Cloud Operations Center (COC)

User Guide

Issue	01
Date	2025-08-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 COC Enablement and Permissions Granting

1.1 Enabling COC

Enabling COC

When you log in to Cloud Operations Center (COC) for the first time, you need to obtain the agency permissions for accessing other cloud services and enable COC. The procedure is as follows:

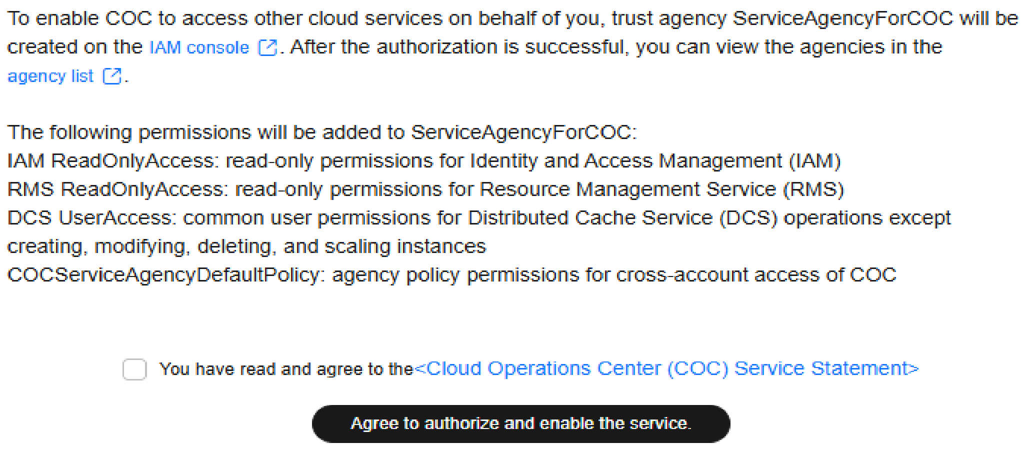
Step 1 Log in to **COC**.

Step 2 The service authorization page is displayed, prompting you to create the **ServiceAgencyForCOC** agency. This agency is used to grant COC the permissions to access other cloud services. For details about the permissions included in the agency, see **Table 1**.

NOTE

The **COCServiceAgencyDefaultPolicy** policy is added to the **ServiceAgencyForCOC** agency to support new service scenarios. If you enabled COC and authorized it during the open beta test of COC in the first half of 2024, manually add the **COCServiceAgencyDefaultPolicy** policy. This policy is compatible with the permissions required for future scale-out scenarios and does not affect the COC service features in use. For details, see **ServiceAgencyForCOC Agency Supplement Policy**.

Figure 1-1 Enabling COC and obtaining required permissions



To enable COC to access other cloud services on behalf of you, trust agency ServiceAgencyForCOC will be created on the IAM console. After the authorization is successful, you can view the agencies in the agency list.

The following permissions will be added to ServiceAgencyForCOC:
IAM ReadOnlyAccess: read-only permissions for Identity and Access Management (IAM)
RMS ReadOnlyAccess: read-only permissions for Resource Management Service (RMS)
DCS UserAccess: common user permissions for Distributed Cache Service (DCS) operations except creating, modifying, deleting, and scaling instances
COCServiceAgencyDefaultPolicy: agency policy permissions for cross-account access of COC

□ You have read and agree to the<Cloud Operations Center (COC) Service Statement>

Table 1-1 Permissions in ServiceAgencyForCOC

Permission	Description	Project [Region]	Application Scenario
IAM ReadOnlyAccess	Read-only permissions for IAM	Global service [Global]	Used to read personnel information under an IAM account in the **Personnel Management** module.
RMS ReadOnlyAccess	Read-only permissions for RMS	Global service [Global]	Used to synchronize managed cloud service resources in the **Resource Management** module.
DCS UserAccess	Common user permissions for DCS operations (excluding creating, modifying, deleting, and scaling instances).	Permissions on all resources (including new projects in the future)	Used to inject faults into DCS resources in the **Chaos Drills** module.

Permission	Description	Project [Region]	Application Scenario
COCServiceAgencyDefaultPolicy	Service agency policy for cross-account access to COC	Permissions on all resources (including new projects in the future)	Used to subscribe to notification channels in the personnel management module. Used to batch restart ECSs and RDS DB instances and change OSs in the **Batch Resource Operations** module. Used to query organization information in the cross-account scenario.

Step 3 Select "I have read and agree to the *Cloud Operations Center (COC) Service Statement* and click **Agree to authorize and enable the service**.

Step 4 After the authorization, you can enable COC and access the COC console to use its automatic O&M and fault management functions.

----End

ServiceAgencyForCOC Agency Supplement Policy

You can authorize a missing policy for an agency on the COC console or on the IAM console.

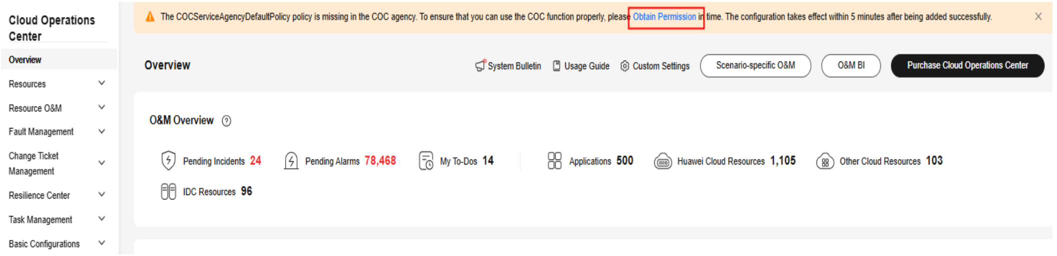
The following are two methods for adding missing policies. You can select one as needed.

Authorizing a Missing Policy for an Agency on the COC console

Step 1 Log in to COC.

Step 2 The alerting information about the missing policy is displayed on the top of the page. Click **Obtain Permission**.

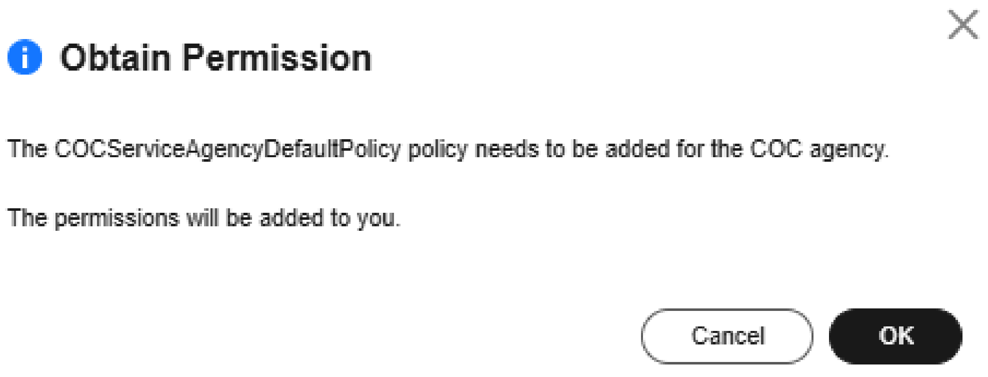
Figure 1-2 Authorizing a user



The COCServiceAgencyDefaultPolicy policy is missing in the COC agency. To ensure that you can use the COC function properly, please Obtain Permission in time. The configuration takes effect within 5 minutes after being added successfully.

Step 3 In the **Obtain Permission** dialog box, click **OK**.

Figure 1-3 Confirming an authorization



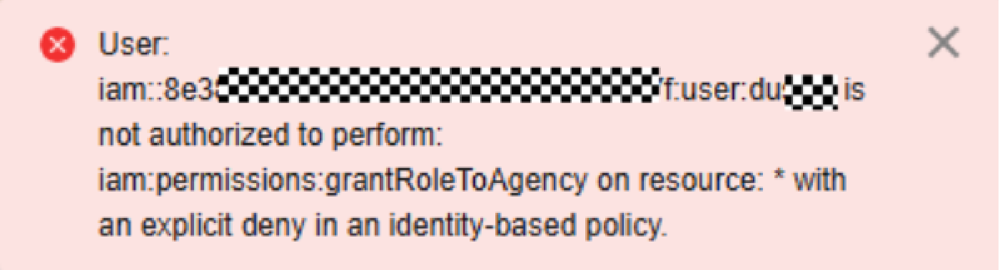
Obtain Permission

The COCServiceAgencyDefaultPolicy policy needs to be added for the COC agency.

The permissions will be added to you.

- If the system prompts that the authorization succeeded, the policy has been added to the **ServiceAgencyForCOC** agency. The alerting information on the top of the COC page disappears.
- If the following error message is displayed, the current user does not have the permissions in **iam:permissions:grantRoleToAgency**, contact the master account or an account with administrator permissions to add the missing policy displayed in the error information to the **ServiceAgencyForCOC** agency.

Figure 1-4 Error message



User: iam::8e3[redacted]f:user:du[redacted] is not authorized to perform: iam:permissions:grantRoleToAgency on resource: * with an explicit deny in an identity-based policy.

----End

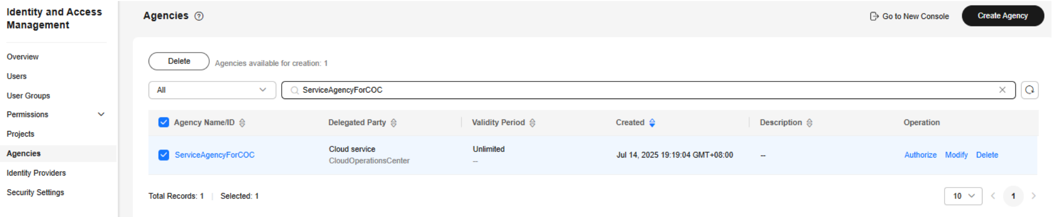
Authorizing a Missing Policy for an Agency on the IAM Console

Step 1 Log in to the **IAM console**.

Step 2 In the navigation pane, choose **Agencies**.

Step 3 Search for **ServiceAgencyForCOC**.

Figure 1-5 Searching for ServiceAgencyForCOC



☑ Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
☑ ServiceAgencyForCOC	Cloud service CloudOperationsCenter	Unlimited --	Jul 14, 2025 19:19:04 GMT+08:00	--	Authorize Modify Delete

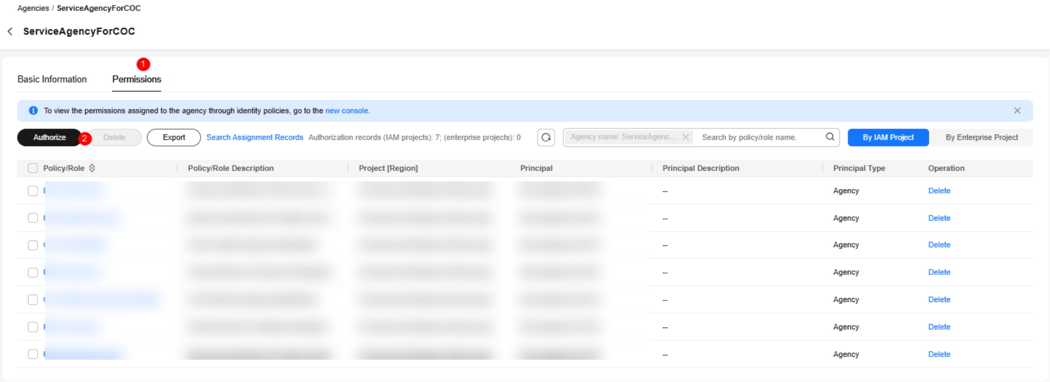
Total Records: 1 | Selected: 1

Step 4 In the list below, click **ServiceAgencyForCOC**.

Step 5 Click **Permissions**.

Step 6 Click **Authorize**.

Figure 1-6 Granted permissions



Agencies / ServiceAgencyForCOC

ServiceAgencyForCOC

To view the permissions assigned to the agency through identity policies, go to the new console.

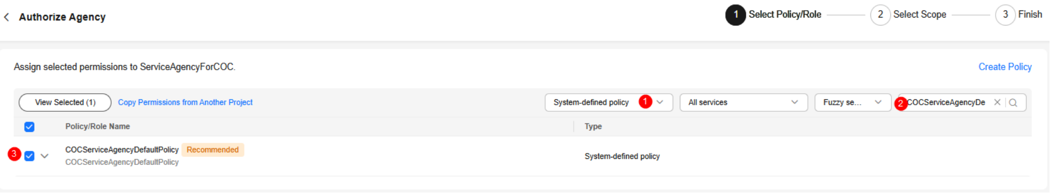
Authorization records (IAM projects): 7; (enterprise projects): 0

Agency name: ServiceAgenc...

Policy/Role	Policy/Role Description	Project [Region]	Principal	Principal Description	Principal Type	Operation
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete
[redacted]	[redacted]	[redacted]	[redacted]	--	Agency	Delete

Step 7 Set **Type** to **System-defined policy**, enter the missing policy name (for example, **COCServiceAgencyDefaultPolicy**) in the text box on the right, and select the policy.

Figure 1-7 Selecting a policy



Authorize Agency

Assign selected permissions to ServiceAgencyForCOC.

System-defined policy

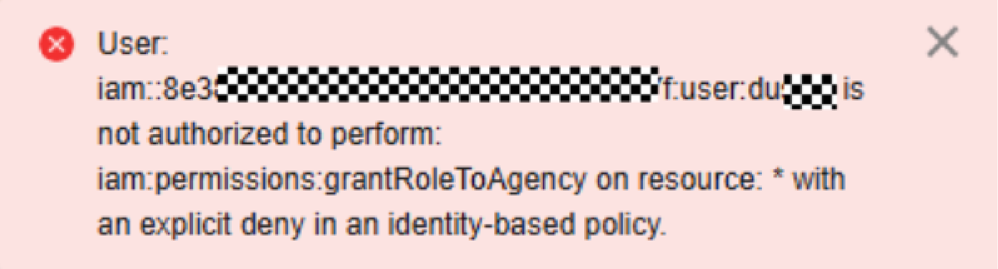
COCServiceAgencyDe

☑	Policy/Role Name	Type
☑	COCServiceAgencyDefaultPolicy Recommended COCServiceAgencyDefaultPolicy	System-defined policy

Step 8 Click **Next**, confirm the authorization scope, and click **OK**.

- If the system prompts that the authorization succeeded, the policy has been added to the **ServiceAgencyForCOC** agency. The alerting information on the top of the COC page disappears.
- If the following error message is displayed, the current user does not have the permissions in **iam:permissions:grantRoleToAgency**, contact the master account or an account with administrator permissions to add the missing policy displayed in the alerting information to the **ServiceAgencyForCOC** agency.

  Figure 1-8 Error message

  User: iam::8e3[redacted]f:user:du[redacted] is not authorized to perform: iam:permissions:grantRoleToAgency on resource: * with an explicit deny in an identity-based policy.

----End

Modifying or Deleting Agency Permissions

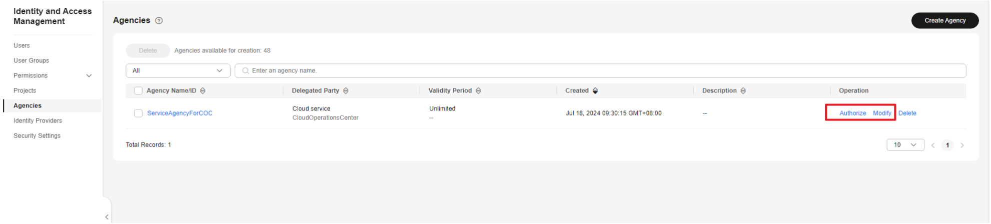
After COC is enabled, if an agency has excessive or insufficient permissions, you can modify the agency policy on **IAM**.

NOTE

- You can change the cloud service, validity period, description, and permissions for cloud service agencies, but not the agency name and type.
- Modifying the permissions of cloud service agencies may affect the usage of certain functions of cloud services. Exercise caution when performing this operation.
- For more information about agencies, visit **IAM**.

- To modify the permissions, validity period, and description of an agency, locate the agency you want to modify and click **Modify**.

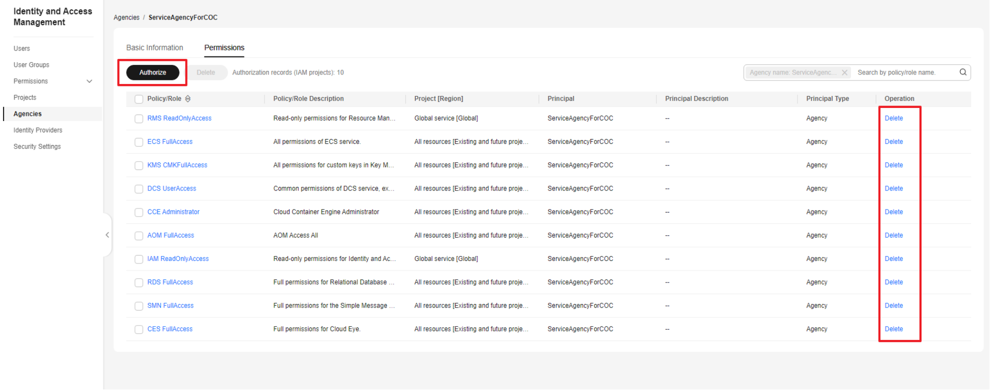
Figure 1-9 Agencies



Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
ServiceAgencyForCOC	Cloud service CloudOperationsCenter	Unlimited --	Jul 18, 2024 09:30:15 GMT+08:00	--	Authorize Modify Delete

- If you need to authorize the agency or delete the authorized permissions, perform operations on the permission granting page.

Figure 1-10 Granted permissions


Identity and Access Management
Users
User Groups
Permissions
Projects
Agencies
Identity Providers
Security Settings
Agencies / ServiceAgencyForCOC
Basic Information
Permissions
Authorize
Delete
Authorization records (IAM projects): 10
Agency name: ServiceAgenc...
Search by policy/role name.

Policy/Role	Policy/Role Description	Project [Region]	Principal	Principal Description	Principal Type	Operation
RMS ReadOnlyAccess	Read-only permissions for Resource Man...	Global service [Global]	ServiceAgencyForCOC	--	Agency	Delete
ECS FullAccess	All permissions of ECS service.	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
KMS CMKFullAccess	All permissions for custom keys in Key M...	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
DCS UserAccess	Common permissions of DCS service, ex...	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
CCE Administrator	Cloud Container Engine Administrator	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
AOM FullAccess	AOM Access All	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
IAM ReadOnlyAccess	Read-only permissions for Identity and Ac...	Global service [Global]	ServiceAgencyForCOC	--	Agency	Delete
RDS FullAccess	Full permissions for Relational Database ...	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
SMN FullAccess	Full permissions for the Simple Message ...	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete
CES FullAccess	Full permissions for Cloud Eye.	All resources [Existing and future proje...	ServiceAgencyForCOC	--	Agency	Delete

1.2 Granting COC Permissions Based on Roles

This section describes how to use **IAM** to implement fine-grained permissions control for your COC resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing COC resources.
- Grant only the minimum permissions required for users to perform a given task.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your COC resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

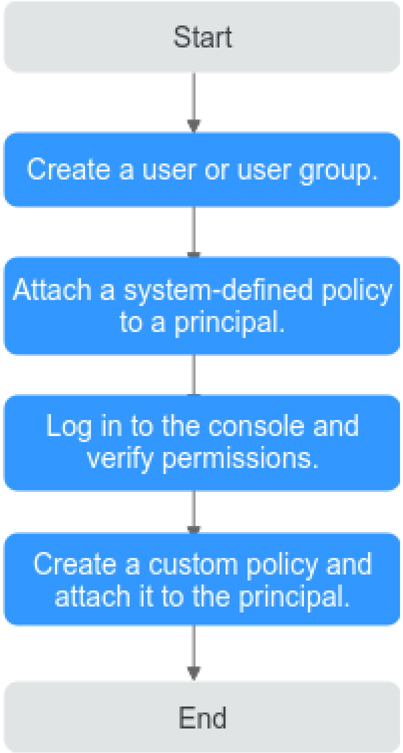
This section describes the procedure for granting COC permissions (see **Figure 1-11**).

Prerequisites

Before assigning permissions to a user group, ensure that you have learned about the permissions supported by COC. For details about the system-defined permissions supported by COC, see **Permissions Management**. To grant permissions for other services, learn about all **system-defined permissions**.

Example Workflow

Figure 1-11 Process of granting COC permissions to a user


Start
Create a user or user group.
Attach a system-defined policy to a principal.
Log in to the console and verify permissions.
Create a custom policy and attach it to the principal.
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and grant the read-only system permission **COC ReadOnlyAccess** and the administrator system permission **COC FullAccess** to the user group.

2. **Create an IAM user and add it to the group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** to COC and verify permissions.

   – Log in to COC, choose **Task Management** > **To-do Center** in the navigation pane. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task fails to be created (assume that you have only the **COC ReadOnlyAccess** permission), the **COC ReadOnlyAccess** permission has been applied.

  - Log in to COC, choose **Task Management** > **To-do Center** in the navigation pane. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task can be created (assume that you have only the **COC FullAccess** permission), the **COC FullAccess** permission has been applied.

4. If the system-defined COC permissions do not meet your authorization requirements, create custom policies. For actions supported for custom policies, see **Policies** and **Actions**.

   You can create custom policies in either of the following ways:

   - Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
   - JSON: Create a JSON policy or edit an existing one.

   For details, see **Creating a Custom Policy**. The following lists examples of common COC custom policies.

Example Custom Policies for COC

- Example 1: Allow users to create O&M tasks.

  ```
  {
   "Version": "1.1",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "coc:task:create"
      ]
    }
   ]
  }
  ```

- Example 2: Grant permissions to deny topic deletion.

  A policy with only the **Deny** permissions must be used along with other policies to take effect. If the permissions granted to an IAM user contain both **Allow** and **Deny**, the **Deny** permissions take precedence over the **Allow** permissions.

  Assume that you want to grant the permissions of the **COC FullAccess** policy to a user but want to prevent them from deleting documents. You can create a custom policy for denying document deletion, and attach both policies to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on COC resources except deleting documents. The following is an example of a deny policy:

  ```
  {
   "Version": "1.1",
   "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "coc:document:delete"
      ]
    }
   ]
  }
  ```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "coc:document:create",
        "scm:cert:complete"
      ]
    }
  ]
}
```

1.3 Granting COC Permissions Based on Policies

To **manage permissions on COC**, **access IAM** to:

- Create IAM users or user groups for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing COC resources.
- Grant only the minimum permissions required for users to perform a given task.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your COC resources.

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

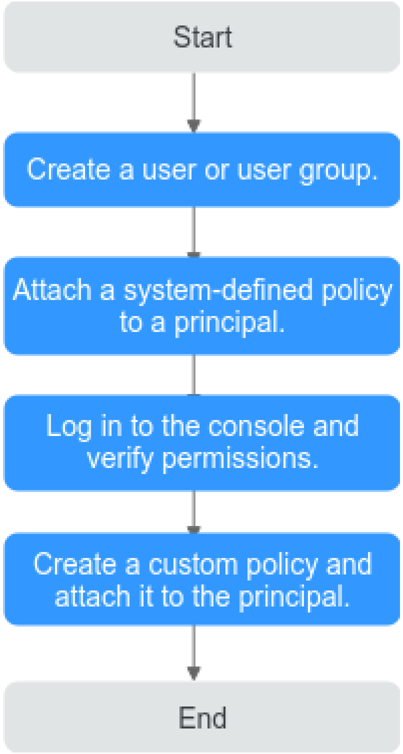
This section describes how to perform policy-based authorization. **Figure 1-12** shows the process.

Prerequisites

Before granting permissions, ensure that you have learned about COC permissions. For details about the system policies supported by COC, see **Policy-based Authorization Model**. To grant permissions for other services, learn about all permissions supported by IAM by referring to **System-defined Permissions**.

Example Workflow

Figure 1-12 Process of granting COC permissions to a user


Start
Create a user or user group.
Attach a system-defined policy to a principal.
Log in to the console and verify permissions.
Create a custom policy and attach it to the principal.
End

1. **Create a user** or **Create a user group**.

   Log in to the IAM console to create an IAM user or user group.

2. Grant a system policy to **the user** or **the user group**.

   Assign the system read-only permission **COC ReadOnlyPolicy** and the service administrator permission **COC FullAccessPolicy** to the user or add them to the user group.

3. **Log in** to COC and verify permissions.

   Log in to the console as an authorized user and verify the permissions.

   - Log in to COC, choose **Task Management** > **To-do Center** in the navigation pane. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task fails to be created (assume that you have only the **COC ReadOnlyPolicy** permission), the **COC ReadOnlyPolicy** permission has been applied.
   - Log in to COC, choose **Task Management** > **To-do Center** in the navigation pane. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task can be created (assume that you have only the **COC FullAccessPolicy** permission), the **COC FullAccessPolicy** permission has been applied.

4. Custom policies can be created as a supplement to the system policies of COC. For actions supported for custom policies, see **Policies** and **Actions**.

   You can create custom policies in either of the following ways:

   - Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.

– JSON: Create a JSON policy or edit an existing one.

For details, see **Creating a Custom Policy**. The following lists examples of common COC custom policies.

Example Custom Policies for COC

- Example 1: Allow users to create O&M tasks.

  ```
  {
    "Version": "5.0",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "coc:task:create"
        ]
      }
    ]
  }
  ```

- Example 2: Grant permissions to deny topic deletion.

  A policy with only the **Deny** permissions must be used along with other policies to take effect. If the permissions granted to an IAM user contain both **Allow** and **Deny**, the **Deny** permissions take precedence over the **Allow** permissions.

  Assume that you want to grant the permissions of the **COC FullAccessPolicy** policy to a user but want to prevent them from deleting documents. You can create a custom policy for denying document deletion, and attach both policies to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on COC resources except deleting documents. The following is an example of a deny policy:

  ```
  {
    "Version": "5.0",
    "Statement": [
      {
        "Effect": "Deny",
        "Action": [
          "coc:document:delete"
        ]
      }
    ]
  }
  ```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

