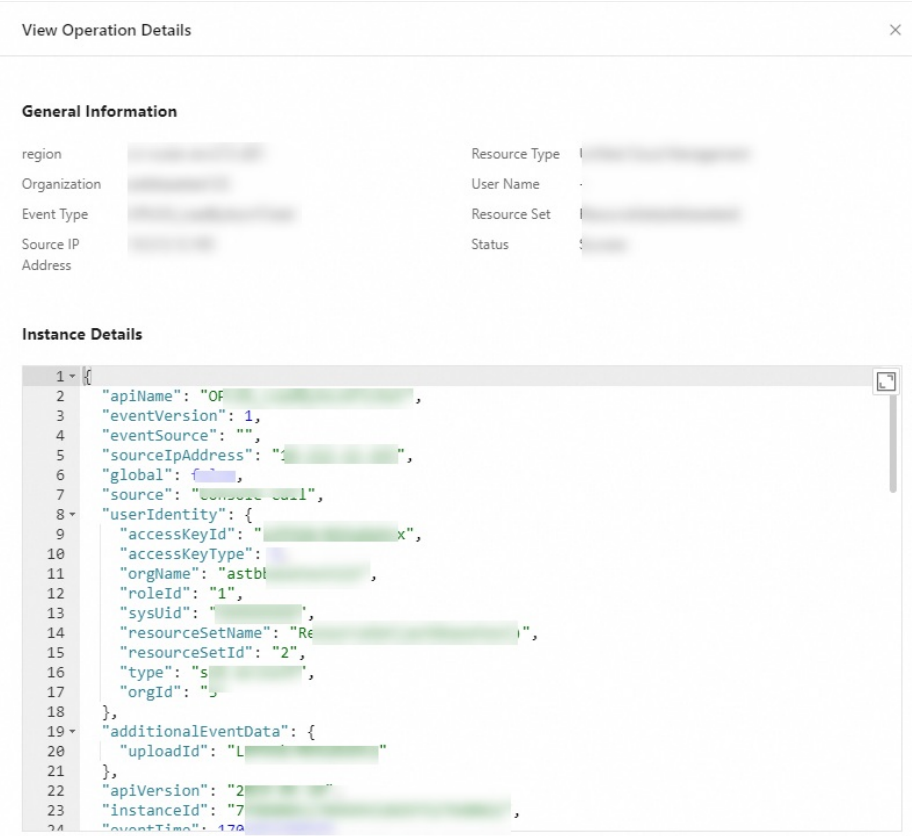
1. Log on to the Apsara Uni-manager Management Console as a security administrator.
2. In the top navigation bar, choose **Security** > **Global Platform Security** > **Operation Logs**.
3. In the left-side navigation pane, click **Event Query**.
4. On the Event Query page, click the **Events** tab.
5. Optional. Click **Advanced Filter**, configure the following parameters: **Username**, **Organization**, **Product Type**, **Resource Type**, **Event Type**, **Start And End Time**, **Resource ID**, **Source IP Address**, and **Keywords**, and then click Search to efficiently search for events that meet the specified filter conditions.

   > **Note**
   >
   > After you configure the Product Type and Resource Type parameters, the corresponding values are displayed in the Event Type drop-down list.

6. View events in the list.

Column	Description
Organization Name	The organization that is associated with the event.
Resource Set	The resource set that is associated with the event.
Product Type	The type of the resource that is associated with the event.
Event ID	The ID of the event.
Event types	The operation that triggers the event.
Status	The status of the event.

<table>
<tr><td><b>Product Type</b></td><td>The type of the cloud service that is associated with the event.</td></tr>
<tr><td><b>Call Source</b></td><td>The source of the event.</td></tr>
<tr><td><b>Source IP Address</b></td><td>The IP address of the operator who triggers the event.</td></tr>
<tr><td><b>Username</b></td><td>The identifier of the operator who triggers the event. The value can be the username, user ID, Resource Access Management (RAM) role ID, or organization ID of the operator, depending on the call method.</td></tr>
<tr><td><b>Time</b></td><td>The completion time of the operation that triggers the event.</td></tr>
<tr><td><b>Operation Name</b></td><td>The name of the operation that triggers the event.</td></tr>
<tr><td>Details</td><td>Click <b>View</b> in the Details column to go to the View Operation Details panel and view the information displayed in the <b>Basic Information</b> and <b>Instance Details</b> sections.



View Operation Details

General Information

region [redacted]
Organization [redacted]
Event Type [redacted]
Source IP Address [redacted]
Resource Type [redacted]
User Name -
Resource Set [redacted]
Status [redacted]

Instance Details

<pre>
{
  "apiName": "OP[redacted],
  "eventVersion": 1,
  "eventSource": "",
  "sourceIpAddress": "[redacted]",
  "global": [redacted],
  "source": "[redacted]",
  "userIdentity": {
    "accessKeyId": "[redacted]x",
    "accessKeyType": [redacted]
    "orgName": "astb[redacted],
    "roleId": "1",
    "sysUid": "[redacted]",
    "resourceSetName": "Re[redacted]",
    "resourceSetId": "2",
    "type": "s[redacted]",
    "orgId": "[redacted]
  },
  "additionalEventData": {
    "uploadId": "L[redacted]"
  },
  "apiVersion": "2[redacted]
  "instanceId": "7[redacted],
  "eventTime": 170[redacted]
</pre>
</td></tr>
</table>

Create an event export task

You can create asynchronous event export tasks to export specific operation logs to OSS buckets for permanent storage.

1. On the **Events** tab, click **Event Export**.
2. In the **Event Export** dialog box, specify the operations logs that you want to export.

Parameter		**Description**
Basic Report Information	**Task name**	The name of the export task.
Export Objects	**Organization**	The organization to which the exported logs belong.
	Filter Condition Name	The filter conditions for logs. You can filter logs by service name or resource type. However, you can select only a cloud service or a resource type.
	Start and End Time	The time range within which the operations are performed.
	Username	The username of the operator. You can enter only one username.
	Resource ID	The ID of the resource.
	Source IP Address	The IP address of the operator.
	Keywords	The keywords that are used to filter operation logs. You can enter keywords based on your business requirements. You can search for operation logs by event ID, resource ID, resource IP address, or operation name.

3. Click **OK**. The created task is displayed on the Export Records tab.

Export records

After an event export task is created, you can view the status of the task on the Export Records tab. After the task is complete, you can save the **.xlsx** log file for backup.

> **Important**
>
> Before you export records, create an event export task first.

1. On the **Event Query** page, click the **Export Records** tab.
2. Optional. Click **Advanced Filter**, configure the following parameters: **Task Name**, **Creator**, **Status**, and **Task Start and End Time**, and then click Search to search for tasks that meet the specified filter conditions.

3. In the event export task list, view the task information displayed in the following columns: **Task Name**, **Creator**, **Task Type**, **Status**, **Start Time**, and **End Time**.

> **Note**
>
> A task is in one of the following states:
>
> - **In Progress**: The task is being executed.
> - **Downloading**: The task is being downloaded.
> - **Completed**: The task is complete. You can click **Download Report** in the **Actions** column to download the report from the OSS bucket to your computer.
> - **Failed**: The task failed. You can click **Retry** in the **Actions** column to execute the task again.
> - **Expired**: The task has expired.

7.3. AccessKey pairs of a personal account

An AccessKey pair consists of an AccessKey ID and an AccessKey secret. AccessKey pairs are used to authenticate the identity of request senders, which can ensure cloud resource security.

> **Important**
>
> A user can have up to two AccessKey pairs, and at least one AccessKey pair must be enabled.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the upper-right corner of the homepage, click the profile picture and click **User Information** in the menu that appears.

Operation	Procedure
View AccessKey pairs	In the AccessKey Pair section, view the AccessKey pairs of your account. **Note** The AccessKey IDs and AccessKey secrets provide full permissions on cloud resources within your Apsara Stack tenant account. Keep them confidential.
Create an AccessKey pair	You can delete your existing AccessKey pairs and create new ones to implement the rotation of AccessKey pairs. i. In the AccessKey Pair section, click **Create AccessKey Pair**. ii. In the message that appears, click **Close**.

Disable an AccessKey pair	**Important** If you disable an AccessKey pair, errors may occur in the services or applications that depend on the AccessKey pair. Proceed with caution. i. In the AccessKey Pair section, find the AccessKey pair that you want to disable and click **Disable** in the **Actions** column. ii. In the message that appears, click **Disable**.
Enable an AccessKey pair	In the AccessKey Pair section, find the AccessKey pair that you want to enable and click **Enable** in the **Actions** column.
Delete an AccessKey pair	**Important** If you delete an AccessKey pair, errors may occur in the services or applications that depend on the AccessKey pair. Proceed with caution. i. In the AccessKey Pair section, find the AccessKey pair that you want to delete and click **Delete** in the **Actions** column. ii. In the message that appears, click **Delete**.
View the logs of an AccessKey pair	i. In the AccessKey Pair section, find the AccessKey pair whose logs you want to view and click **View AccessKey Logs** in the **Actions** column. The **AccessKey Logs** page appears. For more information about AccessKey pair logs, see AccessKey logs.

7.4. MFA

7.4.1. Overview

Multi-factor authentication (MFA) is an authentication method. In addition to username and password authentication, MFA provides an extra layer of protection.

Introduction to MFA

When MFA is enabled, you must enter your username and password (first security factor) and then a variable verification code (second security factor) from an MFA device when you log on to the Apsara Uni-manager Management Console. Two-factor authentication enhances security for your account.

MFA devices use the Time-based One-time Password (TOTP) algorithm to generate time-dependent 6-digit dynamic verification codes. The Apsara Uni-manager Management Console supports software-based virtual MFA devices. You can install software (such as the Alibaba Cloud app) that supports MFA on your mobile device (such as your mobile phone) to act as a virtual MFA device.

Precautions

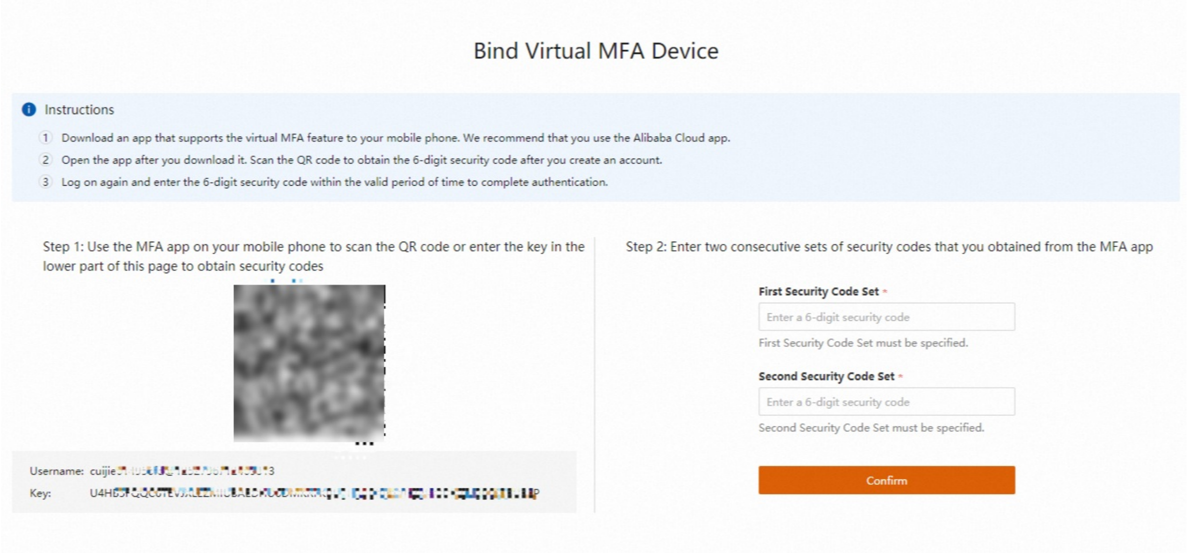
The TOTP algorithm requires that the time of the system clock of the Apsara Uni-manager Management Console remain consistent with the standard time on the Internet. Otherwise, discrepancies in time can lead to inconsistent MFA verification codes and you may be unable to log on to the Apsara Uni-manager Management Console.

7.4.2. Manage MFA

Multi-factor authentication (MFA) is an authentication method. In addition to username and password authentication, MFA provides an extra layer of protection. You can enable or disable the MFA feature in the console.

Bind a virtual MFA device

1. Log on to the Apsara Uni-manager Management Console.
2. In the upper-right corner of the Home page, click the profile picture and select **User Information** in the menu that appears.
3. In the upper-right corner of the **MFA** section, click **Bind Virtual MFA Device**.
4. On the **Bind Virtual MFA Device** page, bind an MFA device as prompted. After an MFA device is bound, the value of the MFA Status parameter changes to Enabled and the value of the Device Status changes to Bound.



Bind Virtual MFA Device

Instructions

1. Download an app that supports the virtual MFA feature to your mobile phone. We recommend that you use the Alibaba Cloud app.
2. Open the app after you download it. Scan the QR code to obtain the 6-digit security code after you create an account.
3. Log on again and enter the 6-digit security code within the valid period of time to complete authentication.

Step 1: Use the MFA app on your mobile phone to scan the QR code or enter the key in the lower part of this page to obtain security codes

Username: cuijie[redacted]
Key: U4H[redacted]

Step 2: Enter two consecutive sets of security codes that you obtained from the MFA app

First Security Code Set *
Enter a 6-digit security code
First Security Code Set must be specified.

Second Security Code Set *
Enter a 6-digit security code
Second Security Code Set must be specified.

> **Note**
>
> After a virtual MFA device is bound, you must enter a 6-digit MFA verification code in addition to your username and password before you can log on to the Apsara Uni-manager Management Console.

Disable a virtual MFA device

1. In the upper-right corner of the **MFA** section on the **User Information** page, click **Disable Virtual MFA Device**.
2. In the message that appears, click **Disable Virtual MFA Device**.

   After you disable the MFA feature, you need to only enter your username and password next time you log on to the Apsara Uni-manager Management Console.

Forcibly enable the MFA feature

Administrators, including the platform administrator, operations administrator, and organization administrator, can check whether the MFA feature is enabled for their users. If the MFA feature is disabled for the users, the administrators can forcibly enable the MFA feature for the users.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Users** > **Users**.
4. On the Users page, click the **System Users** tab.
5. Find the user for which you want to enable the MFA feature, move the pointer over the ··· icon in the **Actions** column, and then click **MFA Settings**.
6. In the MFA Settings dialog box, turn on **MFA Settings** and click **OK**.

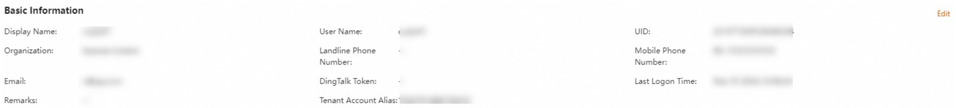
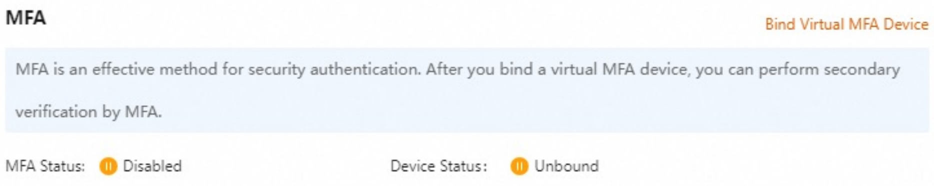
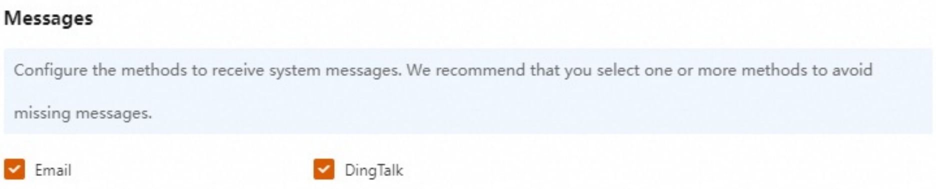
> **Note**
>
> The MFA feature can be forcibly enabled for users, but cannot be forcibly disabled.
>
> - Before the MFA feature is enabled, the MFA feature of the user is in the **Disabled and Unbound** state.
> - After the MFA feature is enabled, the MFA feature of the user is in the **Enabled and Unbound** state. After the MFA feature is forcibly enabled for a user, the user must go to the Bind Virtual MFA Device page to bind a virtual MFA device before the user can log on to the Apsara Uni-manager Management Console.

8.User information management

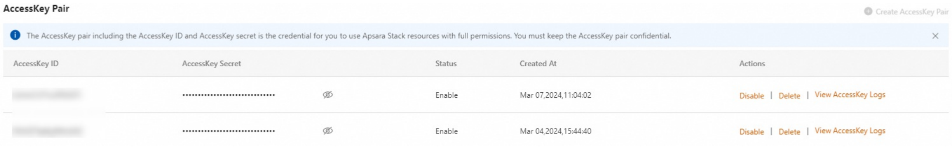
On the User Information page, you can manage the information of your account, such as the basic information, password, multi-factor authentication (MFA) devices, methods to receive system messages, and AccessKey pairs.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the upper-right corner of the page, click the profile picture of the current user.
3. Select **User Information**.

Section or tab	Description
Basic Information	In the **Basic Information** section, you can view the detailed information about your account. You can also click **Edit** in the upper-right corner of the section to modify the account information, such as mobile phone number, landline phone number, email address, DingTalk token, and remarks.  Basic Information Display Name: [redacted] Organization: [redacted] Email: [redacted] Remarks: [redacted] User Name: [redacted] Landline Phone Number: - DingTalk Token: - Tenant Account Alias: [redacted] UID: [redacted] Mobile Phone Number: [redacted] Last Logon Time: [redacted]
MFA	In the **MFA** section, you can enable or disable the MFA feature. For more information about MFA, see Manage MFA.  MFA MFA is an effective method for security authentication. After you bind a virtual MFA device, you can perform secondary verification by MFA. MFA Status: Disabled Device Status: Unbound
Messages	In the **Messages** section, you can select one or more methods for receiving system messages. Make sure that the selected methods are configured. For more information, see Message gateway.  Messages Configure the methods to receive system messages. We recommend that you select one or more methods to avoid missing messages. ☑ Email ☑ DingTalk

<table>
<tr>
<td>AccessKey pairs</td>
<td>
In the <b>AccessKey Pair</b> section, you can manage your AccessKey pairs. For more information, see AccessKey.



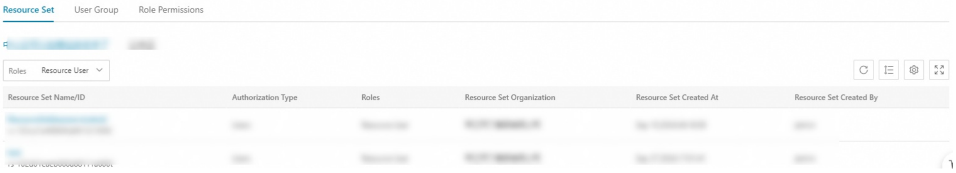
AccessKey Pair

Create AccessKey Pair

The AccessKey pair including the AccessKey ID and AccessKey secret is the credential for you to use Apsara Stack resources with full permissions. You must keep the AccessKey pair confidential.

<table>
<tr><th>AccessKey ID</th><th>AccessKey Secret</th><th>Status</th><th>Created At</th><th>Actions</th></tr>
<tr><td>[redacted]</td><td>••••••••••••••••••••••••••••••</td><td>Enable</td><td>Mar 07,2024,11:04:02</td><td>Disable | Delete | View AccessKey Logs</td></tr>
<tr><td>[redacted]</td><td>••••••••••••••••••••••••••••••</td><td>Enable</td><td>Mar 04,2024,15:44:40</td><td>Disable | Delete | View AccessKey Logs</td></tr>
</table>
</td>
</tr>
<tr>
<td>Resource Set</td>
<td>
On the <b>Resource Set</b> tab, you can switch between different roles and view the resource sets to which each role is added.

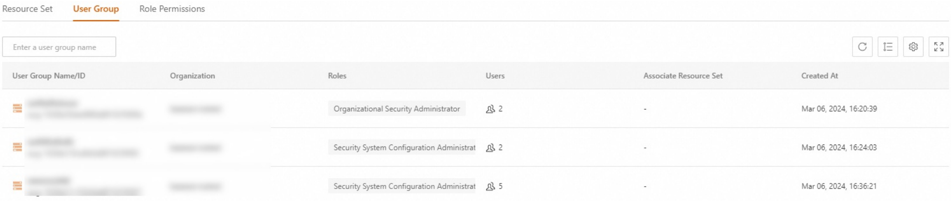
> **Note**
>
> If multiple clouds have been bound, you can switch to the cloud tabs to view the corresponding resource sets.



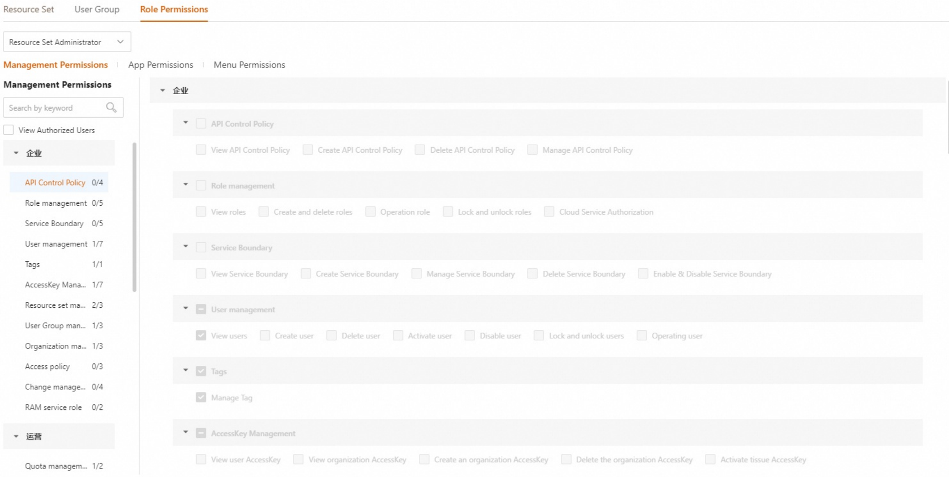
[redacted]

Roles: Resource User

<table>
<tr><th>Resource Set Name/ID</th><th>Authorization Type</th><th>Roles</th><th>Resource Set Organization</th><th>Resource Set Created At</th><th>Resource Set Created By</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
</table>
</td>
</tr>
<tr>
<td>User Group</td>
<td>
On the <b>User Group</b> tab, you can view the user groups to which the user belongs.