  ```
  {
    "Version": "5.0",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "coc:document:create",
          "scm:cert:complete"
        ]
      }
    ]
  }
  ```

1.4 Cross-Account Management

Overview

COC provides secure and reliable cross-account data aggregation and resource O&M capabilities. If your account is an organization account, you can centrally manage the resources of all member accounts in your enterprise and access the automated O&M and O&M BI dashboards on COC without logging in to the member accounts one by one.

Assume that account A needs to manage account B. To use COC to perform cross-account O&M and management on account B, perform the following operations:

1. If account A is an organization administrator, skip this step. If account A is not an organization administrator, the organization administrator should add account A as a delegated administrator. For details, see **Specifying a Delegated Administrator**.

   NOTE

   The administrator can delegate the administrator rights to a member and revoke them. The right change takes effect after you refresh the page 1 to 2 minutes later.

2. The organization administrator or delegated administrator invites account B to join the organization. For details, see **Inviting an Account to Join the Organization**.
3. After account B is added to the organization, log in to the COC console as account A and perform cross-account O&M and management on the O&M BI dashboard, resource management, and job management pages.

For details about organizations, see the **Organization User Guide**.

NOTE

To access the data asset information of account B, COC automatically creates a service agency in account B.

- The agency is a cloud service agency. Its permission is **COCAssumeServiceLinkedAgencyPolicy,** and name is **ServiceLinkedAgencyForCOC**.
- If account B is deleted, COC automatically deletes the COC agency in account B.

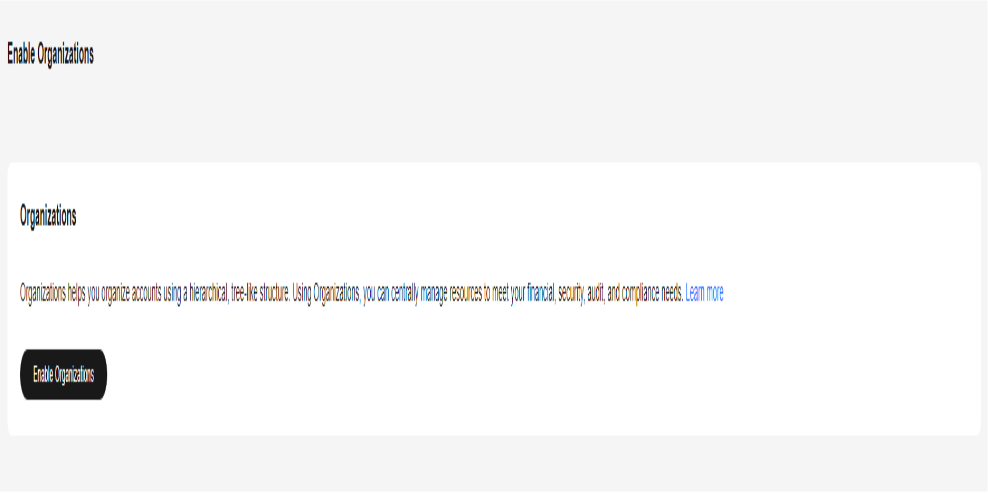
Enabling Cross-Account Management

After the cross-account management function is enabled, the organization or delegated administrator can perform unified resource management and access automated O&M and O&M BI dashboards for all member accounts in the organization on COC without logging in to the member accounts one by one. This section describes how to enable the cross-account management function.

Prerequisites

- You have enabled an organization service. If not, enable it by referring to **Enabling the Organizations Service**.

Figure 1-13 Enabling an organization service



Enable Organizations

Organizations

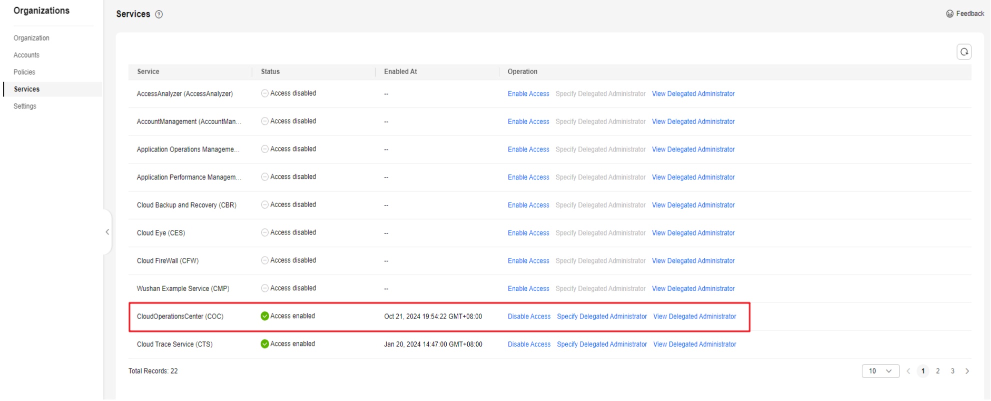
Organizations helps you organize accounts using a hierarchical, tree-like structure. Using Organizations, you can centrally manage resources to meet your financial, security, audit, and compliance needs. Learn more

NOTE

- Only the enterprise master account in the enterprise center can create organizations.
- After an organization is created in the enterprise center, you need to be re-authorized to access all its functions.
- After the organization service is enabled, access the organization management page, and perform the following steps to create an organization:
  - Create an organization as the organization administrator. One account can belong to only one organization.
  - A member account can only have the permission to view the control panel.
  - The member account must also be an enterprise-level account.

- Enable COC as a trusted service. For details, see **Enabling a Trusted Service**.

Figure 1-14 Enabling a trusted service

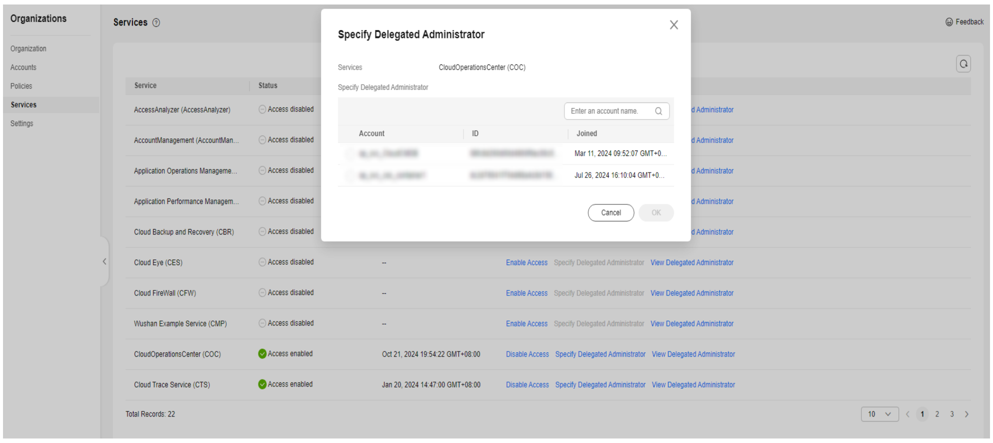


Service	Status	Enabled At	Operation
AccessAnalyzer (AccessAnalyzer)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
AccountManagement (AccountMan...	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Application Operations Manageme...	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Application Performance Managem...	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Backup and Recovery (CBR)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Eye (CES)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud FireWall (CFW)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Wushan Example Service (CMP)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
CloudOperationsCenter (COC)	Access enabled	Oct 21, 2024 19:54:22 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator
Cloud Trace Service (CTS)	Access enabled	Jan 20, 2024 14:47:00 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator

Total Records: 22

- The account is an administrator or delegated administrator. For details, see **Adding a Delegated Administrator**.

Figure 1-15 Adding a delegated administrator



Services CloudOperationsCenter (COC)

Specify Delegated Administrator

Account	ID	Joined
[redacted]	[redacted]	Mar 11, 2024 09:52:07 GMT+0...
[redacted]	[redacted]	Jul 26, 2024 16:10:04 GMT+0...

Service	Status		
AccessAnalyzer (AccessAnalyzer)	Access disabled		d Administrator
AccountManagement (AccountMan...	Access disabled		d Administrator
Application Operations Manageme...	Access disabled		d Administrator
Application Performance Managem...	Access disabled		d Administrator
Cloud Backup and Recovery (CBR)	Access disabled		d Administrator
Cloud Eye (CES)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud FireWall (CFW)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Wushan Example Service (CMP)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
CloudOperationsCenter (COC)	Access enabled	Oct 21, 2024 19:54:22 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator
Cloud Trace Service (CTS)	Access enabled	Jan 20, 2024 14:47:00 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator

Constraints

After a member account is invited to join an organization, the administrator or delegated administrator can view and manage the data and resources of the member account in the organization on COC. The cross-account management functions include O&M BI dashboards, resource management, and job management.

2 Overview

2.1 Overview

Scenarios

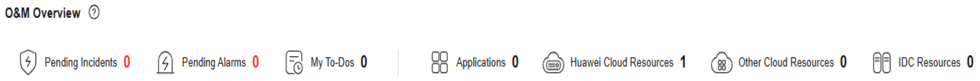
You can query and trace O&M to-do items (incident tickets, aggregated alarms, and my to-do lists), and query statistics about managed applications and resources under your account.

Overview

Step 1 Log in to **COC**.

On the **Overview** page, check the number of pending incidents, pending alarms, my to-dos, applications, and resources in the **O&M Overview** area.

Figure 2-1 Tracing O&M transactions



O&M Overview

Pending Incidents 0 | Pending Alarms 0 | My To-Dos 0 | Applications 0 | Huawei Cloud Resources 1 | Other Cloud Resources 0 | IDC Resources 0

If **O&M Overview** is not displayed on the **Overview** page, perform the following operations:

1. Click **Custom Settings** in the upper right corner.
2. On the displayed page, toggle on **O&M Overview**.
3. Click **OK**.

Step 2 Click **Pending Incidents** or other transactions.

The corresponding O&M transaction is displayed.

----End

2.2 Using Quick Configuration Center

Scenarios

Quick Configuration Center of COC provides a centralized configuration entry for all Huawei Cloud services, catering to various O&M scenarios. It enables automated operations across multiple regions and accounts, utilizing simplified configurations derived from best practices. This reduces the complexity of subsequent O&M tasks.

There are **Cloud O&M Configurations** and **Cloud Service Configurations** in the **Quick Configuration Center** area.

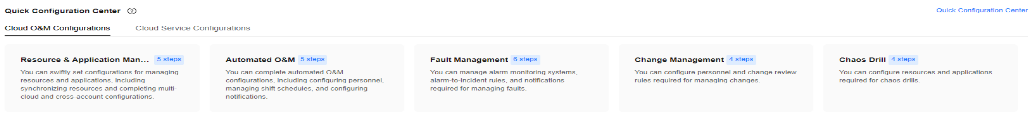
- **Cloud O&M Configurations** encompasses five features: resource and application management, automated O&M, fault management, change ticket management, and chaos drills. You can complete configurations by service scenario as required.
- **Cloud Service Configurations** allows you to configure alarm rules for multiple regions of Cloud Eye at a time.

Cloud O&M Configurations

Step 1 Log in to **COC**.

On the **Overview** page of COC, check the information in the **Quick Configuration Center** area.

Figure 2-2 Quick Configuration Center


Quick Configuration Center
Quick Configuration Center
Cloud O&M Configurations
Cloud Service Configurations

Resource & Application Man... 5 steps
You can swiftly set configurations for managing resources and applications, including synchronizing resources and completing multi-cloud and cross-account configurations.

Automated O&M 5 steps
You can complete automated O&M configurations, including configuring personnel, managing shift schedules, and configuring notifications.

Fault Management 6 steps
You can manage alarm monitoring systems, alarm-to-incident rules, and notifications required for managing faults.

Change Management 4 steps
You can configure personnel and change review rules required for managing changes.

Chaos Drill 4 steps
You can configure resources and applications required for chaos drills.

If **Quick Configuration Center** is not displayed on the **Overview** page, perform the following operations:

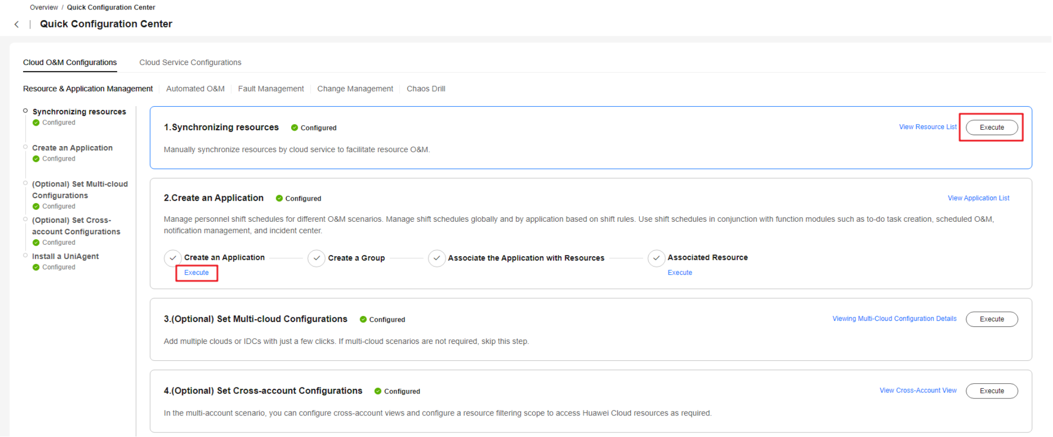
1. Click **Custom Settings** in the upper right corner.
2. On the displayed page, toggle on **Quick Configuration Center**.
3. Click **OK**.

Step 2 Choose **Cloud O&M Configurations** > **Early configuration**.

Step 3 Click the name of the target configuration item.

Step 4 Select a scenario and click **Execute**.

Figure 2-3 Selecting a scenario for configuration



Manually synchronize resources by cloud service to facilitate resource O&M.

Manage personnel shift schedules for different O&M scenarios. Manage shift schedules globally and by application based on shift rules. Use shift schedules in conjunction with function modules such as to-do task creation, scheduled O&M, notification management, and incident center.

Add multiple clouds or IDCs with just a few clicks. If multi-cloud scenarios are not required, skip this step.

In the multi-account scenario, you can configure cross-account views and configure a resource filtering scope to access Huawei Cloud resources as required.

----End

Cloud Service Configurations

Currently, the **Quick Configuration Center** module supports alarm rule configuration cross region for Cloud Eye.

Step 1 Log in to **COC**.

Step 2 On the **Overview** page, click **Cloud Service Configurations** in the **Quick Configuration Center** area.

Step 3 Click the name of the target configuration item.

Cloud Eye can be used as an example.

Step 4 Configure the basic information.

Table 2-1 Basic information parameters

Parameter	Description
Name	Name of a custom job.
Enterprise Project	Select an enterprise project from the drop-down list.
Description	Description of the alarm configuration.

Step 5 Set parameters in the **Execution Account & Region** area base on **Execution Type** you set.

- **Single**: A rule can only be executed by the current account.
  - **Region**: region where the target object is located.
  - **IAM Agency**: scope of permissions that can be used on COC to execute jobs.
- **Cross Account**: You can select multiple organization member accounts to create a rule.

- **Account**: tenant account name, which can be viewed on the **My Credentials** page.
- **Region**: region where the target object is located.
- **Organization Administrator Delegation**: The organization administrator or the COC service delegated administrator in the organization trusts the COC service.
- **Executable Delegation**: The execution account (a member tenant in the organization) trusts the COC service and the administrator's delegation.

Step 6 Set parameters in the **Alarm Rule** area.

For details, see **Creating an Alarm Rule and Notification**.

Step 7 Click **OK**.

The cloud service is configured.

----End

2.3 Viewing the Resource Dashboard

Scenarios

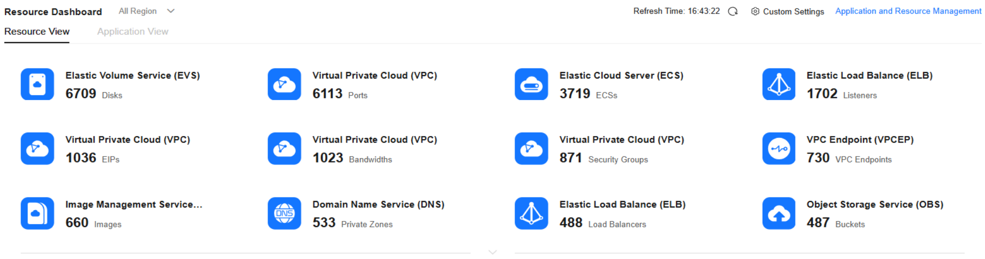
You can check the resources (such as ECSs, EIPs, and cloud databases) purchased under your account and the current alarm information of the resources (the alarms are generated after Cloud Eye is configured).

Viewing the Resource Dashboard

Step 1 Log in to **COC**.

On the **Overview** page, check the information in the **Resource Dashboard** area. By default, resources in all regions are displayed.

Figure 2-4 Resource information



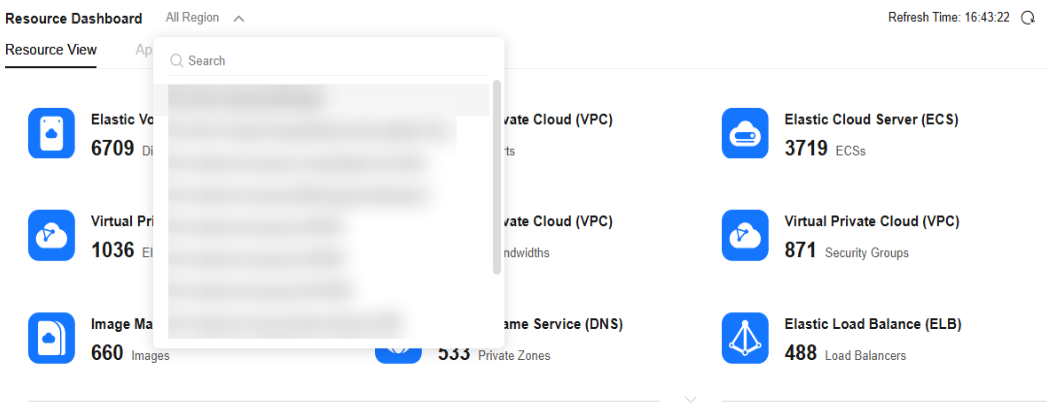
Elastic Volume Service (EVS) 6709 Disks
Virtual Private Cloud (VPC) 6113 Ports
Elastic Cloud Server (ECS) 3719 ECSs
Elastic Load Balance (ELB) 1702 Listeners
Virtual Private Cloud (VPC) 1036 EIPs
Virtual Private Cloud (VPC) 1023 Bandwidths
Virtual Private Cloud (VPC) 871 Security Groups
VPC Endpoint (VPCEP) 730 VPC Endpoints
Image Management Service... 660 Images
Domain Name Service (DNS) 533 Private Zones
Elastic Load Balance (ELB) 488 Load Balancers
Object Storage Service (OBS) 487 Buckets

Step 2 Click ↻ in the upper right corner of this area.

Synchronize resources and alarm information.

Step 3 Click **All Region** to choose a specified region and check resources in the region.

Figure 2-5 Choosing a region



Resource Dashboard All Region

Refresh Time: 16:43:22

Resource View Ap

Search

Elastic Vo
6709 Di

vate Cloud (VPC)
ts

Elastic Cloud Server (ECS)
3719 ECSs

Virtual Pri
1036 El

vate Cloud (VPC)
ndwidths

Virtual Private Cloud (VPC)
871 Security Groups

Image Ma
660 Images

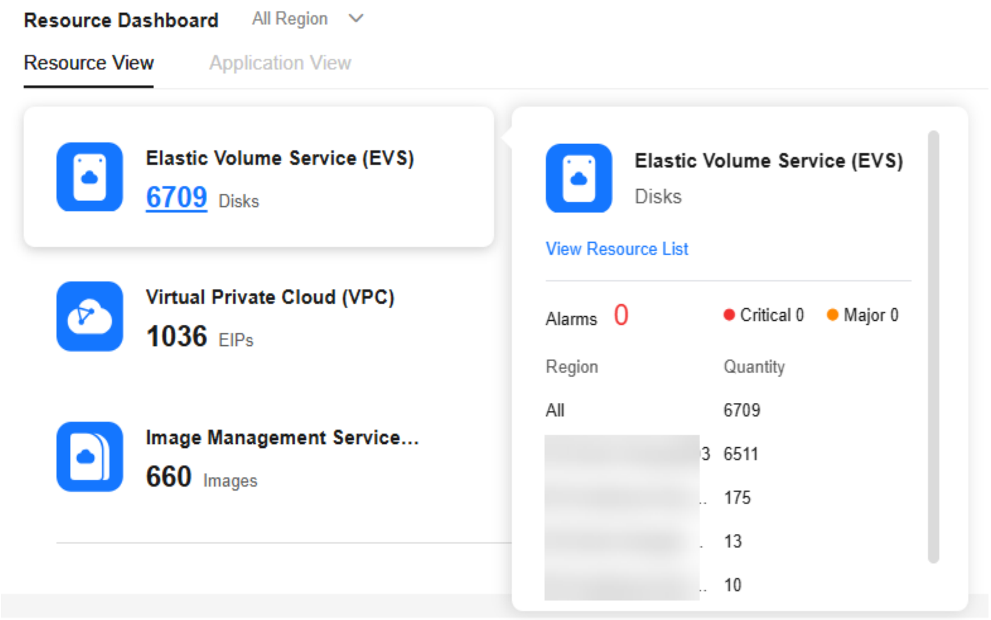
ame Service (DNS)
533 Private Zones

Elastic Load Balance (ELB)
488 Load Balancers

Step 4 Hover the mouse pointer over the cloud service icon.

The number of critical and major alarms and the region distribution of resource instances are displayed. The number in red in the upper right corner of the cloud service icon indicates the number of alarms.

Figure 2-6 Checking resource information



Resource Dashboard All Region

Resource View Application View

Elastic Volume Service (EVS)
6709 Disks

Virtual Private Cloud (VPC)
1036 EIPs

Image Management Service...
660 Images

Elastic Volume Service (EVS)
Disks

View Resource List

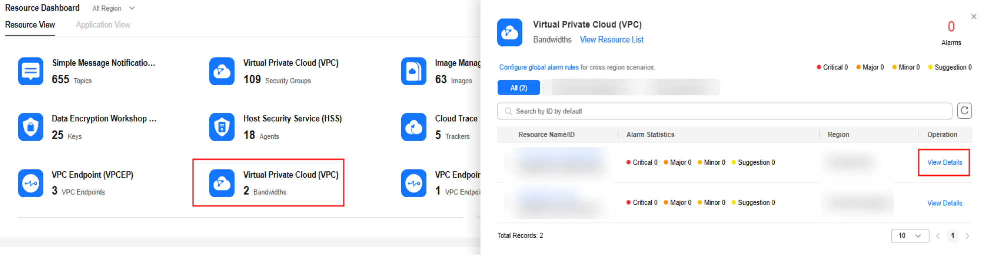
Alarms 0 ● Critical 0 ● Major 0

Region	Quantity
All	6709
3	6511
..	175
.	13
..	10

Step 5 Click the cloud service icon.

All resource information of the related resource type is displayed.

Figure 2-7 Checking resource information



Resource Dashboard All Region

Resource View Application View

Simple Message Notificatio... 655 Topics

Virtual Private Cloud (VPC) 109 Security Groups

Image Manag 63 Images

Data Encryption Workshop ... 25 Keys

Host Security Service (HSS) 18 Agents

Cloud Trace 5 Trackers

VPC Endpoint (VPCEP) 3 VPC Endpoints

Virtual Private Cloud (VPC) 2 Bandwidths

VPC Endpoi 1 VPC Endpoi

Virtual Private Cloud (VPC)

Bandwidths View Resource List

0 Alarms

Configure global alarm rules for cross-region scenarios.

● Critical 0 ● Major 0 ● Minor 0 ● Suggestion 0

All (2)

Search by ID by default

Resource Name/ID	Alarm Statistics	Region	Operation
	● Critical 0 ● Major 0 ● Minor 0 ● Suggestion 0		View Details
	● Critical 0 ● Major 0 ● Minor 0 ● Suggestion 0		View Details

Total Records: 2

Step 6 Locate the resource to be checked and click **View Details** in the **Operation** column.

The resource details page of the service is displayed.

Step 7 Locate the resource to be viewed and click ⌄ on the left of the resource name.

All alarm information (obtained from Cloud Eye) is displayed.

Step 8 Locate the alarm to be checked and click the alarm rule name.

The alarm rule page of Cloud Eye is displayed.

Step 9 Locate the alarm to be checked and click **Automatic Alarm Handling**.

Go to the **Execute Contingency Plan** page to quickly handle alarms.

----End

2.4 Setting and Viewing Resource Monitoring

Scenarios

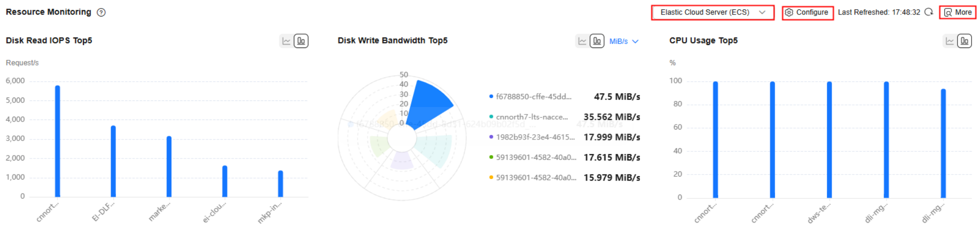
You can check the monitoring metrics of resources (such as ECSs, OBS instances, and cloud DB instances) purchased under your account. Taking ECS as an example, you can check TPS, CPU usage, disk read/write bandwidth, and the total number of OBS storage objects.

Resource Monitoring

Step 1 Log in to COC.

On the **Overview** page, check the information in the **Resource Monitoring** area. The monitoring metrics of Cloud Eye are displayed.

Figure 2-8 Cloud Eye monitoring information



Step 2 Click the drop-down list in the upper right corner in this area.

Choose the cloud service you want to check.

Step 3 Click **Configure**.

Customize the monitoring metrics on the displayed page.

Step 4 Click **More**.

Go to the **Server Monitoring** page of Cloud Eye to check the original information.

----End

2.5 Using OA to Handle Resource Risks

Scenarios

You can use Optimization Advisor (OA) to check resource risk items by referring to a large number of check items and optimization recommendations, such as ECS instance specifications check and whether to enable automated backup for resource instances or clusters.

Using OA to Handle Resource Risks

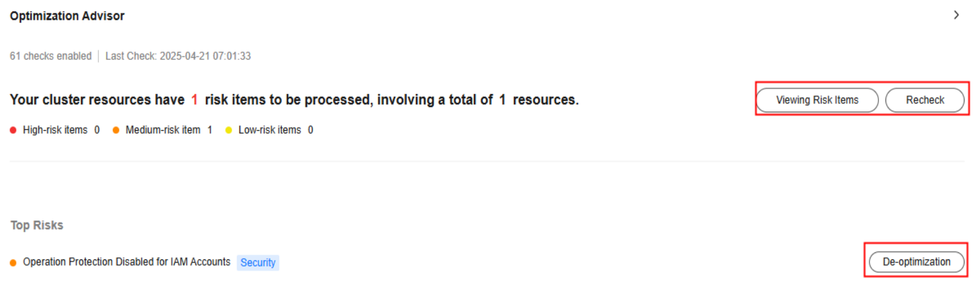
Step 1 Log in to COC.

On the **Overview** page, check the information in the **Optimization Advisor** area.

Step 2 Click **Viewing Risk Items** on the right in this area.

The top 10 risk items are displayed.

Figure 2-9 Viewing risk items



Optimization Advisor

61 checks enabled | Last Check: 2025-04-21 07:01:33

Your cluster resources have 1 risk items to be processed, involving a total of 1 resources.

● High-risk items 0 ● Medium-risk item 1 ● Low-risk items 0

Top Risks

● Operation Protection Disabled for IAM Accounts Security

Step 3 Click **Recheck**.

The risk items are rechecked.

Step 4 Click **De-optimization**.

The affected resources are handled based on the optimization suggestions.

----End

2.6 Viewing Security Score

Scenarios

You can check the secure score and risks of SecMaster. The security score is centered on threat alarms, compliance checks, and vulnerability reports.

⚠ CAUTION

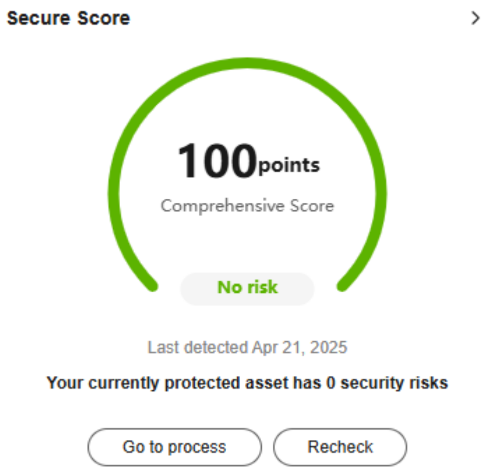
If you go to the **Secure Score** area on the **Overview** page by creating an IAM 3.0 delegation and switching the role, and set the policy authorization scope to global service resources, you need to add the **SecMaster ReadOnlyAccess-All resources** authorization for the delegation.

Viewing Security Score

Step 1 Log in to COC.

On the **Overview** page, check information in the **Security Score** area

Figure 2-10 Checking information in the Security Score area



Secure Score

100points

Comprehensive Score

No risk

Last detected Apr 21, 2025

Your currently protected asset has 0 security risks

Step 2 Click **Go to process**.

The SecMaster page is displayed.

Step 3 Click **Recheck**.

The security score is rechecked.

----End

2.7 Viewing O&M Metrics on O&M BI Dashboards

Prerequisites

If you use O&M BI dashboard in single-account scenarios, skip this section and go to **O&M BI Dashboards**.

If you use O&M BI dashboards in cross-account scenarios, ensure that the following conditions are met:

1. **Cross-account management has been enabled** for the current account, and the account is an organization or delegated administrator account.

2. The COC service has been enabled for the organization member accounts of the current account.

Scenarios

This module provides O&M BI dashboards with diverse metrics, including those for monitoring incidents, alarms, security compliance, service level objectives (SLOs), and production readiness reviews (PRRs). It offers an enterprise-grade O&M sandbox to help you understand your overall O&M situation from both bird's eye and ground level views.

- The dedicated O&M BI dashboard caters to various O&M personnel, aiding in O&M optimization, insights, and decision-making.
- COC provides 30+ preset O&M metrics, delivering insights into your cloud resources across seven-perspective BI dashboards and a comprehensive enterprise-grade O&M sandbox.
- Organization administrators or delegated administrators can view the O&M situation data of organization member accounts across accounts, and aggregate data of multiple regions and applications across accounts.

O&M BI Dashboards

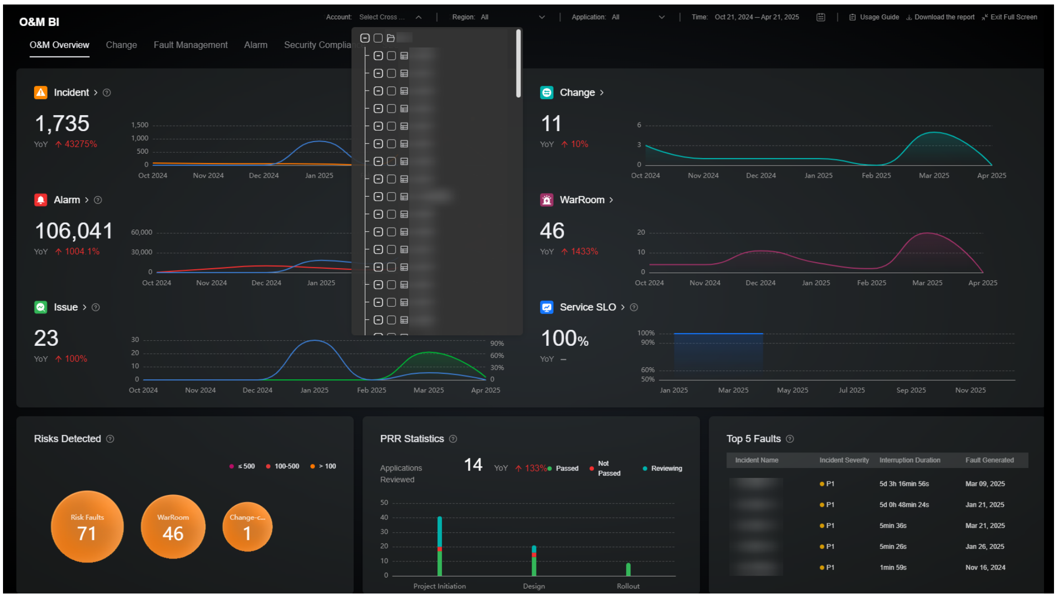
Step 1 Log in to **COC**.

Choose **Overview**.

Step 2 Click **O&M BI** in the upper right corner.

The **O&M BI** page is displayed. Filter O&M situation information by organization account, region, application, and date.

Figure 2-11 Filtering data by organization account

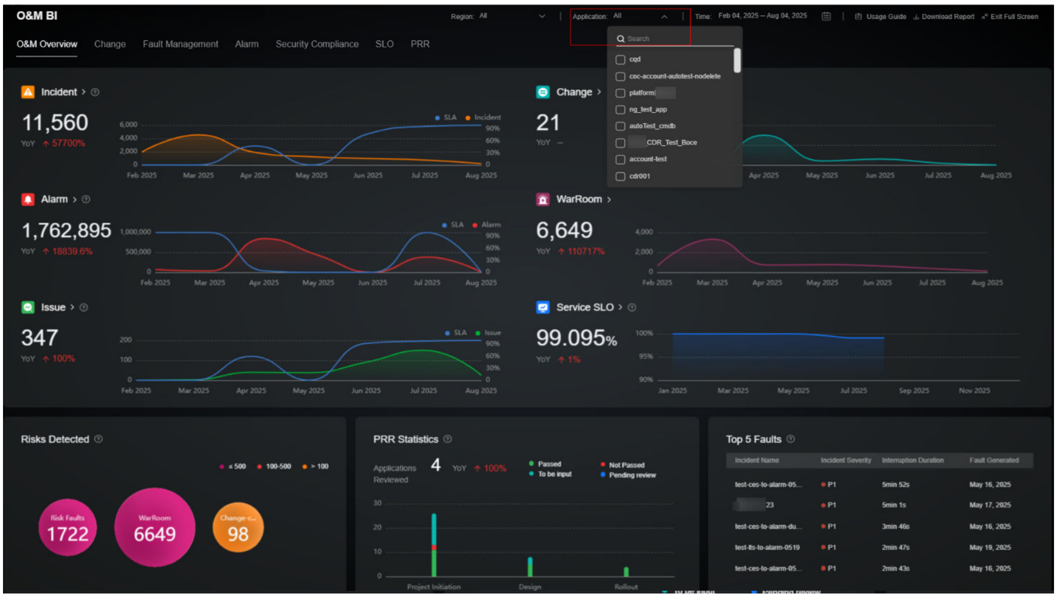


NOTE

In the cross-account scenario, if no account is selected, the O&M situation data of the current account is displayed by default.

Except the raw alarm data, other O&M BI dashboard data is updated at T+1.

Figure 2-12 Application data aggregation in cross-account scenarios

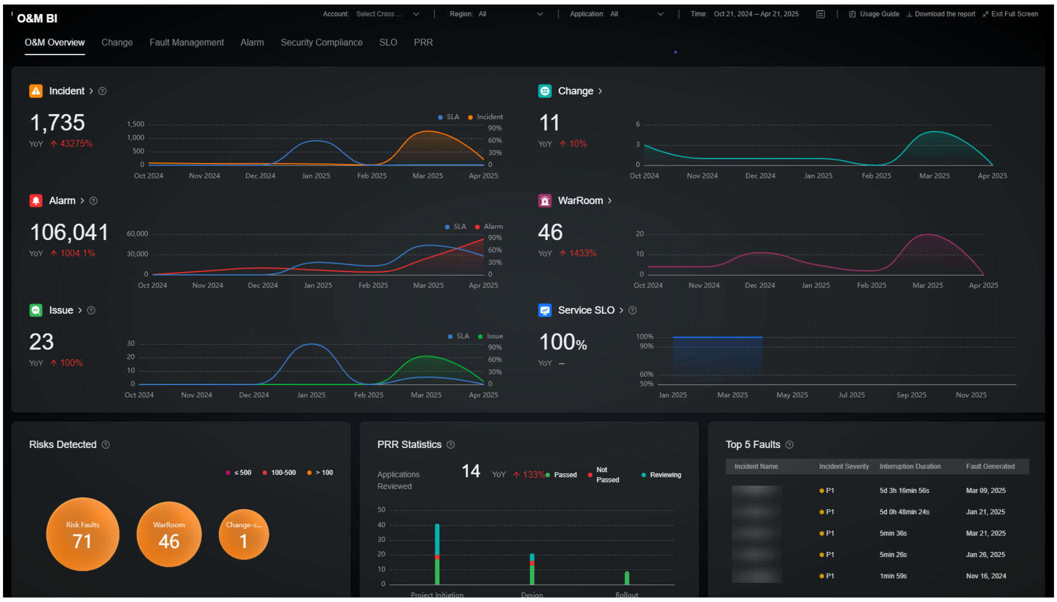


----End

O&M Overview

The **O&M Overview** page consists of overview data, risks detected, PRR statistics, and top 5 faults. The overview module enables you to observe the O&M situation from the global perspective, facilitating O&M optimization, insights, and decision-making. The risks detected module displays the number of risk faults, war rooms, and change-caused faults. The PRR statistics module provides the review statuses of your applications before they are released or put into commercial use. The top 5 faults module displays the incidents that have the most severe impacts on your services to help you quickly identify major fault scenarios. For details about the metrics included, see **Table 2-2**.

Figure 2-13 O&M overview



Account: Select Cross ...
Region: All
Application: All
Time: Oct 21, 2024 – Apr 21, 2025

Incident Name	Incident Severity	Interruption Duration	Fault Generated
[redacted]	● P1	5d 3h 16min 56s	Mar 09, 2025
[redacted]	● P1	5d 0h 48min 24s	Jan 21, 2025
[redacted]	● P1	5min 36s	Mar 21, 2025
[redacted]	● P1	5min 26s	Jan 26, 2025
[redacted]	● P1	1min 59s	Nov 16, 2024

Table 2-2 Metrics on the O&M Overview page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Overview	Incident	Incident center	Collects the trend of the incident ticket quantity.	Collect the number of incident tickets created in a selected period.	Day or month	Count
	Alarm	Alarm center	Collects the trend of the aggregated alarm quantity.	Collect the number of aggregated alarms created in a selected period.	Day or month	Count
	Issue	Issue management	Collects the trend of the number of issue tickets created	Collect the number of issue tickets created in a selected period.	Day or month	Count

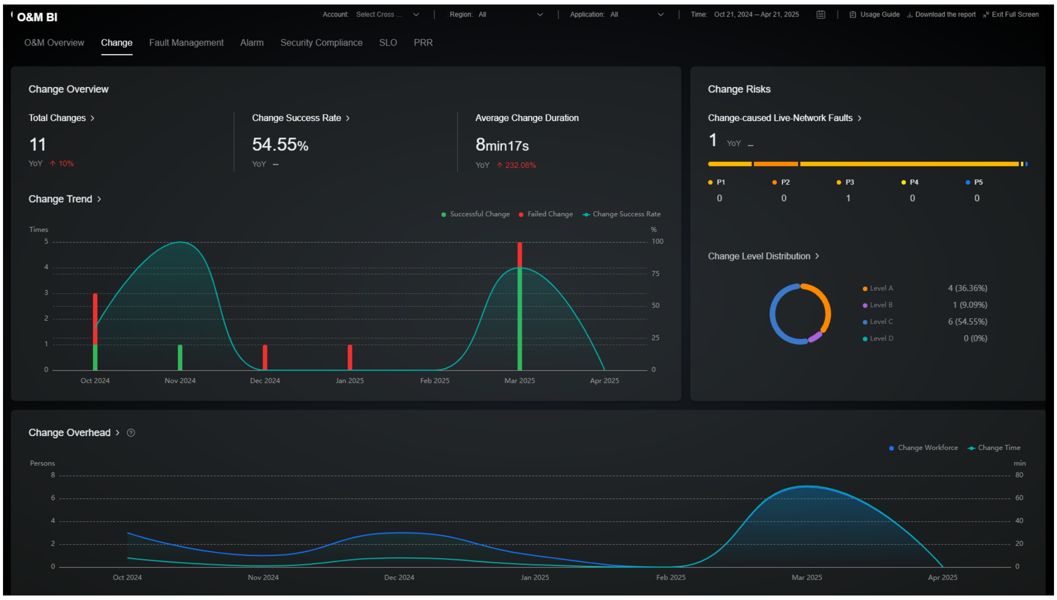
Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	WarRoom	War rooms	Collects the war room quantity trend.	Collect the number of all war rooms set up in a selected period.	Day or month	Count
	Change	Change management	Collects the trend of the number of change tickets created	Collect the number of change tickets created in a selected period.	Day or month	Count
	Service SLO	SLO management	Collects the change trend of the actual SLO value of a cloud service.	Actual SLO value = 1 – (Service unavailability duration/Total cloud service duration) × 100%	Day or month	%
Risks Detected	Change-caused Faults	Incident management	Collects the number of incidents caused by changes.	Collect the number of incident tickets whose incident type is change operation.	Day or month	Count
	Risk Faults	Incident management	Calculates the number of P3 or more severe incidents.	Collect the total number of P1, P2, and P3 incidents, including unhandled incidents.	Day or month	Count
	WarRoom	Alarm center	Collects the number of war rooms.	Collect the number of all war rooms set up in a selected period.	Day or month	Count
PRR Statistics	Applications covered by PRR	PRR	Collects the number of applications that are covered by a PRR.	Collect the number of applications that are covered by a PRR.	Day or month	Count
	Applications Passed in PRR Statistics	PRR	Collects the number of services passed or failed a PRR in each PRR phase.	Collect the number of services passed or failed a PRR in each PRR phase.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Top 5 Faults	Top 5 Faults	Incident management	Collects the top 5 most severe incidents.	Collect the number of handled P3 or more severe incidents in a specified period, rank the incidents by severity first and then by interruption duration to obtain the top 5 most severe incidents.	Day or month	Incident information

Change Management

The **Changes** page consists of change overview, change overhead, and change risks, which are key change metrics. The change overview area displays key change metrics, such as the average change duration and success rate, and provides Period over Period (PoP) data and trend charts to show the overall change status. The change risks area displays the faults caused by changes and provides the change level distribution charts. The change overhead area displays the trends of the persons required and time consumed by your services in a specified period so that you can control your change overhead as required. For details about the metrics included, see **Table 2-3**.

Figure 2-14 Change management



O&M BI

Account: Select Cross ... | Region: All | Application: All | Time: Oct 21, 2024 — Apr 21, 2025

Change Overview

Total Changes: 11 YoY ↑ 10%

Change Success Rate: 54.55% YoY –

Average Change Duration: 8min17s YoY ↑ 232.08%

Change Risks

Change-caused Live-Network Faults: 1 YoY –

P1	P2	P3	P4	P5
0	0	1	0	0

Change Level Distribution

Level	Count
Level A	4 (36.36%)
Level B	1 (9.09%)
Level C	6 (54.55%)
Level D	0 (0%)

Table 2-3 Metrics on the Change page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Change Overview	Total Changes	Change management	Collects the number of change tickets.	Collect the number of change tickets completed in a selected period.	Day or month	Count
	Change Success Rate	Change management	Collects the success rate of change tickets.	Metric value = Number change tickets that are handled/Total number of change tickets that are handled and failed × 100%	Day or month	%
	Average Change Duration	Change management	Collects the average duration for handling change tickets.	Metric value = Total duration required by handled change tickets in a selected period/ Number of handled change tickets × 100%	Day or month	dd hh mm
	Change Trend	Change management	Collects the number of successful and failed changes and change success rate trend.	Collect the number of successful and failed changes and change success rate trend.	Day or month	Count
Change Overhead	Change Manpower	Change management	Collects the number of O&M engineers required in changes.	Collect the number of change coordinators and the number of change implementers.	Day or month	Person-time
	Change Duration	Change management	Collects the average handling duration of change tickets.	Metric value = Total duration required by handled change tickets in a selected period/ Number of handled change tickets × 100%	Day or month	dd hh mm

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Change Risks	Change-caused Live-Network Faults	Change management	Collects the number of change-caused incidents of each level on the live network.	Collect the number of incident tickets created for each level of incidents that are caused by changes within a selected time range.	Day or month	Count
	Change Level	Change management	Collects the number of change tickets for each level of changes.	Collect the number of change tickets for each level of changes in a selected period.	Day or month	Count

Fault Management

The **Fault Management** page consists of incident statistics, war rooms, and problem improvement, which are key metrics of incident management. The incident statistics area displays incident quantity, closure rate, rectification duration, affected applications, and SLA fulfillment the rate. Incident risks are analyzed in forms of PoP changes, trend charts, and top or bottom incidents. The **WarRoom** area displays affected applications, incident level statistics, and handling time window distribution, which are key metrics for the occurrence and improvement of major faults. The problem improvement area includes the issue closure rate and trend analysis of problem improvement to ensure that experience in handling known faults is accumulated, reducing the frequency and handling duration of similar faults. For details about the metrics included, see **Table 2-4**.

Figure 2-15 Fault management page

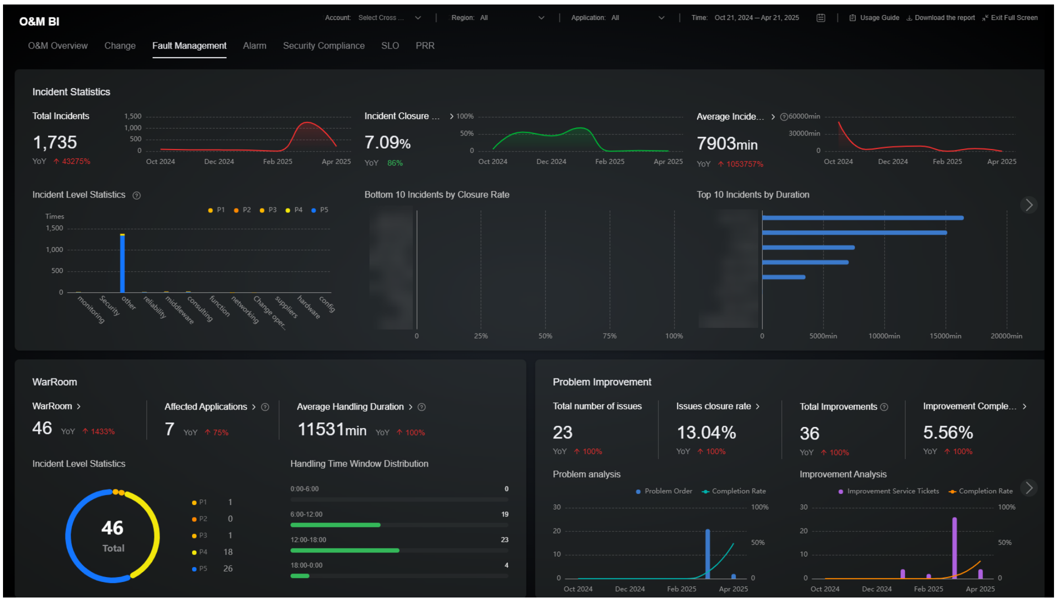


Table 2-4 Metrics on the Incident Management page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Incident statistics	Total Incidents	Incident management	Collects the total number of incident tickets.	Collect the number of incident tickets created in a selected period. Note: Incident tickets in the draft or closed state are not counted.	Day or month	Count
	Incident Level	Incident management	Collects the number of incident tickets of each type and level.	Collect the number of incident tickets of each type and level within a selected time range.	Day or month	Count
	Incident Closure Rate	Incident management	Collects the closure rate of incident tickets.	Metric value = Number of incident tickets in the "Completed" status in the selected time period/Total number of incident tickets × 100%	Day or month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	Average Incident Duration	Incident management	Collects the average handling duration of incident tickets.	Metric value = Total handling duration of closed incidents/ Number of closed incidents × 100%	Day or month	ddhhmm
	Affected Applications	Incident management	Collects the number of applications affected by an incident ticket.	Collect the number of affected applications (including deleted applications) of an incident ticket after deduplication.	Day or month	Count
	Incident SLA Fulfillment Rate	SLA management	Collects statistics on the SLA fulfillment status of incident tickets.	Metric value = Number of incident tickets that do not violate the SLA/ Total number of incident tickets included in the statistics × 100%	Day or month	%
War Rooms	WarRoom	War rooms	Collects the number of all war rooms set up.	Collect the number of all war rooms set up in a selected period.	Day or month	Count
	Incident Level	Incident management	Collects the number of incidents of each level for setting up war rooms.	Collect the number of incidents of each level for setting up war rooms.	Day or month	Count
	Affected Applications	War rooms	Collects the number of affected applications for setting up war rooms.	Calculate the number of affected applications for setting up war rooms after deduplication.	Day or month	Count
	Average Handling Duration	War rooms	Collects the average duration for fault recovery from setting up war rooms.	Collect the total handling time of stopped war rooms in the selected period/ Number of stopped war rooms.	Day or month	ddhhmm

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	Handling Time Window Distribution	War rooms	Collects the number of times war rooms are set up in each time window.	Collect the number of times war rooms are set up in each time window.	Day or month	Count
Problem Improvement	Total Issues	Issue management	Collects the number of issue tickets.	Collect the number of all issue tickets within a specified period except those in the canceled and to-be-submitted states.	Day or month	Count
	Issue Closure Rate	Issue management	Collects the closure rate of issue tickets.	Metric value = Number of completed issue tickets/Total number of issue tickets × 100%	Day or month	%