<table>
<tr><th>User Group Name/ID</th><th>Organization</th><th>Roles</th><th>Users</th><th>Associate Resource Set</th><th>Created At</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Organizational Security Administrator</td><td>2</td><td>-</td><td>Mar 06, 2024, 16:20:39</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Security System Configuration Administrat</td><td>2</td><td>-</td><td>Mar 06, 2024, 16:24:03</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Security System Configuration Administrat</td><td>5</td><td>-</td><td>Mar 06, 2024, 16:36:21</td></tr>
</table>
</td>
</tr>
<tr>
<td>Role Permissions</td>
<td>
On the <b>Role Permissions</b> tab, you can switch between different roles and view the <b>management permissions</b>, <b>application permissions</b>, and <b>menu permissions</b> of each role.



企业

☐ API Control Policy

☐ View API Control Policy ☐ Create API Control Policy ☐ Delete API Control Policy ☐ Manage API Control Policy

☐ Role management

☐ View roles ☐ Create and delete roles ☐ Operation role ☐ Lock and unlock roles ☐ Cloud Service Authorization

☐ Service Boundary

☐ View Service Boundary ☐ Create Service Boundary ☐ Manage Service Boundary ☐ Delete Service Boundary ☐ Enable & Disable Service Boundary

⊟ User management

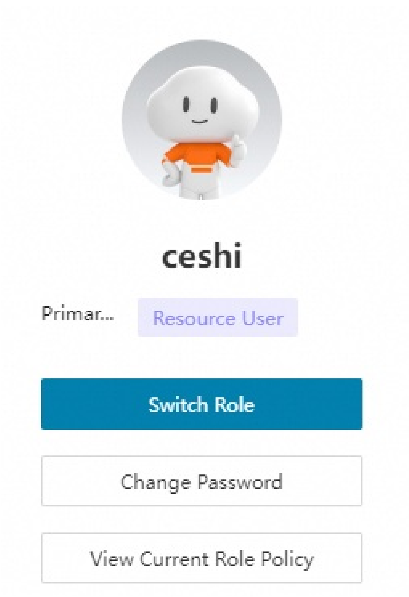
☑ View users ☐ Create user ☐ Delete user ☐ Activate user ☐ Disable user ☐ Lock and unlock users ☐ Operating user

☑ Tags

☑ Manage Tag

⊟ AccessKey Management

☐ View user AccessKey ☐ View organization AccessKey ☐ Create an organization AccessKey ☐ Delete the organization AccessKey ☐ Activate tissue AccessKey
</td>
</tr>
</table>

Left-side section	 ceshi Primar... Resource User Switch Role Change Password View Current Role Policy **Note** If the user has been granted a multi-cloud role, multi-cloud identity information is also displayed. - Click **Switch Role**. If the current user has multiple roles, you can switch to another role. In the Switch Role dialog box, you can also set a role as the default role. - Click **Change Password**. In the Change Password dialog box, specify the current password and new password and confirm the password. Click **OK** to change the password. - Click **View Current Role Policy** to view the Resource Access Management (RAM) role, policies, and trusted policies of the level-1 organization to which the current role belongs.

9.OpenAPI Explorer

9.1. Overview

This topic describes the permissions and overview of OpenAPI Explorer.

OpenAPI Explorer is an integrated external portal for Apsara Stack capabilities. It provides documentation, debugging tools, SDKs, and sample code. OpenAPI Explorer provides a series of APIs and share its core capabilities and services with the external developers. This way, the external developers can access and use these resources to develop innovative and growth services.

Permissions

The following table describes the default permissions in OpenAPI Explorer.

Permission	Description
View call statistics	You can view all features in the Call Statistics section.
View page integration configurations	You can view all features in Page Integration Configurations. You cannot modify these features.
Modify page integration configurations	You can view and modify all feature configurations in Page Integration Configurations.

Different roles have different permissions in OpenAPI Explorer. The following table describes the default roles and their permissions.

Role name	Permission
Organization administrator	Views call statistics and page integration configurations.
Operations administrator	Views call statistics and views and modifies page integration configurations.
Security auditor	Views call statistics and page integration configurations.

Overview of OpenAPI Explorer

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Development Tools** > **API & SDK** > **OpenAPI Explorer**.
3. On the **OpenAPI Explorer** page, select a service or feature based on your business requirements. The following table describes the services and features.

Menu	Description

Home	◦ The **API Integration** tab provides API developer guides, debugging tools, SDK sample code, and API call statistics (permissions required). You can search by cloud service or text content. This tab contains the Popular Services and Recent Calls tabs. **Note** You can click **View Cloud Service Endpoint** to go to the Service Endpoints page and query the endpoints of each cloud service. ◦ On the **Page Integration** tab, you can view the process of page integration configuration. You can click **Page Integration Configuration** to go to the **Overview** page. For more information, see the Page Integration section of this topic.
API Integration	Includes API Documentation, API Debugging, API Change History, and SDK Sample Code. ◦ **API Documentation**: provides the API references of cloud services. ◦ **API Debugging**: allows you to debug API operations. ◦ **API Change History**: records the change history of cloud service API operations. ◦ **SDK Sample Code**: allows you to view and download the SDK demos that are used to call API operations.
Call Statistics	You can view data on the **Call Overview**, **Call Statistics**, and **Statistical Reports** pages. For more information, see the Call Statistics section of this topic. ◦ **Call Overview**: displays the call trends and error distribution. ▪ **Call Trend**: You can select a period of time and view the total number of calls, the number of errors, and the error rate within the selected period of time. The number of calls to each cloud service is displayed in a column chart. Move the pointer over the column chart to view the number of successful calls and the number of failed calls. ▪ **Error Distribution**: You can view the distribution of API errors based on filter conditions such as the call date, cloud service, and API version. ◦ **Call Statistics**: You can specify the filter conditions such as service, API version, and API name to search for the call details of an API operation of a cloud service. You can view the namespace, number of calls each time, average call duration per call, and call success rate of an API operation. Click **Call Source Distribution** in the Actions column of an API operation to view the AccessKey ID that is used for calls and identify the source of the operation. ◦ **Statistical Reports**: You can configure the following parameters to create a statistical report task based on your business requirements: Interval, Data Source, Statistical Policy, Keyword, and Custom Aggregation Policy. After a statistical report task is created, you can view the task status and report details at any time. This helps you understand the status of your business. In addition, you can start, stop or delete statistical report tasks.

IaC Management	The Infrastructure as Code (IaC) management module includes the Template and Task sections. For more information, see the IaC Management section of this topic. ◦ Template: includes Template Management and Template Center. Apsara Stack provides a series of templates based on Terraform to manage cloud resources in a standardized manner. You can also upload custom templates and edit templates online. ◦ Task: orchestrates resources based on templates and tracks the status of resources during the orchestration process.
Page Integration	You can configure page integration for Apsara Stack pages to directly embed cloud management pages into third-party platforms. You can hide the top navigation bar and adjust the color of a page to ensure that the page adapts to third-party platforms. This minimizes the effort required to integrate pages into third-party platforms. For more information, see Page Integration.

9.2. API integration

This topic describes the operations performed in the API Integration module.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Development Tools** > **API & SDK** > **OpenAPI Explorer**.
   - **View the API reference of a cloud service**
     a. On the **OpenAPI Explorer** page, choose **API Integration** > **API Documentation** in the top navigation bar.
     b. In the upper-left corner, click the ≡ icon to select the cloud service that you want to manage.
     c. In the left-side navigation pane, click Change History or Development Guide.
        - On the Change History page, view the change history of API operations. Click the + icon in front of an API operation to view the change details of the API operation in the JSON format.
        - In the Development Guide section, view the methods to call API operations and the API references.
   - **Debug an API operation**
     a. On the **OpenAPI Explorer** page, choose **API Integration** > **API Debugging** in the top navigation bar.
     b. In the upper-left corner, click the ≡ icon to select the cloud service that you want to manage.
     c. Select an API version from the **Version** drop-down list.
     d. In the left-side navigation page, enter the name of the API operation that you want to debug in the search box to search for the API operation.

e. Click the API operation, configure the parameters on the **Parameter** and **Request Header** tabs, and then click **Initiate Call**.

> **Important**
>
> - OpenAPI Explorer obtains a temporary AccessKey pair of the current account by using the user logon information. If you initiate a call, you may perform an operation on online resources within the current account. Proceed with caution.
> - Click **Clear** to clear the configured parameters.
> - On the **Debug Parameters** tab, view the information about the request parameters.
> - On the **SDK Sample Code** tab, view sample code for SDKs in Java, Python, and Go. You can also click **Download Project**, **View Dependencies**, and **Copy** in the upper-right corner of the tab.
> - On the **Call Result** tab, view the call result.
> - On the **API Reference** tab, view the API reference.

- **View the change history of API operations**

a. On the **OpenAPI Explorer** page, choose **API Integration** > **API Change History** in the top navigation bar.

b. Configure the **Service Category**, **Service Name**, and **Change Type** parameters and click **Search**.

c. View the change history of API operations in the **Change Result** section.

- **View SDK sample code**

a. On the **OpenAPI Explorer** page, choose **API Integration** > **SDK Sample Code** in the top navigation bar.

b. In the upper-left corner, click the ≡ icon to select the cloud service that you want to manage.

c. Select an SDK version from the **Version** drop-down list.

d. On the **SDK Sample Code** tab, select **SDK Type**. You can select Common Edition or Advanced Edition.

> **Note**
>
> - Common Edition refers to generic calls and supports debugging.
> - If you select Advanced Edition, you can click View Release Report. In the release report, you can view the SDK version, SDK API list, and Availability Description. Advanced Edition does not support debugging.
> - If the SDK Type field is dimmed and cannot be selected, the product does not support Advanced Edition or no data is available.

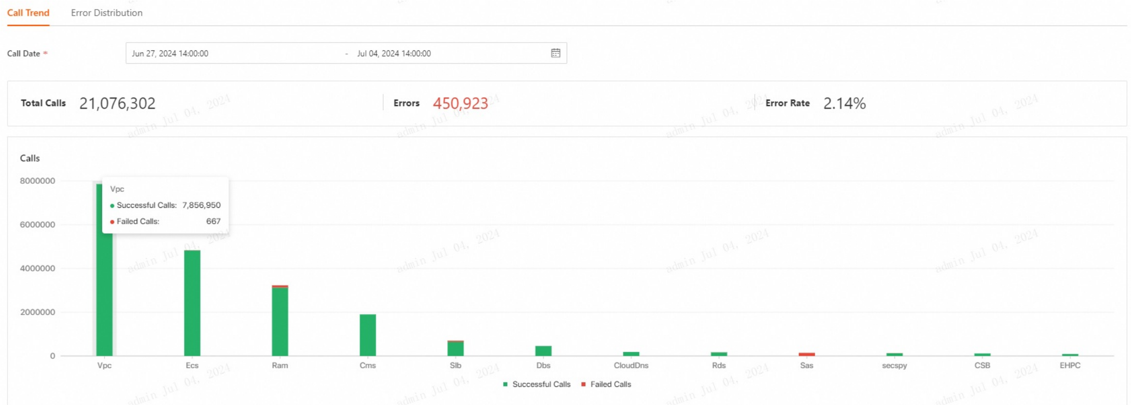
e. Change the language and view the SDK sample code for that language. You can also click **Download Project**, **View Dependencies**, and **Copy** in the upper-right corner of the tab.

9.3. Call Statistics

This topic describes how to use the Call Statistics module in OpenAPI Explorer.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Development Tools** > **API & SDK** > **OpenAPI Explorer**.
3. On the **OpenAPI Explorer** page, click **Call Statistics** in the top navigation bar.
4. Perform the following operations in the **Call Statistics** module:
    - **Call Overview**: In the left-side navigation pane, click **Call Overview**.
        - **Call Trend**: Configure the **Call Date** parameter to select a time range and view the total number of calls, the number of errors, and the error rate within the specified time range. The number of calls to each cloud service is displayed in a column chart. Move the pointer over the column chart to view the numbers of successful and failed calls.



Call Trend | Error Distribution

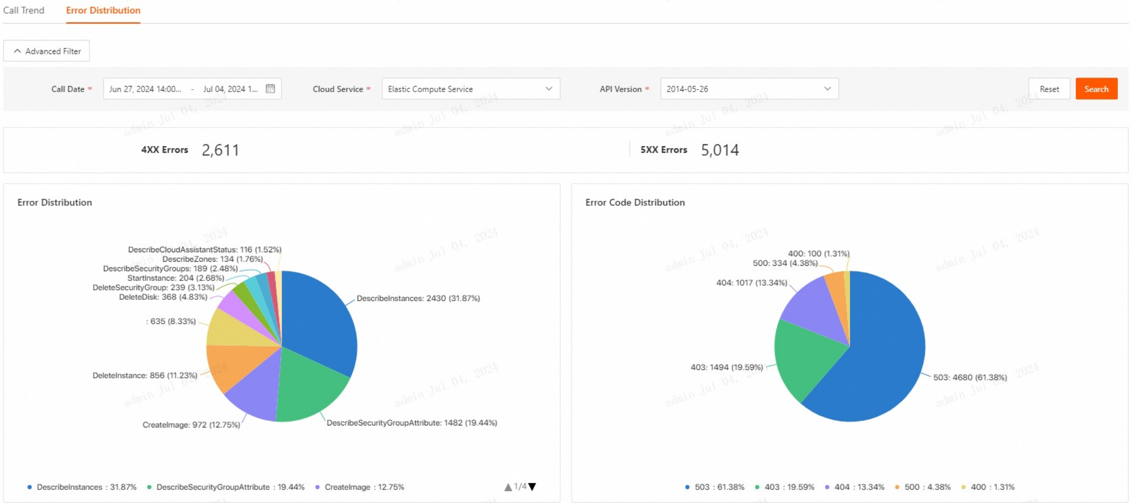
Call Date * Jun 27, 2024 14:00:00 - Jul 04, 2024 14:00:00

Total Calls 21,076,302

Errors 450,923

Error Rate 2.14%

        - **Error Distribution**: Configure the **Call Date**, **Cloud Service**, and **API Version** parameters to view the distribution of API errors based on the specified filter conditions.



Call Trend | Error Distribution

Advanced Filter

Call Date * Jun 27, 2024 14:00... - Jul 04, 2024 1...

Cloud Service * Elastic Compute Service

API Version * 2014-05-26

Reset | Search

4XX Errors 2,611

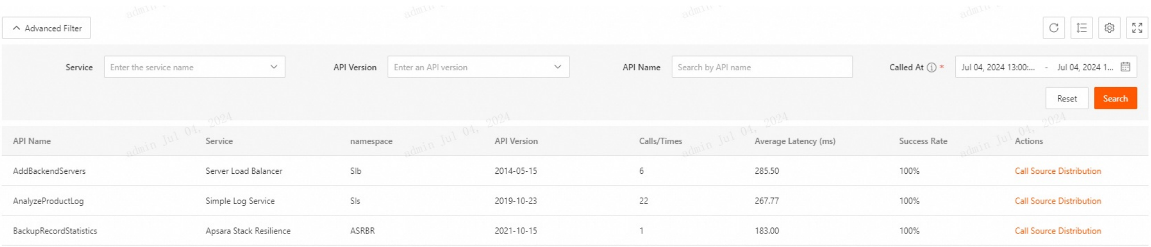
5XX Errors 5,014

Error Distribution
DescribeCloudAssistantStatus: 116 (1.52%)
DescribeZones: 134 (1.76%)
DescribeSecurityGroups: 189 (2.48%)
StartInstance: 204 (2.68%)
DeleteSecurityGroup: 239 (3.13%)
DeleteDisk: 368 (4.83%)
: 635 (8.33%)
DeleteInstance: 856 (11.23%)
CreateImage: 972 (12.75%)
DescribeInstances: 2430 (31.87%)
DescribeSecurityGroupAttribute: 1482 (19.44%)
DescribeInstances : 31.87%
DescribeSecurityGroupAttribute : 19.44%
CreateImage : 12.75%
1/4
Error Code Distribution
400: 100 (1.31%)
500: 334 (4.38%)
404: 1017 (13.34%)
403: 1494 (19.59%)
503: 4680 (61.38%)
503 : 61.38%
403 : 19.59%
404 : 13.34%
500 : 4.38%
400 : 1.31%

    - **Call Statistics**: In the left-side navigation pane, click **Call Statistics**.

      Configure the **Service**, **API Version**, **API Name**, and **Called At** parameters to search for the call details of an API operation of a cloud service. The information is displayed in the following columns: **API Name**, **Service**, **Namespace**, **API Version**, **Calls/Times**, **Average Latency (ms)**, and **Success Rate**.

> **Note**
>
> - The value of the **Called At** parameter must be within seven days.
> - Click **Call Source Distribution** in the **Actions** column of an API operation to view the **AccessKey** ID and the source service of the API operation.



Service: Enter the service name

API Version: Enter an API version

API Name: Search by API name

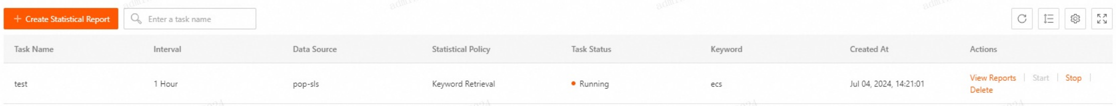
Called At * : Jul 04, 2024 13:00:... - Jul 04, 2024 1...

API Name	Service	namespace	API Version	Calls/Times	Average Latency (ms)	Success Rate	Actions
AddBackendServers	Server Load Balancer	Slb	2014-05-15	6	285.50	100%	Call Source Distribution
AnalyzeProductLog	Simple Log Service	Sls	2019-10-23	22	267.77	100%	Call Source Distribution
BackupRecordStatistics	Apsara Stack Resilience	ASRBR	2021-10-15	1	183.00	100%	Call Source Distribution

- **Statistical Reports**: In the left-side navigation pane, click **Statistical Reports**.
  - Create a statistical report task: On the Statistical Reports page, click **Create Statistical Report**. In the Create Task dialog box, configure the parameters described in the following table and click **OK**.

Parameter	Description
Task Name	The name of the statistical report task.
Interval	The interval at which the statistical report task retrieves statistics. Valid values: - **1 Hour** - **6 Hours** - **12 Hours** - **24 Hours**
Data Source	The source of the statistics. Valid value: **pop-sls**.
Statistical Policy	The method used to retrieve statistics. Valid value: **Keyword Retrieval**.
Keyword	The keywords used to retrieve statistics. Click **Add Entry** and specify keywords in key-value pairs.
Custom Aggregation Policy	The aggregation policy. Select an aggregation policy from the drop-down list.

- View a statistical report task: The created statistical report tasks are displayed in the task list.



Task Name	Interval	Data Source	Statistical Policy	Task Status	Keyword	Created At	Actions
test	1 Hour	pop-sls	Keyword Retrieval	● Running	ecs	Jul 04, 2024, 14:21:01	View Reports | Start | Stop | Delete

a. Find the statistical report task that you want to view and click **View Reports** in the **Actions** column.

b. The execution history of the statistical report task is displayed. Click **View Details** in the **Actions** column of a report to view the report details in the following sections: **Basic Information**, **Matching Info**, and **Time Distribution**.

- Start a statistical report task: Find the statistical report task that you want to start and click **Start** in the **Actions** column If the task changes to the **Running** state, the task is started.

> **Note**
>
> You can start tasks only in the **Canceled** state.

- Stop a statistical report task: Find the statistical report task that you want to stop and click **Stop** in the **Actions** column. If the task changes to the **Canceled** state, the task is stopped.

> **Note**
>
> You can stop tasks only in the **Running** state.

- Delete a statistical report task: Find the statistical report task that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

9.4. IaC Management

This topic describes how to use the IaC Management module.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Development Tools** > **API & SDK** > **OpenAPI Explorer**.
3. On the **OpenAPI Explorer** page, click **IaC Management** in the top navigation bar.
4. In the upper-left corner, select an organization and a resource set.
5. Perform the following operations in the **IaC Management** module:
    - **Template Management**: In the left-side navigation pane, choose **Template** > **Template Management**

- Create a template: On the Template Management tab, click **Create Template**. In the Create Template panel, configure the parameters described in the following table and click **OK**.

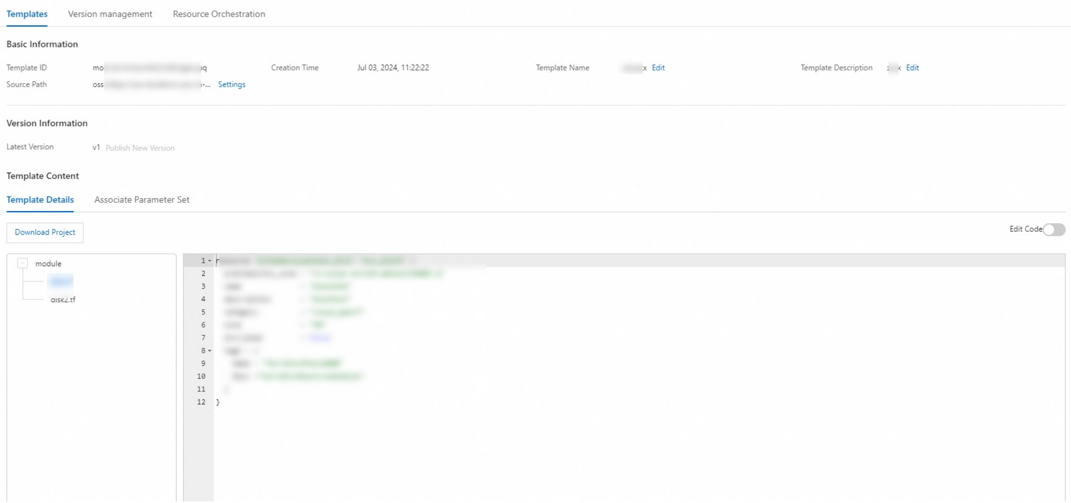
Parameter	Description
Template Name	The name of the template.
Description	The description of the template.
Template File	The template file. Click **Upload File** to upload a template file. **Note** The template file must meet the following requirements: - The file must be a ZIP package. - The file name must be encoded in UTF-8. - The file name is case-sensitive. - The file name must be 1 to 1,023 bytes in length. - The file name cannot contain forward slashes (/) or backslashes (\). - The file cannot exceed 10 MB in size.

- View a template: The created templates are displayed in the template list.

a. Find the template that you want to manage and click its ID to go to the template details page.

b. On the template details page, view the template information on the Templates, Version management, and Resource Orchestration tabs.

- **Templates**: The information is displayed in the following sections: **Basic Information**, **Version Information**, **Template Content**.



Basic Information

Template ID mo[redacted]q
Creation Time Jul 03, 2024, 11:22:22
Template Name [redacted]x Edit
Template Description [redacted] Edit
Source Path oss[redacted]-... Settings

Version Information

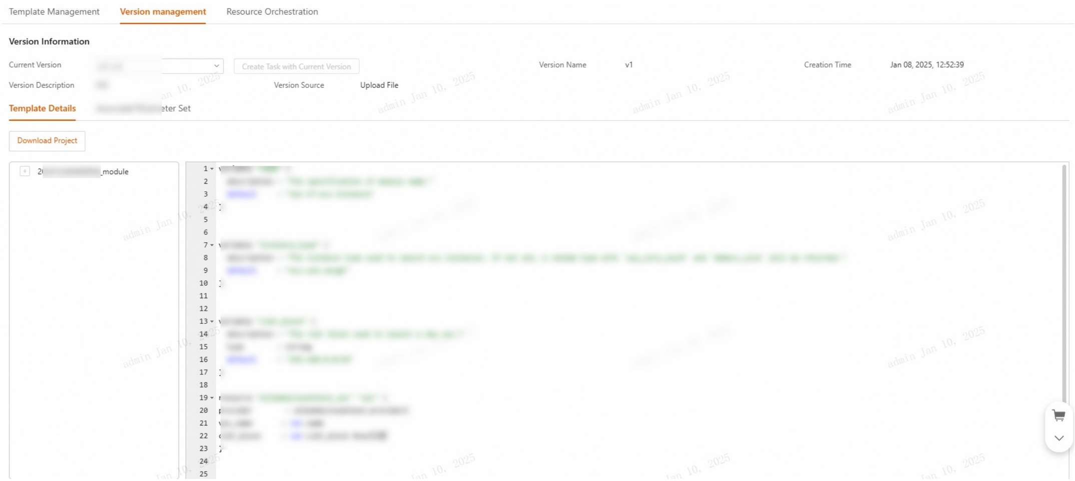
Latest Version v1 Publish New Version

Template Content

```
[redacted]
}
```

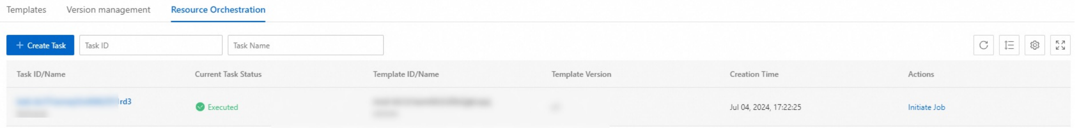
  - **Basic Information**: The following parameters are displayed: **Template ID**, **Creation Time**, **Template Name**, **Template Description**, and **Source Path**.
    - Click **Edit** next to the template name to modify the template name.
    - Click **Edit** next to the template description to modify the template description.
    - Click **Settings** next to the source path to update the template file.
  - **Version Information**: displays the latest version of the template. If the template details change, click **Publish New Version** to generate a new version.
  - **Template Content**: displays the Template Details and Associated Parameter Set tabs.
    - On the Template Details tab, click **Download Project** to download the template file in the **ZIP** format to your computer for storage.
    - On the Template Details tab, turn on **Edit Code** to manually edit the template.
    - On the Associated Parameter Set tab, view the parameter sets that are associated with the template.
      - Click **Associate Existing Parameter Set**. In the Associate Existing Parameter Set dialog box, select existing parameter sets that you want to associate with the template. You can associate up to five parameter sets with a template.
      - If you no longer need an associated parameter set, click **Disassociate** in the Actions column to disassociate the parameter set from the template.
      - If the existing parameter sets do not meet your business requirements, click **Create Parameter Set** to create a custom parameter set.

- **Version management**: displays the version information about the template.



  - Select a version from the **Current Version** drop-down list to view the corresponding version information.
  - Click **Create Task with Current Version** to create a task based on the current version.
  - On the Template Details tab, click **Download Project** to download the template file in the **ZIP** format to your computer for storage.
  - On the Associated Parameter Set tab, click **Associate Existing Parameter Set**. In the Associate Existing Parameter Set dialog box, select existing parameter sets that you want to associate with the template. You can associate up to five parameter sets with a template. If the existing parameter sets do not meet your business requirements, click **Create Parameter Set** to create a custom parameter set.

- **Resource Orchestration**: displays the tasks that are associated with the template.



Task ID/Name	Current Task Status	Template ID/Name	Template Version	Creation Time	Actions
[redacted]rd3	Executed	[redacted]	[redacted]	Jul 04, 2024, 17:22:25	Initiate Job

  - Click **Create Task** to create a task based on the template.
  - Click the ID of a task to go to the task details page.
  - Find the task that you want to manage and click **Initiate Job** in the Actions column. In the Initiate Job dialog box, enter a description and click **OK** to start a job.

- Modify a template: Find the template that you want to modify and click **Edit** in the Actions column. In the Edit panel, modify the template name and description and click **OK**.
- Delete a template: Find the template that you want to delete and click **Delete** in the Actions column. In the message that appears, click **OK** to delete the template.
- Create a task: Find the template that you want to manage and click **Create Task** in the Actions column to create a resource orchestration task based on the template.

- **Parameter Set Management**: In the left-side navigation pane, choose **Template** > **Template Management**. On the Template Management page, click the **Parameter Set Management** tab.

- Create a parameter set: Click **Create Parameter Set**. In the Create Parameter Set panel, configure the parameters described in the following table and click **OK**.

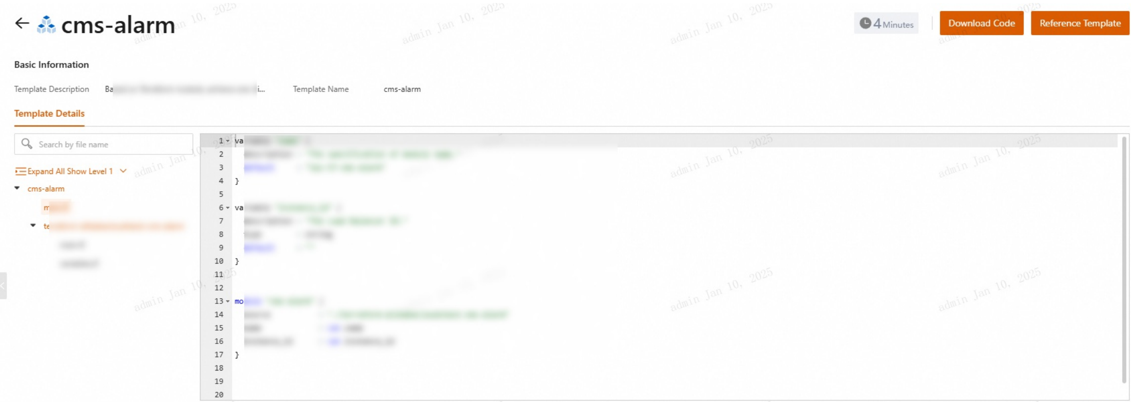
Parameter	Description
Parameter Set Name	The name of the parameter set. The name must start with a letter and cannot start with http:// or https://. The name must be 2 to 25 characters in length and can contain hyphens (-), underscores (_), letters, and digits.
Parameter Set Description	The description of the parameter set.
Parameter	The parameters in the parameter set. You can create, modify, and delete parameters based on your business requirements. ▪ Create a parameter: Click **Add Parameter**. In the Add Parameter dialog box, configure the Parameter Name, Parameter Type, and Parameter Value parameters and click **OK**. ▪ Modify a parameter value: Find the parameter that you want to modify and click **Edit** in the Actions column. In the Edit dialog box, modify the parameter value and click **OK**. You cannot modify the parameter name or parameter type. ▪ Delete a parameter: Find the parameter that you want to delete and click **Delete** in the Actions column. In the message that appears, click **OK** to delete the parameter. To delete multiple parameters at a time, select the parameters that you want to delete and click **Batch Delete** in the lower part of the panel. In the message that appears, click **OK**.

- View a parameter set: The created parameter sets are displayed in the parameter set list. Find the parameter set that you want to view and click **Details** in the Actions column. In the Parameter List message, view the parameters in the parameter set.
- Modify a parameter set: Find the parameter set that you want to modify and click **Modify** in the Actions column. In the Modifying Parameter Set panel, modify the parameter set name, parameter set description, and parameters based on your business requirements.
- Delete a parameter set: Find the parameter set that you want to delete and click **Delete** in the Actions column. In the message that appears, click **Delete**.

> **Important**
>
> You cannot delete the parameter sets that are associated with tasks or templates.

- **Template Center**: In the left-side navigation pane, choose **Template** > **Template Center** to view the preset Terraform templates.

- View details: Move the pointer over a template and click **View Details** to view the basic information and details of the template.



Template Description

Template Name cms-alarm

  - The template description and template name are displayed in the Basic Information section.
  - The Template Details section displays the content of the template, including the directory structure and the details of each file.
  - In the upper-right corner of the page, click **Download Code** to download the template code to your computer and save it.
  - In the upper-right corner of the page, click **Reference Template** to reference the content of the template file. In the New Template panel, you can create a template.
  - The time displayed in the upper-right corner of the page indicates the estimated time to use the template to call cloud resources.

- Download code: Move the pointer over the template and click **Download Code** to download the template content to your computer and save it. You can also click **Download Code** on the template details page.

- **Resource Orchestration**: In the left-side navigation pane, choose **Task** > **Resource Orchestration**.

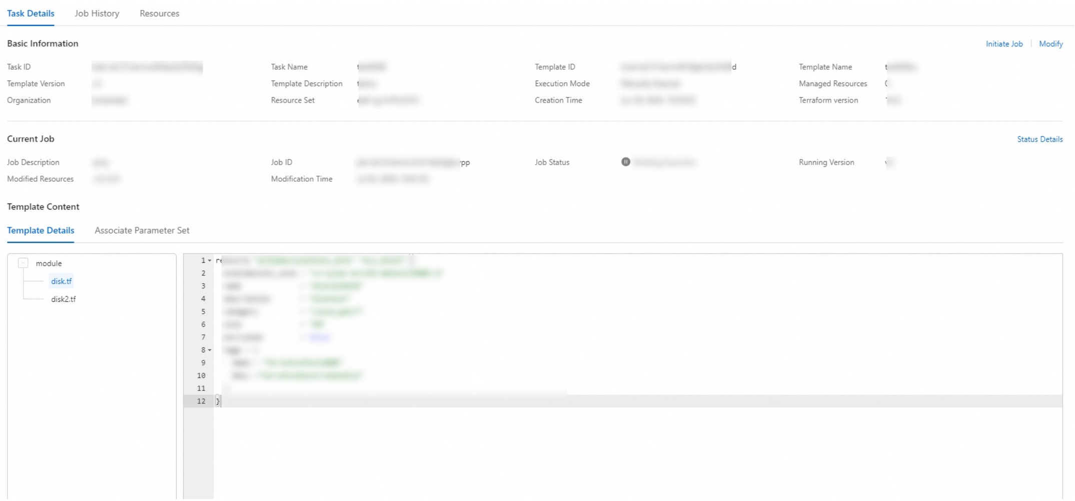
- Create a task: On the Resource Orchestration page, click **Create Task**. In the Create Task panel, configure the parameters described in the following table and click **OK**.

Parameter	Description
Task Name	The name of the task. The task name must start with a letter and cannot start with http:// or https://. The name must be 2 to 128 characters in length and can contain hyphens (-), underscores (_), letters, and digits.
Organization	The organization in which you want to create the task. By default, the selected organization is displayed. You cannot modify this parameter.
Resource Set	The resource set in which you want to create the task. By default, the selected resource set is displayed. You cannot modify this parameter.
Select Template ID/Version	The template based on which you want to create the task and the template version.
Associate Parameter Set	The existing parameter sets that you want to associate with the task. You can select multiple parameter sets. **Important** You cannot associate a parameter set that is already associated with a template and a template version or an empty parameter set with the task.
Execution Mode	The method used to execute the task. Valid values:**Manually Execute** and **Automatic Execution**. **Note** If you select Manually Execute, when the preview of the execution plan is complete and the preview result changes, a manual execution plan enters the pending state, and manual confirmation is required to complete the execution. If you select Automatic Execution, the execution plan skips manual confirmation and is automatically executed.

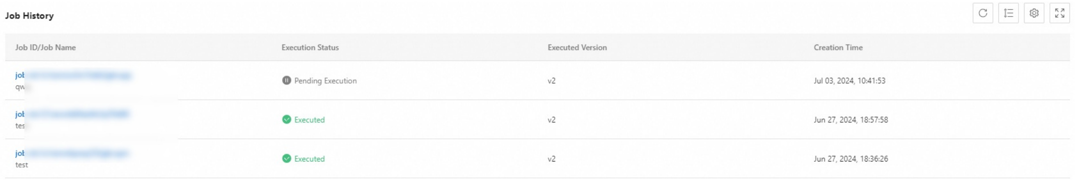
- View tasks: View the information about created tasks in the following columns: **Task ID/Name**, **Status**, **Template ID/Name**, **Template Description**, **Template Version**, **Organization**, **Resource Set**, and **Creation Time**.

- Find the task that you want to manage and click its ID to go to the task details page. On the task details page, view the information on the **Task Details**, **Job History**, and **Resources** tabs.
  - **Task Details**: The information is displayed in the Basic Information, Current Job, and Template Content sections.

    > **Note**
    >
    > - Click **Initiate Job** in the Basic Information section to initiate a new job.
    > - Click **Modify** in the Basic Information section to modify the task.
    > - Click **Status Details** in the Current Job section to go to the execution details page to view the task execution details.



  - **Job History**: displays the information about historical jobs in the following columns: **Job ID/Job Name**, **Execution Status**, **Executed Version**, and **Creation Time**.

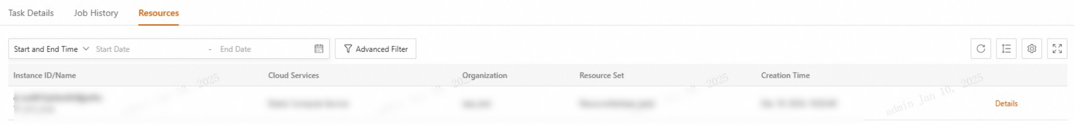


Job History

Job ID/Job Name	Execution Status	Executed Version	Creation Time
[illegible]	Pending Execution	v2	Jul 03, 2024, 10:41:53
[illegible]	Executed	v2	Jun 27, 2024, 18:57:58
[illegible] test	Executed	v2	Jun 27, 2024, 18:36:26

  - **Resources**: displays the information about resource instances generated by the task in the following columns: **Instance ID/Name**, **Cloud Services**, **Organization**, **Resource Set**, and **Creation Time**.

    > **Note**
    >
    > After the resource is created, click **Details** to go to the resource details page.



Instance ID/Name	Cloud Services	Organization	Resource Set	Creation Time	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Details

- Find the template that you want to manage and click its ID to go to template details page. On the template details page, view the information on the **Templates**, **Version management**, and **Resource Orchestration** tabs.

- Modify a task: Find the task that you want to modify and click **Modify** in the Actions column. In the Edit Task panel, modify the task information.

  > **Note**
  >
  > You cannot modify the organization, resource set, or template ID of the task.

- Initiate a job: Find the task that you want to manage and click **Initiate Job** in the Actions column. In the Initiate Job dialog box, enter a description and click **OK**.
- Refresh resource status: Find the task that you want to manage and click **Refresh Status** in the Actions column. In the message that appears, click **OK**.
- Destroy a resource: If you no longer need the resource generated by a task, find the task and click **Destroy Resource** in the ... Actions column. In the message that appears, click **OK**.

  > **Important**
  >
  > - You can destroy the resource of a task only if the task is in the **Executed** state and the resource is generated.
  > - A job plan is created to destroy the resource. The plan destroys all infrastructure managed by the associated Terraform template. Proceed with caution.

- Delete a task: Find the task that you want to delete, click the ... icon in the Actions column, and then click **Delete Task**. In the message that appears, click **OK**.

9.5. Page integration

This topic describes how to integrate pages.

Background information

The Apsara Uni-Manager Management Console allows you to customize the display language, appearance, theme color, brand logo, and version declaration of the pages that you integrate into your console. You can also hide the brand information, adjust the layouts, and change the styles for the integrated pages to match the style of your console that is developed by yourself or provided by third-party independent software vendors (ISVs). This way, you can provide consistent user experience.

Prerequisites

You must complete the single sign-on (SSO) authentication provided by the Apsara Uni-manager Management Console to implement a unified identity verification mechanism between the Apsara Uni-manager Management Console and the console to which you want to integrate pages. In the mechanism, the Apsara Uni-manager Management Console serves as the service provider and the console to which you want to integrate pages servers as the identity provider (IdP). This way, you can log on to the Apsara Uni-manager Management Console or the console to which you want to integrate pages from the other console without the need for identity verification.

For more information about how to configure third-party authentication in the Apsara Uni-manager Management Console, see Third-party authentication.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Development Tools** > **API & SDK** > **OpenAPI Explorer**.
3. On the **OpenAPI Explorer** page, click **Page Integration** in the top navigation bar.
4. On the **Overview** page, click **Page Integration Configuration** to complete the page integration settings.
   i. **Destination Application Configuration**: In this step, configure the information about the console to which you want to integrate the pages of the Apsara Uni-manager Management Console. The following table describes the parameters.

Section	Parameter	Description
Switch Settings	**Embedded Switch**	Specifies whether to embed the integrated pages in your console. If you turn on this switch, the integrated pages are embedded in your console, and the navigation bars of the integrated pages are automatically hidden. If you turn off this switch, the integrated pages cannot be embedded to your console by using iFrame.
	Hide Left-side Navigation Pane	Specifies whether to hide the left-side navigation pane of the integrated pages. If you turn on this switch, the left-side navigation panes of the integrated pages are hidden. In this case, you can choose to display only specific pages that are related to the integrated pages by configuring the URLs of the specific pages.
Basic Information	**Application Name**	The name of the application to which you want to integrate the pages of the Apsara Uni-manager Management Console. The name must be 3 to 25 characters in length.
	Application Domain Name	The domain name of the application to which you want to integrate the pages of the Apsara Uni-manager Management Console. The domain name must be an HTTPS domain name. Example: https://console.example.com. **Note** You must specify all domain names that are involved in the application, including the domain name of the iFrame page. Otherwise, the integrated pages may not be properly displayed due to the security restrictions of your browsers. Separate multiple domain names with commas (,).
	Application Description	The description of the application to which you want to integrate the pages of the Apsara Uni-manager Management Console.

ii. **Page Style Configuration**: In this step, configure the style of the integrated pages to match the style of your console.

Section	Parameter	Description
Platform Language	**Supported Languages**	The languages that are supported by the pages of the Apsara Uni-manager Management Console. Valid values: Simplified Chinese, Traditional Chinese, and English.
	Default Language	The default language of the integrated pages.
Appearance & Theme	**Appearance**	The style of the integrated pages. Valid values: Light Mode and Dark Mode.
	Theme Color	The theme color of the integrated pages.
Page Watermark	**Switch**	Specifies whether to add watermarks to integrated pages. After you turn on the switch, you can configure the content of the watermark. A watermark can contain up to 10 characters.

iii. **Embedded Page Configuration**: In this step, configure the URLs of the pages that you want to integrate into your console from the Apsara Uni-manager Management Console. Some pages of the following services in the Apsara Uni-manager Management Console can be integrated into other consoles: Elastic Compute Service (ECS), Auto Scaling, ApsaraDB for MongoDB, ApsaraDB RDS, Lindorm, Server Load Balancer (SLB), Virtual Private Cloud (VPC), and Cloud Enterprise Network (CEN).

To create or scale resources in the corresponding pages of your console by clicking buttons in the integrated pages, you must configure operational URLs for the buttons. This way, you can use the integrated pages with your console in a unified manner.

> **Note**
>
> The operational URLs must be a lower-level domain name of the application domain name that you specified in the Destination Application Configuration step and must be complete URLs that can be accessed.

5. After the configuration is complete, the pages of the Apsara Uni-manage Management Console are embedded to the page of your console.

   On the **Overview** page, you can click **Page URL Embedding** to view the operational URLs of the integrated pages.

10.Edge Cloud management

10.1. View edge entities

The EDGE list page displays the connected edge entities. You can view the connection status of the edge entities and log on to the console of an edge entity.

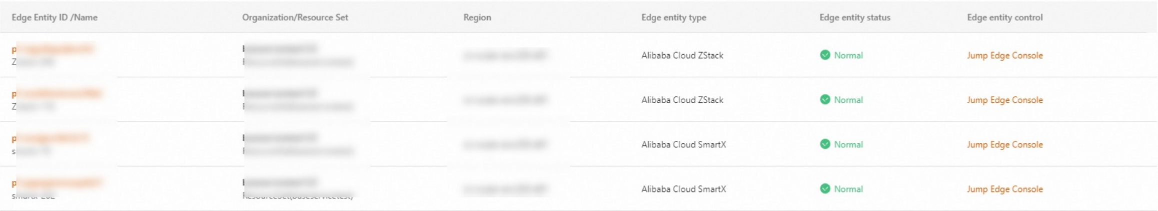
Prerequisites

Edge entities are connected. For more information, see Configure edge entities.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Computing** > **Edge Computing** > **Edge Entity**.
3. In the left-side navigation pane, click **Edge Entity**.
4. In the top navigation bar, select an organization, a resource set, and a region.
5. On the **EDGE list** page, view the information about the connected edge entity in the following columns: **Edge Entity ID/Name**, **Organization/Resource Set**, **Region**, **Edge Entity Type**, **Edge Entity Status**, and **Edge Entity Control**.

   > **Note**
   >
   > You can click **Jump Edge Console** in the Edge Entity Console column to go to the console of an edge entity.



Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Edge entity status	Edge entity control
[redacted]	[redacted]	[redacted]	Alibaba Cloud ZStack	Normal	Jump Edge Console
[redacted]	[redacted]	[redacted]	Alibaba Cloud ZStack	Normal	Jump Edge Console
[redacted]	[redacted]	[redacted]	Alibaba Cloud SmartX	Normal	Jump Edge Console
[redacted]	[redacted]	[redacted]	Alibaba Cloud SmartX	Normal	Jump Edge Console

6. Find an edge entity and click the ID of the edge entity to go to the **Edge Entity Overview** page.

   - **View the basic information**

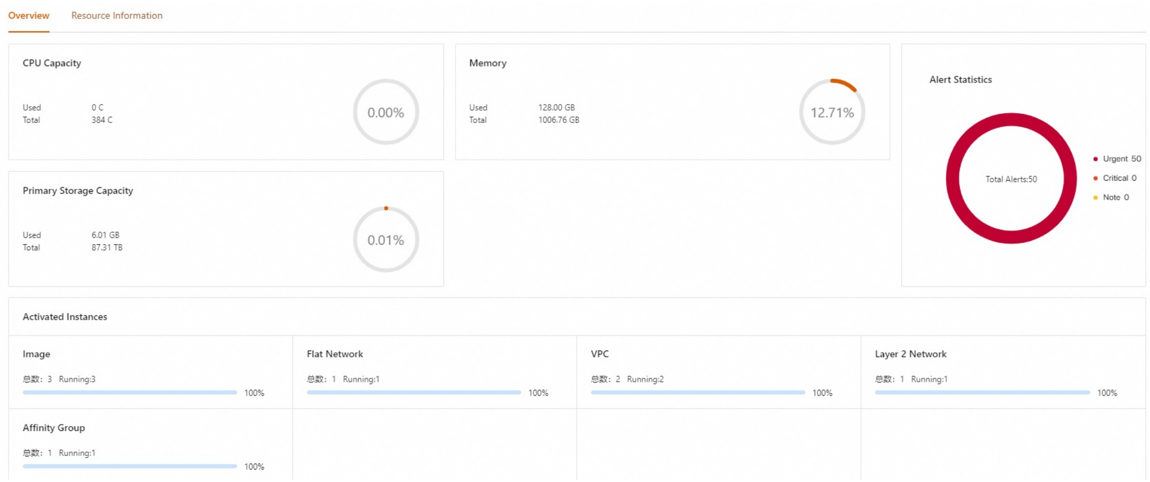
     In the **Basic Information** section, view the following information about the edge entity: the edge entity name, edge entity ID, edge entity type, organization, resource set, region, and link to the edge entity console.

   - **View the overview information**

     On the **Overview** tab, view the CPU capacity, memory capacity, primary storage capacity, alert statistics, and number of activated instances of the edge entity.

Item	Description
CPU Capacity	Displays the used CPU capacity, total inventory, and percentage of the used CPU capacity.

Memory	Displays the used memory capacity, total inventory, and percentage of the used memory capacity.
Primary Storage Capacity	Displays the used primary storage capacity, total inventory, and percentage of the used primary storage capacity.
Alert Statistics	Displays the total number of alerts for the edge entity and the number of alerts at the **Urgent**, **Critical**, and **Note** levels.
Activated Instances	Displays the resources that are activated for the edge entity, including the total number of resources of each type, the number of resources in the **Running** state, and the percentage of resources in the **Running** state.



CPU Capacity
Used 0 C
Total 384 C

Memory
Used 128.00 GB
Total 1006.76 GB

Primary Storage Capacity
Used 6.01 GB
Total 87.31 TB

Alert Statistics
Urgent 50
Critical 0
Note 0

Activated Instances

Image
总数：3 Running:3

Flat Network
总数：1 Running:1

VPC
总数：2 Running:2

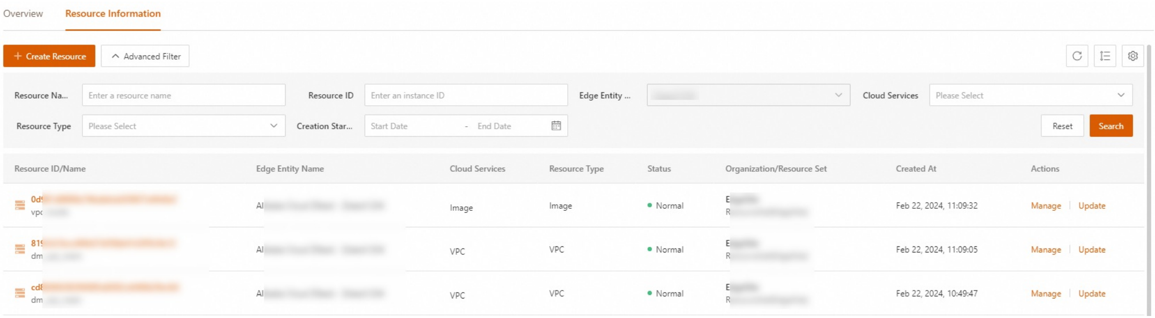
Layer 2 Network
总数：1 Running:1

Affinity Group
总数：1 Running:1

- ### View the resource information

  On the **Resource Information** tab, view the detailed resource information of the edge entity. You can configure the **Cloud Services**, **Resource Type**, **Creation Start and End Time**, **Resource Name**, and **Resource ID** parameters to filter resources.

  > **Note**
  >
  > - Click **Create Resource**. In the **Select Resource Type** dialog box, configure the **Organization**, **Resource Set Name**, **Edge Entity**, and **Cloud Services** parameters.
  > - Find a resource and click the resource ID. In the panel that appears, view the basic information of the resource, including the cloud platform, resource name, resource ID, region, organization, resource set, creation time, and state.
  > - Find a resource and click **Manage** in the **Actions** column to go to the cloud service resource management page of the edge site. You can manage the resource on the page.
  > - By default, cloud resource information is automatically updated every hour. Find a resource and click **Update** in the **Actions** column to manually update the information about the cloud resource in real time.



Resource Na... Enter a resource name
Resource ID Enter an instance ID
Edge Entity ...
Cloud Services Please Select
Resource Type Please Select
Creation Star... Start Date - End Date

Resource ID/Name	Edge Entity Name	Cloud Services	Resource Type	Status	Organization/Resource Set	Created At	Actions
0d vpc	Al	Image	Image	● Normal	E R	Feb 22, 2024, 11:09:32	Manage | Update
81 dm	Al	VPC	VPC	● Normal	E R	Feb 22, 2024, 11:09:05	Manage | Update
cd dm	Al	VPC	VPC	● Normal	E R	Feb 22, 2024, 10:49:47	Manage | Update

10.2. Manage resources

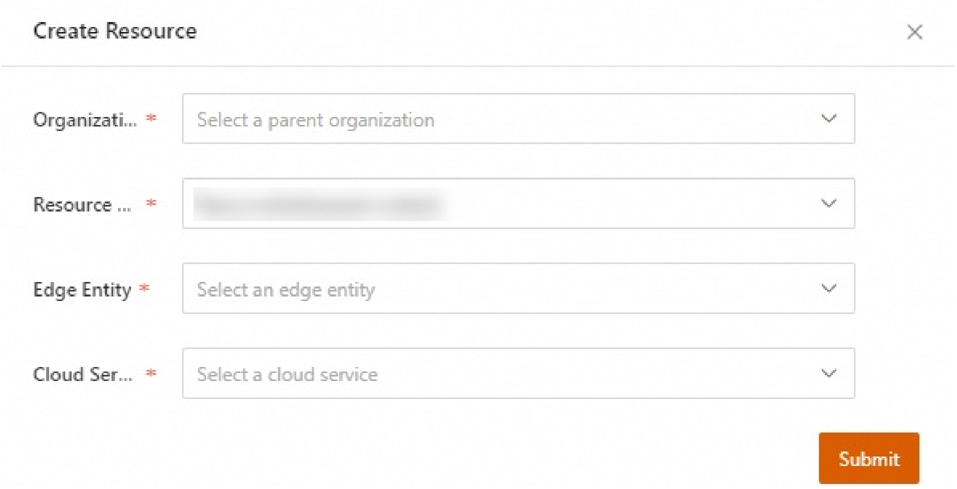
On the Resources page, you can view all edge entity resources that you can manage.

Limits

Before you create a resource, make sure that you have created an organization and a resource set, and an edge entity is connected.

Create a resource

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Computing** > **Edge Computing** > **Edge Entity**.
3. In the left-side navigation pane, click **Resources**.
4. In the top navigation bar, select an organization, a resource set, and a region.
5. On the **Resources** page, click **Create Resource**.
6. In the **Create Resource** dialog box, configure the **Organizations**, **Resource Set Name**, **Edge Entity**, and **Cloud Services** parameters.



Create Resource

Organizati... * Select a parent organization

Resource ... *

Edge Entity * Select an edge entity

Cloud Ser... * Select a cloud service

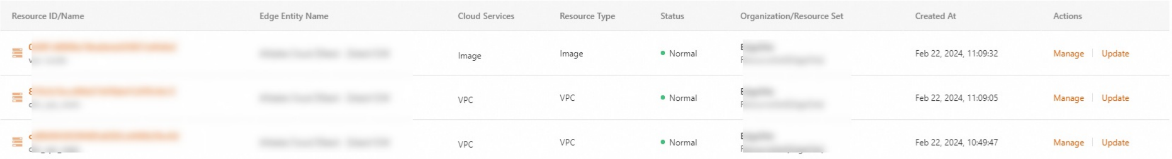
7. Click **Submit**.

View resources

1. On the **Resources** page, configure the **Resource Name**, **Resource ID**, **Edge Entity Name**, **Cloud Services**, **Resource Type**, and **Creation Start and End Time** parameters to filter resources.

2. On the Resources page, view the information about resources in the following columns: **Resource ID/Name**, **Edge Entity Name**, **Cloud Services**, **Resource Type**, **Status**, **Organization/Resource Set**, and **Created At**.

> **Note**
>
> - Find a resource and click **Manage** in the **Actions** column to go to the cloud service resource management page of the edge site. You can manage the resource on the page.
> - Find a resource and click **Update** in the **Actions** column to manually update the information and state of the resource.



Resource ID/Name	Edge Entity Name	Cloud Services	Resource Type	Status	Organization/Resource Set	Created At	Actions
[redacted]	[redacted]	Image	Image	● Normal	[redacted]	Feb 22, 2024, 11:09:32	Manage | Update
[redacted]	[redacted]	VPC	VPC	● Normal	[redacted]	Feb 22, 2024, 11:09:05	Manage | Update
[redacted]	[redacted]	VPC	VPC	● Normal	[redacted]	Feb 22, 2024, 10:49:47	Manage | Update

3. Find a resource and click the resource ID. In the panel that appears, view the basic information of the resource, including the cloud platform, resource name, resource ID, region, organization, resource set, creation time, and state.

10.3. Configure edge entities

On the Edge Entity Configuration page, you can view the connected edge entities and manage the edge entities that do not belong to an organization or a resource set.

Limits

Before you connect to an edge entity, make sure that you have created an organization and a resource set.

Connect to an edge entity

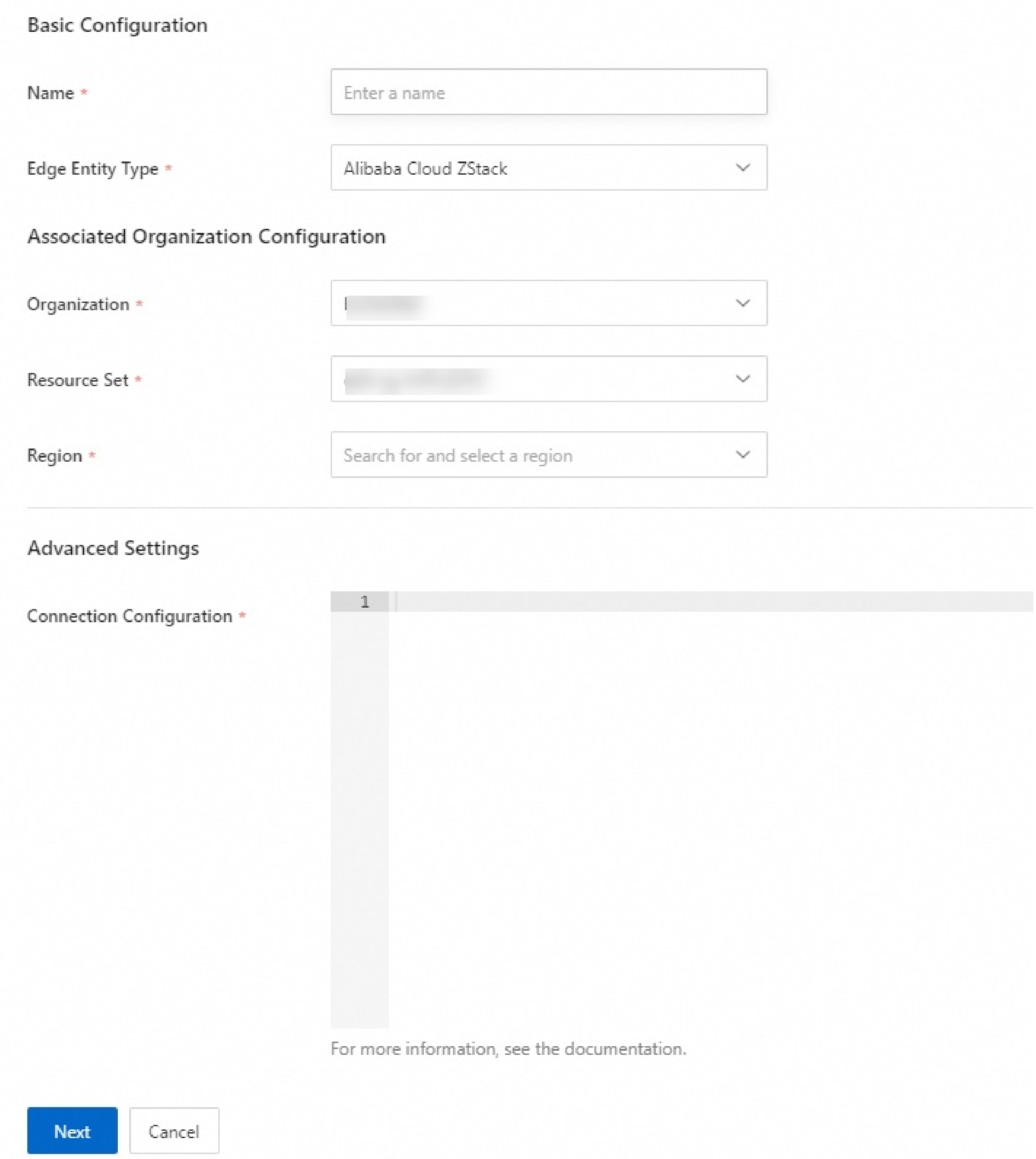
1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Computing** > **Edge Computing** > **Edge Entity**.
3. In the left-side navigation pane, click **Edge Entity Configuration**.
4. On the **Edge Entity Configuration** page, click **Connect Edge Entity**.
5. Configure the parameters in the following steps as prompted:

> **Note**
>
> If you have questions when you connect to an edge entity, contact Apsara Stack technical support.

i. **Basic Information**: Select an edge entity type and configure information in the **Basic Configuration**, **Associated Organization Configuration**, and **Advanced Settings** sections for the edge entity.

Section and parameter	Description

Basic Configuration	**Name**	The custom name of the edge entity.
	Edge Entity Type	The type of the edge entity. Valid values:**Alibaba Cloud ZStack** and **Alibaba Cloud SmartX**.
Associated Organization Configuration	**Organization**	The organization to which the edge entity belongs.
	Resource Set	The resource set to which the edge entity belongs.
	Region	The region in which the edge entity resides.
Advanced Settings	**Connection Configuration**	The connection configurations of the edge entity. ▪ For more information about the connection configurations of an Alibaba Cloud ZStack edge entity, see the Configuration template for Alibaba Cloud ZStack section of this topic. ▪ For more information about the connection configurations of an Alibaba Cloud SmartX edge entity, see the Configuration template for Alibaba Cloud SmartX section of this topic.



Basic Configuration

Name *: Enter a name

Edge Entity Type *: Alibaba Cloud ZStack

Associated Organization Configuration

Organization *: [redacted]

Resource Set *: [redacted]

Region *: Search for and select a region

Advanced Settings

Connection Configuration *

For more information, see the documentation.

Configuration template for Alibaba Cloud ZStack

JSON

```
{
  "endPoint": "http://{ip1}:{port1}/zstack",
  "properties":{
    "oidcAuthEndpoint":"http://{ip2}:{port2}/zstack",
    "consoleEndpoint":"http://{ip3}:{port3}"
  }
}
```

Note

- endPoint: the IP address and port that are mapped to the Server Load Balancer (SLB) API in the configurations for virtual private cloud (VPC)-based reverse access.
- oidcAuthEndpoint: the IP address and port that are mapped to the API in the SLB configurations.
- consoleEndpoint: the IP address and port that are mapped to the portal in the SLB configurations.

Configuration template for Alibaba Cloud SmartX

JSON

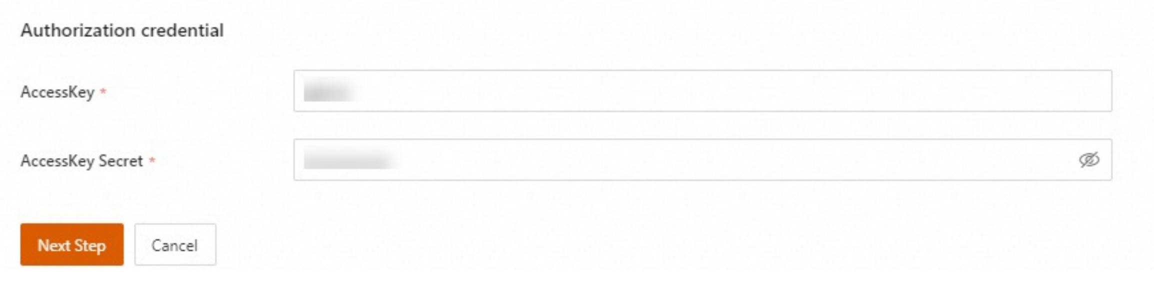
```
{
 "endPoint": "http://{ip1}:{port1}/api/alpha/proxy/cloudtower-alpha-ali-cmp-service
",
 "properties": {
  "consoleEndpoint": "http://{ip2}:{port2}"
 }
}
```

Note

- endPoint: the IP address and port that are mapped to the SLB API in the configurations for VIP-based reverse access.
- consoleEndpoint: {ip2} indicates the IP address of the SLB instance. {port2} indicates the listener port of the SLB instance that is used to listen to the specified service.

ii. **Account Authorization**: Enter the authorization credentials of the edge entity to grant permissions to the current account and synchronize the role of the account.

Parameter	Description
AccessKey ID	The AccessKey ID of the edge entity.
AccessKey Secret	The AccessKey secret of the edge entity.



Authorization credential

AccessKey * [redacted]

AccessKey Secret * [redacted]

- **Obtain the authorization credentials of an Alibaba Cloud ZStack edge entity**

  a. Log on to the Alibaba Cloud ZStack console**.**

  b. On the **Operational Management** tab, click **AccessKey Management** in the left-side navigation pane. On the **AccessKey Management** page, view the AccessKey ID and AccessKey secret.

  > **Note**
  >
  > If no AccessKey pair is available, click **Generate AccessKey** to create an AccessKey pair.

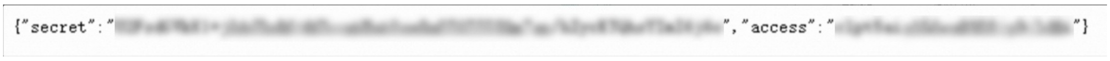
- **Obtain the authorization credentials of an Alibaba Cloud SmartX edge entity**

  a. Log on to an Alibaba Cloud SmartX edge entity by using a URL in the following format: `http://{IP address of the Alibaba Cloud SmartX edge entity}/api/alpha/proxy/cloudtower-alpha-ali-cmp-service/admin/get-access-key` .

  > **Note**
  >
  > {IP address of the Alibaba Cloud SmartX edge entity} indicates the IP address of the portal of the Alibaba Cloud SmartX console. Replace the value based on the actual situation.

  b. Enter the root account and password of the Cluster Manager role to obtain the AccessKey ID and AccessKey secret.

  > **Note**
  >
  > - access: the AccessKey ID of the edge entity.
  > - secret: the AccessKey secret of the edge entity.

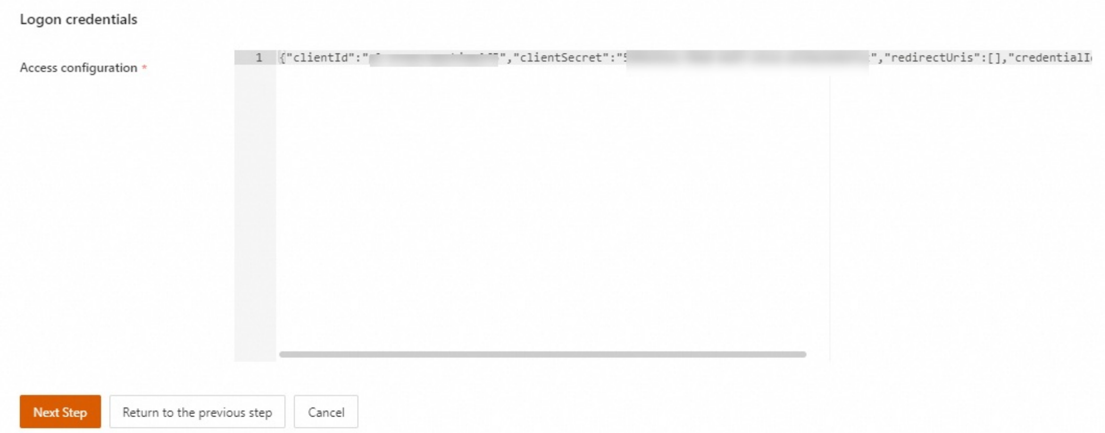


```
{"secret":"[redacted]","access":"[redacted]"}
```

iii. **Federated Logon Settings**: Complete federated logon settings for third-party cloud management.

- **Federated logon settings for Alibaba Cloud ZStack**

  a. In the **Access configuration** field of the **Federated Logon Settings** step, obtain the values of the **clientId** and **clientSecret** parameters.