	Total Improvement Tickets	Improvement ticket management	Collects the number of improvement tickets.	Collect the number of all improvement tickets within a specified period except those in the draft state.	Day or month	Count
	Improvement Ticket Completion Rate	Improvement ticket management	Collects the closure rate of improvement tickets.	Metric value = Number of completed improvement tickets/ Total number of improvement tickets × 100%	Day or month	%

Monitoring and Alerting

The **Alarm** page displays alarm analysis, alarm costs, and alarm quality. These are key metrics displayed in charts. O&M personnel can quickly learn about the overall service status. The alarm analysis area displays the total number of alarms, alarm severity, top applications, alarm reduction, and alarm trend. By analyzing historical alarm data, the O&M supervisor can understand the trend and mode of service alarms and identify potential faults or performance deterioration. The alarm cost statistics include the alarm closure rate and automatic alarm handling rate. The O&M supervisor can effectively control the labor cost of changes based on the alarm cost. The alarm quality statistics collects incident ticket- and war room-triggered alarm detection rates, helping O&M supervisors evaluate the validity of current alarms and optimize alarm configurations in a timely manner. For details about the metrics included, see **Table 2-5**.

Figure 2-16 Monitoring and alarm reporting

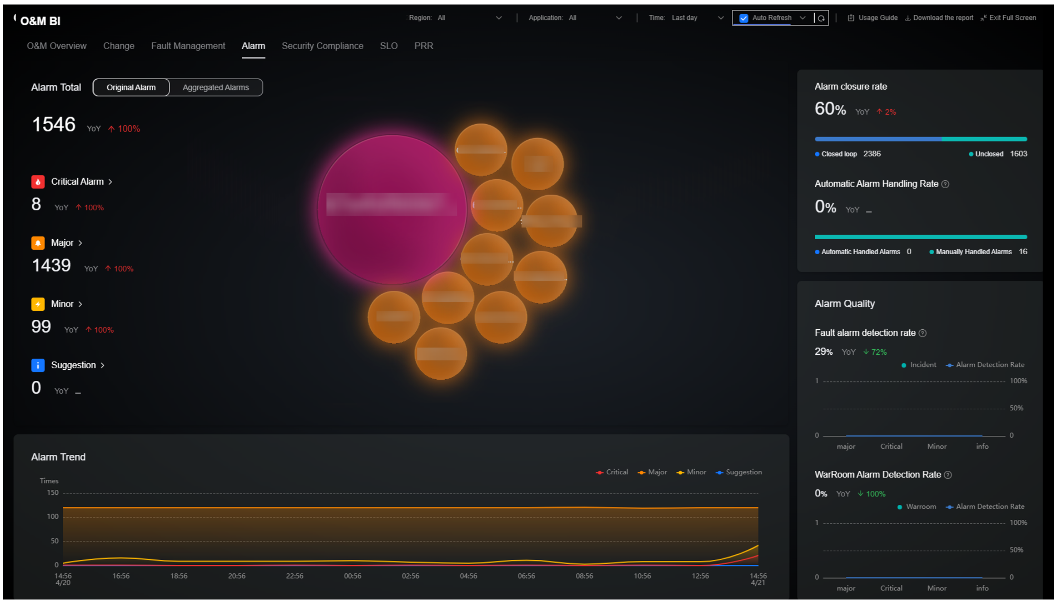


Table 2-5 Metrics on the Alarm page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Alarm analysis	Total Alarms	Alarm management	Collects the number of alarms in the alarming state.	Collect the number of alarms within a specified period in the alarming state.	Day or month	Count
	Alarm Severity	Alarm management	Collects the number of alarms of each severity in the alarming state.	Collect the number of alarms of each severity within a specified period in the alarming state.	Day or month	Count
	Alarm Trend	Alarm management	Collects the trend of the number of alarms of each severity within the selected time range.	Collect the number of alarms of each severity within a selected time range	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Alarm Cost	Alarm Closure Rate	Alarm management	Collects statistics on alarm closure.	Metric value = Number of closed alarms in the selected time range/ Total number of alarms × 100%	Day or month	%
	Automatic Alarm Handling Rate	Alarm management	Collects statistics on automatic alarm handling.	Metric Value = Number of automatically handled alarms in the selected time range/Total number of alarms ×100%	Day or month	%
Original Alarm > Alarm Quality	Fault Alarm Detection Rate	Incident management	Collects statistics on the number of incident tickets triggered by alarms.	Metric value = Number of incident tickets converted from alarms in the selected time range/Total number of incident tickets in the selected time range × 100%	Day or month	%
	WarRoom Alarm Detection Rate	War rooms	Collects the number of war rooms triggered by alarms.	Metric value = Number of war rooms triggered by incidents converted from alarms in the selected time range/ Total number of war rooms × 100%	Day or month	%
Aggregated Alarms > Alarm SLA	Alarm SLA Fulfillment Rate	SLA management	Collects statistics on the SLA fulfillment status of aggregated alarms.	Metric value = Number of alarm tickets that do not violate the SLA/ Total number of alarm tickets included in the statistics × 100%	Day or month	%

NOTE

For the **Total Alarms** metric, the bubbles on the page indicate the applications with top alarms of each severity. Top 1 is critical alarms, top 5 is major alarms, top 10 is minor alarms, and another top 10 is warning alarms.

Security Compliance

The **Security Compliance** page consists of statistics on scanned patches and account management. Patch scanning allows you to view instance compliance data by region, application, and OS, and display the number of scanned instances by time range.

Figure 2-17 Security Compliance page

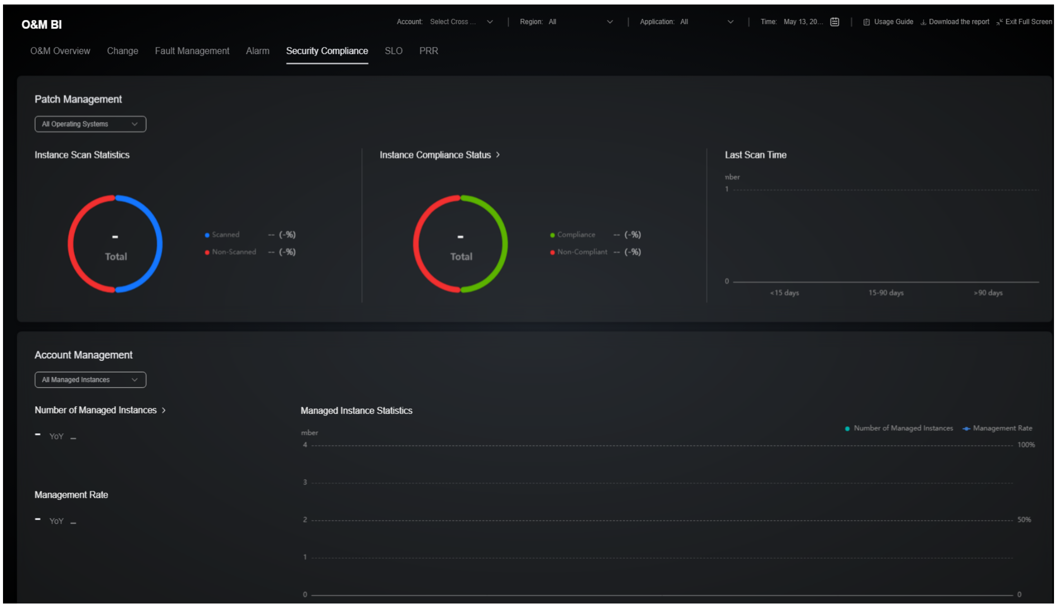


Table 2-6 Metrics on the Security Compliance page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Patch Management	Instances Scan Statistics	Patch management/CloudCMDB	Collects the number of ECSs where patches have been scanned and have not been scanned under a tenant account.	The number of unscanned instances is the total number of instances minus the number of scanned instances.	Area and application	Count
	Instance Compliance Status	Patch management	Collects the number of compliant and non-compliant instances in the scanned instances	Collect the number of instances in each compliance status in patch management.	Area and application	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	Last Scan Time	Patch management	Collects statistics on the latest scanning time range of scanned instances.	Collect statistics on the latest scanning time range of scanned instances.	Area and application	Count
Account Management	Number of Managed Instances	Account management	Collects the number of managed cloud service instances in account management	Collect the number of managed cloud service instances in account management.	Area and application	Count
	Management Rate	Account management	Collects the proportion of the managed cloud service instances to all instances	Management rate = Number of managed instances/Total number of instances × 100%.	Area and application	%
	Managed Instance Statistics	Account management	Collects the statistics on the instance management trend by time period.	Collect the statistics on instance management trend by time period.	Area and application	-

Service Level Objective (SLO)

The **SLO** page covers the overall SLO achievement, SLO statistics by application, and error budget management. The overall SLO achievement area displays average annual and monthly SLO data and the overall SLO trend. The SLO statistics by application area displays SLO values by time and application for you to evaluate the service level of each application. The error budget area shows the error cost calculated on the SLO data of each application for you to evaluate changes or other high-risk operations. For details about the metrics included, see **Table 2-7**.

Figure 2-18 SLO dashboard

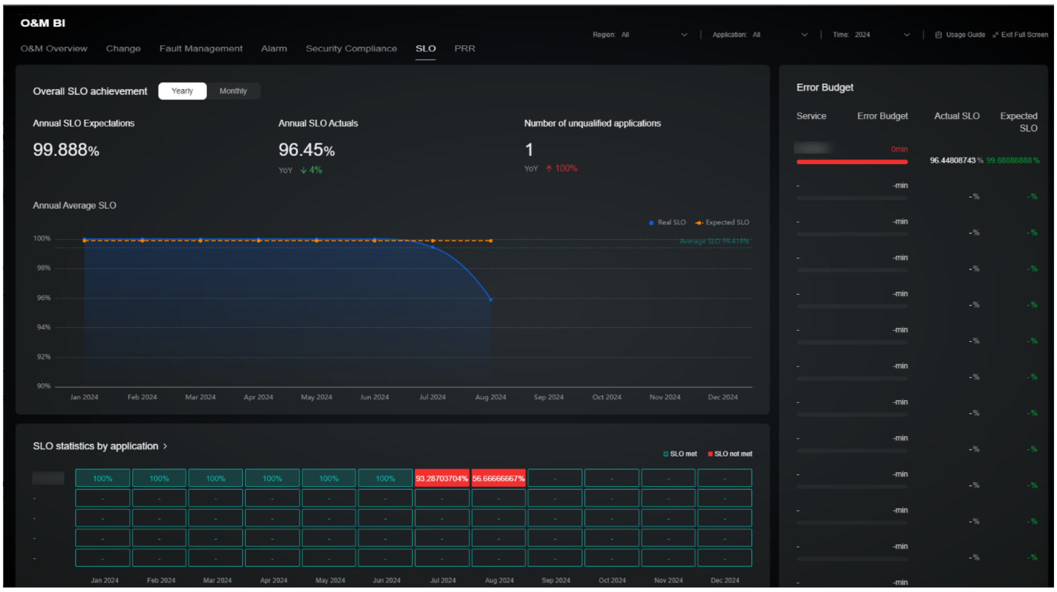


Table 2-7 Metrics on the SLO page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Overall SLO Achievement	Expected Annual SLO	SLO management	Collects the expected SLO value of an application in a year.	Expected SLO value = Expected SLO value set in the SLO management module Expected SLO value of multiple applications = Average expected SLO value of applications	Year	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	Annual Actual SLO Value	SLO management	Collects the actual SLO achievement of an application in a year.	Actual SLO value in a year = 1 – (Annual service unavailability duration/Total application duration in a year) × 100% Actual SLO value of multiple applications in a region = Yearly average SLO value of an application in a region Actual SLO value of an application in multiple regions = Yearly minimum SLO value of an application in a region Actual SLO value of multiple applications in multiple regions = Average actual SLO value of an application in multiple regions	Day or month	%
	Non-compliant Applications	SLO management	Collects the number of applications that do not meet SLO expectations.	Calculate the number of applications that fail to achieve the SLO expectation. If all regions are selected and the actual SLO value of applications in any region in a year is less than the annual expected SLO value, the SLO exception is not met.	Day or month	Count

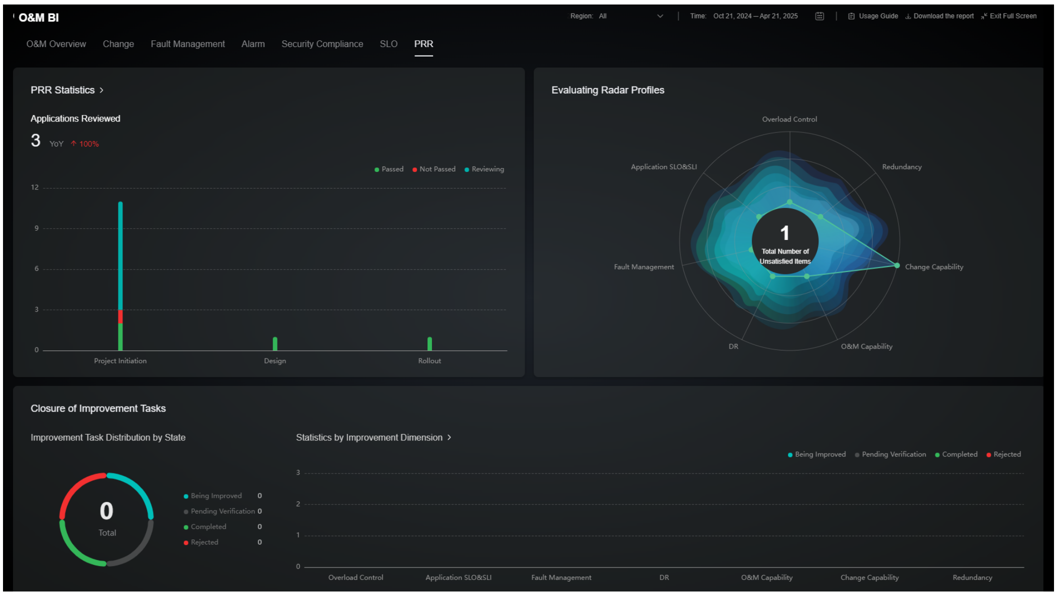
Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
	Expected Monthly SLO	SLO management	Collects the expected SLO achievement of an application in a month.	Expected SLO value = Expected SLO value set in the SLO management module Expected SLO value of multiple applications = Average expected SLO value of applications	Day or month	%
	Actual Monthly SLO	SLO management	Collects the actual SLO achievement in a month.	Actual SLO value in a month = 1 – (Monthly service unavailability duration/Total service duration in a month) × 100% Actual SLO value of multiple applications in a region = Monthly average SLO value of an application in a region Actual SLO value of an application in several regions = Monthly minimum SLO value of an application in a region Actual SLO value of multiple applications in multiple regions = Average actual SLO value of an application in multiple regions	Day or month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
SLO Statistics by Application	SLO Statistics by Application	SLO management	Collects SLO statistics by application.	Collect the monthly SLO actual value by application. Actual SLO value in a month = 1 – (Monthly service unavailability duration/Total service duration in a month) × 100% Actual SLO value of an application in several regions = Monthly minimum SLO value of an application in a region	Day or month	%
Error Budget	Error Budget	SLO management	Measures the difference between the actual performance and the expected performance and provides the error budgets.	If the actual SLO value is greater than the expected SLO value: Error budgets = (Actual annual SLO value – Expected annual SLO value) × Total service duration in a year (minutes) If the actual SLO value is less than or equal to the expected SLO value, the error budget is 0.	Day or month	Minute

PRR Dashboard

The **PRR** page consists of PRR statistics, evaluation radar profiles, and improvement task closure. The PRR statistics area shows the review phase of each service before the service is put into production and the review status. The evaluation radar profiles area shows the distribution of review items that do not meet service requirements. The improvement task closure area presents the rectification statuses of the items that do not meet the review requirements. For details about the metrics included, see **Table 2-8**.

Figure 2-19 PRR dashboard



Region: All

Time: Oct 21, 2024 – Apr 21, 2025

Being Improved 0
Pending Verification 0
Completed 0
Rejected 0

Table 2-8 Metrics on the PRR page

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
PRR Statistics	Services Reviewed	PRR	Collects the number of services that are covered by the PRR.	Collect the total number of services are covered by the PRR within a selected time range. (Deduplicated services are excluded.)	Day or month	Count
	Applications Reviewed	PRR	Collects the number of applications that are included in each PRR phase and the approval status.	Collect the number of applications included in each PRR phase and the review status within a selected time range. (Deduplicated applications are collected.)	Day or month	Count
Evaluation Radar Profiles	Evaluation Radar Profiles	PRR	Collects the distribution of PRR items that fail to be met.	Collect the number of review items that are not met in a selected time range.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Unit
Closure of Improvement Tasks	Improvement Task Distribution by Status	PRR	Collects the number of improvement tasks and their statuses.	Collect the number of improvement tasks and the statuses of the tasks within a selected time range.	Day or month	Count
	Improvement Tasks	PRR	Collects the number of improvement tasks in each dimension and their closure statuses.	Collect the number of improvement tasks by review item and the statuses of these tasks.	Day or month	Count

3 Resource Management

3.1 Overview

In the Information Technology Infrastructure Library (ITIL) process, the infrastructure resource-oriented management approach can cause problems such as data isolation and information inconsistency between O&M services. The resource management function of Cloud Operations Center can centrally manage core resources of Huawei Cloud and other clouds and offline IDC resources, quickly providing accurate and consistent resource configuration data for features such as change management and batch O&M.

COC leverages the following mechanisms to implement unified resource management:

- Resource discovery and identification: COC can automatically discover and identify offline resources of Huawei Cloud, peer vendor clouds, and IDCs, and manage them centrally.
- Resource monitoring and management: Through a unified monitoring page, O&M engineers monitor resource usage in real time and dynamically adjust resource usage.
- Data synchronization and consistency: COC supports data synchronization to ensure data consistency and accuracy between O&M services.

3.2 Synchronizing Resources

Scenarios

If resource data is not properly displayed, you can trigger the resource synchronization function to manually update the data. This operation can calibrate the data status in a timely manner, ensure that the resource information is always up to date and reliable, and provide accurate basis for service decision-making and system operations.

The system now employs real-time resource synchronization, replacing the outdated asynchronous approach. This great improves the synchronization efficiency and enables instant response with zero delay.

Concepts:

- A resource is an entity that you can use on the cloud platform. A resource can be an Elastic Cloud Server (ECS), an Elastic Volume Service (EVS) disk, or a Virtual Private Cloud (VPC).
- To synchronize resources, you must have the **rms:resources:list** permission. This permission is used to call RMS APIs to obtain resources in all regions to which the current user belongs.

Prerequisites

- To synchronize resources of other cloud vendors, ensure that you have added accounts of other cloud vendors in the multi-cloud configuration. For details, see **3.3 Connecting to Other Cloud Vendors**.
- Prerequisites for synchronizing Alibaba Cloud resources:

  You have enabled the resource center service on Alibaba Cloud.

  You have logged in to the Alibaba Cloud web page, accessed the resource management page, and enabled the resource center feature. If you have already enabled the resource center feature, you can use it directly.
- Prerequisites for synchronizing AWS resources:
  - The master account has enabled the Config service.

    You have accessed the Config service, select the region where resources you want to synchronize are located, and enabled the Config service in one click.
  - Add actions to the account corresponding to the AK or SK.
    - Creating a policy: Access the IAM console, create a policy on the **Policies** page. Select the **EC2** service, filter operations and select **DescribeRegions**, add the **Config** service, filter operations and select **SelectResourceConfig** and **BatchGetResourceConfig**, click **Next** and create the policy.
    - Adding a policy to a user: On the IAM console, choose **Users** user and add permissions, select the policy created in the previous step, and click **Next** to complete permissions adding.
- Prerequisites for synchronizing Azure resources:
  - You have registered an application so that the Microsoft Entra ID can be used for identity authentication.

    [Azure] Log in to Azure, search for **Microsoft Entra ID**. Choose **manage** in the navigation pane and click **App registrations**. On the page that is displayed, specify **Name** and **Supported account types**.
  - You have set the application credentials.

    In the navigation pane, choose **manage** > **Certificates & secrets** > **Client secrets**. Click **New Client secret**, and specify **Description** and **Expires**. Confirm the information and click **Add**.
  - You have configured the API access permission for the application.

    In the navigation pane, choose **manage** > **API permissions**. On the **API permissions** page, click **Add a permission** > **Azure Service Management**, select **user_impersonation**, and click **Add permissions**.

The API permission list is displayed. On the **API permissions** page, click **Grant admin consent for Azure Active Directory**.

- You have added the permissions for accessing the application on the **Subscriptions** page.

  On the **Subscriptions** page, select **Access control (IAM)**. On the access control page, click **Add role assignment**. Select **Reader** and click **Next**. Select **User**, group, or **service principal** and click **Select members**. Search for and select the newly created application to complete the binding.

Synchronizing Resources Based on Cloud Vendors

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the cloud vendor whose resources are to be synchronized.

Huawei Cloud is selected by default.

Step 4 Select the account to which the resources to be synchronized belong.

By default, **My Resources** is selected.

Step 5 Select the resource type to be synchronized.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Click **Synchronize Resource** to synchronize resources.

----End

Synchronizing Resources Based on Accounts

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Multi-cloud Configurations** in the upper right corner.

Step 4 In the access list, select the account whose resources you want to synchronize and click **Synchronize Resource** in the **Operation** column.

The system will synchronize resources under the selected account.

----End

3.3 Connecting to Other Cloud Vendors

Scenarios

COC allows you to configure accounts of other cloud vendors and synchronize their resources. Currently, Alibaba Cloud, AWS, Azure, and Huawei Cloud Stack are supported. If you need to manage resources of other cloud vendors on COC, perform the operations in **Adding an Account of Another Cloud Vendor**.

Precautions

- To use the multi-cloud vendor management capability, upgrade the version first.
- After an account is added, click **Synchronize Resource** to synchronize existing resources of the account.
- If the resources of an existing account have changed, you need to **synchronize the resources** again.

Adding an Account of Another Cloud Vendor

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Multi-cloud Configurations** in the upper right corner.

Step 4 Click the target cloud vendor.

Step 5 Set the information about the new account.

Table 3-1 Parameters for adding an Alibaba Cloud or AWS account

Parameter	Description
Main Account ID	Account ID of the cloud vendor. Enter a master account ID. If you enter a non-master account ID, resources may fail to be synchronized.
Account	Account name of the cloud vendor.
Access Key ID	Access key ID of the cloud vendor. It is a unique access key ID associated with the secret access key.
Secret Access Key	Secret access key of the cloud vendor. Secret access key is used together with an access key ID to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Table 3-2 Parameters for adding an Azure account

Parameter	Description
Azure Tenant ID	Enter the Azure tenant ID. Microsoft Entra ID [formerly known as Azure Active Directory (Azure AD)] is used to uniquely identify your organization's identity authentication and directory service instance in Azure.
Azure Tenant Name	Account name of the cloud vendor.
Application ID	Enter the Azure application ID. An application ID is a unique identifier allocated by an application and is used to identify a specific application during identity authentication and authorization.
Application Secret Value	Enter the application secret value of Azure (added to **Certificates & secrets**). Secret string used by an application to authenticate itself when requesting a token.

Table 3-3 Parameters for adding a Huawei Cloud Stack account

Parameter	Description
Domain name/IP Address	Enter the Huawei Cloud Stack domain name or IP address. Domain names and IP addresses are network identifiers for accessing Huawei Cloud Stack and related resources. They are used to locate and connect to Huawei Cloud Stack service components in the network environment.
Environment Name	Enter the name of the Huawei Cloud Stack environment to be managed.
Account	Enter the Huawei Cloud Stack account name.
Password	Enter the Huawei Cloud Stack account and password.

Step 6 Click **OK**.

The account is created.

----End

Modifying an Account of Another Cloud Vendor

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Multi-cloud Configurations** in the upper right corner.

Step 4 Locate the target account and click **Modify** in the **Operation** column.

Step 5 Modify the account information by referring to the following table.

Table 3-4 Parameters for modifying the Alibaba Cloud or AWS account

Parameter	Description
Account	Account name of the cloud vendor.
Access Key ID	Access key ID of the cloud vendor. It is a unique access key ID associated with the secret access key.
Reuse Secret Access Key	Whether to reuse the secret access key. If you select **Yes**, the latest secret access key is reused. If you select **No**, enter a new secret access key.
Secret Access Key	Set this parameter only when **Reuse Secret Access Key** is set to **Yes**. Secret access key of the cloud vendor. Secret access key is used together with an access key ID to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Table 3-5 Parameters for modifying an Azure account

Parameter	Description
Azure Tenant ID	Enter the Azure tenant ID. Microsoft Entra ID [formerly known as Azure Active Directory (Azure AD)] is used to uniquely identify your organization's identity authentication and directory service instance in Azure.
Account name of the cloud vendor.	Account name of the cloud vendor.
Application ID	Enter the Azure application ID. An application ID is a unique identifier allocated by an application and is used to identify a specific application during identity authentication and authorization.

Parameter	Description
Application Secret Value Reuse	This parameter is mandatory only when **Application Confidential Value Reuse** is set to **Yes**. Enter the application secret value of Azure (added to **Certificates & secrets**). Secret string used by an application to authenticate itself when requesting a token.

Step 6 Click **OK**.

The account is modified.

----End

Deleting an Account of Another Cloud Vendor

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Multi-cloud Configurations** in the upper right corner.

Step 4 Locate the target account and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The account is deleted.

----End

3.4 Managing On-premises IDCs

Scenarios

You can manage both cloud resources and on-premises devices. When you manage your on-premises physical machines, virtual machines, and middleware using Huawei Cloud in a unified manner, such as performing resource statistics and unified resource O&M, you can use the **On-premises IDCs** function.

Constraints and Limitations

To use the IDC resource management capability, upgrade the version first.

Importing On-premises IDCs

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Multi-cloud Configurations** in the upper right corner.

Step 4 Click **On-premises IDCs**.

Step 5 Set parameters on the **Import On-premises IDC** page.

- **Import Type**: Select **Physical machine**, **Virtual machine**, or **Middleware device**.
- **Region**: Select a region from the drop-down list.
- **File to Be Uploaded**: Upload resource information in an Excel file.
  a. Click **Download Template**.
     Download the table template and enter information.
  b. Click to **Add File**.
     Select and upload the completed template.

Table 3-6 Physical machine parameters

Parameter	Description	Constraint
Xrn	Unique ID of the physical machine.	(Mandatory) The value can contain a maximum of 128 characters.
Name	Name of the physical machine.	(Mandatory) The value can contain a maximum of 128 characters.
Serial Number	Serial number of the physical machine.	(Mandatory) The value can contain a maximum of 128 characters.
Private IP	Private IP address of the physical machine.	(Mandatory)
Pm Model	Type of the physical machine.	(Mandatory) The value can contain a maximum of 64 characters.
Manufacturer	Vendor of the physical machine.	(Mandatory) The value can contain a maximum of 64 characters.
OS Type	OS (Linux or Windows).	(Mandatory)
UniAgent Id	Unique ID of UniAgent.	(Optional) The value can contain a maximum of 128 characters.
Description	Description of the physical machine.	(Optional) The value can contain a maximum of 256 characters.

Table 3-7 Virtual machine parameters

Parameter	Description	Constraint
Xrn	Unique ID of the virtual machine.	(Mandatory) The value can contain a maximum of 128 characters.
Name	Name of the virtual machine.	(Mandatory) The value can contain a maximum of 128 characters.
Private IP	Private IP address of the virtual machine.	(Mandatory)
OS Type	OS (Linux or Windows).	(Mandatory)
Ecs Id	Unique ID generated by OpenStack.	(Optional) The value can contain a maximum of 128 characters.
UniAgent Id	Unique ID of UniAgent.	(Optional) The value can contain a maximum of 128 characters.
Description	Description of the virtual machine.	(Optional) The value can contain a maximum of 256 characters.

Table 3-8 Middleware parameters

Parameter	Description	Constraint
Xrn	Unique ID of the middleware.	(Mandatory) The value can contain a maximum of 128 characters.
Name	Middleware name.	(Mandatory) The value can contain a maximum of 128 characters.
Middleware Model	Middleware type, for example, MySQL.	(Mandatory) The value can contain a maximum of 64 characters.
Version	Version	(Optional) The value can contain a maximum of 64 characters.
Port	Port	(Optional) The port number ranges from 0 to 65535.

Parameter	Description	Constraint
Instance Id List	IDs of virtual machines that the middleware is associated with.	(Optional) Use commas (,) to separate multiple values. A maximum of 50 values are supported.
Description	Description of the middleware.	(Optional) The value can contain a maximum of 256 characters.

----End

Modifying On-premises IDCs

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 In the cloud vendor list on the left, select **On-premises IDCs**.

Step 4 Select the resource type to be modified.

Physical machine is selected by default.

Step 5 Click **Modify** in the **Operation** column.

Step 6 Configure the on-premises IDC information.

Table 3-9 Physical machine parameters

Parameter	Description	Example Value
Name	Name of the physical machine.	Test devices
SN	Serial number of the device.	-
Private IP	Private IP address of the physical machine.	192.168.1.1
Type	Type of the physical machine.	Laptop
UniAgent Id	(Optional) Unique ID of UniAgent.	-
Manufacturer	Vendor of the physical machine.	Huawei
OS	OS from the drop-down list.	Linux
Description	(Optional) Description of the device.	-

Table 3-10 Virtual machine parameters

Parameter	Description	Example Value
Name	Name of the virtual machine.	Test devices
Private IP	Private IP address of the virtual machine.	192.168.1.1
OS	OS from the drop-down list.	Linux
UniAgent Id	(Optional) Unique ID of UniAgent.	-
Ecs Id	(Optional) Unique ID generated by OpenStack.	-
Description	(Optional) Description of the device.	-

Table 3-11 Middleware parameters

Parameter	Description	Example Value
Name	Middleware name. This parameter cannot be changed.	Test devices
Type	Middleware type, for example, MySQL. The parameter cannot be modified.	MySQL
Version	Middleware version.	V1.1
Port	Middleware port number.	8000
Description	(Optional) Description of the device.	-
Instance Id List	(Optional) In the resource list, you can select a maximum of 50 virtual machines.	-

Step 7 Click **OK**.

The on-premises IDC is modified.

----End

Deleting On-premises IDCs

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 In the cloud vendor list on the left, select **On-premises IDCs**.

Step 4 Select the resource type to be deleted.

Physical machine is selected by default.

Step 5 Click **Delete** in the **Operation** column.

Step 6 Click **OK**.

The on-premises IDC is deleted.

----End

3.5 Managing Cross-account Resources

Scenarios

Cloud Operations Center provides secure and reliable cross-account data aggregation and resource O&M capabilities. If your account is an enterprise-level account and is an administrator of an organization (set in the organizations cloud service) or a delegated administrator of COC, you can perform unified automatic O&M operations on resources in other accounts in the organization, preventing manpower waste caused by multi-account operations, and reducing risks such as account omission caused by manual operations.

A view consists of a group of filters. You can configure the filter criteria to access desired resources on Huawei Cloud in cross-account scenarios.

Procedure: Set basic view information, add the organization unit filtering scope, and add the resource type filtering scope.

Precautions

- A maximum of 10 views can be created.
- After a view is created, you need to synchronize existing resources in the current view. For details, see **3.2 Synchronizing Resources**.
- If the resources of an existing view have changed, you need to synchronize the resources again. For details, see **3.2 Synchronizing Resources**.

Creating a View

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

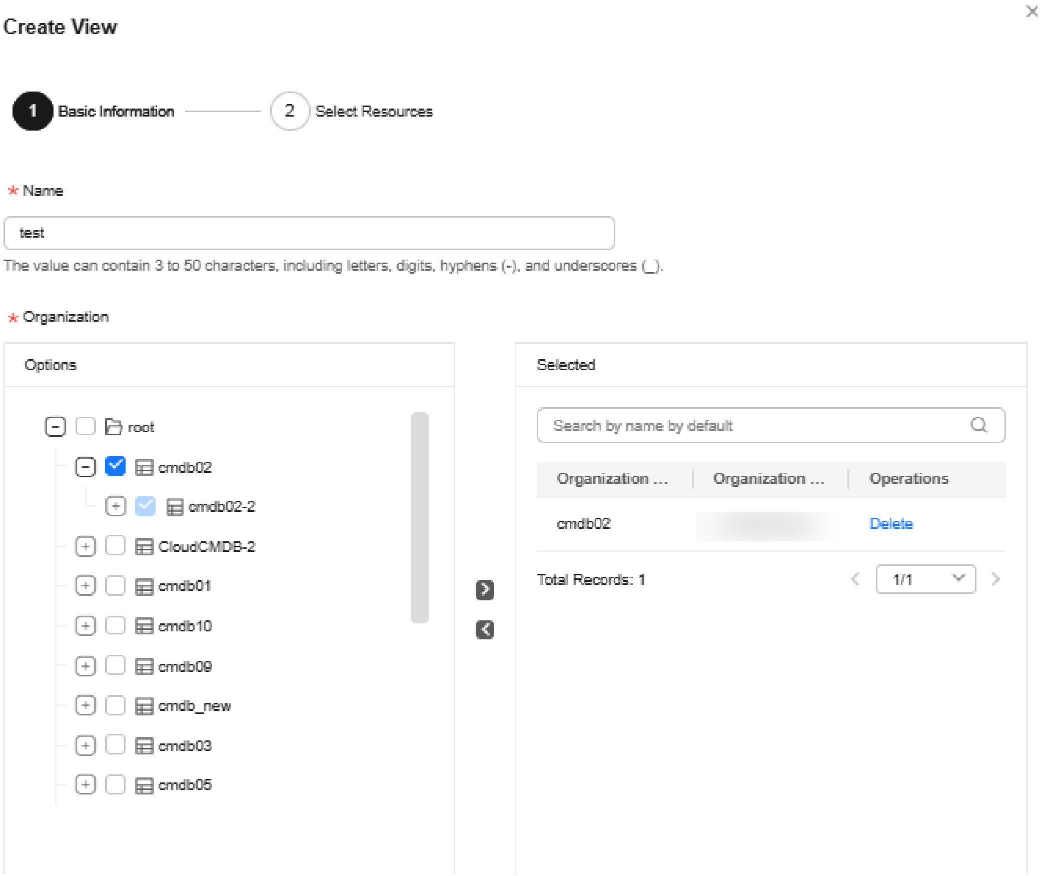
Step 3 Click **Cross-Account Resources** above the filter box.

Step 4 Click **View Management** in the upper right corner of the filter box.

Step 5 On the **View Management** page, click **Create View**.

Step 6 Set basic view information based on **Table 3-12**.

Figure 3-1 Setting basic information



Create View

1 Basic Information — 2 Select Resources

* Name

test

The value can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).

* Organization

Options

- ⊟ □ root
  - ⊟ ☑ cmdb02
    - ⊞ ☑ cmdb02-2
  - ⊞ □ CloudCMDB-2
  - ⊞ □ cmdb01
  - ⊞ □ cmdb10
  - ⊞ □ cmdb09
  - ⊞ □ cmdb_new
  - ⊞ □ cmdb03
  - ⊞ □ cmdb05

Selected

Search by name by default

Organization ...	Organization ...	Operations
cmdb02	[redacted]	Delete

Total Records: 1 ‹ 1/1 ›

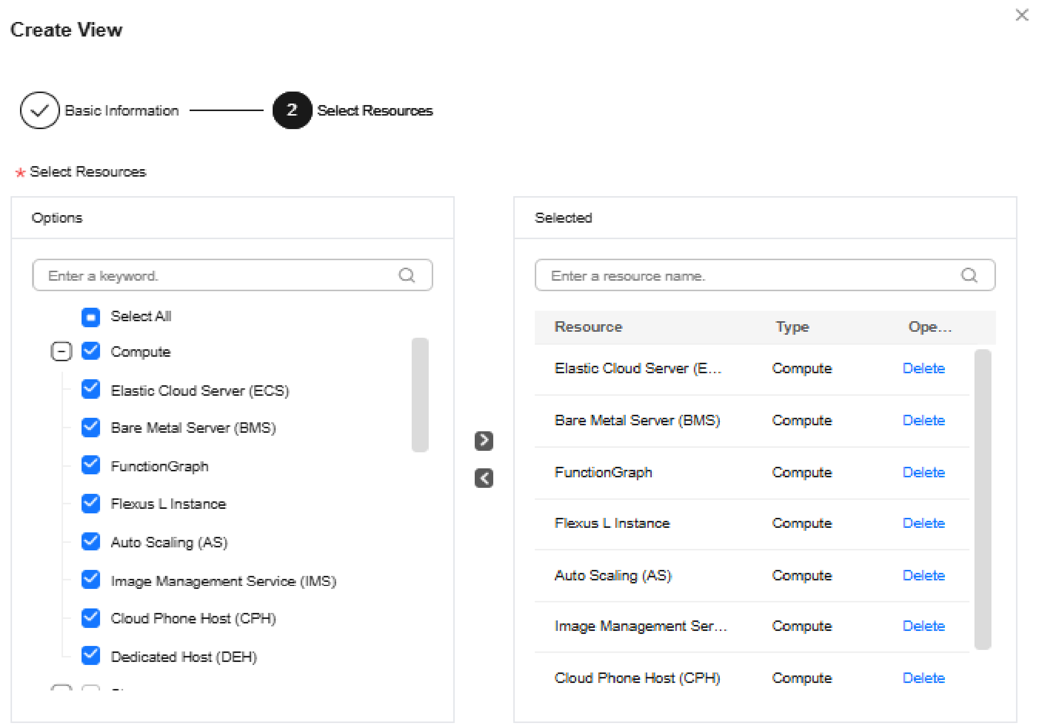
Table 3-12 Parameters for creating a view

Parameter	Description
Name	Customize the view name based on the naming rule. The view name can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).
Select Organization	Select the target organizational units. An OU is a container of accounts. You can group accounts into an OU and apply policies to the OU based on your business requirements.
Select Resource	Select the target resource type.

Step 7 Click **Next**.

Step 8 Select the target resource type.

Figure 3-2 Select Resource



Create View

Basic Information — 2 Select Resources

* Select Resources

Options

Enter a keyword.

- ▣ Select All
- ⊟ ☑ Compute
  - ☑ Elastic Cloud Server (ECS)
  - ☑ Bare Metal Server (BMS)
  - ☑ FunctionGraph
  - ☑ Flexus L Instance
  - ☑ Auto Scaling (AS)
  - ☑ Image Management Service (IMS)
  - ☑ Cloud Phone Host (CPH)
  - ☑ Dedicated Host (DEH)

Selected

Enter a resource name.

Resource	Type	Ope...
Elastic Cloud Server (E...	Compute	Delete
Bare Metal Server (BMS)	Compute	Delete
FunctionGraph	Compute	Delete
Flexus L Instance	Compute	Delete
Auto Scaling (AS)	Compute	Delete
Image Management Ser...	Compute	Delete
Cloud Phone Host (CPH)	Compute	Delete

Step 9 Click **OK**.

The view is created.

----End

Modifying a View

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Cross-Account Resources** above the filter box.

Step 4 Click **View Management** in the upper right corner of the filter box.

Step 5 Click **Modify** in the **Operation** column.

Step 6 Modify the view by referring to **Table 3-13**.

Table 3-13 Parameters for modifying a view

Parameter	Description
Name	Customize the view name based on the naming rule.
Select Organization	Select the target organizational units. An OU is a container of accounts. You can group accounts into an OU and apply policies to the OU based on your business requirements.

Parameter	Description
Select Resource	Select the target resource type.

Step 7 Confirm the modification and click **OK**.

The view is modified.

----End

Deleting a View

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Cross-Account Resources** above the filter box.

Step 4 Click **View Management** in the upper right corner of the filter box.

Step 5 Click **Delete** in the **Operation** column.

Step 6 In the dialog box that is displayed, click **OK**.

The view is deleted.

----End

3.6 Configuring a UniAgent

Scenarios

A Unified Data Collection Agent (UniAgent) mainly serves as the foundation for the cloud service O&M system, providing capabilities for middleware metric collection, custom metric collection, and script delivery and execution channels. This chapter introduces the installation, reinstallation, upgrade, uninstallation, and status synchronization operations of UniAgent. After the installation is complete, you can perform automated O&M on resources using a UniAgent.

Precautions

- Currently, you can only perform operations on UniAgent for ECSs.
- You can install UniAgent tools on a maximum of 100 ECSs in batches.
- The OS usage has restrictions.

Table 3-14 Linux operating systems and versions supported by a UniAgent

OS	Version	
Euler OS	1.1 64bit	2.0 64bit

OS	Version				
CentOS	7.1 64bit	7.2 64bit	7.3 64bit	7.4 64bit	7.5 64bit
	7.6 64bit	7.7 64bit	7.8 64bit	7.9 64bit	8.0 64bit
Ubuntu	16.04 server 64bit	18.04 server 64bit	20.04 server 64bit	22.04 server 64bit	

NOTE

- For Linux x86_64 servers, all the listed OSs and versions are supported.
- For Linux Arm hosts, CentOS 7.4/7.5/7.6, EulerOS 2.0, and Ubuntu 18.04 are supported.

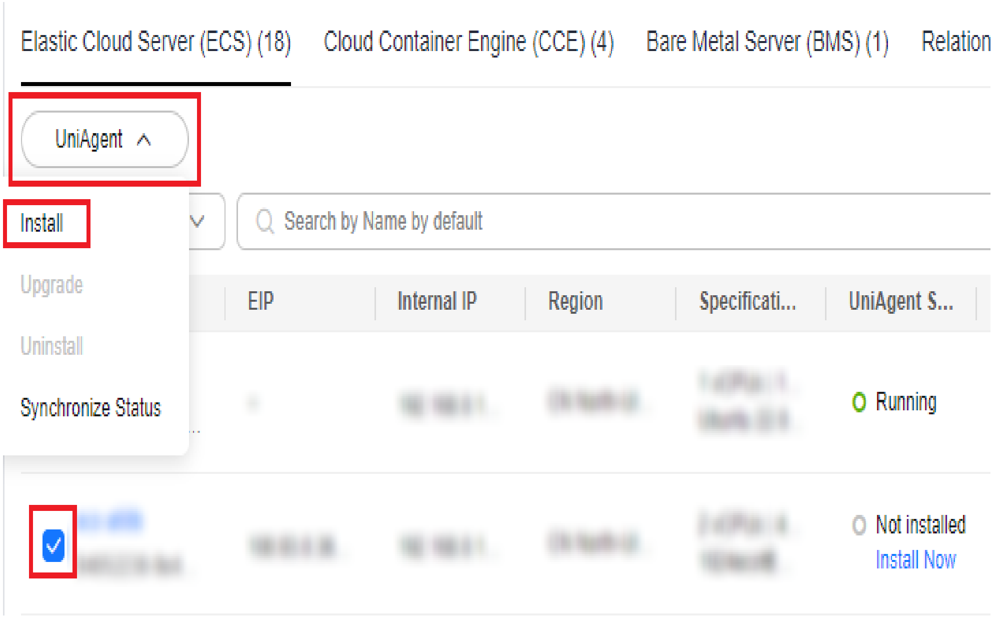
Installing a UniAgent

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 On the **Resources** page, select the target instances and choose **UniAgent** > **Install**.

Figure 3-3 Installing a UniAgent



NOTE

When UniAgent is installed in a single VPC for the first time, you need to manually install the UniAgent and set a host with UniAgent installed as the installation host. For details, see **How Do I Install UniAgent for the First Time?**

Step 4 Set the parameters for installing UniAgent.

Table 3-15 Parameters for installing UniAgent

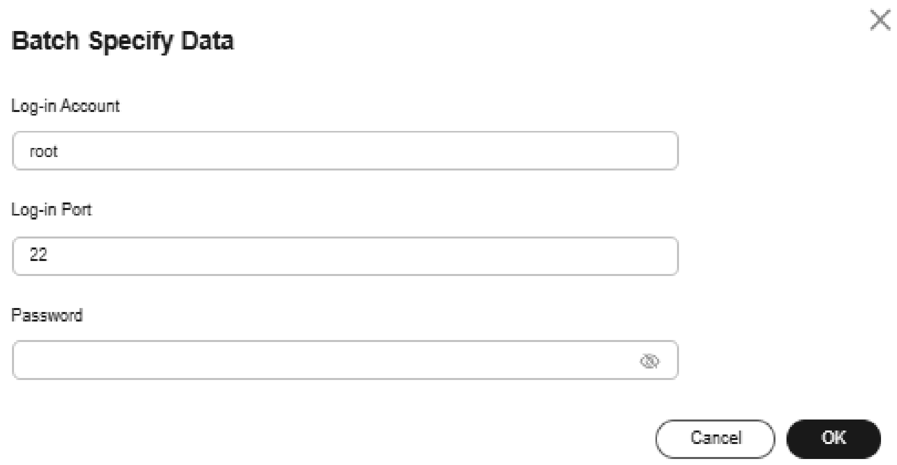
Parameter	Description
UniAgent Version	Select a UniAgent version from the drop-down list.
Host Access Mode	There are three access modes: **Direct access (private network)**, **Direct access (public network)**, and **Proxy access**. ● **Direct access (intranet)**: intended for Huawei cloud hosts. ● **Direct access (public network)**: intended for non-Huawei Cloud hosts. ● **Proxy access**: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy.
Proxy Area	When **Proxy access** is selected, you need to select a proxy area. An agent area is used to manage agents by category. A proxy is a Huawei Cloud ECS purchased and configured on Huawei Cloud to implement network communication between multiple clouds.
Installation Host	Select an installation host from the drop-down list. Select a host where the UniAgent has been installed. The installation host helps install the UniAgent on other hosts in the same VPC.

Parameter	Description
Hosts About to Accommodate UniAgent	Enter detailed information about the host where the UniAgent is to be installed. ● **Host Name**: host name. ● **Host IP Address**: IP address of a host. ● **OS**: operating system of the host, which can be **Linux** or **Windows** ● **Login Account**: account for logging in to the host. For the Linux OS, using the **root** account is recommended so that you have sufficient read and write permissions. ● **Login Port**: port for accessing the host. ● **Authentication Mode**: Currently, only password-based authentication is supported. ● **Password**: password for logging in to the host. ● **O&M Test Result**: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal. ● **Operation**: – Test Network – Delete **NOTE** The Windows OS does not support connection tests.

Step 5 (Optional) Perform batch operations.

- **Test Connection**: Select multiple hosts to be installed and click **Test Connection** to perform O&M connection tests on the selected hosts in batches.
- **Batch Specify Data**
  - Manual batch parameter settings: Login accounts, login ports, and passwords can be filled in batches.

Figure 3-4 Manual input



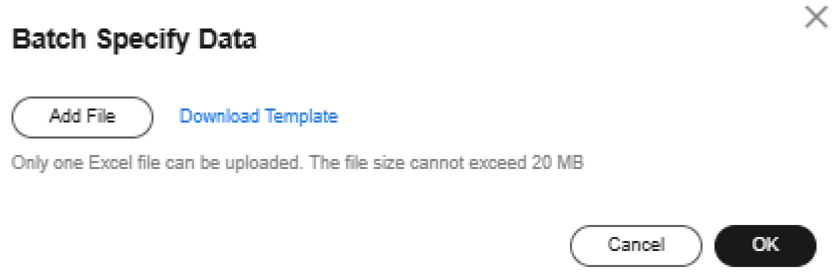
Log-in Account: root

Log-in Port: 22

Password:

- Importing data in batches using an Excel file: You can click **Download Template**, manually enter data based on the template, and import data in batches using an Excel file.

Figure 3-5 Importing data in batches



Only one Excel file can be uploaded. The file size cannot exceed 20 MB

- Batch export: Export all data of the hosts to be installed in batches.

Step 6 Click **OK**.

Wait until the installation is complete.

----End

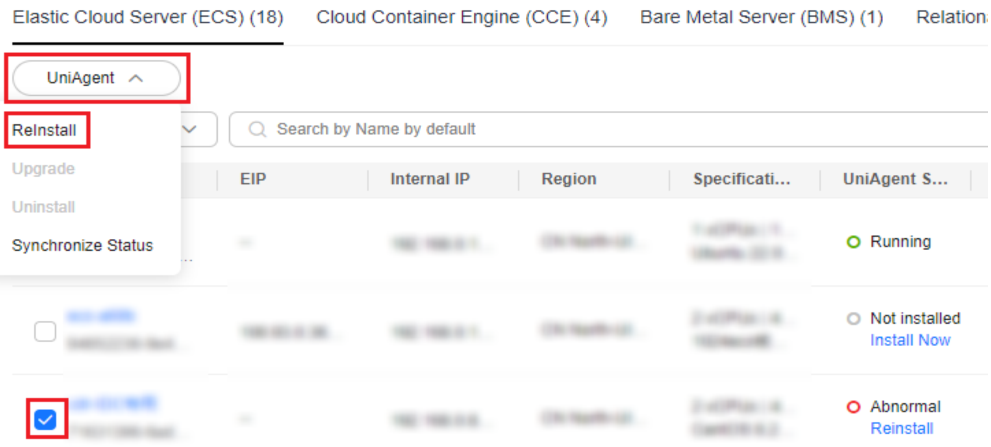
Reinstalling the UniAgent

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the instances with the UniAgent status of **Abnormal**, **Uninstalled**, or **Installation failed**, then choose **UniAgent** > **Reinstall** or click reinstall in the **UniAgent Status** column.

Figure 3-6 Reinstalling the UniAgent



Step 4 The parameter information is essentially the same as that when the UniAgent is installed. For details, see **Step 4**.

Step 5 Click **OK**.

Wait until the reinstallation is complete.

----End

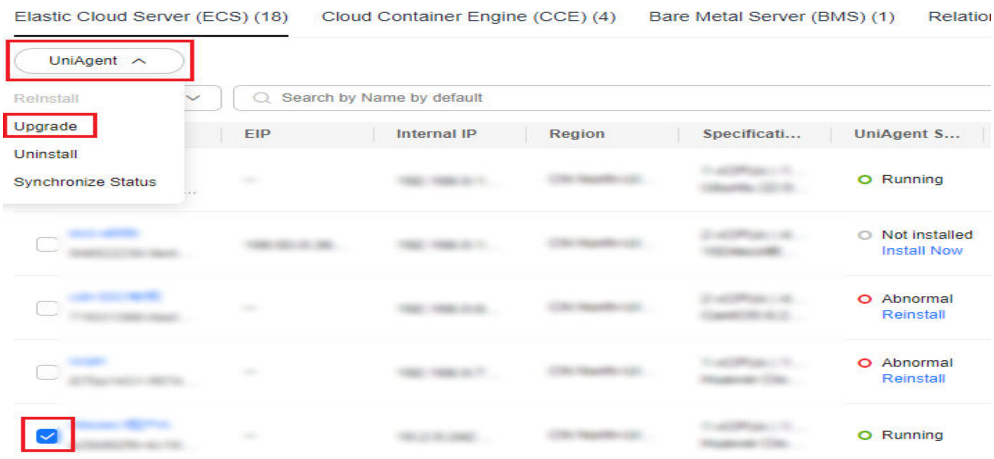
Upgrading a UniAgent

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the instances where UniAgent has been installed and choose **UniAgent** > **Upgrade**.

Figure 3-7 Upgrading a UniAgent



Step 4 Set parameters for upgrading UniAgent.

Table 3-16 Parameters for upgrading the UniAgent

Parameter	Description
UniAgent Version	(Mandatory) Version of a UniAgent.

Step 5 Click **OK**.

Wait until the upgrade is completed.

----End

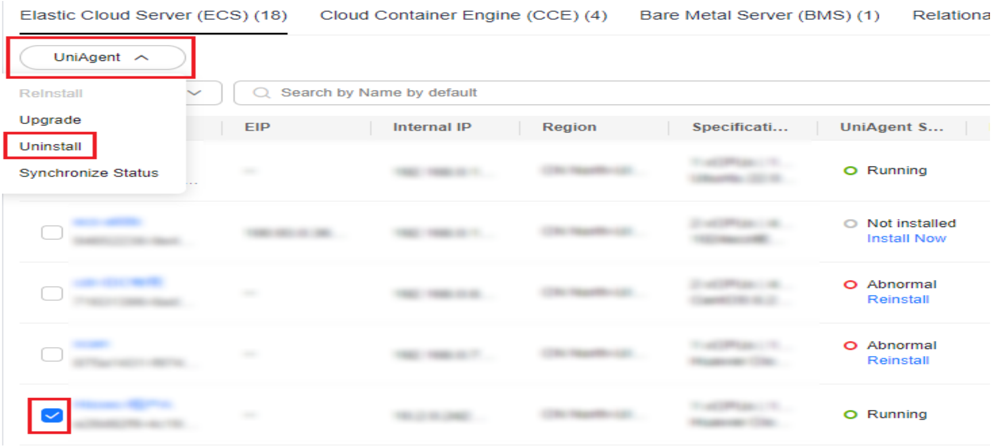
Uninstalling a UniAgent

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the instances where UniAgent has been installed and choose **UniAgent** > **Uninstall**.

Figure 3-8 Uninstalling a UniAgent



Step 4 Click **OK**.

Wait until the uninstallation is complete.

----End

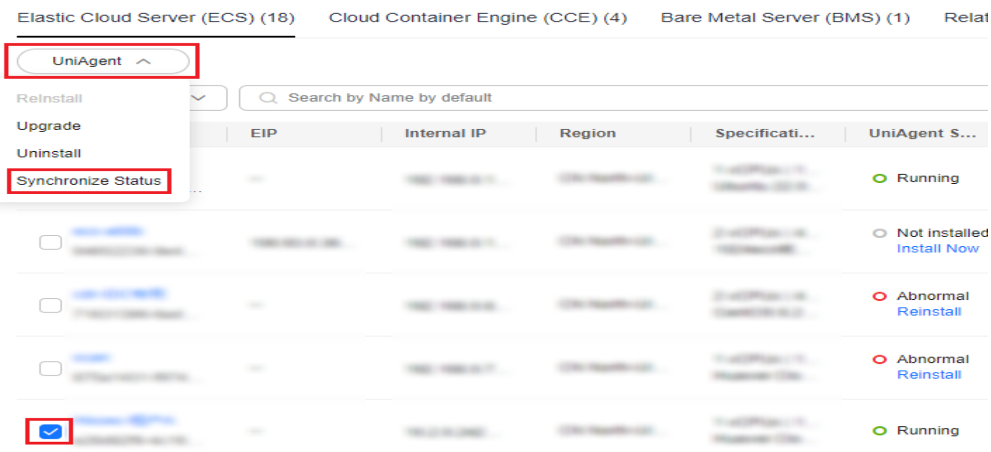
Synchronizing Statuses

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the instances where UniAgent is installed and choose **UniAgent** > **Synchronize Status**.

Figure 3-9 Status synchronization



----End

3.7 Viewing Resource Details on the Resource Management Page

Scenarios

Resource List only displays some resource attributes. The following example shows how to query more details about a resource.

Precautions

- Currently, Alibaba Cloud resource details cannot be viewed.
- For on-premises IDCs, only VM resource details can be viewed.

Viewing Resource Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the cloud vendor whose resources are to be viewed.

Huawei Cloud is selected by default.

Step 4 Select the resource type to be synchronized.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 5 Click the target DB instance to go to the DB instance details page.

You can view the resource name, ID, enterprise project, region, cloud server information, application, group, and component. In addition, you can switch to the corresponding group page.

Step 6 Click **View Resource Details**.

The resource service details page is displayed.

----End

3.8 Viewing Resource Topologies

Scenarios

The resource topology is presented in graphs. Nodes represent resources, and lines represent the resource relationships. It displays the relationships between resources more intuitively, facilitating the use, monitoring, and management of resources.

Precautions

The topology of Huawei Cloud resources can be viewed.

Currently, only the topologies of instances of Elastic Cloud Servers (ECS), MapReduce Services (MRS), Bare Metal Server (BMS), and Cloud Container Engine (CCE) can be viewed.

Viewing Resource Topologies

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Select the cloud vendor whose resources are to be viewed.

Huawei Cloud is selected by default.

Step 4 Select the resource type to be synchronized.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 5 Select the target instance and click **View Topology** in the **Operation** column.

----End

3.9 Managing Tags

Scenarios

Tag Management Service (TMS) enables you to use tags on the management console to manage resources. TMS works with other cloud services to enable tag management. TMS manages tags globally, and other cloud services use these tags to manage their specific tasks. If you need to manage a lot of cloud resources, use TMS.

- You are advised to set pre-defined tags on the TMS console.
- A tag consists of a key and value. You can add only one value for each key.
- Each instance can have up to 10 tags.

Modifying a Tag

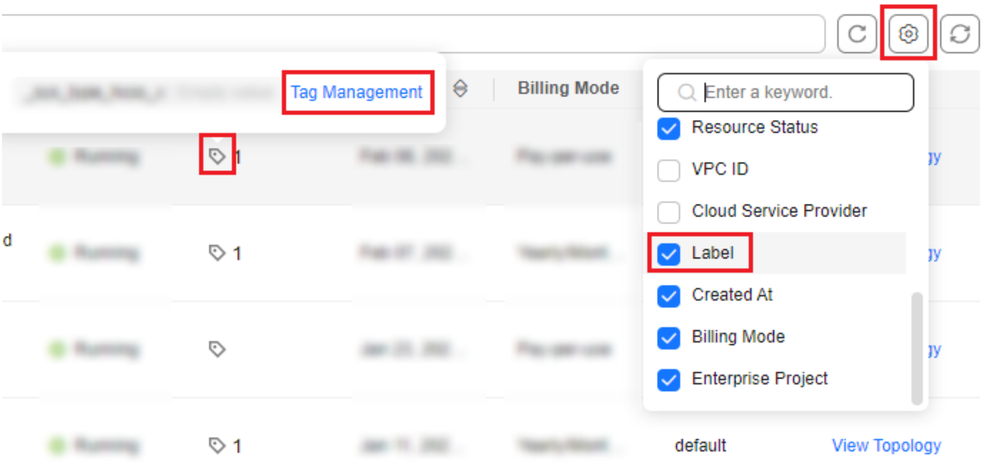
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click ⚙ on the right of the filter column and select **Tag**.

Step 4 Select the target instance, click 🏷 in the label column, and then click **Tag Management**.

Figure 3-10 Managing tags



Step 5 Click **Add Tag**.

- When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user.
- The tag key cannot start or end with a space, or start with _sys_. It can contain letters, digits, spaces, and the following special characters: _.:=+-@. A maximum of 128 characters are allowed.
- The tag value cannot start or end with a space. It can contain letters, digits, spaces, and the following special characters: _.:=+-@. A maximum of 256 characters are allowed.

You can modify an existing tag. Click the key or value of a tag and enter a new key or value.

Step 6 Click **OK**.

The tag is modified.

----End

Deleting a Tag

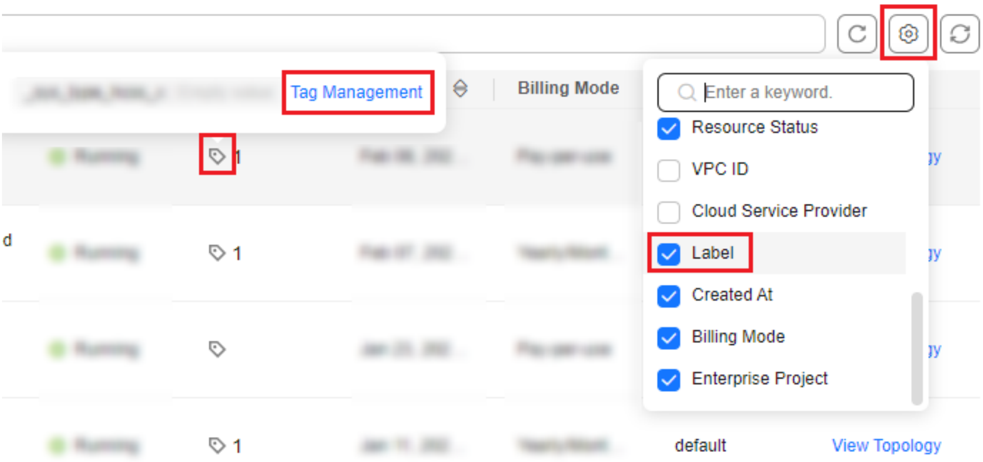
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click ⚙ on the right of the filter column and select **Tag**.

Step 4 Select the target instance, click 🏷 in the label column, and then click **Tag Management**.

Figure 3-11 Managing tags



☑ Resource Status
□ VPC ID
□ Cloud Service Provider
☑ Label
☑ Created At
☑ Billing Mode
☑ Enterprise Project

Step 5 Select the tag to be deleted and click 🗑.

Step 6 Click **OK**.

The tag is deleted.

----End

3.10 Adding an Enterprise Project to Favorites

Scenarios

Resources enables you to favorite enterprise projects and filter resources by enterprise project. If there are a large number of resources, you can select a favorited enterprise project to quickly filter resources.

Adding an Enterprise Project to Favorites

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Favorite Configuration** in the upper right corner.

Step 4 Select the enterprise projects you want to add to favorites.

Step 5 Click **OK**.

Step 6 In the displayed dialog box, confirm the operation and click **OK**.

The enterprise project is added to favorites.

----End

Viewing the Resources of Enterprise Projects in Favorites

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click the drop-down list on the left of the filter box and select **Favorited enterprise projects**.

----End

4 Application Management

4.1 Overview

You can use the application management function of COC to manage resources by group and manage the relationship between cloud service objects and applications. The management scope includes core resources of Huawei Cloud, other clouds (currently, Alibaba Cloud, AWS, and Azure are supported), and on-premises IDC resources, provides unified and reliable resource group information for functions such as chaos drills, change management, and account management.

Applications are classified into lightweight and large-scale types based on their complexity.

- **Lightweight**: Lightweight applications feature fewer layers and a simpler structure.

  The structure of a lightweight application: Applications > Components > Groups > Resources.

- **Large-scale**: Large-scale applications have complex structures.

  The structure of a large-scale application: applications > sub-applications (supporting multi-layer) > components > groups > resources.

Concepts

Applications: Independently running software or an independently running organization or department

Sub-application: Software that runs independently under an organization or department, or an independent functional module.

Component: basic unit of a functional module, such as the logging, authentication, frontend, and backend module

Group: A group is the minimum unit that can be associated with resources. Resources used by a component are logically separated, for example, different environments (test, grayscale, and formal environments) of a component.

Intelligent resource association: Resources bound to groups are automatically updated based on enterprise projects and tags (optional).

4.2 Creating an Application

Scenarios

If your organization is complex and you need to divide resources by organization for centralized and refined management, you can create applications to logically classify components. After an application is created, you can add sub-applications and new components to the application, making service module management clear and intuitive.

Constraints and Limitations

- If the large-scale application structure is selected, you can configure sub-applications.
- Only one type of node (sub-application/component) is allowed at the same level under an application or sub-application.
- A maximum of 50 components and 50 groups can be configured for an application.

Creating an Application

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications**.

Step 4 Click **Create Application**.

Step 5 On the application creation page, you can create an application based on your service scenario.

COC provides two creation modes: advanced creation and quick creation.

----End

Setting Advanced Creation

If the resource structure is complex, for example, an application has multiple components, and each component involves resources in multiple regions, you can use the advanced creation method.

Step 1 On the application creation page, click the **Advanced Creation** tab.

Step 2 Select an application structure type based on the complexity of the application structure.

- **Lightweight**: Lightweight applications feature fewer layers and a simpler structure. Application layer structure: Applications > Components > Groups > Resources

- **Large-scale**: Large-scale applications have complex structures. Application layer structure: Applications > Sub-applications (multi-layer) > Components > Groups > Resources.

Step 3 Set the application structure by referring to **Table 4-1**.

NOTE

After setting all mandatory fields of the current level, click **OK** to go to the next level. After all mandatory fields of all levels are specified, click **OK** to complete application creation.

Table 4-1 Parameters for creating an application

Parameter	Description	Example Value
Application	Customize an application name based on the naming rule. The application name can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).	Test_application
Description	(Optional) Description of the application.	-
Subapplication Name	This parameter is required only when the large-scale application type is selected. Customize the sub-application name based on the naming rule. The sub-application name can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).	Test_Sub-application
Description	(Optional) Description of a sub-application.	-
Component	Customize the component name based on the naming rule. The component name can contain 3 to 60 characters, including letters, digits, hyphens (-), and underscores (_).	Test-component
Group	Customize a group name based on the naming rule. The group name can contain 3 to 60 characters, including letters, digits, hyphens (-), and underscores (_).	Test-group
Available Cloud Service Providers	Select the cloud service provider to which the target instance belongs.	Huawei Cloud

Parameter	Description	Example Value
Resource Association Method	Select a resource association mode. ● **Manual association**: You can manually associate resources with the group you created for unified management. ● **Automatic association**: You can add all resources with the same tag in an enterprise project to a resource group.	Manual association
Region	Select a region from the drop-down list.	-
Enterprise Project	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Select an enterprise project from the drop-down list.	-
Tag Key	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Enter the tag key of the target instance.	testKey
Tag Value	This parameter is required only when **Resource Association Method** is set to **Automatic association**. (Optional) Enter the tag value of the target instance.	testValue
Associate Resource with APM Environment	(Optional) Configure the application, component, and environment of the APM service corresponding to the group. APM service performance information can be obtained through this field during fault diagnosis.	-

Step 4 Click **Create** to complete application creation.

----End

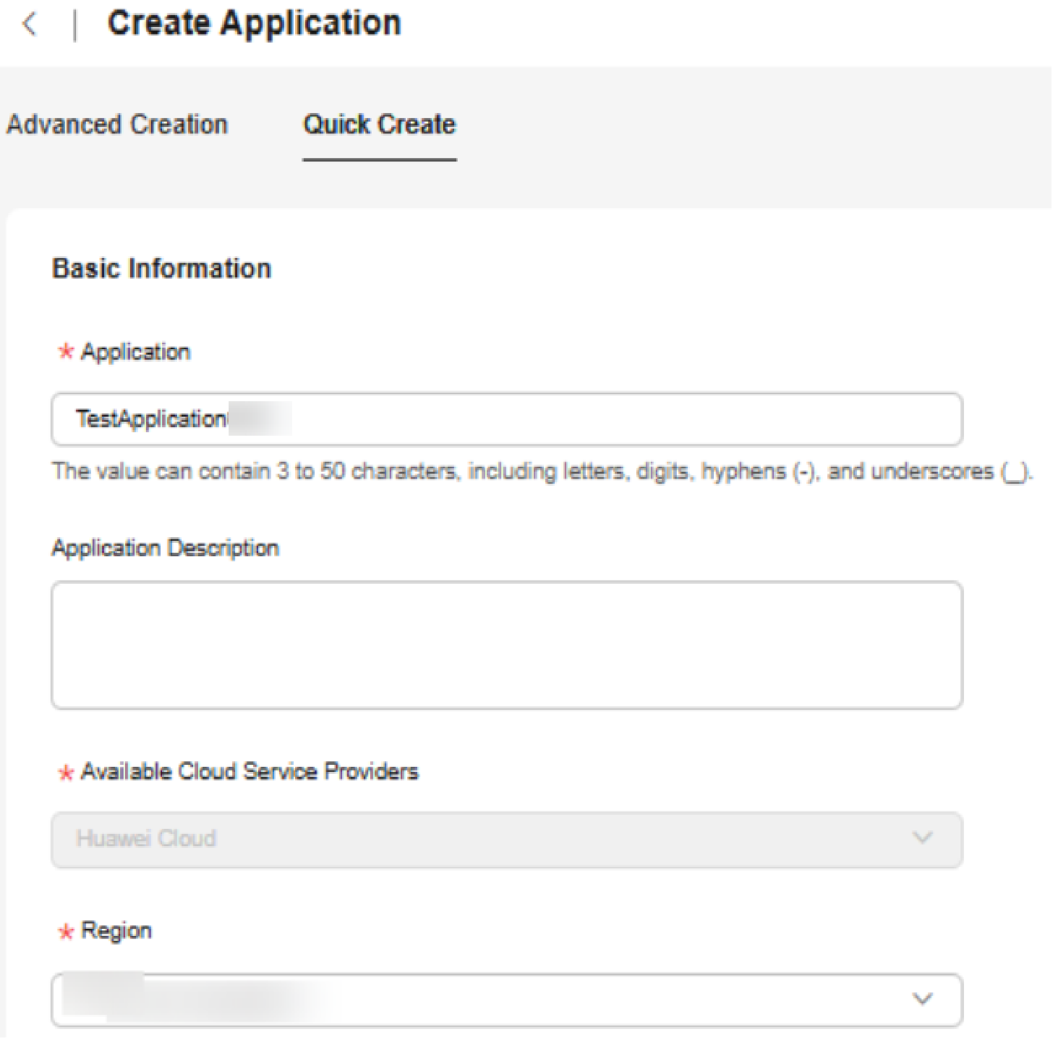
Setting Quick Creation

If the resource structure is simple, for example, an application requires only Huawei Cloud resources and the resources need to be associated with only one group, you can use the quick creation function.

Step 1 On the application creation page, click the **Quick Creation** tab.

Step 2 Set basic application information.

Figure 4-1 Basic information



Create Application

Advanced Creation

Quick Create

Basic Information

* Application

TestApplication

The value can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).

Application Description

* Available Cloud Service Providers

Huawei Cloud

* Region

Table 4-2 Basic information parameters

Parameter	Description	Example Value
Application	Customize an application name based on the naming rule. The name can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).	Test_application
Application Description	(Optional) Description of the application scenario.	-
Available Cloud Service Providers	The default value is **Huawei Cloud** and cannot be changed.	Huawei Cloud
Region	Select a region from the drop-down list.	CN North-Beijing4

Step 3 Add resources by referring to **Table 4-3**.

Table 4-3 Parameters for adding a resource

Parameter	Description	Example Value
Resource Association Method	Select a resource association mode. - **Manual association**: Click **Select Resource** to manually associate the resource data with the group for management. - **Automatic association**: You can add all resources with the same tag in an enterprise project to a resource group.	Automatic association
Enterprise Project	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Select an enterprise project from the drop-down list.	default
Tag Key	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Enter the tag key of the target instance.	testKey
Tag Value	This parameter is required only when **Resource Association Method** is set to **Automatic association**. (Optional) Enter the tag value of the target instance.	testValue

Step 4 Click **OK**.

The system automatically generates components and groups named {*Application-name*}**-component** and {*Application name*}**-group**, respectively.

----End

Creating a Sub-application

You can create sub-applications under an application only when you select the **Large-scale** application structure type during application creation.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications**.

Step 4 In the navigation pane on the left, select the application for which you want to create a sub-application for and click +.

Step 5 Set parameters for creating a sub-application.

Table 4-4 Parameters for creating a sub-application

Parameter	**Description**	**Example Value**
Subapplication Name	Customize the sub-application name based on the naming rule.	Test_Sub-application
Description	(Optional) Description of a sub-application.	-

Step 6 Click **OK**.

----End

4.3 Modifying an Application

Scenarios

After an application is created, you can modify its name or description by performing the following operations.

Modifying an Application

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the application to be modified and click ✎.

Step 5 Set parameters for modifying an application.

Table 4-5 Parameters for modifying an application

Parameter	**Description**	**Example Value**
Application	Customize an application name based on the naming rule.	**Test Application**
Description	(Optional) Description of the application.	-

Step 6 Click **OK**.

The application is modified.

----End

Modifying a Sub-application

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the sub-application to be modified and click ✎.

Step 5 Set parameters for modifying a sub-application.

Table 4-6 Parameters for modifying an application

Parameter	Description	Example Value
Subapplication Name	Customize the sub-application name based on the naming rule.	Test sub-application
Description	(Optional) Description of a sub-application.	-

Step 6 Click **OK**.

The sub-application is modified.

----End

4.4 Deleting an Application

Scenarios

This section describes how to delete an application or sub-application.

Precautions

When an application or sub-application contains groups, components, or sub-applications, it cannot be deleted. You can delete a node only when the node does not contain sub-nodes.

Deleting an Application

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the application to be deleted and click 🗑.

Step 5 Click **OK**.

The application is deleted.

----End

Deleting a Sub-application

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select the sub-application to be deleted, and click ⊗.

Step 5 Click **OK**.

The sub-application is deleted.

----End

4.5 Managing Application Topologies

Scenarios

The application topology is displayed in graphs. Nodes indicate the application hierarchy and resources, and lines indicate the relationships between nodes. It displays the application hierarchy and relationships between resources more intuitively, facilitating resource usage, monitoring, and management.

Precautions

Only the connections between components can be modified in the topology.

Modifying a topology does not affect the layers and functions of applications and components.

Viewing and Modifying a Topology

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

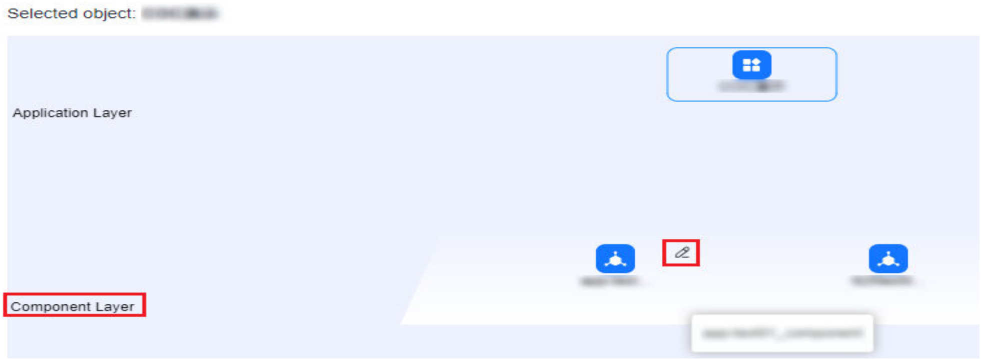
Step 4 In the application list on the left, select the application you want to view and modify, and click ⤧.

Step 5 Click ✎.

Step 6 Click Custom Modification in the upper right corner.

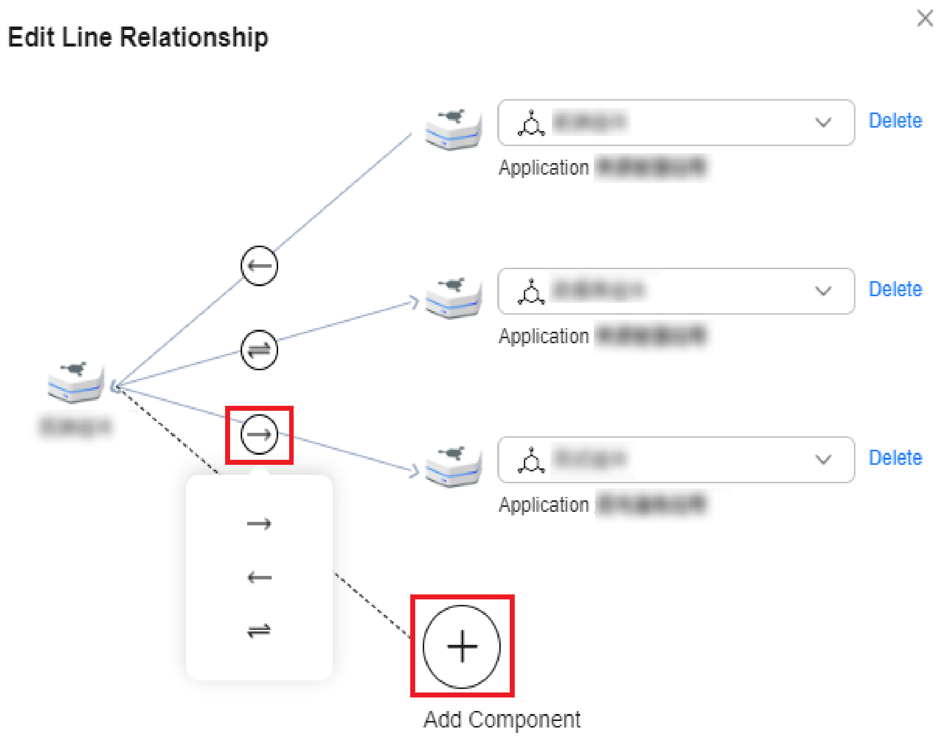
Step 7 Select the component to be modified and click ✎.

Figure 4-2 Modifying a component



Step 8 Set **Edit Line Relationship**.

Figure 4-3 Modifying line relationship



Step 9 Click **OK**.

Step 10 Click **OK**.

The topology is modified.

----End

4.6 Creating a Component

Scenarios

After creating an application or a sub-application by referring to **Creating an Application** or **Creating a Sub-application** respectively, perform the operations in this section to create a component under the application or sub-application.

Creating a Component

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the application for which you want to create a component, and click +.

Step 5 Set parameters for creating a component.

Table 4-7 Parameters for creating a component

Parameter	Description	Example Value
Component	Customize the component name based on the naming rule.	Test Component

Step 6 Click **OK**.

The component is created.

----End

4.7 Modifying a Component

Scenarios

After a component is created, you can modify its name by performing the following actions.

Modifying a Component

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select the component to be modified, and click ✎.

Step 5 Set parameters for modifying a component.

Table 4-8 Parameters for modifying a component

Parameter	Description	Example Value
Component	Customize the component name based on the naming rule.	Test Component

Step 6 Click **OK**.

The component is modified.

----End

4.8 Deleting a Component

Scenarios

This section describes how to delete a component.

Precautions

When a component contains groups, it cannot be deleted. You can delete a node only when the node does not contain sub-nodes.

Deleting a Component

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select the component to be deleted, and click 🗑.

Step 5 Click **OK**.

The component is deleted.

----End

4.9 Creating a Group

Scenarios

After **creating a component**, you can perform the following operations to create a group under the component.

Creating a Group

Step 1 Log in to **COC**.

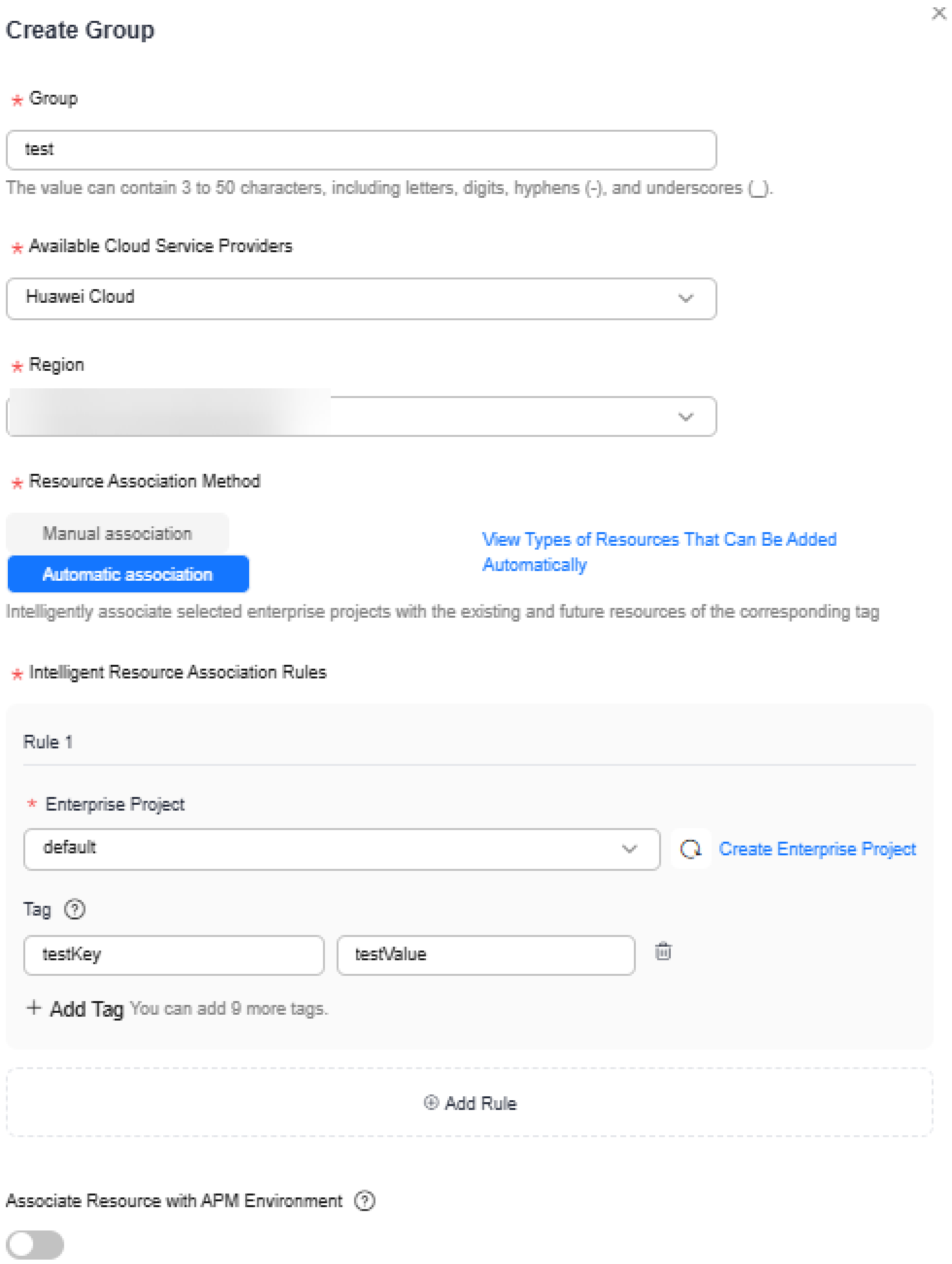
Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the target application, select the target component, and click +.

Step 5 Set parameters for creating a group.

Figure 4-4 Creating a group



Create Group

* Group

test

The value can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).

* Available Cloud Service Providers

Huawei Cloud

* Region

* Resource Association Method

Manual association | Automatic association

View Types of Resources That Can Be Added Automatically

Intelligently associate selected enterprise projects with the existing and future resources of the corresponding tag

* Intelligent Resource Association Rules

Rule 1

* Enterprise Project

default

Create Enterprise Project

Tag

testKey testValue

+ Add Tag You can add 9 more tags.

Add Rule

Associate Resource with APM Environment

Table 4-9 Parameters for creating a group

Parameter	Description	Example Value
Group	Customize a group name based on the naming rule. The value can contain 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_).	Test Group
Available Cloud Service Providers	Select the cloud service provider to which the target instance belongs.	Huawei Cloud
Account which the resource belongs to	This parameter is mandatory only when **Available Cloud Service Providers** is set to **Cross-Account Resources**.	-
Resource Association Method	Select a resource association mode. ● **Manual association**: You can manually associate resources with the group you created for unified management. ● **Automatic association**: You can add all resources with the same tag in an enterprise project to a resource group.	Automatic association
Region	Select a region from the drop-down list.	-
Enterprise Project	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Select an enterprise project from the drop-down list.	default
Tag	This parameter is required only when **Resource Association Method** is set to **Automatic association**. In the enterprise project, only resources that match all the configured tags will be automatically allocated to the application group. ● Tag key: Enter the tag key of the target instance. ● Tag value: Enter the tag value of the target instance.	● Tag key: testKey ● Tag value: testValue

Parameter	Description	Example Value
Associate Resource with APM Environment	(Optional) Configure the application, component, and environment of the APM service corresponding to the group. APM service performance information can be obtained through this field during fault diagnosis.	-

Step 6 Click **OK**.

The group is created.

----End

4.10 Modifying a Group

Scenarios

After a group is created, you can modify its parameters by performing the following operations.

Modifying a Group

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the target application, select the target group, and click ✎.

Step 5 Set parameters for modifying a group.

Table 4-10 Parameters for modifying a group

Parameter	Description	Example Value
Group	Customize a group name based on the naming rule.	Test Group

Parameter	Description	Example Value
Resource Association Method	Select a resource association mode. ● **Manual association**: You can manually associate resources with the group you created for unified management. ● **Automatic association**: You can add all resources with the same tag in an enterprise project to a resource group.	Manual association
Region	Select a region from the drop-down list.	-
Enterprise Project	This parameter is required only when **Resource Association Method** is set to **Automatic association**. Select an enterprise project from the drop-down list. If no enterprise project is available, click **Create Enterprise Project** to create one.	default
Tag	This parameter is required only when **Resource Association Method** is set to **Automatic association**. In the enterprise project, only resources that match all the configured tags will be automatically allocated to the application group. ● Tag key: Enter the tag key of the target instance. ● Tag value: Enter the tag value of the target instance.	● Tag key: testKey ● Tag value: testValue
Associate Resource with APM Environment	(Optional) Configure the application, component, and environment of the APM service corresponding to the group. APM service performance information can be obtained through this field during fault diagnosis.	-

Step 6 Click **OK**.

The group is modified.

----End

4.11 Deleting a Group

Scenarios

After a group is created, you can delete it by following the operations in this section.

Deleting a Group

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the target application, select the target group, and click 🗑.

Step 5 Click **OK**.

The group is deleted.

----End

4.12 Manually Associating Resources with an Application

Scenarios

After creating an environment for a group, you can bind resources to this environment. Then, you can monitor the resource usage in real time through application monitoring.

Constraints and Limitations

In Elastic Load Balance (ELB), a listener is automatically associated with a load balancer. Manual association is not supported.

Manually Associating Resources with an Application

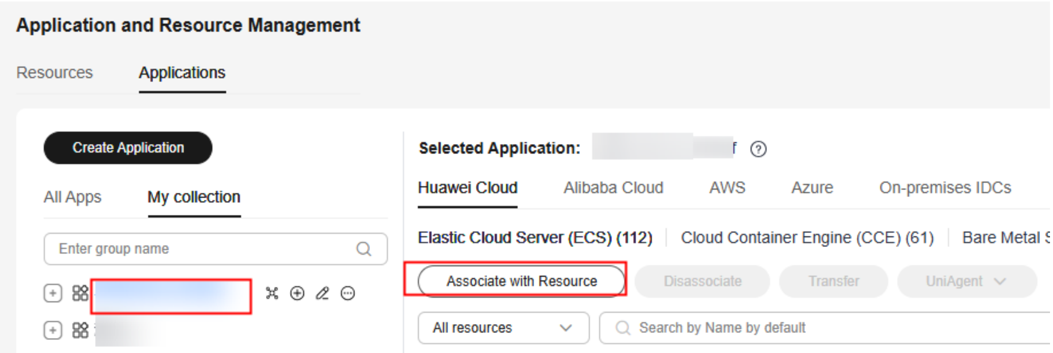
Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the application to be associated with resources and click **Associate with Resource**.

Figure 4-5 Manually associating resources with an application



Step 5 Set parameters for associating resources with an application.

Table 4-11 Parameters for associating resources with an application

Parameter	Description	Example Value
Select a group under the application	Select an application, component, and group from the drop-down list.	Test application/ test component/ test group