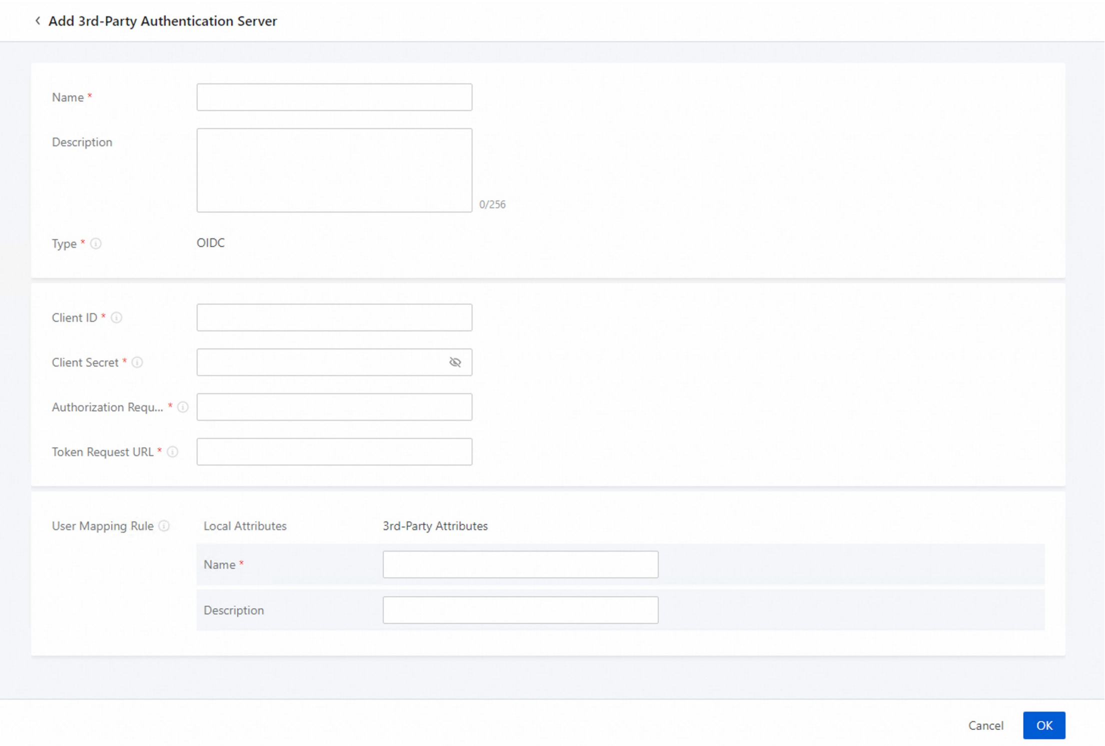
Logon credentials

Access configuration *

```
{"clientId":"[redacted]","clientSecret":"[redacted]","redirectUris":[],"credentialI
```

b. Log on to the Alibaba Cloud ZStack console. On the **Settings** tab, click **Add 3rd-Party Authentication Server**. On the page that appears, add a third-party server for authentication.

Parameter	Description
Name	The custom name of the third-party server.
Description	The description of the third-party server.
Type	The type of the third-party server. Set the value to OIDC.
Client ID	The client ID that is obtained from the access configurations of the federated logon settings.
Client Secret	The client secret that is obtained from the access configurations of the federated logon settings.
Authorization Request URL	The authorization request URL, in the following format: `https://{Domain name}/auth/realms/cmp/protocol/openid-connect/auth` . **Note** Replace {Domain name} with the domain name of the corresponding environment based on the environment configurations. ▪ **Versions earlier than V3.18.2** Concatenate a domain name in the following format: mcm.${global:internet-domain}. ▪ **V3.18.2 and later** Concatenate a domain name in the following format: mcm.console.${global:internet-domain}.
Token Request URL	The token request URL, in the following format: `http://{IP address}/auth/realms/cmp/protocol/openid-connect/token` . **Note** Replace {IP address} with the IP address of SingleTunnel based on the environment configurations.
User Mapping Rule	▪ **Name**: the name of the user mapping rule. Set the value to **preferred_username**. ▪ **Description**: the description of the user mapping rule.



‹ Add 3rd-Party Authentication Server

Name *

Description

0/256

Type * ⓘ OIDC

Client ID * ⓘ

Client Secret * ⓘ

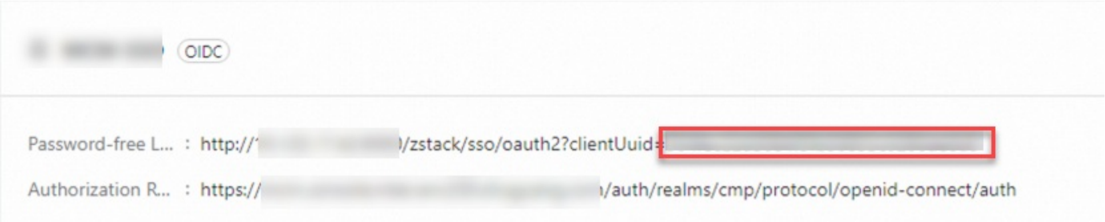
Authorization Requ... * ⓘ

Token Request URL * ⓘ

User Mapping Rule ⓘ	Local Attributes	3rd-Party Attributes
	Name *	
	Description	

Cancel OK

c. Click **OK** to obtain the client UUID.

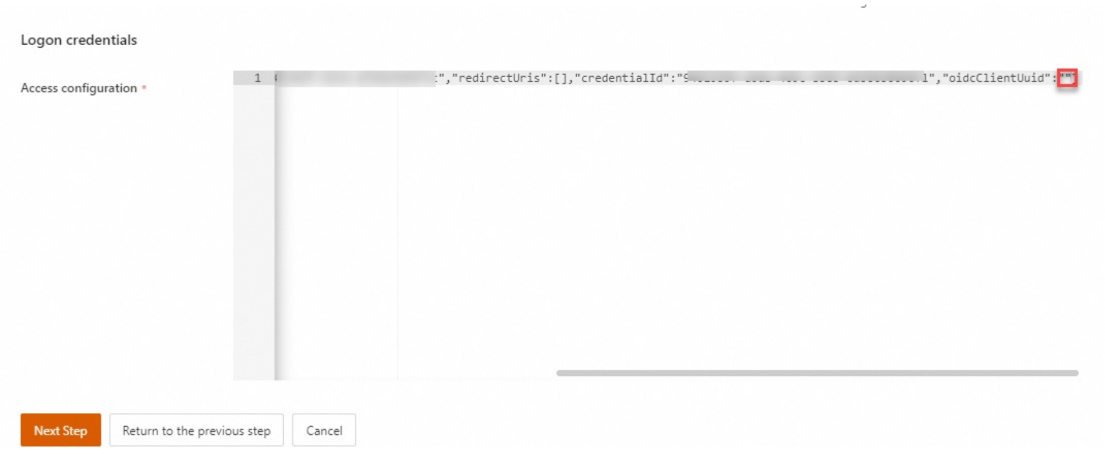


[redacted] OIDC

Password-free L... : http://[redacted]/zstack/sso/oauth2?clientUuid=[redacted]

Authorization R... : https://[redacted]/auth/realms/cmp/protocol/openid-connect/auth

d. Go back to the **Federated Logon Settings** step and enter the client UUID that is obtained in the previous step as the value of the **oidcClientUuid** parameter in the **Access configuration** field.



Logon credentials

Access configuration *

```
{[redacted]","redirectUris":[],"credentialId":"[redacted]","oidcClientUuid":""
```

Next Step Return to the previous step Cancel

- **Federated logon settings for Alibaba Cloud SmartX**

  a. Log on to an Alibaba Cloud SmartX edge entity by using a URL in the following format: `https://{IP address of the Alibaba Cloud SmartX edge entity}/api/alpha/proxy/cloudtower-alpha-ali-cmp-service/authentication/sso/saml/metadata` to obtain authentication information for password-free logon.

  b. Go back to the **Federated Logon Settings** step and copy all the authentication information for password-free logon to the **Access configuration** field.

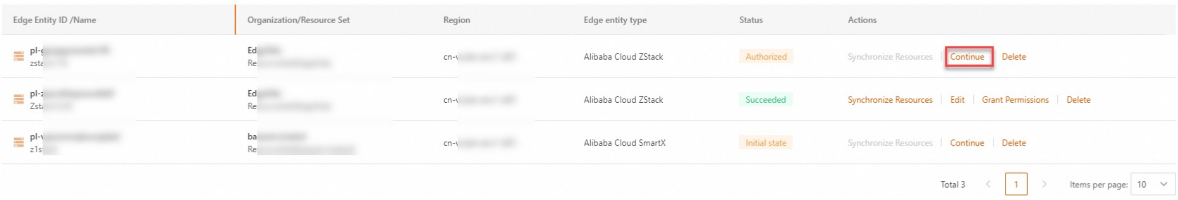
iv. **Data Synchronization**: Select the required region and supported cloud services to synchronize data.

v. **Complete**: After the synchronization is complete, go back to the Edge Entity Configuration page.

Resume the connection to an edge entity

1. On the **Edge Entity Configuration** page, find an edge entity and click **Continue** in the **Actions** column.

> **Note**
>
> If you do not complete the wizard for connecting to an edge entity, the last operation is automatically saved. You can resume the connection to the edge entity from the last operation.



Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Status	Actions
pl-[redacted] zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Authorized	Synchronize Resources | Continue | Delete
pl-[redacted] Zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Succeeded	Synchronize Resources | Edit | Grant Permissions | Delete
pl-[redacted] z1s[redacted]	ba[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud SmartX	Initial state	Synchronize Resources | Continue | Delete

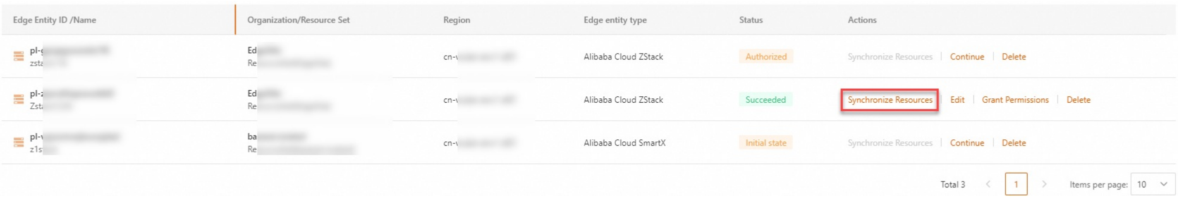
Total 3 < 1 > Items per page: 10

2. In the edge entity connection wizard, resume the connection to the edge entity form the last operation.

Synchronize edge entity resources

1. On the **Edge Entity Configuration** page, find an edge entity and click **Synchronize Resources** in the **Actions** column.

> **Note**
>
> - After you connect to an edge entity, the cloud resources of the edge entity are automatically synchronized every hour by default.
> - You can click **Synchronize Resources** in the **Actions** column of an edge entity to manually synchronize the cloud resources of the edge entity in real time.



Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Status	Actions
pl-[redacted] zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Authorized	Synchronize Resources | Continue | Delete
pl-[redacted] Zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Succeeded	Synchronize Resources | Edit | Grant Permissions | Delete
pl-[redacted] z1s[redacted]	ba[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud SmartX	Initial state	Synchronize Resources | Continue | Delete

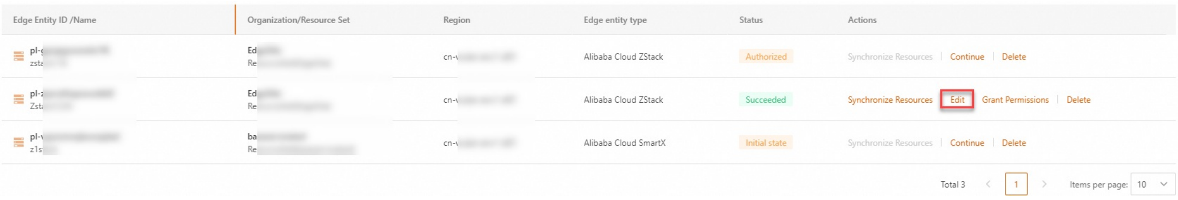
Total 3 < 1 > Items per page: 10

2. In the **Synchronize Resources** message, click **OK**.

Modify the name of an edge entity

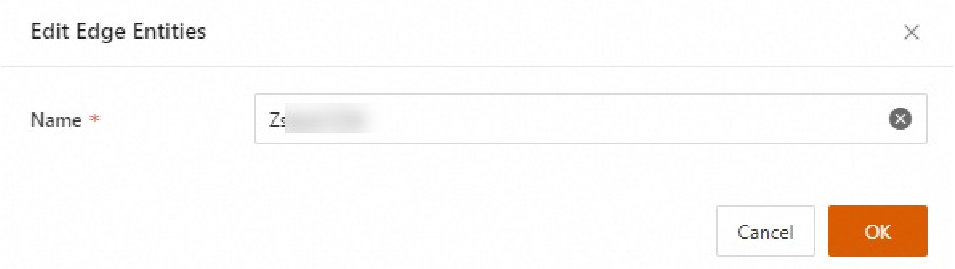
1. On the **Edge Entity Configuration** page, find an edge entity and click **Edit** in the **Actions** column.

> **Note**
>
> If the edge entity is in the **Succeeded** state, you can modify the name of the edge entity.



Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Status	Actions
pl- zsta	Ed Re	cn-	Alibaba Cloud ZStack	Authorized	Synchronize Resources | Continue | Delete
pl- Zsta	Ed Re	cn-	Alibaba Cloud ZStack	Succeeded	Synchronize Resources | Edit | Grant Permissions | Delete
pl- z1s	ba Re	cn-	Alibaba Cloud SmartX	Initial state	Synchronize Resources | Continue | Delete

2. In the **Edit Edge Entities** dialog box, modify the name of the edge entity and click **OK**.



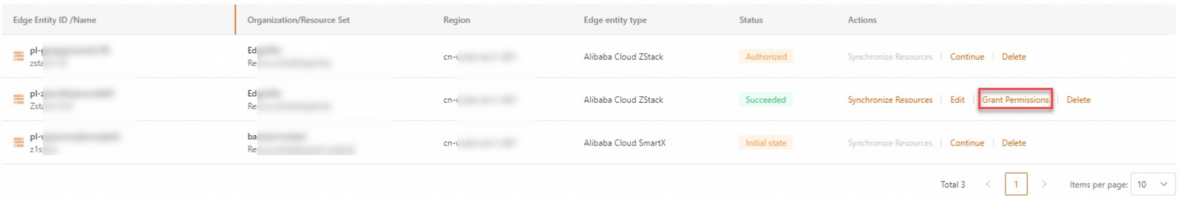
Edit Edge Entities

Name * Zs

Grant permissions to an edge entity

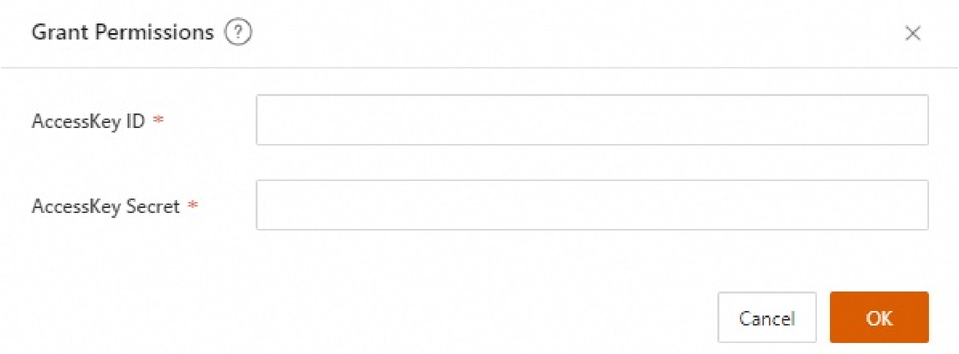
If the permissions granted to an edge entity expire, you can grant permissions to the edge entity by performing the following steps:

1. On the **Edge Entity Configuration** page, find the edge entity to which you want to grant permissions and click **Grant Permissions** in the **Actions** column.



Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Status	Actions
pl- zsta	Ed Re	cn-	Alibaba Cloud ZStack	Authorized	Synchronize Resources | Continue | Delete
pl- Zsta	Ed Re	cn-	Alibaba Cloud ZStack	Succeeded	Synchronize Resources | Edit | Grant Permissions | Delete
pl- z1s	ba Re	cn-	Alibaba Cloud SmartX	Initial state	Synchronize Resources | Continue | Delete

2. In the **Grant Permissions** dialog box, configure the **AccessKey ID** and **AccessKey Secret** parameters.



Grant Permissions

AccessKey ID *

AccessKey Secret *

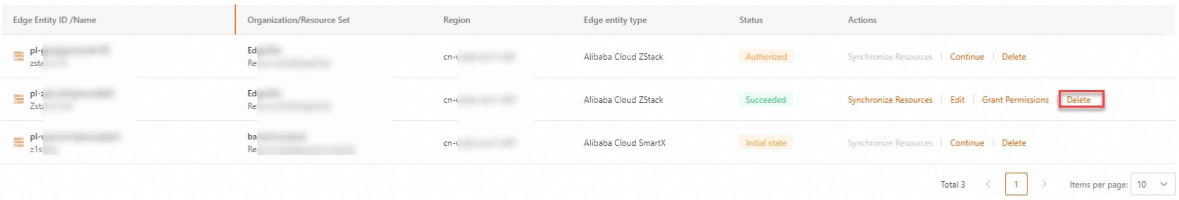
3. Click **OK**.

Delete an edge entity

You can delete an edge entity if you no longer need the edge entity.

1. On the **Edge Entity Configuration** page, find the edge entity that you want to delete and click **Delete** in the **Actions** column.

   > **Note**
   >
   > Make sure that the edge entity is no longer needed.

Edge Entity ID /Name	Organization/Resource Set	Region	Edge entity type	Status	Actions
pl-[redacted] zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Authorized	Synchronize Resources | Continue | Delete
pl-[redacted] Zsta[redacted]	Ed[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud ZStack	Succeeded	Synchronize Resources | Edit | Grant Permissions | Delete
pl-[redacted] z1s[redacted]	ba[redacted] Re[redacted]	cn-[redacted]	Alibaba Cloud SmartX	Initial state	Synchronize Resources | Continue | Delete

2. In the **Confirmation** message, click **OK**.

11.Multi-Cloud Management Platform

11.1. Overview

The multi-cloud management platform consists of multiple modules such as multi-cloud access management, cloud service management, user organization management, permission management, project management, resource management, cross-cloud authorization, multi-cloud metering management, log audit, message management, and system configuration management. The multi-cloud management platform provides various features such as connection management on multiple cloud platforms, cloud service and cloud resource management, and management of organizations, users, and permissions. This helps you implement a unified management portal for multiple cloud centers in a heterogeneous cloud platform environment.

The multi-cloud management platform provides different user interfaces (UIs) to implement different features for multi-cloud platform management based on the user roles on the platform side and tenant side.

- Platform side: Provides management capabilities on cloud platforms, including cloud platform management and cloud service classification. Platform-side users can also use features such as permission management, message management, and system configuration to manage platform-side configurations.
- Tenant side: Provides tenants with the capabilities to manage and use cloud resources of various platforms that have been connected to the multi-cloud management platform. Tenants can implement a more efficient and finer-grained authorization and management on multi-cloud platform resources by configuring organizations, projects, and users. The multi-cloud management platform also provides the centralized management feature for resource metering on multiple cloud platforms, as well as the cross-cloud authorization and operation log audit features.

11.2. Platform-side User Guide

11.2.1. Cloud platform management

All cloud platforms that are managed by the multi-cloud management platform are displayed on the Cloud Platform page. You can connect the multi-cloud management platform to Alibaba Cloud, Apsara Stack, and Edge Cloud for management. The multi-cloud management platform can also manage other heterogeneous cloud platforms by using adapters. For the cloud platforms that are managed by the multi-cloud management platform, you can edit basic information, synchronize account authorization, synchronize tenant and service information, and configure region management. In this case, platform administrators can manage the basic information about the cloud platforms, such as tenants, services, and regions.

Procedure

1. Log on to the multi-cloud management platform by using the account that has the platform administrator role.

> **Note**
>
> - Log on to the Apsara Uni-manager Management Console by using the account that has the administrator role of the multi-cloud management platform and switch to the platform administrator role. Then, you are redirected to the multi-cloud management platform.
> - If you want to log on to the multi-cloud management platform that is independently deployed, contact the platform deployment and delivery engineers to obtain the endpoint of the multi-cloud management platform and the username and password of the platform administrator account.

2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Multi-level Clouds** > **Cloud Platform**.
3. On the Cloud Platform page, you can view all cloud platforms that are managed by the multi-cloud management platform.
4. Click **Create Cloud Platform** or **Create a Cloud Platform with an Adapter** and connect to the cloud platform to be managed as prompted.

   > **Note**
   >
   > We recommend that you ask the platform deployment and delivery engineers to connect to the cloud platform. For more information, see Multi-cloud Management Platform Deployment Guide.

5. After you connect to the cloud platform, you can perform the following operations on the **Cloud Platform** page:
   - **Edit**: You can edit the basic information about the cloud platform, such as the display name, proxy endpoint, and theme color.
     - **Proxy Address**: If the managed cloud platform is accessed by using an HTTP proxy and the proxy endpoint changes after connection, you must update the proxy endpoint at the earliest opportunity. The proxy endpoint is specified in the Proxy IP address:Port format. This ensures that the multi-cloud management platform can access the managed cloud platform as expected.
     - **Theme**: You can modify the theme color of the cloud platform. The dominant color of the cloud platform icon in the multi-cloud management platform distinguishes the cloud platform from other cloud platforms.
   - **Cloud Account Authorization**: You can configure the access credentials for the multi-cloud management platform, including the AccessKey ID and AccessKey secret, to access the managed cloud platform. If the access credentials change after connection, you must update the access credentials at the earliest opportunity. Otherwise, the multi-cloud management platform fails to synchronize data of the managed cloud platform.
   - **Cloud Tenant**: You can view the names and creation time of the synchronized tenants of a managed cloud platform. If the tenant information in the cloud platform changes and the change is not automatically synchronized to the multi-cloud management platform, you can click **Synchronize** to manually synchronize the tenant information. After the tenant information is synchronized, you can view and confirm the information in the **Cloud Tenant** panel.
   - **Cloud Product Configuration**: You can view the synchronized services of a managed cloud platform and the service status. If the service data of the cloud platform changes and the change is not automatically synchronized to the multi-cloud management platform, you can click **Synchronization** to manually synchronize the data. After data is synchronized, you can view and confirm the data in the **Cloud Product Configuration** panel.

> **Note**
>
> Make sure that the access configurations of a cloud platform include the access configurations of the cloud platform services.