Resource Type	Select a cloud vendor and resource type from the drop-down lists.	Huawei Cloud/ Elastic Cloud Server (ECS)/ Cloud Server
Resource List	Please select the resources that need to be associated.	-

Step 6 Click **OK**.

Resources are associated with the group.

----End

4.13 Automatically Associating Resources with an Application

Scenarios

You can associate resource instances with the same tag in an enterprise project with the same resource group for management.

Precautions

- Automatic association is supported for an application only when resources are automatically associated with the corresponding group. For details about how to change the resource association method, see **Modifying a Group**.
- The **Automatic Resource Association** button takes effect only after you click the corresponding group.
- After automatic resource association is triggered, ait for the association task to be executed. The association duration depends on the total number of resources to be associated.

Automatically Associating an Application with Resources

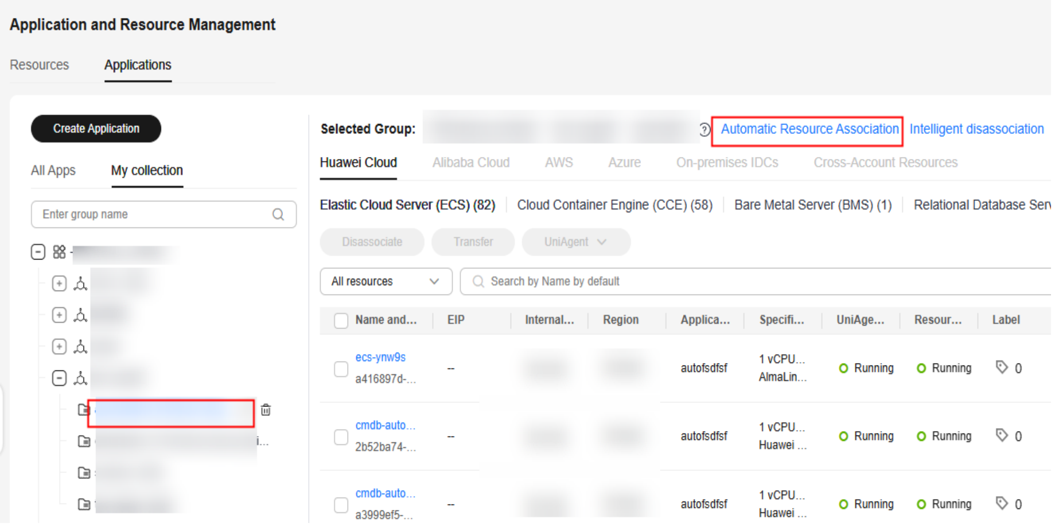
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select the group to be associated with resources, and click **Automatic Resource Association**.

Figure 4-6 Automatically associating resources with an application



Name and...	EIP	Internal...	Region	Applica...	Specifi...	UniAge...	Resour...	Label
ecs-ynw9s a416897d-...	--			autofsdfsf	1 vCPU... AlmaLin...	Running	Running	0
cmdb-auto... 2b52ba74-...	--			autofsdfsf	1 vCPU... Huawei ...	Running	Running	0
cmdb-auto... a3999ef5-...	--			autofsdfsf	1 vCPU... Huawei ...	Running	Running	0

NOTE

Automatic resource association rules can be modified. After the modification, other resources that meet the rules can be automatically associated. For details about modifying an automatic resource association rule, see **Modifying a Group**.

----End

4.14 Transferring Resources

Scenarios

After a group is associated with resources, you can move the resources in the group to another group.

Precautions

Resources can be transferred to application groups only when they belong to the same enterprise project as the application.

Transferring Resources

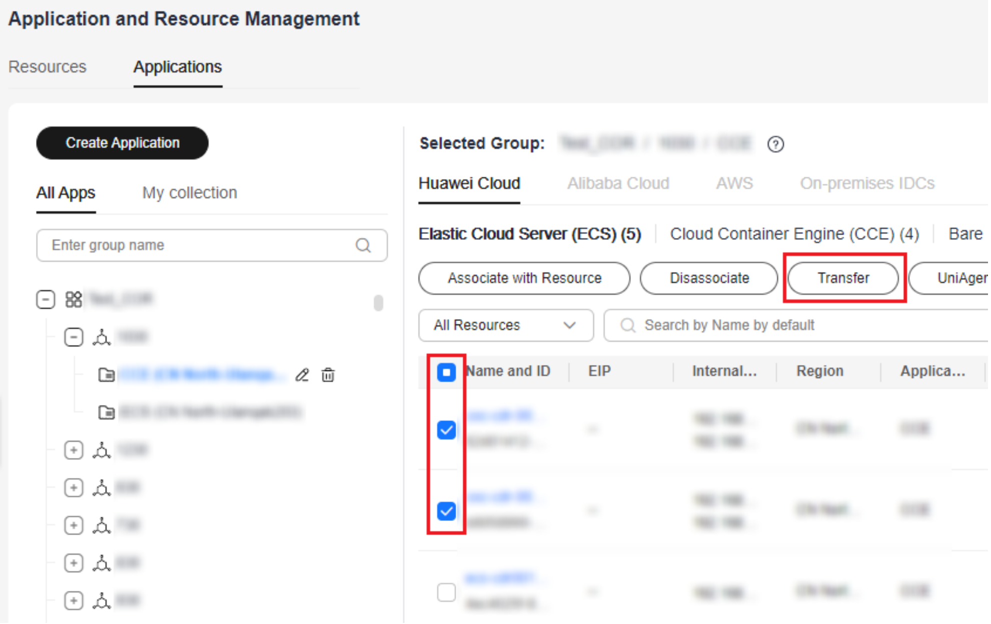
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select a group, select the resources to be transferred, and click **Transfer**.

Figure 4-7 Transferring resources



Step 5 Select the group to which this resource is to be transferred and click **OK**.

----End

4.15 Disassociating Resources from an Application Group

Scenarios

After a group is associated with resources, if you need to disassociate the resources from the group, perform the operations in this section.

Disassociating Resources from an Application Group

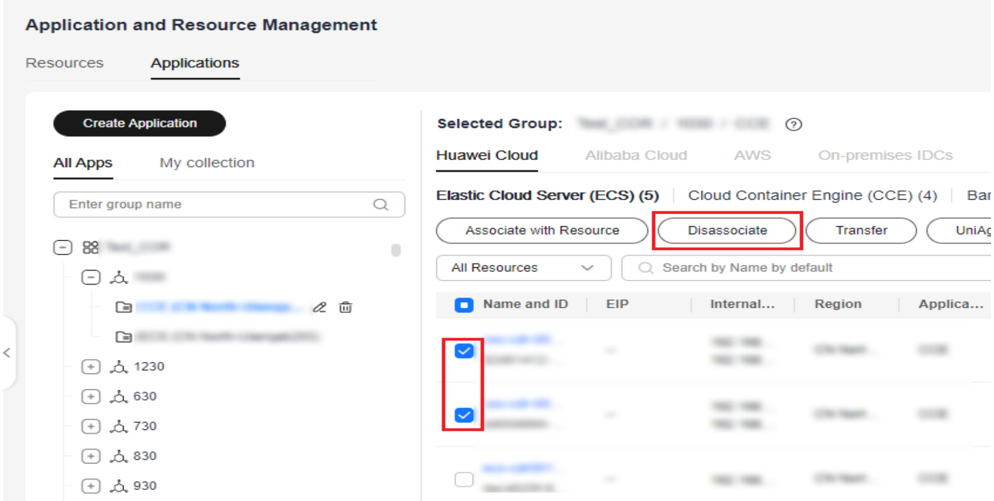
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, expand the application, select a group, select the resources to be disassociated, and click **Disassociate**.

Figure 4-8 Disassociating a resource from a group



Step 5 Click **OK**.

The resource disassociation is complete.

----End

4.16 Viewing Resource Details on the Resource Management Page

Scenarios

Resource List only displays some resource attributes. The following example shows how to query more details about a resource under an application.

Viewing Resource Details

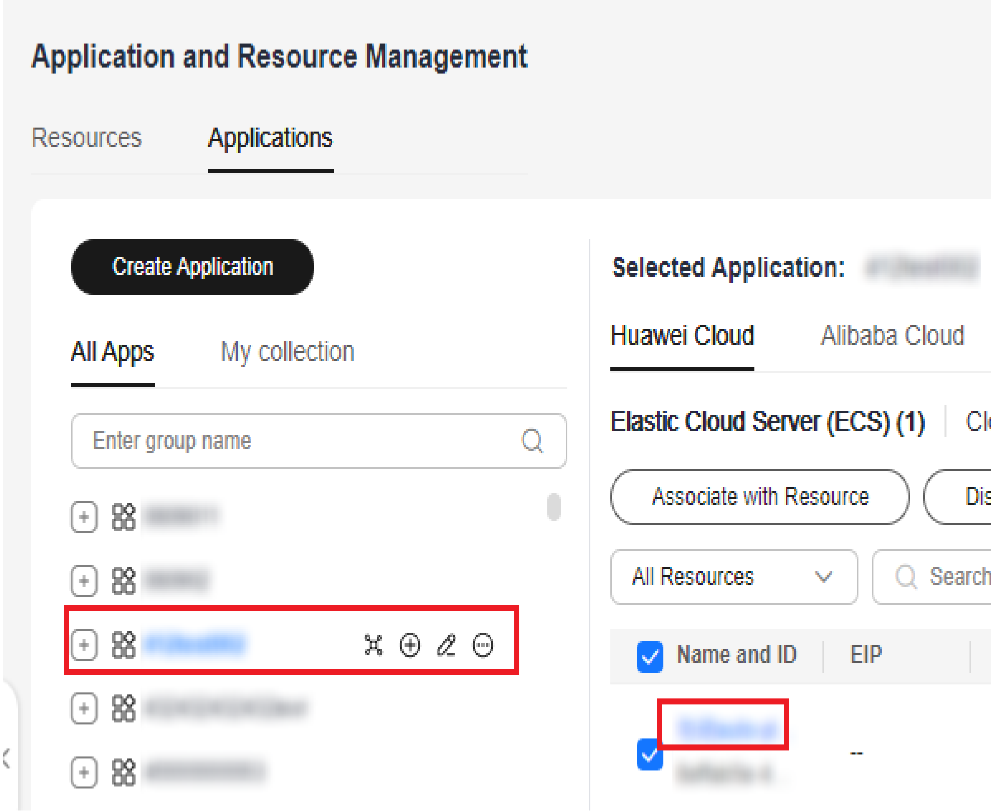
Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select an application, select the target instance, and click the instance name.

Figure 4-9 Viewing resource details



Step 5 Click **View Resource Details**.

View the resource details on the resource service details page.

----End

4.17 Viewing Capacity Details

Scenarios

Cloud Operations Center allows you to view the capacity details of resources associated with applications, sub-applications, components, or groups, and displays core resource data and rankings by resource type.

Viewing Capacity Details

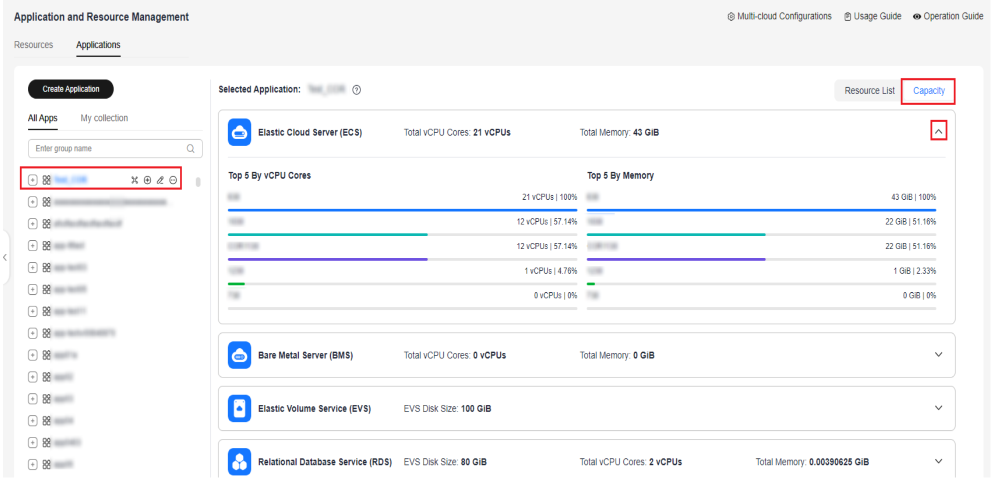
Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 3 Click **Applications** in the upper left corner.

Step 4 In the application list on the left, select the application, sub-application, component, or group to be viewed. Click **Capacity** on the right of the page.

Figure 4-10 Viewing capacity rankings



Elastic Cloud Server (ECS) Total vCPU Cores: **21 vCPUs** Total Memory: **43 GiB**

Top 5 By vCPU Cores	Top 5 By Memory
21 vCPUs | 100%	43 GiB | 100%
12 vCPUs | 57.14%	22 GiB | 51.16%
12 vCPUs | 57.14%	22 GiB | 51.16%
1 vCPUs | 4.76%	1 GiB | 2.33%
0 vCPUs | 0%	0 GiB | 0%

Bare Metal Server (BMS) Total vCPU Cores: **0 vCPUs** Total Memory: **0 GiB**

Elastic Volume Service (EVS) EVS Disk Size: **100 GiB**

Relational Database Service (RDS) EVS Disk Size: **80 GiB** Total vCPU Cores: **2 vCPUs** Total Memory: **0.00390625 GiB**

----End

5 Batch Resource Operations

5.1 Overview

You can perform batch operations on multiple resources, such as Elastic Cloud Servers (ECS), Relational Database Service (RDS), FlexusL , and Bare Metal Servers (BMSs). You can start, stop, and reboot these resources in batches, as well as reinstall and change OSs on them.

Scenarios

Table 5-1 Resources and scenarios

Resource Type	Batch Starting Instances	Batch Stopping Instances	Batch Restarting Instances	Batch Reinstalling OSs	Batch Changing OSs	Executing Commands
Elastic Cloud Server (ECS)	√	√	√	√	√	√
Relational Database Service (RDS)	√	√	√	×	×	×
FlexusL	√	√	√	√	√	×
Bare Metal Server (BMS)	√	√	√	√	×	×

5.2 Batch Operations on ECS Instances

5.2.1 Batch Starting ECSs

Scenarios

COC provides unified operations on ECSs. You can start ECSs one by one or in batches.

Precautions

- You can perform this operation only when the instance is stopped.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Starting ECSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Start ECSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-2 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set parameters for **Batch Policy**, **Suspension Policy**, and **Timeout Interval**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- **Timeout Interval**: Value range: 1 to 1800, in seconds.

Step 6 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 7 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:

- If some or all instance tasks in the service tickets are executed abnormally:
  - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
  - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
  - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
- If all instance tasks in the service tickets are executed successfully no more operation is needed.

----End

5.2.2 Batch Stopping ECSs

Scenarios

COC provides unified operations on ECSs. You can stop ECSs one by one or in batches.

Precautions

- You can perform this operation only when the selected instance is running.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Stopping ECSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Shut Down ECSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-3 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set parameters for **Batch Policy**, **Suspension Policy**, **Stop Mode**, and **Timeout Interval**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

- **Stop Mode**: The value can be **Shutdown** or **Forcible shutdown**.
- **Timeout Interval**: Value range: 1 to 1800, in seconds.

Step 6 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 7 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.2.3 Batch Restarting ECSs

Scenarios

COC provides unified operations on ECSs. You can restart ECSs one by one or in batches.

Precautions

- You can perform this operation only when the selected instance is running or restarting.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Restarting ECSs

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Restart ECSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-4 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set parameters for **Batch Policy**, **Suspension Policy**, and **Timeout Interval**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- **Timeout Interval**: Value range: 1 to 1800, in seconds.

Step 6 Set **Forcible restart**. The value can be **Yes** or **No**.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.2.4 Batch Reinstalling OSs of ECSs

Scenarios

COC provides unified operations on ECSs. You can reinstall the OSs of ECSs one by one or in batches.

Precautions

- If any instance is running, you need to stop the instance before performing this operation.

- If all instances are stopped, you can submit the execution task.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Reinstalling OSs of ECSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Reinstall OSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-5 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set parameters for **Batch Policy**, **Suspension Policy**, **Stop ECS**, and **Timeout Interval**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- Select **Stop now** under **Stop ECS**. When the service ticket starts to be executed, the instances that are not stopped will be stopped automatically.
- **Timeout Interval**: Value range: 1 to 1800, in seconds.

Step 6 Set **Login Mode**.

- **Password**: You can use the original ECS password or enter a new one.
- **Key pair**: You can select a key pair in **Key Pair Service**.
- **Reset password**: Before logging in to the ECS, reset the password.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.

– If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.2.5 Batch Changing OSs of ECSs

Scenarios

COC provides unified operations on ECSs. You can change the OSs of ECSs one by one or in batches.

Precautions

- If any instance is running, you need to stop the instance before performing this operation.
- If no instance is running, you can submit the execution task.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Changing OSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Change OSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-6 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set **Batch Policy**, **Suspension Policy**, and **Stop ECS**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- Select **Stop now** under **Stop ECS**. When the service ticket starts to be executed, the instances that are not stopped will be stopped automatically.

Step 6 Set **Image**.

- **Public image**: A public image is a standard OS image and is visible to all users. A public image consists of an OS and preinstalled public applications. If a public image does not contain the applications or software you need, you can use the public image to create a cloud server and then deploy required software as needed.
- **Private image**: A private image is created from an ECS or external image file and is visible only to the user who created it. A private image contains an OS, preinstalled public applications, and a user's personal applications. Using a private image to create an ECS saves the time for repeatedly configuring the ECS.
- **Shared image**: A shared image is a private image shared with other users.

Step 7 Set **Timeout Interval**. The value ranges from 1 to 1800, in seconds.

Step 8 Set **Login Mode**.

- **Password**: You can use the original ECS password or enter a new one.
- **Key pair**: You can select a key pair in **Key Pair Service**.
- **Reset password**: Before logging in to the ECS, reset the password.

Step 9 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.2.6 Batch Executing Commands on ECSs

Scenarios

COC provides unified operations on ECSs. You can submit script commands to one or more ECSs without login to quickly perform routine maintenance on them.

Precautions

You can perform this operation only when the selected instance is running.

The UniAgent instance must be running. For details, see **Configuring UniAgent**.

If the selected ECSs run on different OSs (Linux and Windows), you need to submit commands to the ECSs separately.

Executing a Command

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Elastic Cloud Server (ECS)** tab and click **Execute Commands**.

Step 4 Set **Execute Commands**.

Table 5-7 Parameter configurations

Parameter	Description
Target Instance	Click **Add** and configure the parameters on the **Select Instance** dialog box. For details about the parameters, see **Table 2 Parameters for selecting an instance**.
Operating System	Operating system of the target instance. Currently, Linux and Windows are supported. Select the operating system of the target instance.
Executed By	User who executes the commands. ● For an ECS running on Windows, the preset value is **system** and the value cannot be changed. ● For an ECS running on Linux, the preset value is **root**. You can change it as needed.
Execution Plan	Execution plan of the commands. The default setting is **Execute Now**.
Timeout Interval	Timeout interval for an individual command execution. If the command execution times out, the command submission will be stopped forcibly. Value range: 6–1,800 seconds (24 hours) Unit: second
Command Type	Type of the script commands that can be submitted. ● For an ECS running on Windows, you can set **Bat**. ● For an ECS running on Linux, **Shell** is set by default and **Python** is also supported.

Parameter	Description
Command Input	Input box of the commands to be submitted. The input content must be a command that can return results after a single execution. Interaction with the command output is not supported.
Command Output	Output box of the commands. You can view the command execution results.

Table 5-8 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Click **OK**.

The command starts to be executed.

----End

5.2.7 Batch Diagnosing ECSs

Scenarios

COC provides unified operations on ECSs. By diagnosing ECSs in batches, you can quickly learn about the overall running status of one or more ECSs and the accurate method of locating and rectifying faults.

Precautions

The UniAgent status of the target instance must be **Running**. For details about UniAgent operations, see **3.6 Configuring a UniAgent**.

The ECS diagnosis plug-in supports only some OSs. For details, see the following table.

Table 5-9 OSs supported by the ECS diagnosis plug-in

Architecture	OS Type		Supported by holmes-agent (Y/N)
x86	Huawei Cloud EulerOS	Huawei Cloud EulerOS 2.0 Standard 64-bit (40 GB)	Y
	CentOS	CentOS 7.9	Y
		CentOS 8.0	Y
		CentOS 8.2 64-bit	Y
		CentOS7.8	Y
		CentOS 7.7	Y
		CentOS 7.6	Y
		CentOS 7.5	Y
		CentOS7.4	Y
		CentOS 7.3	Y
		CentOS7.2	Y
		CentOS6.10	N
	Ubuntu	Ubuntu 20.04 server 64-bit	Y
		Ubuntu 22.04 server 64-bit	Y
		Ubuntu 18.04 server 64-bit	Y

Architecture	OS Type		Supported by holmes-agent (Y/N)
		Ubuntu 16.04 server 64-bit	Y
	EulerOS	EulerOS 2.5 64-bit	Y
	Debian	Debian 9.0.0 64-bit	Y
		Debian 8.8.0 64-bit	Y
		Debian 8.2.0 64-bit	Y
		Debian 12.0.0 64-bit	N
		Debian 11.1.0 64-bit	Y
		Debian 10.0.0 64-bit	Y
	OpenSUSE	openSUSE 15.0 64-bit	Y
	AlmaLinux	AlmaLinux 9.0 64-bit	N
		AlmaLinux 8.4 64-bit	N
		AlmaLinux 8.3 64-bit	N
	Rocky Linux	Rocky Linux 9.0 64-bit	N
		Rocky Linux 8.5 64-bit	N
		Rocky Linux 8.4 64-bit	N
	CentOS Stream	CentOS Stream 9 64-bit	Y
		CentOS Stream 8 64-bit	Y
	CoreOS	CoreOS 2079.4.0 64-bit	N
	openEuler	openEuler 22.03 64-bit	Y
		openEuler 20.03 64-bit	Y
	Others	FreeBSD 11.0-RELEASE 64-bit	N
Arm	Huawei Cloud EulerOS	Huawei Cloud EulerOS 2.0 Standard 64-bit (40 GB)	Y
	Ubuntu	Ubuntu 18.04 server 64-bit	Y
	CentOS	CentOS 7.6 64-bit with Arm	N
	EulerOS	EulerOS 2.8 64-bit with Arm	N
	Debian	Debian 10.2.0 64-bit with Arm	N
	KylinOS	Kylin Linux Advanced Server for Kunpeng V10	N

Architecture	OS Type		Supported by holmes-agent (Y/N)
	openEuler	openEuler 20.03 64-bit with Arm	N
Windows	Windows2012	Windows Server 2012 R2 Datacenter 64-bit English	N
		Windows Server 2012 R2 Standard 64-bit English	N
		Windows Server 2012 R2 Datacenter 64-bit Chinese	N
		Windows Server 2012 R2 Standard 64-bit Chinese	N
	Windows2016	Windows Server 2016 Datacenter 64-bit English_40 GB	Y
		Windows Server 2016 Standard 64-bit-English_40 GB	Y
		Windows Server 2016 Datacenter 64-bit Chinese_40 GB	Y
		Windows Server 2016 Standard 64-bit Chinese_40 GB	Y
	Windows2019	Windows Server 2019 Datacenter 64-bit English_40 GB	Y
		Windows Server 2019 Standard 64-bit English_40 GB	Y
		Windows Server 2019 Datacenter 64-bit Chinese_40 GB	Y
		Windows Server 2019 Standard 64-bit Chinese_40 GB	Y
	Windows2022	Windows Server 2022 Datacenter 64-bit Chinese_40 GB	Y

Architecture	OS Type		Supported by holmes-agent (Y/N)
		Windows Server 2022 Standard 64-bit Chinese_40 GB	Y
		Windows Server 2022 Datacenter 64-bit English_40 GB	Y
		Windows Server 2022 Standard 64-bit English_40 GB	Y

Diagnosing ECSs in Batches

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 Choose **Elastic Cloud Server (ECS)** > **Diagnose ECS**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-10 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS

Parameter	Description	Example Value
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Select **I agree to install the plug-in and collect data based on the *Guest OS Diagnosis Service Frontend Data Collection License*.** and click **OK**.

Step 6 Click **OK**.

The diagnosis details page is displayed. After the diagnosis is complete, you can view the diagnosis report.

----End

5.3 Batch Operations on RDS Instances

5.3.1 Batch Starting RDS DB Instances

Scenarios

COC provides unified operations on RDS DB instances. You can start RDS DB instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is in the stopped state.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Starting RDS DB Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Relational Database Service (RDS)** tab and click **Start RDS DB Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-11 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	RDS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.3.2 Batch Stopping RDS DB Instances

Scenarios

COC provides unified operations on RDS DB instances. You can stop RDS DB instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is in the normal state.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Stopping RDS DB Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Relational Database Service (RDS)** tab and click **Stop RDS DB Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-12 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	RDS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.

  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.3.3 Batch Restarting RDS DB Instances

Scenarios

COC provides unified operations on RDS DB instances. You can restart RDS DB instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is in the normal state.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Restarting RDS DB Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Relational Database Service (RDS)** tab and click **Restart RDS DB Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-13 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	RDS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.3.4 Diagnosing RDS DB Instances in Batches

Scenarios

COC provides unified operations on RDS DB instances. By batch diagnosing RDS DB instances, you can quickly learn about the overall running status of cloud databases from dimensions such as memory usage, disk performance metrics, and slow SQL data, and provide handling suggestions.

Precautions

This operation can only be performed for RDS DB instances.

Diagnosing RDS DB Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 Click **Relational Database Service (RDS)** and select **Diagnose RDS DB Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-14 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Auto select all**: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	RDS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Click **OK**.

The diagnosis details page is displayed. Wait until the diagnosis is complete and view the diagnosis report.

----End

5.4 Batch Operations on FlexusL Instances

5.4.1 Batch Starting FlexusL Instances

Scenarios

Cloud Operations Center (COC) provides unified operations on FlexusL instances. You can start FlexusL instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is stopped.

- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Starting FlexusL Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **FlexusL** tab and click **Start FlexusL Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-15 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	FlexusL
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.

- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.4.2 Batch Stopping FlexusL Instances

Scenarios

Cloud Operations Center (COC) provides unified operations on FlexusL instances. You can stop FlexusL instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is in the running state.

- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Stopping FlexusL Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **FlexusL** tab and click **Stop FlexusL Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-16 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	FlexusL
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Set **Batch Policy**, **Suspension Policy**, and **Stop FlexusL**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- **Stop Mode**: The value can be **Shutdown** or **Forcible shutdown**.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.4.3 Batch Restarting FlexusL Instances

Scenarios

Cloud Operations Center (COC) provides unified operations on FlexusL instances. You can restart FlexusL instances one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is running or restarted.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Restarting FlexusL Instances

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **FlexusL** tab and click **Restart FlexusL Instances**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-17 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources

Parameter	Description	Example Value
Resource Type	The default value is used and cannot be changed.	FlexusL
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Set **Forcible restart**. The value can be **Yes** or **No**.

Step 8 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 9 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:

    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.4.4 Batch Reinstalling OSs of FlexusL Instances

Scenarios

Cloud Operations Center (COC) provides unified operations on FlexusL instances. You can reinstall the OSs of FlexusL instances one by one or in batches.

Precautions

- If any instance is running, you need to stop the instance before performing this operation.
- If no instance is running, you can submit the execution task.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Reinstalling OSs

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **FlexusL Instance** tab and click **Reinstall OSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-18 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. - **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. - **CloudCMDB resources**: Select an instance from the resource list. - **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	FlexusL

Parameter	Description	Example Value
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Set **Batch Policy**, **Suspension Policy**, and **Stop FlexusL**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- Select **Stop now** under **Stop FlexusL**. When the service ticket starts to be executed, the instances that are not stopped will be stopped automatically.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Set **Login Mode**.

- **Password**: You can use the original FlexusL password or enter a new one.
- **Key pair**: You can select a key pair in **Key Pair Service**.
- **Reset password**: Before logging in to the FlexusL, reset the password.

Step 8 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 9 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:

- If some or all instance tasks in the service tickets are executed abnormally:
  - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
  - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
  - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
- If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.4.5 Batch Changing OSs of FlexusL Instances

Scenarios

Cloud Operations Center (COC) provides unified operations on FlexusL instances. You can change the OSs of FlexusL instances one by one or in batches.

Precautions

- If any instance is running, you need to stop the instance before performing this operation.
- If no instance is running, you can submit the execution task.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Changing OSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **FlexusL Instance** tab and click **Change OSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-19 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	FlexusL

Parameter	Description	Example Value
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Set **Batch Policy**, **Suspension Policy**, and **Stop FlexusL**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- Select **Stop now** under **Stop FlexusL**. When the service ticket starts to be executed, the instances that are not stopped will be stopped automatically.

Step 6 Set **Image**.

- **Public image**: A public image is a standard OS image and is visible to all users. A public image consists of an OS and preinstalled public applications. If a public image does not contain the applications or software you need, you can use the public image to create a cloud server and then deploy required software as needed.
- **Private image**: A private image is created from a FlexusL or external image file and is visible only to the user who created it. A private image contains an OS, preinstalled public applications, and a user's personal applications. Using a private image to create a FlexusL saves the time for repeatedly configuring the FlexusL instance.
- **Shared image**: A shared image is a private image shared with other users.

Step 7 Set **Login Mode**.

- **Password**: You can use the original FlexusL password or enter a new one.
- **Key pair**: You can select a key pair in **Key Pair Service**.
- **Reset password**: Before logging in to the FlexusL, reset the password.

Step 8 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 9 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    - Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    - Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    - Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.5 Batch Operations on BMS Instances

5.5.1 Batch Starting BMSs

Scenarios

COC provides unified operations on BMSs. You can start BMSs one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is stopped.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Starting BMSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Bare Metal Server (BMS)** tab and click **Start BMSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-20 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	BMS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.

- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    ii. Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    iii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    iv. Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.5.2 Batch Stopping BMSs

Scenarios

COC provides unified operations on BMSs. You can stop BMSs one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is in the running state.

- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Stopping BMSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Bare Metal Server (BMS)** tab and click **Shut Down BMSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-21 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. - **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	BMS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Set **Batch Policy**, **Suspension Policy**, and **Stop BMS**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

- **Stop Mode**: The value can be **Shutdown** or **Forcible shutdown**.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 8 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    ii. Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
    iii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
    iv. Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.5.3 Batch Restarting BMSs

Scenarios

COC provides unified operations on BMSs. You can restart BMSs one by one or in batches.

Precautions

- This operation can be performed only when the selected instance is running or restarted.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Restarting BMSs

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Bare Metal Server (BMS)** tab and click **Restart BMSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-22 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources

Parameter	Description	Example Value
Resource Type	The default value is used and cannot be changed.	BMS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Set **Forcible restart**. The value can be **Yes** or **No**.

Step 8 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 9 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:

- If some or all instance tasks in the service tickets are executed abnormally:
  1. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
  2. Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.
  3. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  4. Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.
- If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

5.5.4 Batch Reinstalling OSs of BMSs

Scenarios

COC provides unified operations on BMSs. You can reinstall the OSs of BMSs one by one or in batches.

Precautions

- If no instance is running, you can submit the execution task.
- If any service ticket (for example, restart service ticket) is being executed on the selected instance, the current operation cannot be performed. Wait until the existing service ticket is complete and try again.

Batch Reinstalling OSs

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Batch Resource Operations**.

Step 3 On the displayed page, choose the **Bare Metal Server (BMS)** tab and click **Reinstall OSs**.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 5-23 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. - **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. - **CloudCMDB resources**: Select an instance from the resource list. - **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	BMS

Parameter	Description	Example Value
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 5 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances to be executed are in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 6 Set **Timeout Interval**. The value ranges from 1 to 1,800 seconds.

Step 7 Set **Login Mode**.

- **Password**: You can use the original BMS password or enter a new one.
- **Key pair**: You can select a key pair in **Key Pair Service**.
- **Reset password**: Before logging in to the BMS, reset the password.

Step 8 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 9 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:

i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.

ii. Select an abnormal batch and click **Batch Retry** above the instance to re-execute all abnormal tasks in the current batch.

iii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.

iv. Select an abnormal batch and click **Batch Cancel** above the instance to cancel all abnormal tasks in the current batch.

– If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

6 Automated O&M

6.1 Patch Management

6.1.1 Overview

You can manage patches on ECSs, BMSs, or Cloud Container Engine (CCE) instances by scanning and repairing patches.

Constraints and Limitations

Currently, only servers that can access the public network are supported. You can bind an EIP or NAT gateway to perform operations in this function.

Before managing patches, ensure that the regions where the execution machines are deployed and the OSs of the execution machines are supported by the existing patch management feature, and the second-party package, on which the patch management feature is dependent on, is contained in the execution machine, and the package functions are normal. Otherwise, patches may fail to be managed.

- **Table 6-1** lists the OSs and versions supported by the patch management feature.
- **Table 6-2** lists the environment on which patch management depends.

Table 6-1 OSs and versions supported

OS	Product
Huawei Cloud EulerOS	Huawei Cloud EulerOS 1.1 Huawei Cloud EulerOS 2.0

OS	Product
CentOS	CentOS 7.2 CentOS 7.3 CentOS 7.4 CentOS 7.5 CentOS 7.6 CentOS 7.7 CentOS 7.8 CentOS 7.9 CentOS 8.0 CentOS 8.1 CentOS 8.2
EulerOS	EulerOS 2.2 EulerOS 2.5 EulerOS 2.8 EulerOS 2.9 EulerOS 2.10

Table 6-2 Dependencies

Type	Item
Python environment	Python (Python 2 or Python 3) DNF software packages (depended by Huawei Cloud EulerOS 2.0, CentOS 8.0 or later, and EulerOS 2.9 or later) Yum software packages (depended by Huawei Cloud EulerOS 1.1, versions earlier than CentOS 8.0 and EulerOS 2.9) lsb-release software package
Software package management tool	RPM

6.1.2 Managing Patch Baselines

Scenarios

You can customize a patch baseline to scan the patches of an instance. The patches that do not comply with the baseline can be fixed.

You can create patch baselines for ECS, CCE, and BMS instances as required.

Cloud Operations Center has provided the public patch baselines of all OSs as the preset patch baseline when ECS and BMS instances are used initially. Patch baseline for CCE instances needs to be manually created.

Precautions

The common baseline cannot be modified or deleted.

Creating a Patch Baseline

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the displayed page, click the **Patch Baseline** tab.

Step 5 Click **Create Patch Baseline** and set the parameters.

Table 6-3 Basic information parameters

Parameter	Description	Example Value
Baseline Name	Customize the name of the patch baseline based on the naming rule.	Test baseline
Description	(Optional) You can describe the remarks or usage instructions of the baseline.	-
Scenario Type	The value can be **ECS**, **CCE**, or **BMS**.	ECS
OS	The value can be **Huawei Cloud EulerOS**, **CentOS**, or **EulerOS**.	Huawei Cloud EulerOS
Default Baseline or Not	Select the option to set this patch as the default patch baseline.	-
Baseline Type	Select a baseline type. ● If you select **Installation Rule Baseline**, set the parameters by referring to **Table 6-4**. ● If you select **Custom Baseline**, set the parameters by referring to **Table 6-5**.	-

Table 6-4 Installation rule baseline

Parameter	Option	Description
Product	● Huawei Cloud EulerOS – All – Huawei Cloud EulerOS 1.1 – Huawei Cloud EulerOS 2.0 ● CentOS – All – CentOS 7.2 – CentOS 7.3 – CentOS 7.4 – CentOS 7.5 – CentOS 7.6 – CentOS 7.7 – CentOS 7.8 – CentOS 7.9 – CentOS 8.0 – CentOS 8.1 – CentOS 8.2 ● EulerOS – All – EulerOS 2.2 – EulerOS 2.5 – EulerOS 2.8 – EulerOS 2.9 – EulerOS 2.10	Product for which you want to scan patches. Only the patches of the selected product are scanned and fixed.
Category	● All ● Security ● Bugfix ● Enhancement ● Recommended ● New package	Category of patches. Only the patches of the selected category are scanned and fixed.

Parameter	Option	Description
Severity	- All - Critical - Important - Moderate - Low - None	Severity level of patches. Only the patches of the selected severity are scanned and fixed.
Automatic Approval	- Approve the patch after a specified number of days. - Approve patches released before the specified date.	Automatically approve patches that meet specified conditions.
Specified Days	0-365	This parameter is mandatory when **Approve the patch after a specified number of days.** is selected.
Specified Days	-	This parameter is mandatory when **Approve patches released before the specified date.** is selected.
Compliance Reporting	- Unspecified - Critical - High - Medium - Low - Suggestion	Level at which patches that meet the patch baseline are displayed in the compliance report
Install Non-Security Patches	-	If you do not select this option, the patches with vulnerabilities will not be updated during patch repairing.

Parameter	Option	Description
Abnormal Patches	-	Approved patches and rejected patches can be in the following formats: ● Complete software package name: *example*-**1.0.0-1.r1.hce2.x86_64** ● Software package names that contain a single wildcard: *example*-**1.0.0*.x86_64**

Table 6-5 Custom baseline

Parameter	Option	Description
Product	● Huawei Cloud EulerOS – All – Huawei Cloud EulerOS 1.1 – Huawei Cloud EulerOS 2.0 ● CentOS – All – CentOS 7.2 – CentOS 7.3 – CentOS 7.4 – CentOS 7.5 – CentOS 7.6 – CentOS 7.7 – CentOS 7.8 – CentOS 7.9 – CentOS 8.0 – CentOS 8.1 – CentOS 8.2 ● EulerOS – All – EulerOS 2.2 – EulerOS 2.5 – EulerOS 2.8 – EulerOS 2.9 – EulerOS 2.10	Product for which you want to scan patches. Only the patches of the selected product are scanned and fixed.
Compliance Reporting	Unspecified Critical High Medium Low Suggestion	Level at which patches that meet the patch baseline are displayed in the compliance report

Parameter	Option	Description
Baseline Patches	None	You can customize the version and release number of a baseline path. Only the patches that match the customized baseline patch can be scanned and installed. ● A maximum of 1,000 baseline patches can be uploaded for a baseline. ● The patch name can contain a maximum of 200 characters, including letters, digits, underscores (_), hyphens (-), dots (.), asterisks (*), and plus signs (+). ● The data in the second column consists of the version number (including letters, digits, underscores, dots, and colons) and the release number (including letters, digits, underscores, and dots) that are separated by a hyphen (-). Both two types of numbers can contain a maximum of 50 characters.

Step 6 Click **OK**.

The patch baseline is created.

----End

Setting a Default Baseline

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the displayed page, click the **Patch Baseline** tab.

Step 5 Locate the target baseline and click **Set Default Baseline** in the **Operation** column.

The default baseline is set.

----End

Modifying a Patch Baseline

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the displayed page, click the **Patch Baseline** tab.

Step 5 Locate the target baseline and click **Modify** in the **Operation** column.

Table 6-6 Basic information parameters

Parameter	Description	Example Value
Baseline Name	Customize the name of the patch baseline based on the naming rule.	Test baseline
Description	(Optional) You can describe the remarks or usage instructions of the baseline.	-
Scenario Type	This parameter cannot be changed.	ECS
OS	This parameter cannot be changed.	Huawei Cloud EulerOS
Baseline Type	This parameter cannot be changed. ● If you select **Installation Rule Baseline**, set the parameters by referring to **Table 6-4**. ● If you select **Custom Baseline**, set the parameters by referring to **Table 6-5**.	-

Step 6 Click **OK**.

The patch baseline is modified.

----End

Deleting a Patch Baseline

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the displayed page, click the **Patch Baseline** tab.

Step 5 Locate the target baseline and click **Delete** in the **Operation** column.

The patch baseline is deleted.

----End

6.1.3 Managing Patch Scan Tasks

Scenarios

You can scan the patch compliance of the target instance based on the selected patch baseline, instance, and batch execution policy. The scan result displays the compliance status of the instance patch.

You can perform patch scanning or repair using the created patch baseline that matches the OS of the selected instance. Currently, multiple OSs, such as EulerOS and CentOS, are supported. If there is no suitable patch baseline, create one by referring to **6.1.2 Managing Patch Baselines**.

Precautions

If an instance cannot be selected, check the following items:

- Whether the UniAgent status of the instance is normal.
- Whether the OS on which the instance is running is supported by the patch management function.
- Whether the instance is stopped.

Creating a Patch Scan Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the displayed page, click the **Patch Scanning** tab and choose a resource type.

By default, **ECS** is selected.

Step 5 Click **Create Patch Scanning Task**.

Step 6 Set parameters in the **Execution Account & Region** area.

- **Execution Type**: **Single** or **Cross Account**.
  - **Single**: Execute this job only under the current account.
  - **Cross Account**: Execute this job using multiple organization member accounts.

NOTE

- To use this function, you need to add the account to the organization, configure the agency permissions, and enter the agency name in advance. For details, see **1.4 Cross-Account Management**.

Step 7 Set parameters in the **Scheduled Task** area.

- **Execution Mode**: **Execute immediately** or **Scheduled execution**.
  - **Execute immediately**: Execute the scanning task immediately after it is created.
  - **Scheduled execution**: Configure the scheduled task details.

Table 6-7 Scheduled task parameters

Parameter	Description
Time Zone	Select the time zone where the scheduled task is executed from the drop-down list.
Timing Type	Select a timing type. ▪ **Single execution**: Execute the scheduled task once at a specified time. ▪ **Periodic execution**: Execute the task periodically based on the specified rule until the rule expires.
Execution Time	It is used together with the timing type. ▪ For a single execution, set this parameter to the execution time. ▪ For periodic execution, select either of the following options: ○ **Simple**: Select the execution time by week. ○ **Cron**: Set the execution time using a cron expression. For details, see **6.4.5 Using Cron Expressions**.
Rule Expired	This parameter needs to be set when **Timing Type** is set to **Periodic execution**. Enter the end time of the periodic execution rule.
Notification Policy	Select **Start of execution**, **Execution failed**, or **Execution succeeded**. Multiple options can be selected.

Parameter	Description
Recipient	Select **Shift** or **Individual**. ▪ **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ▪ **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Notification Mode	Select a notification mode from the drop-down list. ▪ **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**. ▪ **SMS, WeCom**, **DingTalk**, **Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**.

Step 8 Configure the basic information.

If **Execution Mode** is set to **Execute immediately**, set the parameters by referring to **Table 6-8**. If **Execution Mode** is set to **Scheduled execution**, set the parameters by referring to **Table 6-9**.

Table 6-8 Basic information for immediate execution

Parameter	Description
Executed By	The preset value is **root** and cannot be changed.
Timeout Interval	The maximum duration allowed for a scan.

Table 6-9 Basic information about scheduled task execution

Parameter	Description
Task Name	You are advised to name the task based on the application scenario. The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).
Enterprise Project	Select an enterprise project from the drop-down list.
Version	Enter the version number. The default version is **1.0.0**.
IAM Agency	Select an agency from the drop-down list. If the selected agency does not have required permissions, task execution will fail and you need to select another agency or create one.

Step 9 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 6-10 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS**, **CCE**, or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong

Parameter	Description	Example Value
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 10 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 11 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 12 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    1. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    2. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks are successfully executed, click **Compliance Report** in the upper right corner to view the patch scanning result.

----End

6.1.4 Creating Patch Repair Tasks

Scenarios

After patch scanning is performed on an instance, the scanning result displays the non-compliance status of the instance patch. If there are non-compliant patches, you can repair the patches on the target instance.

Multiple OSs, such as EulerOS and CentOS, are supported. You can scan and repair patches based on the default patch baseline that matches the OS of the selected instance. Before repairing patches, ensure that the corresponding default patch baseline has been created. For details about how to create a patch baseline, see **6.1.2 Managing Patch Baselines**.

Creating a Patch Repair Task

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the **Patch Scanning** tab page, select the resource type of the instance whose patch needs to be repaired.

By default, **ECS** is selected.

Step 5 Locate the target instance and click **Repair** in the **Operation** column.

Step 6 Set parameters in the **Execution Account & Region** area.

- **Execution Type**: **Single** or **Cross Account**.
  - **Single**: Execute this job only under the current account.
  - **Cross Account**: Execute this job using multiple organization member accounts.

NOTE

- To use this function, you need to add the account to the organization, configure the agency permissions, and enter the agency name in advance. For details, see **1.4 Cross-Account Management**.

Step 7 Set parameters in the **Scheduled Task** area.

- **Execution Mode**: **Execute immediately** or **Scheduled execution**.
  - **Execute immediately**: Execute the scanning task immediately after it is created.
  - **Scheduled execution**: Configure the scheduled task details.

Table 6-11 Scheduled task parameters

Parameter	Description
Time Zone	Select the time zone where the scheduled task is executed from the drop-down list.

Parameter	Description
Timing Type	Select a timing type. ■ **Single execution**: A scheduled task is executed once at a specified time. ■ **Periodic execution**: A task is periodically executed based on the specified rule until the rule expires.
Execution Time	It is used together with the timing type. ■ For a single execution, set this parameter to the execution time. ■ For periodic execution, select either of the following options: ○ **Simple**: Select the execution time by week. ○ **Cron**: Set the execution time using a cron expression. For details, see **6.4.5 Using Cron Expressions**.
Rule Expired	This parameter needs to be set when **Timing Type** is set to **Periodic execution**. Enter the end time of the periodic execution rule.
Notification Policy	Select **Start of execution**, **Execution failed**, or **Execution succeeded**. Multiple options can be selected.
Recipient	Select **Shift** or **Individual**. ■ **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ■ **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.

Parameter	Description
Notification Mode	Select a notification channel from the drop-down list box. - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**. - **SMS, WeCom**, **DingTalk**, **Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set the reviewer information, see **Modifying Personnel Information**.

Step 8 Configure the basic information.

If **Execution Mode** is set to **Execute immediately**, set the parameters by referring to **Table 6-12**. If **Execution Mode** is set to **Scheduled execution**, set the parameters by referring to **Table 6-13**.

Table 6-12 Basic information for immediate execution

Parameter	Description
Executed By	The preset value is **root** and cannot be changed.
Timeout Interval	Maximum duration for scanning. The value is 1,800 seconds by default

Table 6-13 Basic information for scheduled execution

Parameter	Description
Task Name	You are advised to name the task based on the application scenario. The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).
Enterprise Project	Select an enterprise project from the drop-down list.
Version	Enter a version. The default version is **1.0.0**.
IAM Agency	Select an agency from the drop-down list. If the selected agency does not have required permissions, task execution will fail and you need to select another agency or create one.

Step 9 Set **Repair Resources**.

- **Resources**: Click **Add**. On the displayed page, select the target instances.
- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches (the selected target instances should be more than the batch number) and add the selected instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.
- **Allow Restart**: Some patches require a restart to take effect. If you choose not to restart, you will need to schedule a restart at a later time.

Step 10 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 11 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    1. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    2. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks are successfully executed, click **Compliance Report** in the upper right corner to view the patch repair result.

----End

6.1.5 Viewing Patch Scan and Repair Details

Scenarios

The results of patch scan and patch repair are also called patch compliance reports. To view details about a patch in the compliance report, perform operations in this section.

Precautions

The patch compliance report will only retain the most recent scan or repair record.

Viewing Patch Scan and Repair Details

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Patch Management**.

Step 4 On the **Patch Scanning** tab page, select the resource type of the instance whose patch needs to be viewed.

By default, **ECS** is selected.

Step 5 Locate the target instance and click **Summary** in the **Operation** column.

Status description:

- **Installed**: The patch complies with the patch baseline, has been installed on an ECS, and no update is available.
- **Non-baseline Patches Installed**: The patch is not compliant with the patch baseline but has been installed on an ECS.
- **Installed-to be Restarted**: The patch has been repaired, and can take effect only after the ECS is restarted.
- **Installed Rejected**: The rejected patch defined in the abnormal patches of a patch baseline. This patch will not be repaired even if it is compliant with the patch baseline.
- **Pending Repair**: The patch complies with the baseline, but the patch version is earlier than the baseline version.
- **Patch Repair Failed**: The patch repair fails.

----End

6.2 Script Management

6.2.1 Overview

You can execute scripts to complete complex or repeated automation tasks. You can detect high-risk scripts using the script management function. This function is supported on Windows and Linux OSs. Currently, scripts can be executed on various types of resources such as ECSs, FlexusL instances, and BMS.

Custom Scripts

You can create and manage Shell, Python, or Bat scripts. The custom scripts can be used for global parameters and the associated parameter center.

📖 NOTE

- The maximum size of the script content is 1 MB.
- A maximum of 200 scripts can be created for all sub-accounts under a tenant account.

Public Scripts

The details of public scripts are visible to all users. Public scripts cannot be added, modified, or deleted.

6.2.2 Setting Review Configurations

Scenarios

When creating or modifying a script, you can forcibly specify a shift or individual user as a reviewer and notify the reviewer through SMS messages or DingTalk. The reviewer needs to review the created or modified script.

Precautions

If you want to configure a reviewer by specifying a shift, you need to create a shift in **11.2.1 Overview** in advance.

If **Manual Review** was enabled, you can select a risk level for scripts. If you select the same risk level when creating a custom script, it means this script needs to be reviewed and the **Manual Review** parameter will be forcibly enabled.

Setting a Review Configuration

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 In the **Custom Scripts** tab page, click **Review Configurations**.

Step 5 Set parameters on the displayed page.

Table 6-14 Parameters of review configurations

Parameter	Description
Manual Review	Disabled by default. If this parameter is disabled, you do not need to set other parameters on this page. If this parameter is enabled, the parameter configuration for creating a custom script is affected. If this parameter was enabled, you can select a risk level for scripts. If you select the same risk level when creating a script, it means this script needs to be reviewed and this parameter will be forcibly enabled.
Risk Level	The value can be **High**, **Medium**, or **Low**. If you select the same risk level when creating a custom script, it means this script needs to be reviewed and the enterprise project, reviewer, and notification mode will be automatically configured to the values you set in this page.
Enterprise Project	Select an enterprise project from the drop-down list.
Reviewer	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Notification Mode	Select a value from the drop-down list. ● **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**. ● **SMS, WeCom**, **DingTalk**, **Phone, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**. ● **No notification**: The system does not notify any recipient.

Step 6 Click **OK**.

The review configuration is complete.

----End

6.2.3 Creating Custom Scripts

Scenarios

If the public scripts provided by COC do not meet your requirements, you can create custom scripts in the format of Shell, Python, or Bat. The scripts can be used for global parameters and the associated parameter center.

Precautions

Confirm and complete the risk level of the script content.

Creating a Custom Script

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 In the **Custom Scripts** tab page, click **Create Script**.

Step 5 Set parameters on the displayed page.

Table 6-15 Basic information parameters

Parameter	Description	Example Value
Script Name	Customize a script name based on the naming rules.	Test Script
Enterprise Project	Select the enterprise project to which the script belongs from the drop-down list.	default
Version	Enter the script version number.	1.0.0
Risk Level	Select **High**, **Medium**, or **Low** as required.	High
Description	Enter a description about the script.	-

Step 6 Set **Script Content**.

- Select **Shell**, **Python**, or **Bat**.
- Enter the script content.
  - The interpreter (for example, **#!/usr/bin/python**) that is automatically generated in the first row needs to be adapted to the Python soft link on your server. If the soft link is not available, you need to modify the interpreter to the one that can be executed by the server.
  - (Optional) If input parameters are defined, use ${*parameter_name*} for the Shell script type in the script content. For the Python script type, use the environment variable (for example, **varValue = os.getenv('*parameter_name*')**) in the Python library of the OS. For the BAT script type, use **%parameter_name%**.

- Click **Verify High-Risk Command**.
  - Verification scope: the high-risk commands involved in the verification. You can click **High-Risk Commands** to view the verification rules.
  - Verification rule: Within the verification scope, the script content is matched with high-risk commands using regular expression matching.
  - Verification result: The regular expression is used to verify whether the script content is high-risk, low-risk, or medium-risk.

    NOTE

    The verification result of high-risk commands is only used as a reference for determining the risk level of scripts. The tool does not forcibly intercept the consistency between the risk level of scripts and the verification result of high-risk commands. Evaluate the risk level based on the actual service impact.

Step 7 (Optional) Set **Script Input Parameters**.

- Add execution parameters of the script. A maximum of 20 parameters can be added, and the parameter value can contain spaces. You can select the **Sensitive** check box to encrypt the parameter.
  - **Sensitive**: Parameters are anonymized and encrypted for storage.

Step 8 (Optional) Set **Advanced Settings**.

- **Manual Review**: If this parameter is enabled, the script needs to be reviewed. For details about how to review, see **Approving a Custom Script**.
- **Reviewer**: **Shift** or **Individual**.
  - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
  - **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
- **Notification Mode**: Select a notification mode from the drop-down list.
  - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**.
  - **SMS, WeCom**, **DingTalk**, **Phone, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**.
  - **No notification**: The system does not notify any recipient.

Step 9 Click **OK**.

The custom script is created.

----End

6.2.4 Managing Custom Scripts

Scenarios

To approve, modify, or delete a custom script, perform the operations in this section.

Precautions

Confirm and complete the risk level of the script content when modifying a script.

Modifying a Custom Script

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 On the **Custom Scripts** tab page, locate the script to be modified and click **Modify** in the **Operation** column.

Step 5 Set parameters on the displayed page. The parameters are the same as those for creating a custom script. For details, see **Step 5**.

Step 6 Click **OK**.

The custom script is modified.

----End

Deleting a Custom Script

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 On the **Custom Scripts** tab page, locate the script to be deleted and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The custom script is deleted.

----End

Approving a Custom Script

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 On the **Custom Scripts** tab page, locate the script to be approved and click **Approve** in the **Operation** column.

Step 5 Set **Review Comment**.

- **Passed or Not**: **Passed** or **Not Passed**.
- **Review Comment**: Enter review comments.

Step 6 Click **OK**.

The custom script is approved.

----End

6.2.5 Executing Custom Scripts

Scenarios

To execute a custom script, perform the operations in this section.

Precautions

Ensure that you have the resource permissions of the component to which the target VM belongs when executing a script.

Notes and Constraints

A maximum of 999 instances can be selected for a task.

Executing a Custom Script

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

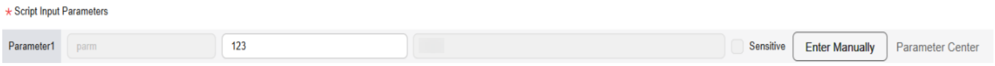
Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 On the **Custom Scripts** tab page, locate the script to be executed and click **Execute** in the **Operation** column.

Step 5 Set **Script Input Parameters**.

- The parameter names and default values have been preset when the custom script is created. When the script is executed, you can manually set the input parameter values or select the input parameter values from the parameter center. You can manually specify parameter values or select a preset parameter value from **the parameter center**. Select the region where the parameter is located, parameter name, and parameter association mode.

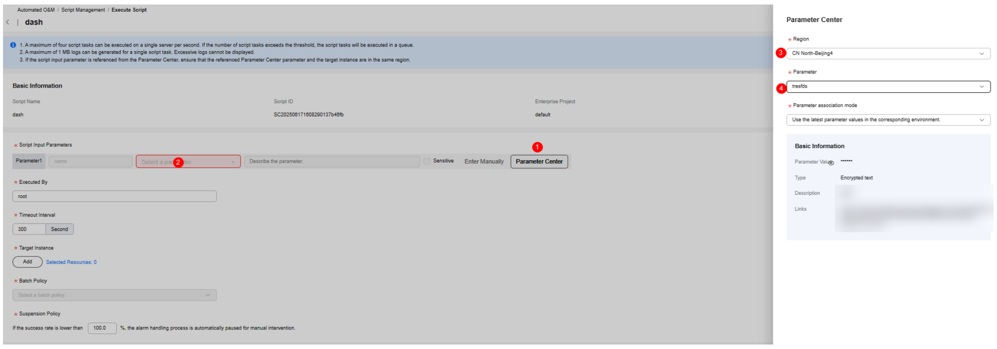
Figure 6-1 Manually entering script parameters



* Script Input Parameters

Parameter1 | parm | 123 | □ Sensitive | Enter Manually | Parameter Center

Figure 6-2 Selecting script parameters from the parameter center



Automated O&M / Script Management / Execute Script

< | dash

1. A maximum of four script tasks can be executed on a single server per second. If the number of script tasks exceeds the threshold, the script tasks will be executed in a queue.
2. A maximum of 1 MB logs can be generated for a single script task. Excessive logs cannot be displayed.
3. If the script input parameter is referenced from the Parameter Center, ensure that the referenced Parameter Center parameter and the target instance are in the same region.

Basic Information

Script Name: dash

Script ID: SC202506171608290137b46fb

Enterprise Project: default

* Script Input Parameters

Parameter1 | name | Select a parameter. | Describe the parameter. | □ Sensitive | Enter Manually | Parameter Center

* Executed By: root

* Timeout Interval: 300 Second

* Target Instance: Add Selected Resources: 0

* Batch Policy: Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Parameter Center

* Region: CN North-Beijing4

* Parameter: tresfds

* Parameter association mode: Use the latest parameter values in the corresponding environment.

Basic Information

Parameter Value: ******

Type: Encrypted text

Description: [redacted]

Links: [redacted]

Step 6 Set **Executed By** and **Timeout Interval**.

- **Executed By**: **root** is set by default. It is the user who executes the script on a target instance node.
- **Timeout Interval**: **300** is set by default. It indicates the timeout interval for executing the script on a single target instance.

Step 7 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 6-16 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 8 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 9 Click **OK** to go to the **Confirm Execution** page. Click **OK** to start the execution.

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:

    Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

6.2.6 Executing Public Scripts

Scenarios

Public scripts are predefined scripts. You can clean disks, reset passwords, start or stop OSs with this function. You can only read and execute public scripts.

Precautions

Ensure that you have the permission on the component to which the target VM belongs when executing a script.

Notes and Constraints

A maximum of 999 instances can be selected for a task.

Executing a Public Script

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

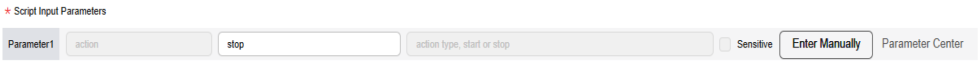
Step 4 Choose **Public Scripts**.

Step 5 Locate the script to be executed and click **Execute** in the **Operation** column.

Step 6 Set **Script Input Parameters**.