- **Regional Management**: You can view the information about the synchronized regions of a managed cloud platform and **disable** or enable the management of a specific region in the multi-cloud management platform. The **Map Configuration** feature allows you to complete the location information about a region, accurate to a district and a county. The multi-cloud management platform identifies the location of the regions of a managed cloud platform in geographic charts, such as the Cloud Platform Overview chart.
- **Delete**: You can delete the configurations of a managed cloud platform. You cannot delete the configurations of Apsara Stack that is deployed together with the multi-cloud management platform.

> ⚠ **Warning**
>
> After you delete the configurations of a managed cloud platform, all information about the cloud platform is deleted. Proceed with caution. If you want to manage the cloud platform in the multi-cloud management platform again, you must re-configure all access configurations of the cloud platform.

11.2.2. Tenant management

The Tenant Management page displays all tenants of the cloud platforms that are managed by the multi-cloud management platform. You can manage tenants in a centralized manner. For example, you can create tenants, modify tenant information, and manage the permissions of tenants to access cloud platforms.

Procedure

1. Log on to the multi-cloud management platform by using the account that has the platform administrator role.

   > **Note**
   >
   > - Log on to the Apsara Uni-manager Management Console by using the account that has the administrator role of the multi-cloud management platform and switch to the platform administrator role. Then, you are redirected to the multi-cloud management platform.
   > - If you want to log on to the multi-cloud management platform that is independently deployed, contact the platform deployment and delivery engineers to obtain the endpoint of the multi-cloud management platform and the username and password of the platform administrator account.

2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Tenants** > Tenants. The **Tenant Management** page appears.
3. On the Tenant Management page, you can view all tenants that are managed by the multi-cloud management platform.
4. Click **Create Tenant**. In the Create Tenant dialog box, enter a tenant name, and then click **OK**.
5. On the **Tenant Management** page, you can perform the following operations:
   - **Modify**: You can modify the name of a tenant.

- **Cloud Platform Authorization**: In the Tenant authorization panel, you can view the cloud platforms that a tenant is authorized to access. In the Tenant authorization panel, click **Cloud Platform Authorization** to authorize the tenant to access a cloud platform or click **Revoke Authorization** to revoke permissions to access a cloud platform from the tenant.

  > **Note**
  >
  > A tenant is authorized to access at least one cloud platform.

- **Delete**: You can delete a tenant. If you want to delete a tenant, you must enter the unique ID of the tenant.

  > ⚠ **Warning**
  >
  > After you delete a tenant, all data of the tenant is deleted and cannot be rolled back.

11.2.3. Personnel management

Personnel management is implemented by using the user management module, which is used to manage users of the multi-cloud management platform. You can create users, grant permissions to users, reset passwords, view user details, and disable users.

> **Note**
>
> If the multi-cloud management platform is deployed together with Apsara Stack, the Apsara Stack account that has the multi-cloud operations administrator role permissions is the platform administrator of the multi-cloud management platform by default. The platform administrator has all operation permissions on the multi-cloud management platform. The user management module is configured in the Apsara Uni-manager Management Console. Therefore, the features of the user management module on the platform side are the same as those on the tenant side. For more information, see User management.

Procedure

1. Log on to the multi-cloud management platform as a platform administrator.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Personnel Management** >**User Management**.
3. On the User Management page, you can view the users of the multi-cloud management platform.

   > **Note**
   >
   > If the multi-cloud management platform is independently deployed, the root and admin users are built in after the platform is deployed. The root user is the platform system administrator and is used to manage the platform-side configurations of the multi-cloud management platform. The admin user is the tenant-side administrator and is used to manage the tenant-side configurations of the multi-cloud management platform.

4. Click **Create User** to create a user that can assume the platform administrator role.

Parameter	Description

User Name	The name of the user. The username must be 3 to 32 characters in length and can contain letters, digits, underscores (_), and hyphens (-). **Note** After the user is created, you cannot modify the username.
Role	The role that you want to assign to the user. The platform administrator and platform security administrator roles are provided. You cannot add custom roles. The platform administrator has permissions on all features on the platform side. The platform security administrator has the permissions on role management, security policy, and log audit features.
Display Name	The display name of the user. The name must be 3 to 32 characters in length and can contain letters, digits, underscores (_), and hyphens (-).
Telephone	The phone number of the user, which is used to receive text messages from the multi-cloud management platform. **Note** After the user is created, the phone number and email address of the user are hidden in the user list by default. The information is displayed only after you click the View icon.
Email address	The email address of the user, which is used to receive emails from the multi-cloud management platform.

5. Click **OK**. Then, the user is created. The system automatically generates an initial password for the user.

   > **Note**
   >
   > When you use the initial password to log on to the multi-cloud management platform for the first time, you must reset the password.

6. After the user is created, you can perform the following operations to manage the user on the **User Management** page:

   - **Edit**: Edit the basic information about the user, such as the display name, phone number, and email address.
   - **Enable** and **Disable**: Enable or disable the user. A disabled user cannot log on to the multi-cloud management platform. If the user is currently logged on to the multi-cloud management platform, all features are disabled for the user.

     > **Note**
     >
     > You cannot disable the user that you currently use to log on to the multi-cloud management platform. To disable this user, you must use another administrator account to log on to the multi-cloud management platform.

- **Role Authorization**: Manage the roles of the user. You can assign only the built-in platform administrator or platform security administrator role to the user.
- **Reset Password**: Reset the password of the user. The system automatically generates a random password when you reset the password. When you use the random password to log on to the multi-cloud management platform for the first time, you must change the password. You cannot reset the password of the user that you currently use to log on to the multi-cloud management platform.
- **Delete**: Delete the user. You cannot delete built-in users or the user that you currently use to log on to the multi-cloud management platform.

11.2.4. Permission management

Permission management is implemented by using the role management module. You can view the permission details of preset roles and the users who are assigned roles by using the role management module. You can also associate roles with and disassociate roles from users on the Roles page.

> **Note**
>
> If the multi-cloud management platform is deployed together with Apsara Stack, the role management module is configured in the Apsara Uni-manager Management Console. Therefore, the features of the role management module on the platform side are the same as those on the tenant side. For more information, see Role management.

Procedure

1. Log on to the multi-cloud management platform as a platform administrator.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Roles**.
3. On the page that appears, view the information about the platform-side preset roles. The preset roles include the platform administrator and platform security administrator. The platform administrator has the permissions on all features. The platform security administrator has the permissions on the role management, security policy, and log audit features.
4. Click the name of a role to go to the role details page.
    - On the **Manage Permissions** tab, you can view the permissions of the role.
    - On the **Authorization Object** tab, you can view the users to whom the role is assigned. You can click **User Authorization** to associate the role with specific users or click **Remove Authorization** to disassociate role from specific users.

11.2.5. Cross-cloud authorization

When you manage multiple cloud platforms, you may need to authorize a user to access and manage cross-cloud resources to achieve cross-cloud data synchronization based on your business requirements. Authorized users can create data synchronization tasks across multiple cloud platforms by using supported cloud services.

Only Alibaba Cloud Container Registry supports cross-cloud authorization. The multi-cloud management platform allows an authorized user of a cloud platform to directly use the image repositories and images in the specified namespace of the specified Container Registry instance on the cloud platform.

Procedure

1. Log on to the multi-cloud management platform as a platform administrator.

2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Cross-cloud Authorizations**.
3. On the page that appears, click **Create Authorization** to grant cross-cloud permissions to the specified user.
    - Select the user of the multi-cloud management platform to which you want to grant cross-cloud permissions.
    - Select the destination cloud platform and tenant to which the cloud service resources to be used by the authorized user belong.
    - Specify the AccessKey pair that is used to access the cloud service resources on the destination cloud platform. Make sure that the AccessKey pair has the required permissions to access the cloud service resources on the destination cloud platform.
    - Select the cloud service that you want to access. You can select only Container Registry.
    - Select the Container Registry instance that can be accessed on the specified cloud platform. You must also specify the region and namespace of the Container Registry instance for cross-cloud access.

    > **Note**
    >
    > You can specify multiple Container Registry instances that can be accessed on the specified cloud platform.

4. After a cross-cloud authorization policy is configured, you can modify or delete the authorization policy in the authorization policy list.
    - Click **Edit** in the Operation column to modify the cross-cloud resources that can be accessed. The authorization principal, cloud platform, and information about cloud services cannot be modified.
    - Click **Delete** in the Operation column to delete the cross-cloud authorization record. After the authorization record is deleted, the authorized user cannot manage instance resources on the authorized cloud platform. Cross-cloud accesses to authorized applications that are running are not affected. You cannot access the applications after you manually stop them.

11.2.6. Multi-cloud service catalog

The multi-cloud service catalog page displays all service categories. The name of a cloud service may vary on different cloud platforms in the multi-cloud platform scenario. You can customize a set of categories for cloud services based on your business requirements, and add cloud services of managed cloud platforms to the corresponding custom categories. This way, the cloud services are displayed by category on the tenant-side multi-cloud management platform. This implements the category management on cloud services of multiple cloud platforms.

> **Note**
>
> A cloud service can belong to only one category. The uncategorized cloud services are displayed in the **Other** category.

Procedure

1. Log on to the multi-cloud management platform as a platform administrator.

> **Note**
>
> If the multi-cloud management platform is deployed together with Apsara Stack, log on to the Apsara Uni-manager Management Console by using the super account.

2. In the top navigation bar, click **Configurations**. In the left-side navigation, click **Multi-cloud Product Catalog**.
3. On the page that appears, click **Add Category**. In the dialog box that appears, specify the category name.

   > **Note**
   >
   > The category name must be 2 to 32 characters in length and can contain letters and digits.

4. After the category is created, click **Manage Cloud Service** in the Operation column to manage the cloud services in the category.

   All cloud services on the cloud platforms that are managed by the multi-cloud management platform are displayed. Select the services that you want to add to the category on the left and add them to the list on the right. This way, the selected cloud services are added to the category. If you remove a cloud service from the right-side list, the cloud service is removed from the category.
5. On the **Cloud Product Category** page, you can also perform the following operations to manage the category:
   - **Edit**: You can modify the category name.
   - **Delete**: You can delete the category. After you delete the category, the cloud services that belong to the category are automatically removed from the category.

11.2.7. Multi-cloud adapter management

The multi-cloud management platform can manage heterogeneous cloud platforms by using third-party cloud management adapters. On the Multi Cloud Adapter page, you can manage third-party cloud management adapters. For example, you can add, edit, or delete adapters.

Procedure

1. Log on to the multi-cloud management platform by using the platform administrator account.

   > **Note**
   >
   > If the multi-cloud management platform is deployed together with Apsara Stack, log on to the Apsara Uni-manager Management Console by using the super account.

2. In the top navigation bar, click **Configurations**. In the left-side navigation pane, click **Multi-cloud Adapter**.
3. On the Multi Cloud Adapter page, click **Add Adapter**. On the page that appears, configure the following parameters to add a third-party cloud management adapter.

Parameter	Description

Name	The name of the adapter. The name must be 2 to 32 characters in length and can contain letters, digits, underscores, and hyphens (-).
Access Configuration	Upload the configuration file of the adapter. ⓘ **Note** To obtain the configuration file, contact the adapter provider.
Proxy Address	If the heterogeneous cloud platform to be managed by using the adapter is accessed by using an HTTP proxy, you must enter the proxy endpoint of the heterogeneous cloud platform. The proxy endpoint is specified in the Proxy IP address:Port format. If a proxy is not required for cloud platform access, you do not need to configure this parameter.

4. After the adapter is added, you can perform the following operations on the **Multi Cloud Adapter** page:
   - **Details**: You can view the details of the adapter, such as the basic information, API endpoint, and cloud platform adaptation capability of the adapter.
   - **Edit**: You can modify the name of the adapter.
   - **Delete**: You can remove the adapter from the multi-cloud management platform. After you remove the adapter, the configurations of the adapter are deleted.

11.3. Tenant-side User Guide

11.3.1. Enterprise

The Enterprise module is an important management module in the multi-cloud management platform. This module is used to manage the core elements, such as cloud platforms, cloud resources, organizations, projects, users, roles, and permissions, in multi-cloud management scenarios.

After multiple cloud platforms are connected to the multi-cloud management platform, the permissions on cloud resources of each cloud platform must be managed based on business scenarios and organizations. The multi-cloud management platform helps enterprises implement fine-grained management of multi-cloud platform resources by providing resource authorization based on organizations, projects, and users. The multi-cloud management platform also provides permission management capabilities based on business features, cloud services on cloud platforms, and roles.

Organization management

- You can create, modify, delete, and query organizations.
- The organizations can be mapped to the platform-side organizations. After a cloud platform is connected to the multi-cloud management platform, two-way synchronization of organization data is supported.
- You can maintain the relationships between users and organizations.
- You can maintain the cloud resources in organizations and authorize organizations to access resources on the multi-cloud management platform.

Project management

A project consists of properties such as user group, cloud instance, and cloud resource. The multi-cloud management platform helps you manage users and cloud service resources on multiple cloud platforms in a centralized manner based on projects. You can implement project-based fine-grained authorization and management on cloud platform resources.

- You can create, modify, delete, and query projects.
- You can maintain the relationships between projects and resources on the connected cloud platforms. A project can be associated with multiple cloud platform resources.
- You can maintain the relationships between projects and users. A project can be associated with multiple users and a user can associate with multiple projects.
- You can maintain the relationships between projects and user groups. A project can be associated with multiple user groups and a user group can associate with multiple projects.

User group management

- You can create, modify, delete, and query user groups.
- You can maintain the relationships between users and user groups.
- You can assign specific roles to multiple users in a user group at a time.
- You can associate one user group with one project for maintenance.

User management

- You can create, modify, delete, and query users.
- You can maintain the relationships between users and cloud platform accounts by using the features to associate users and cloud platform accounts, view associated accounts, and disassociate accounts.
- The users can be mapped to the platform-side users. After a cloud platform is connected to the multi-cloud management platform, two-way synchronization of user data is supported.

Permission management

You can create, modify, delete, and query roles by using the role-based permission management feature. You can also manage the permissions of roles, such as adding, removing, modifying, or querying the permissions of roles and querying management operations on the permissions of roles.

You can implement permission management in multiple scenarios. For example, you can grant permissions based on business features, cloud platforms, cloud services, organizations, and projects. If you grant permissions based on projects, permissions are independently granted to the users and user groups within a project. You can also directly grant permissions to an organization, a user group, a project, or a user.

11.3.1.1. Organization management

An organization is similar to the business organization of an enterprise. You can manage the cloud resources, users, and projects in multi-cloud management scenarios by using a tailored organizational structure.

After you connect a cloud platform to the multi-cloud management platform, the system automatically synchronizes the existing organizational structure, users, and cloud resources of the connected cloud platform to the multi-cloud management platform. You can create organizations, modify organizational structure, add users, create projects, and grant other platform permissions to organizations based on your business requirements.

Procedure

1. Log on to the multi-cloud management platform.

> **Note**
>
> - Log on to the Apsara Uni-manager Management Console by using an account that has the required role permissions on the multi-cloud management platform and switch to the role. You are automatically redirected to the multi-cloud management platform.
> - If the multi-cloud management platform is independently deployed, contact the platform deployment and delivery engineers to obtain the service domain name of the multi-cloud management platform and the username and password of the platform administrator account.

2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Resources** > **Organizations**.
3. On the page that appears, view the organizations that are synchronized to or created in the multi-cloud management platform. You can also view the resources, users, projects, and authorization information about the organizations.
   - Organization tree: All organizations that are granted the permissions on the multi-cloud management platform are displayed in the tree structure on the left.

     > **Note**
     >
     > The organization information that is displayed in the organization tree varies based on the permissions of the logon user.
     >
     > - If you log on to the multi-cloud management platform by using the built-in administrator role or an account that has full permissions, all organization information is displayed.
     > - If you log on to the multi-cloud management platform by using an account that has partial organization permissions, the information about the organizations that are managed by the account and their parent organizations is displayed. Only the names of the parent organizations are displayed. You cannot view the detailed information about the parent organizations.
     > - If you log on to the multi-cloud management platform with an account that has partial project permissions, only the name of the organization to which the account belongs is displayed. You cannot view the detailed information about the organization.

   - Organization details: The detailed information about the selected organization is displayed in the upper-right section of the page. The information includes the creation time and organization description.
   - Resource list: The detailed information about the cloud resources in the projects of the selected organization is displayed in the resource list on the Resources tab of the page. The information includes the resource name, cloud platform, cloud service, resource type, status, and project.

     > **Note**
     >
     > The information about the project resources in the sub-organizations of the selected organization is not displayed in the resource list.

   - User list: The detailed information about the users that belong to the selected organization is displayed in the user list on the User tab of the page. The information includes the username, email address, phone number, and status.

> **Note**
>
> The information about the users that belong to the sub-organizations of the selected organization is not displayed in the user list. Only the users that directly belong to the selected organization are displayed.

- Project list: The detailed information about the projects in the selected organization is displayed in the project list on the Project tab of the page. The information includes the project name, description, and creation time.

> **Note**
>
> The information about the projects in the sub-organizations of the selected organization is not displayed in the project list. Only the projects that directly belong to the selected organization are displayed.

- Cloud platform authorization: The detailed information about the permissions that are granted to the selected organization and the mappings between the selected organization and corresponding organization on the connected cloud platform are displayed in the authorization list on the Cloud Platform Authorization tab of the page. The information includes the cloud platform, cloud tenant, organization on the connected cloud platform, and authorization time.

4. On the **Organizations** page, perform the following operations to manage organizations:

   - Create an organization:
     - Click Create Organization above the organization tree. In the dialog box that appears, specify the organization name and organization description to create a level-1 organization.
     - In the organization tree, select an organization and click the Add Sub-organization icon next to the selected organization. In the dialog box that appears, specify the organization name and organization description to create a sub-organization in the selected organization. You can create sub-organizations with up to five levels.
   - Modify organization information: In the organization tree, select an organization and click **Edit** in the upper-right corner to modify the name and description of the organization.
   - Delete an organization: In the organization tree, select an organization and click **Delete** in the upper-right corner to delete the organization.

> **Note**
>
> You cannot delete an organization if it has sub-organizations or projects.

5. After you select an organization in the organization tree, go to the resource list, user list, project list, or cloud platform authorization list in the lower-right section of the page and perform the following management operations based on your business requirements:

   - Resource list:
     - Find the cloud resource that you want to manage and click **Update** to manually synchronize and update the information about and status of the cloud resource.
     - Find the cloud resource that you want to manage and click **Management** to go to the management page of the cloud resource and manage the cloud resource.
   - User list: Add, enable, disable, and remove users. You can manage only the users that directly belong to the selected organization. The procedures are the same as those on the Users page. For more information, see User management.

> **Note**
>
> If the multi-cloud management platform is independently deployed, you can also perform operations, such as managing user permissions, modifying user information, associating cloud platform accounts to obtain relevant cloud service permissions, and resetting user passwords.

- Project list: Create projects, modify project information, and delete projects. You can manage only the projects that directly belong to the selected organization. The procedures are the same as those on the Projects page. For more information, see Project management.
- Cloud platform authorization list: Click **Cloud Platform Authorization** to associate the selected organization with tenants on a cloud platform that is managed by the multi-cloud management platform. This way, you can grant cloud platform permissions to the organization and the organization information can be mapped to that on the managed cloud platform.
  - If a connected cloud platform does not support organizations, select the cloud platform and tenants with which you want to associate to grant the cloud platform permissions.
  - If a connected cloud platform has existing organizations, you must also select an organization on the cloud platform in addition to the cloud platform and cloud tenants to associate with the selected organization. This way, the organization information mapping can be implemented.

    > **Note**
    >
    > - Each organization of a cloud platform can be associated with only one organization of the multi-cloud management platform.
    > - A sub-organization can be associated only with an organization on the cloud platform that is authorized by its parent organization.
    > - The cloud platform organization that is authorized by the parent organization in the multi-cloud management platform cannot be the sub-organization of the selected organization. For example, if a parent organization on the multi-cloud management platform is associated with a sub-organization on a managed cloud platform, the sub-organization of the parent organization cannot be associated with the parent organization of the sub-organization on the cloud platform.

  If an organization is associated with cloud platform tenants or a cloud platform organization, click **Revoke Authorization** to disassociate the organization from the tenants or cloud platform organization. Then, you can associate the organization with another cloud platform organization.

11.3.1.2. Project management

You can use projects to manage cloud resources on multiple cloud platforms in a centralized manner. You can manage the authorization of cloud resources and accounts based on projects. This allows enterprises to manage their cloud resources on multiple cloud platforms based on projects.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Resources** > **Projects**.

3. On the page that appears, click **Create Project**. In the dialog box that appears, specify the project name and project description, and select the organization to which the project belongs. You can create a project based on your business requirements.

   > **Note**
   >
   > - A project can belong to only one organization. After a project is created, the organization to which the project belongs cannot be modified.
   > - The project name must be globally unique.

4. After the project is created, you can perform the following operations on the **Projects** page:
   - Edit the project: You can modify the project name and project description.
   - Delete the project: After you delete the project, the resources created in the project are not deleted. A project cannot be deleted if a user or a user group exists in the project.

5. Click the project name in the project list to go to the project details page. You can view the project details and manage the resources, members, user groups, and cloud platform authorization of the project.
   - Project details: The detailed information includes the project name, project description, organization to which the project belongs, creation time, number of resources in the project, resource list, project members, user groups, and list of authorized cloud platforms.
   - Resource list: Displays the information about all cloud resources in the project, including the resource name, cloud platform, cloud service, resource type, status, and project.
     - Click **Create Resource**. In the dialog box that appears, specify the cloud platform and cloud service. Click **Submit** to go to the page to create cloud service resources of the specified cloud platform. On the creation page, configure parameters to create cloud service resources in the project.
     - Click **Manage** to go to the page to manage cloud resources.
     - Click **Update** to manually update the information about and status of the cloud resources.
   - Project member list: Displays the information about all members in the project. The information includes the user name, assigned project role, and authorization time. You can add a user as a project member or remove a member from the project.
     - Click **Add Members**. In the dialog box that appears, select the role that you want to assign to the member and the user that you want to add as a project member. You can add multiple users at a time.

       You can select only the roles that are displayed in the drop-down list. You can select project administrator or resource user, both of which are built-in project-specific roles. When you add a member, you can select only one role. After the member is added, you can find the user in the project member list and click Edit Role Authorization to assign multiple roles. For more information about the available roles, see Role management.
     - To remove a project member, find the member in the project member list. Click **Remove Authorization** to remove the user from the project. After the user is removed, the user no longer has the role permissions on the project.
   - Cloud platform authorization list: Click **Cloud Platform Authorization** to grant project permissions to a specific cloud platform. The cloud platform that can be granted permissions must be an authorized cloud platform of the organization to which the current project belongs. You can associate a project with tenants of a cloud platform that is connected to the multi-cloud management platform and grant the cloud platform permissions to the project. The project of the cloud platform is mapped to a project of the multi-cloud management platform.