- **Script Input Parameters**: The parameters are preset in public scripts and cannot be modified. The script input parameter values can be set manually or selected from the parameter center. Currently, disk cleansing is not supported. You can manually specify parameter values or select a preset parameter value from **the parameter center**. Select the region where the parameter is located, parameter name, and parameter association mode.

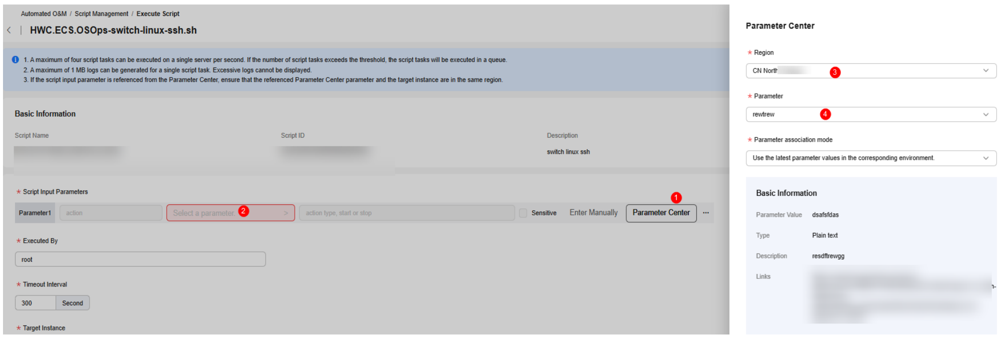
Figure 6-3 Manually specifying script parameters



* Script Input Parameters

Parameter1 | action | stop | action type, start or stop | □ Sensitive | Enter Manually | Parameter Center

Figure 6-4 Selecting script parameters from the parameter center



Automated O&M / Script Management / Execute Script

HWC.ECS.OSOps-switch-linux-ssh.sh

1. A maximum of four script tasks can be executed on a single server per second. If the number of script tasks exceeds the threshold, the script tasks will be executed in a queue.
2. A maximum of 1 MB logs can be generated for a single script task. Excessive logs cannot be displayed.
3. If the script input parameter is referenced from the Parameter Center, ensure that the referenced Parameter Center parameter and the target instance are in the same region.

Basic Information

Script Name: [redacted]
Script ID: [redacted]
Description: switch linux ssh

* Script Input Parameters

Parameter1 | action | Select a parameter. 2 | action type, start or stop | □ Sensitive | Enter Manually | Parameter Center 1 | ···

* Executed By: root

* Timeout Interval: 300 Second

* Target Instance

Parameter Center

* Region: CN North[redacted] 3

* Parameter: rewtrew 4

* Parameter association mode: Use the latest parameter values in the corresponding environment.

Basic Information

Parameter Value: dsafsfdas
Type: Plain text
Description: resdftrewgg
Links: [redacted]

Table 6-17 Parameter association modes

Parameter Association Mode	Description
Use the latest parameter value in the corresponding environment	This parameter is used during script execution. The value is the latest parameter value obtained from the corresponding region in the parameter center in real time.

Step 7 Set **Executed By** and **Timeout Interval**.

- **Executed By**: **root** is set by default. It is the user who executes the script on a target instance node.
- **Timeout Interval**: **300** is set by default. It indicates the timeout interval for executing the script on a single target instance.

Step 8 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 6-18 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 9 Configure **Batch Policy** and **Suspension Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Step 10 Click **OK**. On the displayed page, click **OK**.

Step 11 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.

  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    ii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

6.2.7 Managing Scripts Using Tags

Scenarios

Tag Management Service (TMS) enables you to use tags to manage custom scripts. TMS works with other cloud services to enable tag management. TMS manages tags globally, and other cloud services use these tags to manage their specific tasks. You can manage custom scripts under your account on the TMS console.

- You are advised to set pre-defined tags on the TMS console.
- A tag consists of a key and value. You can add only one value for each key.
- Each script can have a maximum of 20 tags.

Modifying Tags

Step 1 Log in to **COC**.

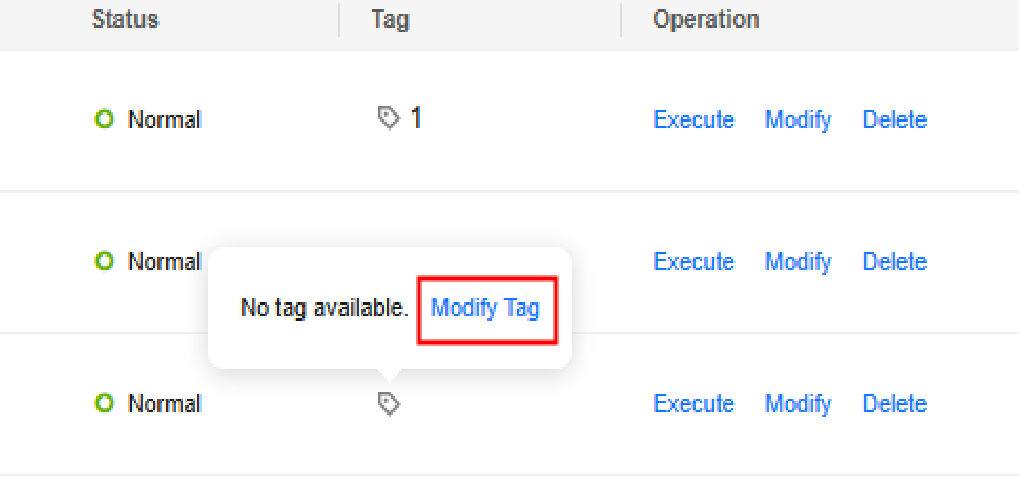
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 Click ⚙ on the right of the filter column and select **Tag**.

Step 5 On the **Custom Scripts** tab page, locate the target script, click 🏷 in the **Tag** column, and click **Modify Tag**.

Figure 6-5 Managing tags



Status	Tag	Operation
Normal	1	Execute Modify Delete
Normal		Execute Modify Delete
Normal		Execute Modify Delete

No tag available. Modify Tag

Step 6 Click **Add Tag**.

- When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user.
- A tag key can contain up to 128 characters. It cannot start with **_sys_** or a space, and cannot end with a space. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@
- A tag value can contain up to 255 characters. It cannot start or end with a space. Only letters, digits, spaces, and the following special characters are allowed: _ . : / = + - @

You can modify an existing tag. Click the key or value of a tag and enter a new key or value.

Step 7 Click **OK**.

The tag is modified.

----End

Deleting Tags

Step 1 Log in to COC.

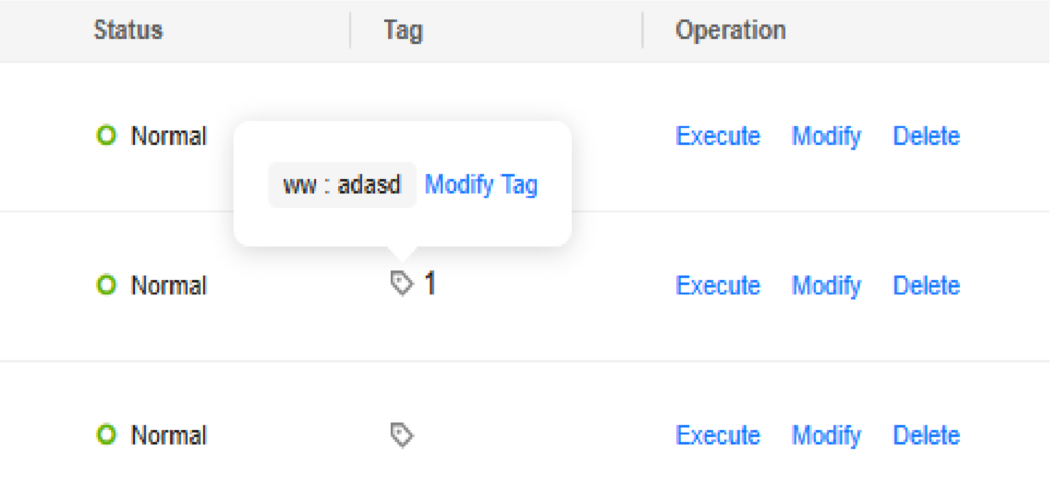
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Script Management**.

Step 4 Click ⚙ on the right of the filter column and select **Tag**.

Step 5 On the **Custom Scripts** tab page, locate the target script, click 🏷 in the **Tag** column, and click **Modify Tag**.

Figure 6-6 Managing tags



Status	Tag	Operation
Normal	ww : adasd Modify Tag	Execute Modify Delete
Normal	1	Execute Modify Delete
Normal		Execute Modify Delete

Step 6 Select the tag to be deleted and click 🗑.

Step 7 Click **OK**.

The tag is deleted.

----End

6.3 Job Management

6.3.1 Overview

A job is a collection of operations (atomic actions). A job can contain one or more operations, such as restarting ECSs and executing scripts.

You can create, modify, clone, and delete public jobs and custom jobs, and execute jobs on target instances. With this function, you can perform specific operations on the target instances. A maximum of 100 job versions are supported.

Public Jobs

Public jobs are solutions for several common O&M scenarios. Job details are visible to all users. Users cannot be added, modified, or deleted in this function.

Custom Jobs

You can create and manage custom jobs, including custom scripts, APIs, and process controls. Custom jobs can be used for global parameters and can be associated with the parameter center.

6.3.2 Executing Public Jobs

Scenarios

Public jobs are predefined jobs that you can read only and execute. Basic public jobs are listed and can be executed on target resources.

Precautions

Before executing a public job, ensure that you have the resource permissions of target instances.

Executing a Public Job

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 Choose **Public Jobs**.

Step 5 Select **All Jobs**, locate the public job to be executed, and click **Execute** in the **Operation** column.

Step 6 Set **Execution Type** and **Basic Information**.

Table 6-19 Parameters related

Parameter	Description	Example Value
Execution Type	Select the scope of the jobs to be executed. ● **Single**: Execute this job only under the current account.	Single
IAM Agency	(Optional) Scope of permissions that can be used on COC to execute jobs.	ServiceAgencyForCOC
Execution Description	(Optional) Description of the job to be executed.	-

Parameter	Description	Example Value
Tag	(Optional) Click **Add Tag** and enter a tag key and value. ● When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user. ● A tag key can contain up to 128 characters. It cannot start with **_sys_** or a space, and cannot end with a space. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ ● A tag value can contain up to 255 characters. It cannot start or end with a space. Only letters, digits, spaces, and the following special characters are allowed: _ . : / = + - @	-

Step 7 Set **Region**, **Target Instance Mode**, and **Job Execution Procedure**.

- **Region**: Select the region where the target instance is located.
- **Target Instance Mode**: Select the execution mode of job step and target instances.
  - **Consistent for all steps**: All steps are executed on all target instances.
  - **Unique for each step**: Set the target instance and batch policy for each job step.
  - **Unique for each task**: Set the target instance and batch policy for each task.
- **Job Execution Procedure**: Customize job details.
  - Click the job name. The **Modifying Parameters** drawer is displayed on the right.
  - Set **Input**, **Output**, and **Troubleshooting**.

Step 8 Perform related operations based on the selected public job type.

- Perform **9** and **10**, if you select a public job whose name starts with restarting ECS, stopping ECS, starting ECS, or starting OS.
- Perform **11**, if you select other public jobs.

Step 9 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 6-20 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. **Select All** is not enabled. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	The default parameter cannot be modified and is determined by **Region** in **Execution Content**.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

Step 10 Set **Batch Policy**.

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

Step 11 (Optional) Set global parameters.

- **Global Parameters**: Set global parameters of the job.

Step 12 Click **OK**. Confirm the execution information and click **OK**.

Step 13 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
  - If you want to pause the next batch when the current batch is executed, click **Pause**.
  - If you want to continue the paused batch, click **Continue**.
  - If you want to end all batches, click **End All Batches**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally, click the abnormal batch to view the exception details.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

6.3.3 Setting Review Configurations

Scenarios

When creating or modifying a job, you can forcibly specify a shift or individual user as a reviewer and notify the reviewer through SMS messages or DingTalk. The reviewer needs to review the created or modified job.

Precautions

If you want to configure a reviewer by specifying a shift, you need to create a shift in **11.2.1 Overview** in advance.

If **Manual Review** was enabled, you can select a risk level for jobs. If you select the same risk level when creating a custom job, it means this job needs to be reviewed and the **Manual Review** parameter will be forcibly enabled.

Setting a Review Configuration

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 In the **Custom Jobs** tab page, click **Review Configurations**.

Step 5 Set parameters on the displayed page.

Table 6-21 Parameters of review configurations

Parameter	Description
Manual Review	Disabled by default. If this parameter is disabled, you do not need to set other parameters on this page. If this parameter is enabled, the parameter configuration for creating a custom job is affected. If this parameter was enabled, you can select a risk level for jobs. If you select the same risk level when creating a job, it means this job needs to be reviewed and this parameter will be forcibly enabled.
Risk Level	The value can be **High**, **Medium**, or **Low**. If you select the same risk level when creating a custom job, it means this job needs to be reviewed and the enterprise project, reviewer, and notification mode will be automatically configured to the values you set in this page.
Enterprise Project	Select an enterprise project from the drop-down list.
Reviewer	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Notification Mode	Select a value from the drop-down list. ● **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**. ● **SMS, WeCom**, **DingTalk**, **Phone, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**. ● **No notification**: The system does not notify any recipient.

Step 6 Click **OK**.

The review configuration is complete.

----End

6.3.4 Creating Custom Jobs

Scenarios

You can create custom jobs, including custom scripts, APIs, and process controls. The jobs can be used for global parameters and can be associated with the parameter center.

Precautions

Confirm and fill in the risk level of the operation according to the operation procedure.

Creating a Custom Job

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 In the **Custom Jobs** tab page, click **Create Job**.

Step 5 Set **Basic Information**.

Table 6-22 Basic information parameters

Parameter	Description	Example Value
Job	Customize a job name based on the naming rules.	Test_Job
Enterprise Project	Select an enterprise project from the drop-down list.	default
Description	Description of a job.	-

Parameter	Description	Example Value
Tag	(Optional) Click **Add Tag** and enter a tag key and value. ● When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user. ● A tag key can contain up to 128 characters. It cannot start with **_sys_** or a space, and cannot end with a space. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ ● A tag value can contain up to 255 characters. It cannot start or end with a space. Only letters, digits, spaces, and the following special characters are allowed: _ . : / = + - @	-

Step 6 Click **Next**.

Step 7 Select a job template. If no proper template is available, select **Customize**. Click **Next**.

Step 8 Set **Job Orchestration**.

- Click ⊕ to add a new step.
- Click the step name or ✎ on the right of the step name to change the step name.
- Click 🗑 on the right of the step name to delete the step.
- Click **+ Add Task** to add a task for the step.
  - Click **+ Operation Type** to set the operation type of the current task. The operation type can be **Cloud service API Task**, **Controls**, or **Custom Scripts**.

Table 6-23 Operation type description

Operation Type		Description
Cloud service API Task	Start OS of ECS	You can start ECSs one by one or in batches.
	Restart OS of ECS	You can restart ECSs one by one or in batches.
	Change OS of ECS	You can change the OS of ECSs one by one or in batches.

Operation Type		Description
	Stop OS of ECS	You can stop ECSs one by one or in batches.
	Reinstall OS of ECS	You can reinstall ECSs one by one or in batches.
	Patch repair	You can repair non-compliant patches on the target instance.
	Patch scan	You can scan the patch compliance of the target instance.
	Execute API	You can call the OpenAPI of a cloud service registered with API Explorer. If the OpenAPI is called asynchronously, you can use the Wait API atom action to wait until the target object reaches the expected state.
	Wait API	It can be used to wait for the target object to reach the expected state. For example, after calling the **StartServer** API of the ECS using the Execute API atomic action, call the **ShowServer** API of the ECS using the Wait API atomic action. Wait until the status in the API response becomes **ACTIVE**, that is, the status is running, then you can confirm that the ECS has been started.
Controls	Review	You can select a shift or an individual for approval.
	Pause	You can pause a job. To resume a job, you need to click **Continue** in the service ticket details.
	Sleep	You can make a job sleep. After the sleep time is reached, the ticket continues to be executed.
Custom Scripts	Execute Command	You can run specific commands. The command types include Shell, Python, and Bat. You can customize command content and input parameters.
	Execute script	You can select a created custom script. For details about how to create a custom script, see **6.2.3 Creating Custom Scripts**.

- Set **Input**, **Output**, and **Troubleshooting**.
- Click **OK**.

- Click a job name or ✎ next to the job name to change the name.

Step 9 (Optional) Set global parameters.

Global Parameters: Global parameters can be customized or obtained from the parameter center. You can manually set parameter values or select a preset parameter value from **the parameter center**. Select the region where the parameter is located, parameter name, and parameter association mode.

Table 6-24 Parameter association modes

Parameter Association Mode	Description
Use the current parameter value in all environments	This parameter is used during job execution. The parameter value is that displayed in the parameter basic information when the parameter is added during job creation.
Use the latest parameter value in the corresponding environment	This parameter is used during job execution. The parameter value is the latest parameter value obtained from the parameter center in real time.

Step 10 Click **Next**.

Step 11 Set **Advanced Settings**.

- **Risk Level**: Select **High**, **Medium**, or **Low** as required.
- **Manual Review**: If this parameter is enabled, the job needs to be reviewed. For details about how to review, see **Approving a Custom Job**.
- **Reviewer**: **Shift** or **Individual**.
  - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
  - **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
- **Notification Mode**: Select a notification mode from the drop-down list.
  - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**.
  - **SMS, WeCom**, **DingTalk**, **Phone, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**.
  - **No notification**: The system does not notify any recipient.

Step 12 Click **OK**.

The custom job is created.

----End

6.3.5 Managing Custom Jobs

Scenarios

To approve, modify, clone, or delete a custom job, perform the operations in this section.

Precautions

When modifying or cloning a job, determine and fill out the risk level of the job.

Modifying a Custom Job

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 On the **Custom Jobs** tab page, locate the job to be modified and click **Modify** in the **Operation** column.

Step 5 Set parameters on the displayed page. The parameters are the same as those for creating a custom job. For details, see **6.3.4 Creating Custom Jobs**.

Step 6 Click **OK**.

The custom job is modified.

----End

Cloning a Custom Job

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 On the **Custom Jobs** tab page, locate the job to be cloned and click **More** > **Clone** in the **Operation** column.

Step 5 Set parameters on the displayed page. The parameters are the same as those for creating a custom job. For details, see **6.3.4 Creating Custom Jobs**.

Step 6 Click **OK**.

The custom job is cloned.

----End

Deleting a Custom Job

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 On the **Custom Jobs** tab page, locate the job to be deleted and click **More** > **Delete** in the **Operation** column.

Step 5 Click **OK**.

The custom job is deleted.

----End

Approving a Custom Job

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 On the **Custom Jobs** tab page, locate the job to be approved and click **Approve** in the **Operation** column.

Step 5 Set **Review Comment**.

- **Passed or Not**: **Passed** or **Not Passed**.
- **Review Comment**: Enter review comments.

Step 6 Click **OK**.

The custom job is approved.

----End

6.3.6 Executing Custom Jobs

Scenarios

To execute a custom job, perform the operations in this section.

Precautions

- Before executing a job, ensure that you have the resource permissions of target instances.
- A maximum of 999 instances can be selected for a task.

Executing a Custom Job

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 On the **Custom Jobs** tab page, locate the job to be executed and click **Execute** in the **Operation** column.

Step 5 Set **Execution Type**.

- If you choose **Single**, perform **7**.
- If you choose **Cross Account**, perform **6**.

NOTE

- Currently, BMS API call and scripts cannot be executed across accounts.
- Currently, jobs that contain review steps cannot be executed across accounts.
- To use this function, you need to add the account to the organization, configure the agency permissions, and enter the agency name in advance. For details, see **1.4 Cross-Account Management**.

Step 6 Set parameters in the **Execution Account & Region** area.

- **Execution Rule**: Ensure that there is one execution rule. A maximum of 20 execution rules are supported.
  - **Account**: tenant account name, which can be viewed on the **My Credentials** page.
  - **Region**: region where the target object is located.
  - **Agency**: name of the agency in IAM
  - **Project ID**: ID of the project to which the target object belongs.
- **Location concurrency**: This parameter is optional. Location concurrency controls the number of sub-tickets that are being executed, which affects the maximum number of sub-tickets that fail to be executed. For example, if the number of concurrent requests is 5, the maximum number of errors is the error threshold plus 5.
- **Error threshold**: This parameter is optional. When the number of failed sub-tickets is greater than the error threshold, the job stops.

Step 7 Set **Basic Information**.

Table 6-25 Basic information parameters

Parameter	Description	Example Value
Version	Select the version of the job from the drop-down list. The version number is automatically incremented each time you save the modification.	V1
IAM Agency	(Optional) Scope of permissions that can be used on COC to execute jobs.	ServiceAgencyForCOC
Execution Description	(Optional) Description of the job to be executed.	-

Parameter	Description	Example Value
Tag	(Optional) Click **Add Tag** and enter a tag key and value. ● When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user. ● A tag key can contain up to 128 characters. It cannot start with **_sys_** or a space, and cannot end with a space. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ ● A tag value can contain up to 255 characters. It cannot start or end with a space. Only letters, digits, spaces, and the following special characters are allowed: _ . : / = + - @	-

Step 8 Set the execution content.

- **Region**: Select the region where the target instance is located.
- **Target Instance Mode**: Select the execution mode of job step and target instances.
  - **Consistent for all steps**: All tasks are executed on the selected instance using the same batch policy.
  - **Unique for each step**: Tasks in one step are executed on the selected instance. Each step uses a batch policy.
  - **Unique for each task**: Set the target instance and batch policy for each task.
- **Job Execution Procedure**: Customize job details.
  - Click the job name. The **Modifying Parameters** drawer is displayed on the right.
  - Set **Input**, **Output**, and **Troubleshooting**.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 6-26 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection

Parameter	Description	Example Value
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	The default parameter cannot be modified and is determined by **Region** in **Execution Content**.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances. **NOTE** Instances cannot be filtered by enterprise project-level IAM permissions.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

Step 9 Click **OK**. On the displayed page, click **OK**.

NOTE

Change control can be enabled for custom jobs. For details about how to enable and use the change control function, see section "Change Control."

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:

i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.

ii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.

– If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

6.3.7 Managing Jobs Using Tags

Scenarios

Tag Management Service (TMS) enables you to use tags to manage custom jobs. TMS works with other cloud services to enable tag management. TMS manages tags globally, and other cloud services use these tags to manage their specific tasks. You can manage custom jobs under your account on the TMS console.

- You are advised to set pre-defined tags on the TMS console.
- A tag consists of a key and value. You can add only one value for each key.
- Each job can have up to 20 tags.

Modifying a Tag

Step 1 Log in to COC.

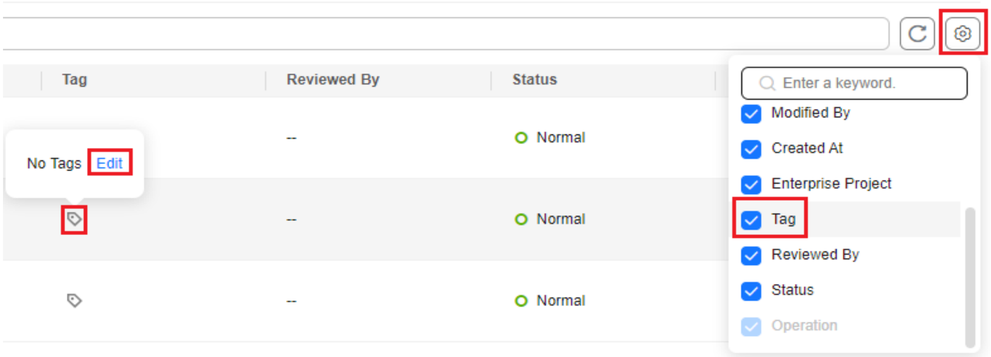
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 Click ⚙ on the right of the filter column and select **Tag**.

Step 5 On the **Custom Jobs** tab page, locate the target job, click 🏷 in the **Tag** column, and click **Modify Tag**.

Figure 6-7 Managing Tags



Step 6 Click **Add Tag**.

- When you enter a tag key and value, the system automatically displays all predefined tags associated with the current user.

- A tag key can contain up to 128 characters. It cannot start with **_sys_** or a space, and cannot end with a space. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@
- A tag value can contain up to 255 characters. It cannot start or end with a space. Only letters, digits, spaces, and the following special characters are allowed: _ . : / = + - @

You can modify an existing tag. Click the key or value of a tag and enter a new key or value.

Step 7 Click **OK**.

The tag is modified.

----End

Deleting a Tag

Step 1 Log in to COC.

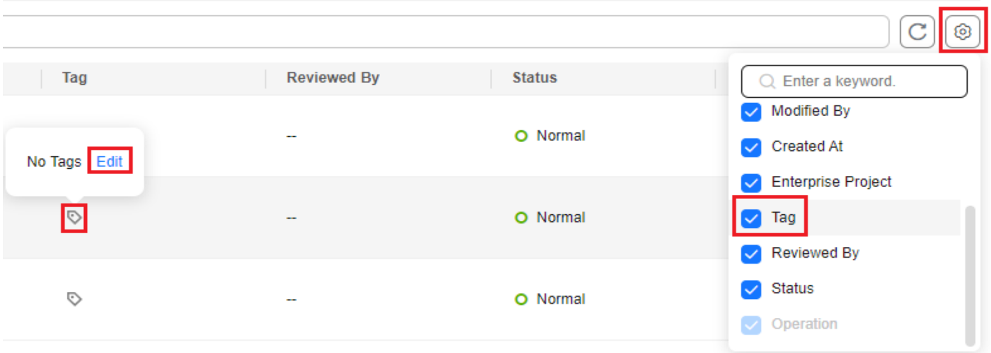
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Job Management**.

Step 4 Click ⚙ on the right of the filter column and select **Tag**.

Step 5 On the **Custom Jobs** tab page, locate the target job, click 🏷 in the **Tag** column, and click **Modify Tag**.

Figure 6-8 Managing Tags



Step 6 Select the tag to be deleted and click 🗑.

Step 7 Click **OK**.

The tag is deleted.

----End

6.4 Scheduled O&M

6.4.1 Overview

The **Scheduled O&M** page displays details and execution records of all scheduled tasks. You can create and manage scheduled tasks on this page. After scheduled tasks are created, operations (such as script execution and job management) are performed at a specified time or periodically.

Scheduled O&M includes the following key elements:

- **Scheduled Type**: One-time execution and periodic execution (including simple execution or cron expression).
- **Task Type**: **Scripts** and **Jobs**.
- **Executed By**: Select as required for the target instance.

Restrictions on Scheduled O&M

- Each account can create a maximum of 200 scheduled tasks.
- The target instance can be an ECS, FlexusL, or BMS instance.
- For a scheduled task, only when the **Status** is **Normal** (for the task that does not need to be approved or has passed the approval) and **Enabled Status** is **Enabled**, the scripts or jobs can be automatically executed.

6.4.2 Creating Scheduled Tasks

Scenarios

You can automatically execute scripts or jobs for target instances at a scheduled time, improving automated O&M efficiency.

You can perform operations on the **Resource O&M** > **Automated O&M** > **Scheduled O&M** > **Create Task** page.

Notes and Constraints

- Each account can create a maximum of 200 scheduled tasks.
- A maximum of 999 instances can be selected for a task.

Creating a Scheduled Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Click **Create Task**.

Step 5 Set **Basic Information**.

Table 6-27 Basic information parameters

Parameter	Description	Example Value
Task Name	Customize a task name based on the naming rules. The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).	Test_Job
Enterprise Project	Select an enterprise project from the drop-down list.	default
Version	Enter the script version number.	1.0.0
Risk Level	Select **High**, **Medium**, or **Low** as required.	Medium

Step 6 Set **Scheduled Settings**.

Table 6-28 Parameters

Parameter	Description
Time Zone	Select the time zone where the scheduled task is executed from the drop-down list.
Scheduled Type	Select a scheduled type. ● **Single execution**: A scheduled task is executed once at a specified time. ● **Periodic execution**: Execute the task periodically based on the specified rule until the rule expires.
Execution Time	It is used together with the timing type. ● For a single execution, set this parameter to the execution time. ● For periodic execution, select either of the following options: – **Simple**: Select the execution time by week. – Cron: Set the execution time using a cron expression. For details, see 6.4.5 Using Cron Expressions.
Rule Expired	This parameter needs to be set when **Timing Type** is set to **Periodic execution**. Configure the end time of the rule. The scheduled task is executed periodically based on the user-defined execution period until the rule end time.

Step 7 Perform operations by setting **Task Type**.

- If you select **Scripts**, perform **8**.
- If you select **Jobs**, perform **9**.

Step 8 Set **Task Type**.

- **Scripts**: Select a script from the drop-down list. You can select a custom script or common script.
- **Script Input Parameters**: If the script does not have input parameters, you do not need to set them.
- **Executed By**: **root** is set by default. It is the user who executes the script on a target instance node.
- **Timeout Interval**: **300** is set by default. It indicates the timeout interval for executing the script on a single target instance.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 6-29 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. – **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong

Parameter	Description	Example Value
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically. **NOTE** If you select a job of ECS startup, ECS shutdown, or ECS restart, and select **Select All** for **Selection Method**, a maximum of 500 instances can be selected at a time. If more than 500 instances need to be selected, select **Manual Selection** for **Selection Method**.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

  Skip step **9** and perform step **10**.

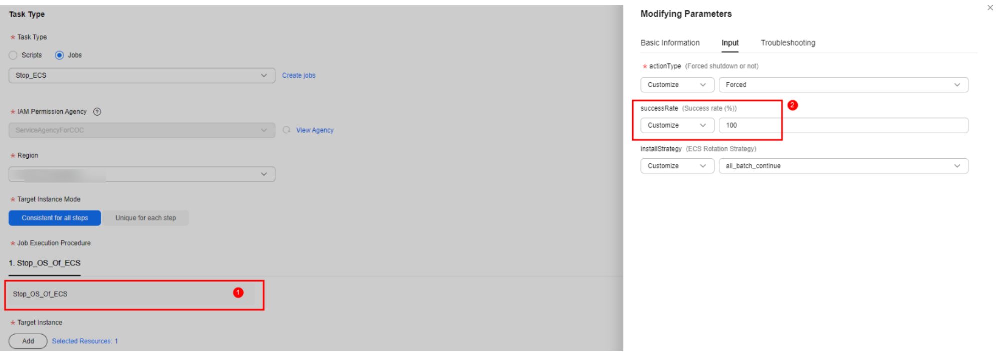
Step 9 Set **Task Type**.

- **Jobs**: Select a job from the drop-down list. You can select a custom job or public job.

  Currently, jobs that reference global parameters and jobs without target instances are not supported.

  If you select a job to set a scheduled task and want to use the suspension policy in the script scenario, set a parameter in the specific job step. For example, if you want to stop an ECS, set the **successRate** parameter.

Figure 6-9 Setting the suspension policy for stopping a scheduled ECS job



Task Type

* Task Type: ○ Scripts ● Jobs

Stop_ECS

* IAM Permission Agency: ServiceAgencyForCOC

* Region

* Target Instance Mode: Consistent for all steps

* Job Execution Procedure

1. Stop_OS_Of_ECS

Stop_OS_Of_ECS

* Target Instance: Selected Resources: 1

Modifying Parameters

* actionType (Forced shutdown or not): Customize, Forced

successRate (Success rate (%)): Customize, 100

installStrategy (ECS Rotation Strategy): Customize, all_batch_continue

- **IAM Agency**: scope of permissions that can be used on COC to execute jobs.
- **Region**: Select the region where the target instance is located.
- **Target Instance Mode**: Select the execution mode of job step and target instances.
  - **Consistent for all steps**: All tasks are executed on the selected instance using the same batch policy.
  - **Unique for each step**: Tasks in one step are executed on the selected instance. Each step uses a batch policy.
- **Job Execution Procedure**: Customize job details.
  - Click the job name. The **Modifying Parameters** drawer is displayed on the right.
  - Set **Input**, **Output**, and **Troubleshooting**.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 6-30 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. – **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	The default parameter cannot be modified and is determined by **Region** in **Execution Content**.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.

  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

Step 10 Set **Manual Review**

- **Manual Review**: If this parameter is enabled, the task needs to be reviewed. For details about how to review, see **Approving a Scheduled Task**.