- If a connected cloud platform does not support projects, select the cloud platform and tenants with which you want to associate to grant the cloud platform permissions.
- If a connected cloud platform has existing projects, you must also select a project on the selected cloud platform in addition to the cloud platform and cloud tenants to associate with the project of the multi-cloud management platform. This way, the project information mapping can be implemented.

> ? **Note**
>
> - Each project on a cloud platform can be associated with only one project on the multi-cloud management platform.
> - If the organization to which a project belongs is associated with an organization on the cloud platform, you can associate the project to only the subordinate projects that belong to the associated organization on the cloud platform. You cannot associate the project with the projects in other organizations on the cloud platform.

If a project is associated with cloud platform tenants or a cloud platform project, click **Revoke Authorization** to disassociate the project from the tenants or project. Then, you can associate the project with another cloud platform project.

11.3.1.3. User management

The username is the credential used to log on to the multi-cloud management platform. After a cloud platform is connected to and managed by the multi-cloud management platform, the system synchronizes the user information from the cloud platform to the multi-cloud management platform. You can add cloud platform users to the multi-cloud management platform, grant users permissions, and associate accounts of other cloud platforms to obtain the service permissions of the corresponding cloud platforms based on your business requirements.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Personnel Management** > **Users**.
3. On the page that appears, you can view the information of users that are synchronized or created in the multi-cloud management platform. The information includes the username, display name, email address, phone number, organization, and status.

   > ? **Note**
   >
   > By default, the email address and phone number of a user are hidden to protect user privacy. To view the information, click the View icon in the corresponding column.

4. Click **Create User**. After you specify the organization to which the user belongs and the username, the system obtains the display name, phone number, and email address of the user from the corresponding cloud platform and displays the information. Select roles that you want to assign to the user and click **OK**. This way, the user is added to the multi-cloud management platform and granted the permissions of the selected roles.

> **Note**
>
> If the multi-cloud management platform is not deployed with Apsara Stack, you can manually create a user, specify the username, display name, phone number, and email address, and select the organization to which the user belongs and roles that the user can assume.
>
> In this case, the initial password is automatically generated after the user is created. When you use the initial password to log on to the multi-cloud management platform for the first time, you must reset the password.

5. On the Users page, you can perform the following operations:
   - Click **Enable** or **Disable** in the Actions column to enable or disable a user. A disabled user cannot log on to the multi-cloud management platform. If the user is currently logged on to the multi-cloud management platform, all features of the platform are disabled for the user.

     > **Note**
     >
     > You cannot disable the user that you currently use to log on to the multi-cloud management platform. To disable this user, you must use another administrator account to log on to the multi-cloud management platform.

   - Click **Role Authorization** in the Operation column to view the roles of a user. In the Role Authorization panel, you can remove roles from the user. You can also assign roles to the user and specify the permission scope of roles. After a role is added to the user, the user is granted the permissions of the role.

     > **Note**
     >
     > - You can assign only the available roles to the user. For more information, see Role management.
     > - If the permission scope of the role that you want to add is project, you must also specify the project.

   - Click **Delete** in the Operation column to delete a user. You cannot delete the user that you currently use to log on to the multi-cloud management platform.

> ? **Note**
>
> If the multi-cloud management platform is independently deployed, you can also perform the following operations on the Users page:
>
> - Click **Edit** in the Operation column to edit the basic information about a user. The information includes the display name, email address, and phone number. The username cannot be modified after the user is created.
> - Click **Associate Cloud Platform Account** in the Operation column to associate a specific cloud platform account to a user. After the cloud platform account is associated with the user, the user has the related cloud service permissions on the cloud platform.
>   - You can select only cloud platforms that support static user associations. The cloud platforms must be authorized by the organization to which the user belongs.
>   - You can select only an account of an organization on a cloud platform that is authorized by the organization to which the user belongs.
>   - Each user or cloud tenant can be associated with only one cloud platform account.
> - Click **Reset Password** in the Operation column to reset the password of a user. The system automatically generates a random password. When you use the random password to log on to the multi-cloud management platform for the first time, you must change the password. You cannot reset the password of the user that you currently use to log on to the multi-cloud management platform.

11.3.1.4. Cloud platform management

The Cloud Platform page lists the cloud platforms that are connected to and managed by the multi-cloud management platform. Tenant-side cloud platform management allows tenant-side administrators to manage resources and assign resources in the cloud platform to specific projects. This allows users to manage resources in a centralized manner based on projects.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Multi-level Clouds** > **Cloud Platform**.
3. On the Cloud Platform page, view the information about the cloud platforms that are managed by the multi-cloud management platform. The information includes the cloud platform name, cloud service provider, platform type, and status.
4. For a cloud platform that does not have organizations or projects, you can perform resource management operations. Click **Resource Management** to go to the Resource Management page.
   - Click **Synchronize Resource** to manually start a resource synchronization task. This way, the latest uncategorized resources on the cloud platform are pulled.
   - Select the resources that you want to manage, click **Change Project**, and then specify a project to assign the resources to the specified project. This meets the requirement of project-based centralized resource management.

> **Note**
>
> Make sure that the specified project is authorized by the cloud platform.

11.3.1.5. Role management

A role is a collection of user permissions. After you grant permissions to a role, you can assign the role to a user. This way, the user has the permissions of the role. You can assign multiple roles to a user. The permissions of the user are the union of the permissions of all roles that are assigned to the user.

Permission types

Permissions include feature permissions and service permissions. You can grant a combination of two types of permissions to a role and assign the role to users to implement permission management on users.

> **Note**
>
> Each role has at least one feature permission.

- Feature permissions are the permissions on feature nodes on the multi-cloud management platform. You can grant users the permissions to use feature nodes and perform operations.
- Service permissions are the permissions on the cloud services of cloud platforms that are managed by the multi-cloud management platform. Service permissions include the permissions to view, modify, and create resources in a cloud service.

Role types

The multi-cloud management platform provides the following types of roles: preset roles and custom roles. Preset roles are created by the system. Preset roles have specific feature and service permissions. You cannot modify or delete preset roles and their permissions. Custom roles are created by users. You can create custom roles and grant permissions to the roles based on your business requirements.

The multi-cloud management platform provides the following four preset roles based on the business requirements of common multi-cloud management scenarios of enterprises:

Preset role	Permission scope	Description
Multi-cloud Resource User	Project	This role can be assigned to users who manage resources in projects. Users who are assigned this role have the query permissions on roles, resources, projects, users, and cloud platform features and management permissions on the cloud service resources on all cloud platforms that are managed by the multi-cloud management platform.

Multi-cloud Project Administrator	Project	This role can be assigned to users who manage projects, add and manage members, activate and manage resources, review resource applications of resources users, and initiate resource or quota applications to superiors. Users who are assigned this role have the query permissions on project management, project member management, resource management, permission management, and cloud platform features and management permissions on the cloud service resources on all cloud platforms that are managed by the multi-cloud management platform.
Multi-cloud Organization Administrator	Current organization and subordinate organizations	This role can be assigned to users who create and manage the current organization and its subordinate organizations, create and manage projects, add and manage members, assign and manage roles, activate and manage resources, assign resources to subordinate organizations, specify project administrators and resource quotas, initiate resource or quota applications to superiors, and review resource or quota applications of subordinate organizations. Users who are assigned this role have the permissions of most of the cloud platform features such as organization management, project management, user management, resource management, permission management, announcement management, and cloud platform viewing and management permissions on the cloud service resources on all cloud platforms that are managed by the multi-cloud management platform.
Multi-cloud Resource Auditor	Global	This role can be assigned to users who monitor the usage of all cloud resources in the entire multi-cloud management scenario. Users who are assigned this role have the query permissions on all cloud platform resources. In addition to the query permissions on roles, resources, projects, users, and cloud platform features and management permissions on the cloud service resources on all cloud platforms that are managed by the multi-cloud management platform, they can also audit feature operation logs and platform operation logs.

Permission scope

The permission scope of a role is used to restrict the data permissions of the role. The following three scope types are provided: global, organization, and project.

- Global: The role has the data permissions on all organizations and projects on the multi-cloud management platform.

> **Note**
>
> The global permission scope is available only for specific preset roles. This permission scope is unavailable for custom roles.

- Current organization and subordinate organizations: The role has the data permissions on the organization to which the user belongs and its subordinate organizations.
- Project: The role has the data permissions on the projects to which the user are added.

Role visibility

The roles that can be assigned to a user are specified based on the role visibility. You can specify that a role is visible only to specific organizations and their subordinate organizations. When you assign roles to a user, the available roles must be visible to the organization to which the user belongs and its superior organizations.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** >**Roles**.
3. In the left-side organization tree, select an organization. You can view or manage roles in the selected organization in the role list on the right side.

   > **Note**
   >
   > If you select the root organization, you can view and manage the roles that are available for all organizations.

4. Click **Create Role** to create a role in the selected organization or its subordinate organization.

   i. Specify the role name, role code, and role description. The role name must be 2 to 32 characters in length and can contain letters, digits, underscores (_), and hyphens (-). The role name must be globally unique. The role code must be 2 to 32 characters in length and can contain letters, digits, underscores (_), and hyphens (-). The role code must be globally unique and cannot be modified after the role is created. The role description can be up to 128 characters in length.

   ii. Specify the role visibility. By default, the role is visible to the selected organization. You can specify that the role is visible to its subordinate organizations or all organizations.

   iii. Specify the permission scope of the role. Grant the role required data permissions based on the organization and project to which the user belongs.

   iv. Grant permissions to the role by feature.

   > **Note**
   >
   > Custom roles cannot audit feature operation logs or platform operation logs, associate cloud platform users, disassociate cloud platform users, or query permission mappings. Only preset roles and built-in users have these permissions.

   v. Select the service permissions that you want to grant to the role. By default, all cloud platforms that are connected to the multi-cloud management platform and their cloud services are displayed. Select the permissions to query, create, and modify cloud services based on your business requirements.

5. On the Roles page, you can perform the following operations:

   > **Note**
   >
   > Preset roles cannot be deleted or modified. You can only clone preset roles and view the details of preset roles.

   - Click **Modify** to modify the name and description of a role.
   - Click **Copy** to create a custom role that has the same configurations as the selected role.
   - Click **Delete** to delete a role. You cannot delete a role that has been assigned to users.

- Click the role name to go to the role details page. On the role details page, you can view the details of the role. You can also modify the feature permissions and service permissions of the role. On the **Authorization Object** tab, you can remove the users or user groups to which the role is assigned or select multiple users or user groups to assign the role to the specified users or user groups.

11.3.2. Resource management

After you configure organizations, projects, users, and roles, you can use the multi-cloud management platform to manage resources of the managed cloud platforms, or to apply for and create cloud service resources based on your business requirements.

Procedure

1. Log on to the multi-cloud management platform. On the homepage, you can view the overview information about the organization to which you belong, the statistics of cloud service resources, and the distribution of the cloud platforms that are authorized in the organization. You can also view the announcements that are issued by administrators in the Announcement section or customize the shortcut features based on your business requirements.
2. In the top navigation bar, click **Product** or **Resource** to go to the Resource List page. Then, you can manage resources.

   > **Note**
   >
   > - If you click **Product**, the cloud service catalogs and cloud services that are configured by platform administrators are displayed. You can switch to the cloud platform that you want to manage and click a cloud service to manage the cloud service resources of the cloud platform.
   > - If you click **Resource**, the Resource List page displays the cloud service resources of all cloud platforms that you can view and manage.
   > - For cloud services that do not support the resource management feature, you can use the Product menu to go to the Resource List page on the cloud platform side. Then, you can manage the cloud service resources.

3. On the Resource List page, you can perform the following operations:
   - Create a resource. To create a resource, click Create Resource. In the dialog box that appears, select a project name, cloud platform, and cloud service and click Submit to go to the corresponding cloud platform. On the page that appears, you can create cloud resources.
   - Search for resources. To search for resources, you can set filter conditions, such as cloud platform, cloud service, resource name, resource type, organization, project, and creation time, and click Search. Then, the resources that meet the specified conditions are displayed.
   - View the basic information about a resource. To view the basic information about a resource, click the resource ID. On the page that appears, you can view the basic information about the resource, including the cloud platform, organization, project, region, resource name, creation time, and status.
   - Update the resource information. To update the resource information, click **Update** to manually update the information about and status of the cloud resources.
   - Manage a resource. To manage a resource, click **Management** in the Operation column. You are redirected to the Resource List page of the cloud service in the corresponding cloud platform.

11.3.3. Multi-cloud metering

The multi-cloud management platform provides management capabilities for usage statistics of resources on multiple cloud platforms in a centralized manner. This feature allows you to collect the usage statistics of organization and project resources on multiple cloud platforms and display the statistics in a centralized manner. This helps you monitor the resource usage on multiple cloud platforms.

> ? **Note**
>
> The information about instances and metering changes are recorded on an hourly basis. Only the metering data of Apsara Stack is displayed.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Operations**. In the left-side navigation, click **Multi-cloud Metering**.
3. On the page that appears, specify an organization, project, cloud service, and a time range. Then, the resource usage data that meets the specified conditions is displayed. You can also specify a cloud platform and a project on the cloud platform to view the resource usage in a more accurate manner.

   > ? **Note**
   >
   > - Only the resource usage of cloud resources that belong to the selected organization is displayed. The resource usage of cloud resources that belong to the subordinate organizations of the selected organization is not displayed.
   > - Metering items vary based on cloud services.

11.3.4. Log audit

The multi-cloud management platform provides the security log audit feature that allows you to view the operation logs of the multi-cloud management platform and operation logs of the cloud services on managed cloud platforms. This helps enterprises implement security audit in multi-cloud management scenarios.

> ? **Note**
>
> The log audit feature is available to users who are assigned the preset resource auditor or tenant security auditor role. Other users cannot use this feature.

Procedure

1. Log on to the multi-cloud management platform.
2. In the top navigation bar, click **Configurations**. In the left-side navigation pane, choose **Log Audit** > **Operation Logs**.
3. On the page that appears, click the Feature Logs or Cloud Service Logs tab to view the corresponding operation logs.

- The logs of the operations performed on the features of the multi-cloud management platform are displayed on the Feature Logs tab. After you specify the log type, operation, operator, result, and time range, the logs that meet the specified conditions are displayed.
- The logs of the operations performed on the cloud service resources on the cloud platforms managed by the multi-cloud management platform are displayed on the Cloud Service Logs tab. After you specify the cloud platform, cloud service, resource type, operator, instance, operation type, result, and time range, the logs that meet the specified conditions are displayed.

  > ? **Note**
  >
  > A maximum of 100,000 records can be returned for each request. The maximum time range for a query is seven days.

12.FAQ

12.1. Errors when you log on to the Apsara Uni-manager Management Console

This topic describes how to troubleshoot the errors when you log on to the Apsara Uni-manager Management Console.

Problem description

The page does not respond or an internal error is returned after you log on to the Apsara Uni-manager Management Console with the correct account and password.

Cause

Three possible causes:

- Network issues.
- An error is reported when the ascm-auth service calls the ASS service.
- The services in the Apsara Uni-manager Management Console and the base services (ASS, RAM, Tair, and Ummak) that the Apsara Uni-manager Management Console depends on have not reached the desired state.

Solution

1. Check on Apsara Infrastructure Management Framework whether the services in the Apsara Uni-manager Management Console cluster have reached the desired state.
   i. Log on to the Apsara Infrastructure Management Framework console.
   ii. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
   iii. In the **Cluster** field, enter `ascm` .
   iv. Find the cluster and then click **Operations** in the Actions column.
   v. Click the **Services** tab and check the current status of services.

      If a service has not reached the desired state, set the service to the desired state. Log on to the Apsara Uni-manager Management Console again.
2. If all services in the cluster have reached the desired state and the logon is still abnormal, you can check network issues in the order of frontend page > Portal dockers > ASAPI dockers > Auth/Manager dockers".

   Troubleshooting procedure: Run the `curl` command in each container to connect the endpoint of the next service.
   i. Click the **Machines** tab.
   ii. In the **Machine** field, enter the name of the docker SR.
   iii. Find the machine and click **Terminal** in the Actions column.
   iv. In the left-side machine list, click the machine and run the following command.

      ```
      bash -c bash
      ```

  v. Run the following command to view the ID of the docker:

```
docker ps
```

  vi. Run the following command to access the docker:

```
sudo docker exec -it <Docker ID> bash
```

  vii. Run the following command in the docker:

  If an endpoint cannot be connected, contact onsite network engineers to solve network issues.

3. If no network issues are found between dockers, you must check logs to discover issues.

  i. Open the Apsara Uni-manager Management Console page, enter the account and password, and then press F12.

  ii. Click **Log On**.

  iii. Click the Headers tab and obtain `eagleeye-traceid`.

  iv. Perform the operations in step 2 to access the **ascm-portal.Portal#** docker.

  v. Run the following command in the docker:

```
grep <eagleeye-traceid>/root/logs/ascm-portal/ascm-error.log*
```

  Find the service that returns errors based on the error logs. Contact onsite O&M engineers to further discover possible causes.

4. If the Auth docker is normal, the username and password are correct, and the logon is still abnormal, the possible cause usually is that an error is reported when the AAS service is called.

  i. Run the following command in the Auth docker:

```
grep {eagleeye-traceid} /logs/ascm-logger/*.log -5
```

  ii. If a return value error is reported in the log, it can be determined that an error is reported when the AAS service is called. Contact AAS O&M engineers to further discover possible causes.

12.2. What do I do if a timeout error occurs when I call the API operations of VPC, ECS, SLB, or ApsaraDB RDS in the Apsara Uni-manager Management Console?

This topic describes how to troubleshoot a timeout error that occurs when you call the API operations of a cloud service such as Virtual Private Cloud (VPC), Elastic Compute Service (ECS), Server Load Balancer (SLB), or ApsaraDB RDS in the Apsara Uni-manager Management Console.

Problem description

A timeout error occurs when you call the API operations of a cloud service such as VPC, ECS, SLB, or ApsaraDB RDS in the Apsara Uni-manager Management Console.

Cause

The timeout error may be caused by full garbage collection (GC) processes that are frequently run on Portable OpenAPI Proxy (POP).

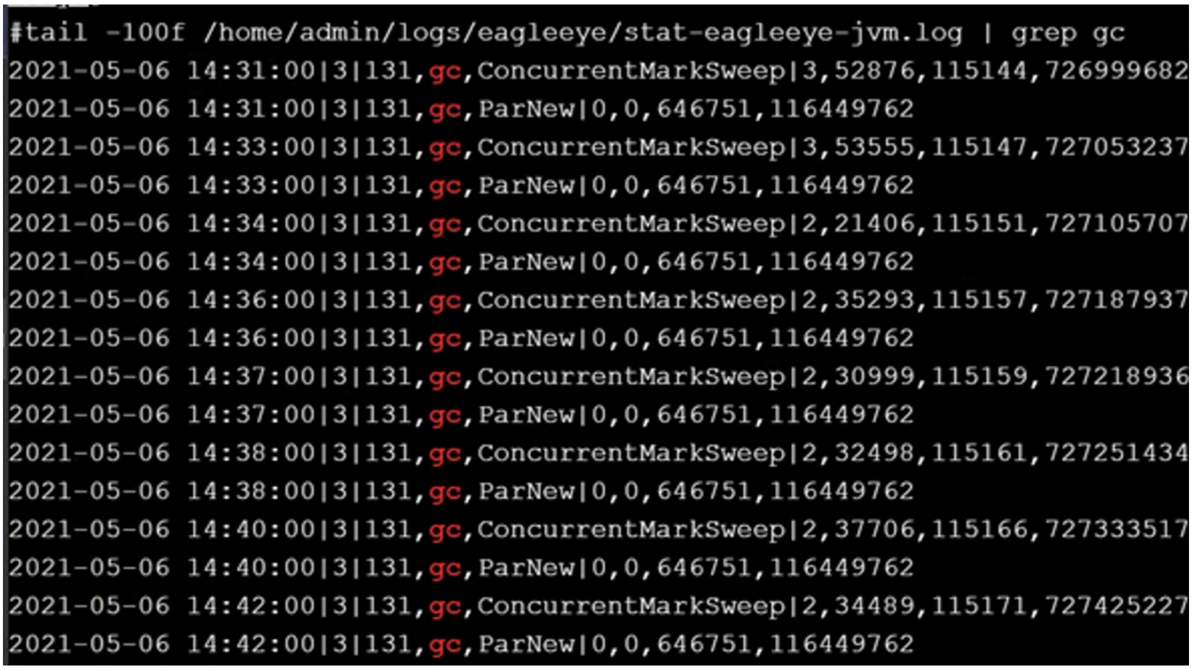
Solution

1. Access the `webapp-pop.PopAliyunCom#` container.

   For more information, see *Routine inspection* in *Apsara Uni-manager Management Console Operations and Maintenance Guide*.

2. Run the following command in the container:

   ```
   tail -f/home/admin/logs/eagleeye/stat-eagleeye-jvm.log | grep gc
   ```

   ```
   #tail -100f /home/admin/logs/eagleeye/stat-eagleeye-jvm.log | grep gc
   2021-05-06 14:31:00|3|131,gc,ConcurrentMarkSweep|3,52876,115144,726999682
   2021-05-06 14:31:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:33:00|3|131,gc,ConcurrentMarkSweep|3,53555,115147,727053237
   2021-05-06 14:33:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:34:00|3|131,gc,ConcurrentMarkSweep|2,21406,115151,727105707
   2021-05-06 14:34:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:36:00|3|131,gc,ConcurrentMarkSweep|2,35293,115157,727187937
   2021-05-06 14:36:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:37:00|3|131,gc,ConcurrentMarkSweep|2,30999,115159,727218936
   2021-05-06 14:37:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:38:00|3|131,gc,ConcurrentMarkSweep|2,32498,115161,727251434
   2021-05-06 14:38:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:40:00|3|131,gc,ConcurrentMarkSweep|2,37706,115166,727333517
   2021-05-06 14:40:00|3|131,gc,ParNew|0,0,646751,116449762
   2021-05-06 14:42:00|3|131,gc,ConcurrentMarkSweep|2,34489,115171,727425227
   2021-05-06 14:42:00|3|131,gc,ParNew|0,0,646751,116449762
   ```

   ConcurrentMarkSweep indicates the logs of the full GC processes. A full GC process is run every one or two minutes.

3. Restart the containers in the following sequence: POP > ASAPI > Manage > ResourceManage > OneConsole.

4. After the containers are restarted, view the full GC processes that are run on POP.

   If the issue persists, contact on-site O&M engineers.

12.3. What do I do if a timeout error occurs when I create an ACK cluster in the Apsara Uni-manager Management Console?

This topic describes how to troubleshoot a timeout error that occurs when you create a Container Service for Kubernetes (ACK) cluster in the Apsara Uni-manager Management Console.

Problem description

An error is reported when you create an ACK cluster in the Apsara Uni-manager Management Console. The error message "java.net.SocketTimeoutException:Read timed out" is returned.

Cause

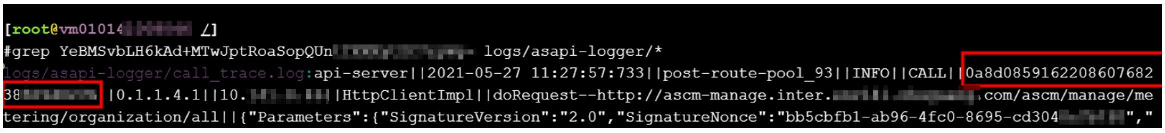
The issue may occur due to the following reasons:

- Network issues occur.
- Performance is degraded due to the high load of the backend service.

Solution

1. Find the call logs for Apsara Stack API (ASAPI) and Portable OpenAPI Proxy (POP).
   1. Press the F12 key. Click **Create** again.
   2. Obtain the request ID from the response.
   3. Log on to the Apsara Infrastructure Management console and then access the **asapi.ApiServer#** container.
   4. Run the following command in the container to query the EagleEye ID:

      ```
      grep <requestid> /logs/asapi-logger/*
      ```

      ```
      [root@vm01014[redacted] ∠]
      #grep YeBMSvbLH6kAd+MTwJptRoaSopQUn[redacted] logs/asapi-logger/*
      logs/asapi-logger/call_trace.log:api-server||2021-05-27 11:27:57:733||post-route-pool_93||INFO||CALL||0a8d0859162208607682
      38[redacted] |0.1.1.4.1||10.[redacted]|HttpClientImpl||doRequest--http://ascm-manage.inter.[redacted].com/ascm/manage/me
      tering/organization/all||{"Parameters":{"SignatureVersion":"2.0","SignatureNonce":"bb5cbfb1-ab96-4fc0-8695-cd304[redacted]","
      ```

   5. Run the following command to query the duration on ASAPI based on the EagleEye ID:

      ```
      grep <EagleEye ID> / logs/asapi-logger/*
      ```

   6. Access the **webapp-pop.PopAliyunCom#** container and run the following command to query the logs from POP and the duration on POP:

      ```
      grep <EagleEye ID> /opt/tianji/alidata/www/logs/java/gateway/logs/trace/*
      ```

2. Compare the duration on ASAPI with that on POP.
   - If the duration on POP is slightly longer than that on ASAPI, such as a time difference within 1 second to 2 seconds, contact service engineers to further troubleshoot the timeout error.
   - If the duration on ASAPI is much longer than that on POP, you can check whether full garbage collection (GC) processes are run on POP. For more information, see What do I do if a timeout error occurs when I call the API operations of VPC, ECS, SLB, or ApsaraDB RDS in the Apsara Uni-manager Management Console?

12.4. What do I do if a timeout error occurs when I obtain ACK clusters in the Apsara Uni-manager Management Console?

This topic describes how to troubleshoot the timeout error when you obtain Container Service for Kubernetes (ACK) clusters in the Apsara Uni-manager Management Console.

Problem description

An error is reported when you obtain ACK clusters in the Apsara Uni-manager Management Console. The error message "java.net.SocketTimeoutException:Read timed out" is returned.

Possible cause

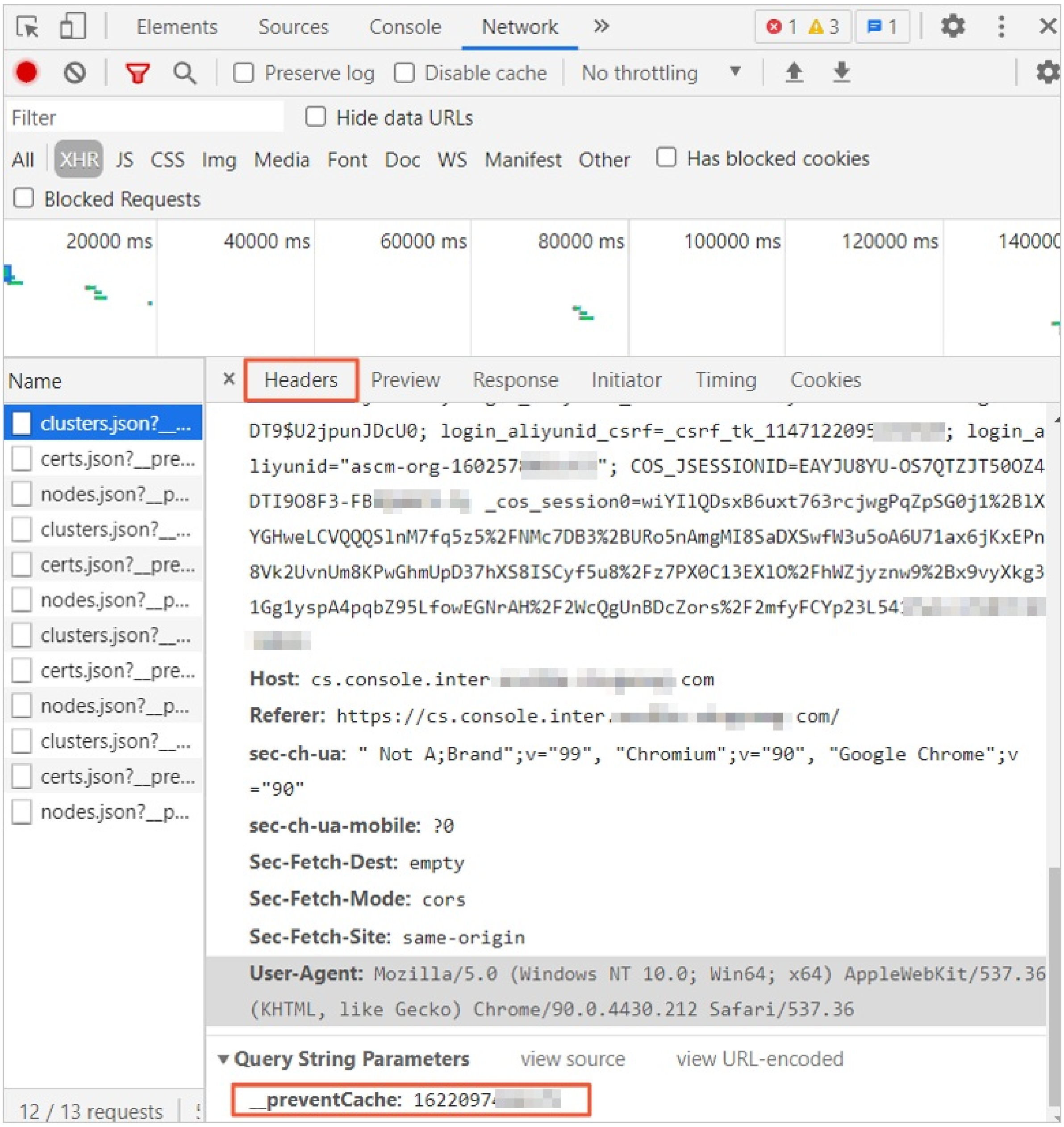
The error may occur due to the following reasons:

- Network issue
- Performance degradation caused by the high load of the backend service

Solution

1. Press the F12 key. Refresh the page and obtain the list of ACK clusters again.

On the **Headers** tab, find the `_preventCache` field.



```
DT9$U2jpunJDcU0; login_aliyunid_csrf=_csrf_tk_1147122095[redacted]; login_aliyunid="ascm-org-160257[redacted]"; COS_JSESSIONID=EAYJU8YU-OS7QTZJT50OZ4DTI908F3-FB[redacted] _cos_session0=wiYI1QDsxB6uxt763rcjwgPqZpSG0j1%2B1XYGHweLCVQQQS1nM7fq5z5%2FNMc7DB3%2BURo5nAmgMI8SaDXSwfW3u5oA6U71ax6jKxEPn8Vk2UvnUm8KPwGhmUpD37hXS8IScyf5u8%2Fz7PX0C13EX1O%2FhWZjyznw9%2Bx9vyXkg31Gg1yspA4pqbZ95LfowEGNrAH%2F2WcQgUnBDcZors%2F2mfyFCYp23L54[redacted]
Host: cs.console.inter[redacted] com
Referer: https://cs.console.inter.[redacted] com/
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
sec-ch-ua-mobile: ?0
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
▼ Query String Parameters    view source    view URL-encoded
_preventCache: 1622097[redacted]
```

2. Access the **asapi.ApiServer#** container.
   i. Run the following command to obtain Manage logs by using _preventCache:

   ```
   cat /logs/ascm-logger/main_trace* | grep <_preventCache>
   ```

   ii. Obtain the EagleEye ID from the Manage logs. Run the following command to find the logs on API operations called by Manage from ASAPI:

   ```
   grep /logs/ascm-logger/* | grep <EagleEye ID>
   ```

iii. Run the following command to obtain the logs on the API operations called by ASAPI through POP based on the EagleEye ID:

```
grep <EagleEye ID> / logs/asapi-logger/*
```

Obtain the `x-acs-signature-nonce` value.

3. Query POP logs.

   - Method 1

     a. Enter the VM where the server role PopAliyunCom# is located.

     b. Access the **pop-aliyun-com** container. Run the following command to query the logs on Portable OpenAPI Proxy (POP) calls:

     ```
     grep <EagleEye ID> /opt/tianji/alidata/www/logs/java/gateway/logs/trace/trace.log
     ```

     > ⓘ **Important**
     >
     > The logs in the container will be refreshed soon. Up to 20 minutes are required to access the POP container and obtain the logs.

   - Method 2

     a. Log on to the Simple Log Service console.

     For more information about how to view logs in Simple Log Service, see View logs.

     b. Select **ali-pop-log** for Project and **pop_rpc_trace_log** for Logstore.

     c. If you cannot query desired logs by using the EagleEye ID, use `CS and DescribeClusters` as the filter condition, and select a small time range for calling the API operation.

4. Based on the preceding logs, analyze which module consumes longer time.

12.5. Errors when Blink API operations are called

This topic describes how to troubleshoot the errors in the Apsara Uni-manager Management Console when Blink API operations are called.

Problem description

An error is reported in the Apsara Uni-manager Management Console when a Blink API operation is called. The error code is "ascm.manage.EntityNotExist.Instance".

Solution

1. Access the **ascm-brm.Manage#** docker. For more information, see Routine inspections.
2. Run the following command in the docker to access the BRM database:

   ```
   mysql -u${db_user} -h${db_host} -p${db_password} -D${db_name} -P${db_port}
   ```

3. Run the following command in the database to check whether the `resource_instance.no_show_count` value is 1 and whether the `instance_id` value contains uppercase letters.

```
select * from resource_instance where type ='foas_project' and instance_id = '$project_name' ;
```

- If the `instance_id` value contains uppercase letters, run the following command to back up the table data and then modify the uppercase letters of the `instance_id` value to lowercase letters.

  If 10 minutes later the `no_show_count` value automatically changes to 0, you can skip subsequent steps.

  ```
  create tableresource_instance_bak20210204 as select * from resource_instance;
  updateresource_instance set instance_id = lower(instance_id) where type ='foas_project';
  ```

- If the `instance_id` value does not contain uppercase letters and the `no_show_count` value is 1, run the following command in the **ascm-brm.ResourceMgr#** docker to obtain logs:

  ```
  cat/logs/ascm-logger/call_trace* |grep foas |grep ListProject |grep ECONNREFUSED |tail -5
  cat/logs/ascm-logger/call_trace* |grep foas |grep ListProject |grepServiceUnavailable | tail -5
  cat/logs/ascm-logger/call_trace* |grep foas |grep ListProject |grep'\"Code\"' | tail -5
  cat/logs/ascm-logger/call_trace* |grep foas |grep ListProject |grepResponseTimeoutError | tail -5
  cat/logs/ascm-logger/call_trace* |grep foas |grep ListProject |grep InternalError| tail -5
  ```

  If no logs are returned, run the following command to obtain logs:

  ```
  cat /logs/ascm-logger/call_trace.log|grep foas |grep ListProject| Region for grep$project | AccessKey pair of the organization for grep$project |grep $project_name | tail -5
  cat /logs/ascm-logger/call_trace.log |grep foas |grep ListProject| Region for grep$project | AccessKey pair of the organization for grep$project | tail -5
  ```

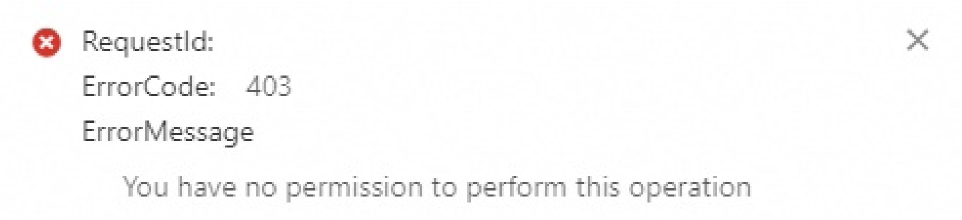
4. Provide the collected logs to onsite O&M engineers for the Apsara Uni-manager Management Console.

12.6. What do I do if an error is reported to indicate that a custom role does not have the required permissions?

This topic describes how to troubleshoot the issue that a custom role does not have the required permissions in the Apsara Uni-manager Management Console.

Problem description

An error is reported in the Apsara Uni-manager Management Console, which indicates that a custom role does not have the required permissions. For example, a custom role does not have the permissions to view DataHub projects.



RequestId:

ErrorCode: 403

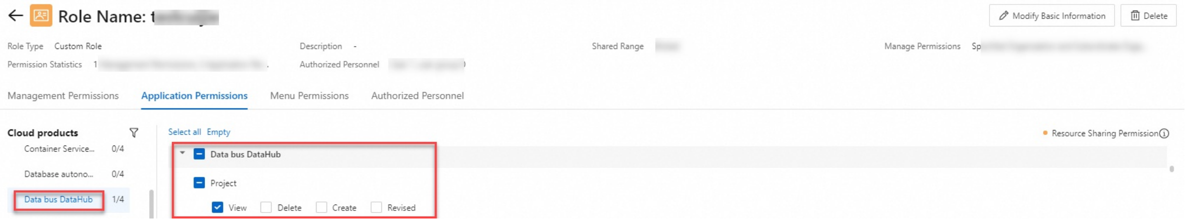
ErrorMessage

You have no permission to perform this operation

Solution

The following example shows how to grant the permissions to view DataHub projects:

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Permissions** > **Role Permissions**.
4. On the **Role Permissions** page, find the custom role that is assigned to the user that you want to manage.
5. Click the name of the custom role to go to the role details page.
6. On the role details page, click the **Application Permissions** tab. Find DataHub and select **View** in the Data bus DataHub section.



Role Name: t[redacted]

Role Type Custom Role

Permission Statistics 1[redacted]

Description -

Authorized Personnel [redacted]

Shared Range [redacted]

Manage Permissions Sp[redacted]

Data bus DataHub

Project

☑ View ☐ Delete ☐ Create ☐ Revised

7. Click **Update**.

12.7. What do I do if an error is reported when I delete an organization in the Apsara Uni-manager Management Console?

This topic describes how to troubleshoot an error that occurs when you delete an organization in the Apsara Uni-manager Management Console.

Problem description

An error occurs when you delete an organization in the Apsara Uni-manager Management Console and the organization fails to be deleted.

Cause

- The organization contains cloud resources.
- The organization has sub-organizations.
- The organization contains users.

- The organization contains user groups.
- The organization contains visible Resource Access Management (RAM) policies and RAM roles.
- The organization contains visible logon policies.

Solution

Delete cloud resources from the organization

Delete the cloud resources based on the error message.

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Resource Sets**.
4. On the Resource Sets page, find the resource set that you want to manage and click its ID to go to the Resource Set Details page.
5. On the Resource Set Details page, click the **Resources** tab. On the Resources tab, find the resources that you want to delete and click the number before the resources to go to the console of the service to which the resources belong.
6. Delete the resources in the service console.

Delete sub-organizations from the organization

Delete the sub-organizations based on the error message.

1. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Resources** > **Organizations**.
2. In the navigation tree, find the sub-organization that you want to delete and click **Delete** in the Basic Information section of the sub-organization on the right side of the Organizations page.

Delete users from the organization

Delete the users based on the error message.

1. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Users** > **Users**.
2. On the Users page, click the **System Users** tab. On the System Users tab, click Username and select Organization from the drop-down list. Then, enter an organization name in the Organization field to display users in the organization.
3. Find the user that you want to delete, click the ... icon in the Actions column, and then select **Delete**.
4. In the dialog box that appears, view the information about the associated AccessKey pair, select the check box before **I have known the risks and confirmed this delete operation**, and then click **Delete**.

Delete user groups from the organization

Delete the user groups based on the error message.

1. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Users** > **User Groups**.
2. On the User Groups page, click User Group Name and select Organization from the drop-down list. Enter an organization name in the Organization filed to display user groups in the organization.

3. Find the user group that you want to delete, click the ... icon in the Actions column, and then select **Delete**.
4. In the message that appears, click **OK**.

Delete RAM policies and RAM roles from the organization

Delete the RAM policies and RAM roles based on the error message.

1. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Role Permissions**.
2. On the Role Permissions page, find and delete a RAM policy or RAM role.
   - To delete a RAM policy, perform the following operations: Go to the details page of a RAM role-based batch authorization role or RAM-based batch authorization role, and find the policy list. In the policy list, find and delete the policy.
   - To delete a RAM role, perform the following operations: In the role list, find the role, click the ... icon in the Actions column, and then select **Delete**. In the message that appears, click **OK**.

Delete logon policies from the organization

Delete the logon policies based on the error message.

1. In the top navigation bar, click **Enterprise**. In the left-side navigation pane, choose **Permissions** > **Access Control**.
2. On the Access Control page, find the logon policy that you want to delete.
3. Click **Delete** in the Actions column.
4. In the Confirm message, click **OK**.

12.8. How do I view and export the logon and logoff records of accounts?

This topic describes how to view and export the logon and logoff records of accounts in the Apsara Uni-manager Management Console.

View the logon and logoff records of accounts

1. Log on to the Apsara Uni-manager Management Console as a security administrator.
2. In the top navigation bar, choose **Security** > **Global Platform Security** > **Operation Logs**.
3. On the **Event Query** page, click the **Event List** tab. On the Event List tab, enter **OPLOG_Login** or **OPLOG_Logout.html** in the **Key Words** field for advanced filtering, configure the **Organization** and **Start And End Time** parameters, and then click **Search**.

> **Note**
>
> - If you enter **OPLOG_Login** in the **Key Words** field, the logon records of accounts are queried.
> - If you enter **OPLOG_Logout.html** in the **Key Words** field, the logoff records of accounts are queried.

4. Find a record and click **View** in the **Details** column to view the details of the operation.

Export the logon and logoff records of accounts

1. On the **Event Query** page, click the **Event List** tab and then click **Export Event**.
2. In the **Export Event** dialog box, configure the **Task Name**, **Organization and Resource Set**, and **Start And End Time** parameters. In the **Key Words** field, enter **OPLOG_Login** or **OPLOG_Logout.html**. Then, click **OK**.

   > **Note**
   >
   > - If you enter **OPLOG_Login** in the **Key Words** field, the logon records of accounts are exported.
   > - If you enter **OPLOG_Logout.html** in the **Key Words** field, the logoff records of accounts are exported.

3. Click the **Export Records** tab.
4. In the task list, view the task status. After the state of the task changes to **Completed**, click **Download Report** in the **Download Operation** column to export the records as a **.xlsx** file to your computer for backup.

12.9. How do I attach disks to an instance across resource sets of different organizations?

This topic describes how to attach disks to an Elastic Compute Service (ECS) instance across resource sets of different organizations.

Solution

Add the ECS instance to the resource set of the organization to which the disks to be attached belong and then attach the disks to the instance.

Procedure

1. Log on to the Apsara Uni-manager Management Console as an operations administrator or organization administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Changes**.
4. In the left-side organization tree of the Changes page, find the resource set of the organization to which the ECS instance belongs.
5. On the right side of the page, set the **Product Type** parameter to **Elastic Compute Service**.
6. Set the **Resource Type** parameter to **ECS**.
7. In the instances list, find the ECS instance whose resource set you want to change and click **Change Ownership** in the **Actions** column.
8. In the **Change Resource Set** dialog box, select a resource set of an organization to which the disks belong from the **Change Resource Set To** drop-down list. Change the resource set of the ECS instance to that of the organization to which the disks belong, and then attach the disks to the ECS instance.

Important

You can change the resource set of a resource only in the same level-1 organization.

12.10. How do I view the AccessKey pairs of an organization and a user?

This topic describes how to view the AccessKey pairs of an organization and a user in the Apsara Uni-manager Management Console.

View the AccessKey pairs of an organization

Note

Up to two AccessKey pairs can be created for each level-1 organization. By default, only operations administrators and level-1 organization administrators have permissions to view the AccessKey pairs of organizations.

- An operations administrator can view the AccessKey pairs of all level-1 organizations.
- A level-1 organization administrator can view only the AccessKey pairs of the organization to which the level-1 organization administrator belongs.

1. Log on to the Apsara Uni-manager Management Console as an operations administrator or a level-1 organization administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Organizations**.
4. On the Organizations page, find the level-1 organization whose AccessKey pairs you want to view and click the organization name in the left-side organization tree.
5. In the Basic Information section on the right side of the page, click **Management Accesskey**.
6. In the Management AccessKey dialog box, view the AccessKey IDs and AccessKey secrets of the organization.

View the AccessKey pairs of a user

1. Log on to the Apsara Uni-manager Management Console.
2. In the upper-right corner of the page, click the profile picture of the user.
3. Select **User Information**.
4. On the page that appears, view the AccessKey IDs and AccessKey secrets in the AccessKey Pair section.