- **Reviewer**: **Shift** or **Individual**.
  - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
  - **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
- **Notification Mode**: Select a notification mode from the drop-down list.
  - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**.
  - **SMS, WeCom**, **DingTalk, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**.
  - **No notification**: The system does not notify any recipient.

Step 11 Enable **Send Notification**. This operation is optional.

- **Send Notification**: Enable it and set **Recipient** and **Notification Mode** based on the selected notification policy.
- **Notification Policy**: Select **Start of execution**, **Execution failed**, or **Execution succeeded**. Multiple options can be selected.
- **Recipient**: Select **Shift** or **Individual**.
  - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
  - **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
- **Notification Mode**: Select a notification mode from the drop-down list.
  - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**.
  - **SMS, WeCom**, **DingTalk, Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set reviewer information, see **Modifying Personnel Information**.

Step 12 Click **OK**.

The scheduled task is created.

NOTE

You can set the jobs and scripts to be executed on the **Automated O&M** > **Script Management** page or **Automated O&M** > **Job Management** page.

----End

6.4.3 Managing Scheduled Tasks

Scenarios

You can approve, enable, disable, modify, and delete scheduled tasks.

Approving scheduled tasks: If the enterprise administrator configures manual review for scheduled tasks, the tasks can be enabled, disabled, or modified only after being approved by the reviewer.

Enabling/Disabling scheduled tasks: Scheduled tasks in the disabled state do not take effect but can be enabled. Scheduled tasks in the enabled state can be disabled.

Modifying scheduled tasks: You can modify the name, version number, and task type of a scheduled task as needed.

Deleting scheduled tasks: If a scheduled task is no longer needed, you can delete it.

Enabling and Disabling a Scheduled Task

NOTE

- You can enable or disable only the scheduled tasks created by yourself. You can view scheduled tasks created by other users under the current tenant account.
- A task takes effect after it is enabled. When the execution time is reached, the task is executed. After a scheduled task is disabled, it can be deleted and cannot be executed.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Locate the target task and click **Enable** or **Disable** in the **Operation** column.

The scheduled task is enabled or disabled.

----End

Modifying a Scheduled Task

NOTE

- Only scheduled tasks in the pending review or disabled state can be modified.
- After a scheduled task is modified and enabled again, it will be executed at the new execution time.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Locate the task to be modified and click **Modify** in the **Operation** column.

Step 5 Set parameters on the displayed page. The parameters are the same as those for creating a schedule task. For details, see **6.4.2 Creating Scheduled Tasks**.

Step 6 Click **OK**.

The scheduled task is modified.

----End

Deleting a Scheduled Task

NOTE

Only disabled scheduled tasks can be deleted.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Locate the task to be deleted and choose **More** > **Delete** in the **Operation** column.

Step 5 Click **OK**.

The scheduled task is deleted.

----End

Approving a Scheduled Task

NOTE

Only the task whose reviewer is the current login account can be reviewed. Only approved scheduled tasks can be enabled.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Locate the task to be approved and click the task name.

Step 5 Click **Approve**.

Step 6 Set **Review Comment**.

- **Passed or Not**: **Passed** or **Not Passed**.
- **Review Comment**: Enter review comments.

Step 7 Click **OK**.

The scheduled task is approved.

----End

6.4.4 Viewing the Execution Records of a Scheduled Task

Scenarios

You can view the execution records of a scheduled task. The records include script and job tickets. You can click each ticket to view its details.

Viewing the Execution Records of a Scheduled Task

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** area, click **Scheduled O&M**.

Step 4 Locate the target task and choose **More** > **Execution Record** in the **Operation** column.

Step 5 Click the service ticket ID in the **Service Tickets** area.

For details about operations on the service ticket details page, see **10.1.2 Viewing a Job Service Ticket** or **10.1.1 Viewing a Script Service Ticket**.

----End

6.4.5 Using Cron Expressions

Scenarios

A cron expression is a time expression used to specify the execution time, frequency, and interval of a scheduled task. It consists of six fields: **Seconds**, **Minutes**, **Hours**, **Day of month**, **Month**, and **Day of week**.

Field Values

Table 6-31 Cron expression field values

Field	Allowed Value	Allowed Special Character	Remarks
Seconds	0–59	None	-
Minutes	0–59	* /	The task execution interval is greater than 30 minutes.
Hours	0–23	- * /	-
Dy of month	1–31	- * ? / L	-
Month	1–12	JAN-DEC - * /	-
Day of week	1–7	SUN-SAT - * ? / L	The value **1** indicates **Sunday**, the value **2** indicates **Monday**, and so on.

Special Characters

Table 6-32 Supported special characters in a cron expression

Character	Description	Example Value
,	Used to specify additional values.	1,3,4,7,8.
*	Used to select all values within a field.	If the **Minutes** field is set to *****, an incident is triggered every minute.
?	Used to match any value of a field. However, it can be used only in the **Day of month** and **Day of week** fields because the two fields affect each other.	To trigger a scheduled task on the 20th day of each month, regardless of the day of week, use the following format: 13 13 15 20 *? Because the 20th day is specified in the **Day of month** field, the last character of the **Day of week** field can only be a question mark (?) instead of an asterisk (*). If the last character is *, it indicates that the incident is triggered on any day of a week, which is exclusive with the 20th day of the date field. In this case, the expression is incorrect.
-	Used to specify ranges.	For the **Hours** field, the value ranges from 8 to 10, indicating that the incident is triggered every hour from 8:00 to 10:00.
/	Used to specify increments. An incident is triggered from the specified time and at a fixed interval.	In the **Hours** field, ***/3** is equivalent to "every three hours". That is, an incident is triggered at the following time points in a day: 0, 3, 6, 9, 12, 15, 18, and 21.
L	Indicates "last". It can appear only in the **Day of month** and **Day of week** fields.	If **5L** is used as the value of the **Day of week** field, the incident is triggered on the last Thursday.

Example Value

0 15 10 ? * *: indicates that a task is executed at 10:15 a.m. every day.

0 0 10,14,16 * * ?: indicates that a task is executed at 10:00, 14:00, and 16:00 every day.

0 40 9-17 * * ?: indicates that a task is executed at the 40th minute of each hour from 09:00 to 17:00 each day.

0 0/30 10-16 ? * 2: indicates that a task is executed every 30 minutes from 10:00 to 16:00 every Monday.

6.5 Account Management

6.5.1 Overview

Account Management allows you to centrally manage human-machine accounts of Huawei Cloud ECSs, RDS DB instances, and middleware. We collect multiple accounts in one place to avoid risks like forgetting passwords or having them leaked. You can get host passwords using account management. With security controls, you can log in to Linux hosts and run commands without entering passwords. Here are the steps for account password management, automated password changes, and password-free logins.

Account management process:

1. Account management: You can manage accounts by using this capability. For example, you can **configure keys**, **import accounts**, and **view account passwords**.

2. Account encryption: You can change the password of an account on this page.

- Automatic password change for existing resources: Configure account baselines on the **Account Management** > **Account Password Change** > **Account Baselines** tab page.
- Automatic password change for new resources: Configure the password change policy on the **Account Management** > **Account Password Change** > **Password Change Policies** tab page.
- Periodic region-based password change: Add regions on the **Account Management** > **Account Password Change** > **Password Change Tasks** tab page.

After the configuration, you can view the **account password** and set **password-free login**.

Regions allowing automated password change

Table 6-33 Regions allowing automated password change

Region
CN North-Beijing1
CN North-Beijing4
CN East-Shanghai2
CN East-Shanghai1
CN South-Guangzhou
CN-Hong Kong
AP-Singapore

Region
AP-Bangkok
AP-Manila
ME-Riyadh
AF-Johannesburg
LA-Mexico City2
LA-Sao Paulo1

6.5.2 Key Management

Scenarios

The Cloud O&M Center uses DEW to encrypt your host account password for secure protection. Before using Key Management Service (KMS), create a key on DEW.

Configuring a Key

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Click **Keys** in the upper right corner.

Step 5 Check whether a key has been bound.

- If this is the first time you use KMS and no key has been bound, click **Bind Key**.
- If a key has been bound, click **Update**.

Step 6 Select the key to be bound and click **OK**.

NOTE

If no key is available, click **Create Key** to go to the DEW service to create a key. After the key is created, return to the **Bind Key** or **Update key** page and click ↻ on the right to update the key list.

Step 7 Click **OK**.

The key is bound.

----End

6.5.3 Account Baselines

Scenarios

Account baselines are classified into global baselines and component baselines.

- Global baseline: It is a built-in baseline of the system. It cannot be deleted for hosts that are not bound to components. To use the global baseline, you need to add a baseline account by referring to **Modifying an Account Baseline**. After the password change policy of the global baseline is enabled, the password will be changed periodically based on the account created in the baseline.
- Component baseline: When creating an account baseline, you establish a component baseline instead. You can create a component baseline as needed. After the password change policy of the component baseline is enabled, the password will be changed periodically based on the account created in the baseline.

Constraints and Limitations

The prerequisites for an account to be successfully managed are as follows:

- UniAgent 1.1.5 or later is installed and the UniAgent is running.
- The host is in the running state.
- The account configured in the baseline exists on the host and can be used to log in to the host.

Precautions

- Component baselines must be associated with components. If no proper component is available, create one. For details, see **4.6 Creating a Component**.
- To ensure that incremental host instances of a component can be automatically managed, you need to enable **Password Change Policy for Component Baseline** in **Component Baseline Dimension** on the **Change Account Password** > **Password Change Policies** tab page.

Creating an Account Baseline

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Click **Change Account Password** in the upper left corner.

Step 5 Click **Create Account Baseline**.

Step 6 Set parameters for creating an account baseline.

Table 6-34 Parameters for creating an account baseline

Parameter		Description	Example Value
Baseline Name		Specify a baseline name based on naming rules.	Test baseline
Baseline Type		Account baseline type, which cannot be modified.	Component Baseline
Baseline	Account Type	Account OS type, which cannot be changed. Only Linux servers are supported.	Linux
	Account	Enter an account name. The account name is the server account of the resource. This account is required for subsequent operations such as password change.	root
	Account Class	Available options are **Read-only account** and **Non-read-only account**. This parameter is used only to distinguish accounts and does not affect actual functions.	Read-only account
Associated Components		Select the required application or component. If you select an application, all components of the application are automatically selected.	-

Step 7 Click **OK**.

The account baseline is created.

----End

Modifying an Account Baseline

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Click **Change Account Password**.

Step 5 Click **Modify** in the **Operation** column.

Step 6 Set **Modify**.

Table 6-35 Parameters for modifying an account baseline

Parameter		Description	Example Value
Baseline	Account Type	Account OS type, which cannot be changed. Only Linux servers are supported.	Linux
	Account	Enter an account name. The account name is the server account of the resource. This account is required for subsequent operations such as password change.	root
	Account Class	Available options are **Read-only account** and **Non-read-only account**. This parameter is used only to distinguish accounts and does not affect actual functions.	Read-only account
Associated Components		This parameter can be set only when **Baseline Type** is set to **Component Baseline**. Select the required application or component. If you select an application, all components of the application are automatically selected. Associated components can be deleted.	-

Step 7 Click **OK**.

The account baseline is modified.

----End

Deleting an Account Baseline

Before deleting a baseline, you need to unbind all associated components.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Click **Change Account Password**.

Step 5 Click **Delete** in the **Operation** column.

The account baseline is deleted.

----End

6.5.4 Password Change Policies

Scenarios

You can set policies based on service requirements to ensure that the passwords of new host instances can be changed periodically.

Password change policies are categorized into the global baseline policies and component baseline policies.

- Global baseline password change policies: After a global password change policy is enabled, the passwords for logging in to all incremental host instances that are not bound to components will be changed periodically.
- Component baseline password change policies: After a component password change policy is enabled, the passwords for logging in to all incremental host instances that are associated with the selected component will be changed periodically.

To exclude some hosts from automatic password change, go to the **Resource Management** > **Application Resource Management** page. Set the tag key to **COCAccountPasswordAutoManagement** and the tag value to **NotManagePassword** by referring to **Managing Tags**. The settings take effect within one hour.

Setting a Password Change Policy

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Account Password Change** > **Password Change Policies**.

Step 5 Set a password change policy.

- Global baseline password change policies: After a global password change policy is enabled, the passwords for logging in to all incremental host instances that are not bound to components will be changed periodically.
- Component baseline password change policies: After a component password change policy is enabled, the passwords for logging in to all incremental host instances that are associated with the selected component will be changed periodically.
- Selecting components: Select the application or component to be selected. If you select an application, all components of the application are automatically selected.

----End

6.5.5 Creating a Scheduled Password Change Task

Scenarios

You can configure the regions where passwords need to be changed periodically on COC. The initial password change period is **0 15 3? * ***, indicating that the task is executed at 03:15 every day. After the configuration, a scheduled password change task is created for each region. You can view and modify the task on the **Managing Scheduled Tasks** page.

Notes and Constraints

A single scheduled password change task can be executed for a maximum of 999 instances. If the number of instances in the selected region exceeds this limit, the task will fail.

Configuring Password Change Regions

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Account Password Change** > **Password Change Tasks**.

Step 5 Set **Periodic password change policy**.

1. Click **Select Region**, select the region to be configured, click the rightward arrow, and click **OK**.
2. After the configuration is complete, click **View Details** in the **Operation** column to view the password change task details.
3. You can click **Delete** in the **Operation** column to delete unnecessary regions.

----End

6.5.6 Managing Account Passwords

Scenarios

The resources displayed on the account management page are synchronized from **Resource Management** and **Application Management**. You can use **Import Account** to manage host accounts and passwords online, use **Synchronize Account** to synchronize new host accounts, use **View Account Password** to view host accounts and passwords, and use **Reset Password** to reset host passwords.

- **Import Account**: Account management enables online hosting of host accounts and passwords. You can import the initial passwords of host accounts using an Excel file. After the import, you can click **View Account Password** to view the account passwords online.
- **Synchronize Account**: If you have added a host account on the OS, select the host on the **Account Management** page and click **Synchronize Account** to synchronize the new OS account. Note: If you want to change the password

of the new account, configure the account in the account baseline. (Ensure that the host is in the baseline.)

- **View Account Password**: You can view the account passwords of resources that are hosted online and resources with the password change policy enabled. Note: Only the account passwords of normal accounts and imported accounts can be obtained.
- **Reset Password**: This function will reset the passwords of all accounts (except the imported accounts) in the normal state, and the change is irreversible. After the password is reset, you can view the password reset result on the View Account Password page.

Precautions

- The imported host accounts are not managed. If you want to automatically manage the imported accounts, you can modify the global baseline or create an account baseline to add these accounts. Then, the system will immediately manage these host accounts.
- DCS, RDS, and DMS host accounts that are imported cannot be managed, that is, their passwords cannot be automatically changed.

Importing an Account

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.
- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Click **Import Account**.

- **Upload File**: Add the host account and password information in an Excel file. You can only upload Excel files. The number of accounts cannot exceed 500, and the file size cannot exceed 1 MB.
  a. Click **download template** and complete the downloaded template.
  b. Click **Upload File** to add the completed excel file.

Table 6-36 Account template parameters

Parameter	Description	Example Value
Host resource ID	Enter the resource ID. You can obtain the resource ID from the **Name/ID** column in the resource list.	-
Account Type	Select an account type based on the type of the imported resource.	Linux
Account	Enter the name of the account to be imported. The account name can contain 1 to 64 characters.	root
Account Class	The options are **Normal** and **Privileged**. ▪ **Normal**: read-only account ▪ **Privileged**: non-read-only account	Normal
Account Password	Enter a password of the account. The password can contain 8 to 64 characters.	-

c. Click **Import**.

The account is imported.

----End

Synchronizing an Account

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.
- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Select the resources whose accounts need to be synchronized and click **Synchronize Account**.

The account is synchronized.

----End

Viewing the Account Password

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.
- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Locate the target resource and click **View Account Password** in the **Operation** column.

NOTE

You can only query the account and password for one host at a time. Ensure that the password change status of the target host account is **Succeeded**, or that the password change failure cause is that the target account is not managed. Otherwise, the password may fail to be obtained. If password change status is **Failed**, rectify the fault based on the failure cause.

- Conditions for changing the password of an ECS host:
  - The resources status of the host is **Running**.
  - The UniAgent status of the host is **Running** and the UniAgent version is 1.1.5 or later.
  - The accounts on the host OS are the same as those in the bound account baseline.
- Conditions for changing the password of an added ECS: The password change policy has been enabled.
- Conditions for periodic password change of a managed host: The password change task has been bound to the host.

Step 7 Click **Obtain Password** in the **Operation** column. View the password.

If no data is displayed on the **Password Change Details** page, check whether the host is bound to a component. If yes, check whether the automatic management policy of the bound component baseline or of the component dimension is enabled. If the host is not bound to a component, check whether the automatic management policy of the global dimension is enabled.

----End

Resetting a Password

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.
- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Locate the target resource and choose **More** > **Reset Password** in the **Operation** column.

Step 7 Click **OK**.

The password reset task is complete.

----End

6.5.7 Logging In to a Host Without Any Passwords

Scenarios

COC supports password-free login to hosts through account management (only Linux ECSs are supported). You can select an account to enter the command execution page. The account is configured in **Account Baseline** and exists on the OS host.

Currently, password-free login is supported only in the CN North-Beijing4 region.

Precautions

Prerequisites for a successful remote login to a host:

- A UniAgent has been installed and is running on the target host. The UniAgent version must be later than 1.1.3.8.
- The host is in the running state.
- The account configured in the baseline exists on the host and can be used to log in to the host.

Logging In to a Host Without Any Passwords

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.

- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Choose **Password-free Login** in the **Operation** column.

Step 7 Select the target account from the drop-down list and click **OK**.

The black screen command page is displayed.

----End

6.5.8 Querying Password Change Records

Scenarios

After you configure password change, the host account password is changed periodically based on the configured period. You can view the final password change result and the new password for the account.

Obtaining the Account Password Change Records

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 Go to the **Routine O&M** page and click **Account Management**.

Step 4 Choose **Accounts** > **By Resource** or **By Application**.

- **By Resource** applies to all purchased host instances.
- **By Application** applies to purchased hosts that have been bound to an application. If you select **By Application**, you need to select the target application or component.

Step 5 Select a resource type.

By default, **Elastic Cloud Server (ECS)** is selected.

Step 6 Select the host to be viewed and choose **More** > **Password change record** in the **Operation** column.

View the password change records of the host.

NOTE

The password change record dialog box displays the password change time and status of the host account. You can filter the password change results by password change status and account name. If the password change status is succeeded, click **Obtain Password** in the **Operation** column to obtain the new password.

----End

6.6 Parameter Center

6.6.1 Overview

Parameter Center provides you secure and reliable data storage management. Parameters can be any data stored on COC, such as accounts, keys, and common text. Parameters can be referenced by scripts and jobs. Parameters and encrypted data can be managed throughout their lifecycles.

6.6.2 Creating a Parameter

Scenarios

You can create parameters to save data, such as accounts, keys, and common text data, which can be referenced by scripts and jobs. You can manage text parameters and encrypted data throughout the lifecycle.

Precautions

Parameter policies may delete parameters. Exercise caution when configuring parameter policies.

Creating a Parameter

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** module, click **Parameter Center**.

Step 4 Click **Create Parameter**.

Step 5 On the displayed page, configure **Basic Information**.

Table 6-37 Basic information parameters

Parameter	Description	Example Value
Parameter Name	Customize a parameter name based on the naming rules. The value can contain 1 to 256 characters, including digits, letters, and special characters _/. Slashes (/) can only be used for classification.	test1
Enterprise Project	Select an enterprise project from the drop-down list.	default
Parameter Description	Optional. Describe the input parameters.	-
Parameter Type	The options are **Plain text** and **Encrypted text**.	Plain text

Parameter	Description	Example Value
Encryption Mode	This parameter is required only when **Parameter Type** is set to **Encrypted text**. The encryption mode cannot be changed. Currently, only KMS encryption is supported.	KMS
Select a key	This parameter is required only when **Parameter Type** is set to **Encrypted text**. Select a key from the drop-down list. Keys are managed on the DEW console. To add or modify a key, go to the DEW console.	-
Parameter Value	Enter a value.	-

Step 6 (Optional) Set **Parameter Policy**.

- **Expired Delete**: Once enabled, you can set the deletion time for a parameter. The parameter will be automatically deleted when it expires.
- **Deletion Time**: The value can be **Absolute Time** or **Relative Time**.
  - **Absolute Time**: Select a date and time.
  - **Relative Time**: Enter the expiration time. The unit can be hour or day.
  - **Add Pre-Deletion Notification**: This parameter is optional. Set the notification time before deletion. The system will **notify you** based on the chosen **notification method** and time. You can add a maximum of two notifications.
- **Unmodified Notification**: This parameter is optional. You can set the notification time. If the parameter is not modified at the specified time, the system will **notify you** based on the chosen **notification method** and time. A maximum of two notifications can be set.
- **Notification Mode**: This parameter is required when you add pre-deletion or unmodified notifications. Select a notification mode from the drop-down list. Notify the recipients based on their reserved information. For details, see **Modifying Personnel Information**.
- **Recipient**: This parameter is mandatory when you add pre-deletion or unmodified notifications. Select a recipient from the drop-down list. For details about how to configure a recipient, see **11.1 O&M Engineer Management**.

NOTE

Rules for pre-deletion and unmodified notifications:

1. The pre-deletion notification time must be earlier than the time of deletion upon expiration.
2. The pre-deletion notification time must be later than the parameter creation or modification time.
3. The unmodified notification time cannot be earlier than the parameter creation or modification time.
4. If there is a policy for deleting the parameter upon expiration, the unmodified notification time cannot be later than the time of deletion upon expiration.

Step 7 (Optional) Click **Adding a Tag**.

- The tag key can contain only digits, letters, and the following special characters: _-.:/=+@. It can be 1 to 128 characters long.
- The tag value can contain only digits, letters, and these special characters: _-.:/=+@. It can be 1 to 256 characters long.

Step 8 Click **OK**.

The parameter is created.

----End

6.6.3 Modifying a Parameter

Scenarios

After a parameter is created, you can perform the following operations to modify the parameter description, parameter value, parameter policy, and tag.

Modifying a Parameter

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** module, click **Parameter Center**.

Step 4 Locate the parameter you want to review and click **Modify** in the **Operation** column.

Step 5 Configure the basic information.

- **Parameter Description**: This parameter is optional. Describe the input parameters.
- **Parameter Value**: Enter the parameter value.

Step 6 (Optional) Set **Parameter Policy**.

- **Expired Delete**: Once enabled, you can set the deletion time for a parameter. The parameter will be automatically deleted when it expires.
- **Deletion Time**: The value can be **Absolute Time** or **Relative Time**.
  - **Absolute Time**: Select a date and time.
  - **Relative Time**: Enter the expiration time. The unit can be hour or day.

  – **Add Pre-Deletion Notification**: This parameter is optional. Set the notification time before deletion. The system will **notify you** based on the chosen **notification method** and time. You can add a maximum of two notifications.

- **Unmodified Notification**: This parameter is optional. You can set the notification time. If the parameter is not modified at the specified time, the system will **notify you** based on the chosen **notification method** and time. A maximum of two notifications can be set.
- **Notification Mode**: This parameter is required when you add pre-deletion or unmodified notifications. Select a notification mode from the drop-down list. Notify the recipients based on their reserved information. For details, see **Modifying Personnel Information**.
- **Recipient**: This parameter is mandatory when you add pre-deletion or unmodified notifications. Select a recipient from the drop-down list. For details about how to configure a recipient, see **11.1 O&M Engineer Management**.

⚠ CAUTION

If the notification time is a relative time, note the following:

1. For unmodified notifications: If you click the modification button, the notification time will change immediately.
2. Pre-deletion notifications: If you change the deletion time, the pre-deletion notification time will also be changed.

Step 7 (Optional) Click **Adding a Tag**.

- The tag key can contain only digits, letters, and the following special characters: _-.:/=+@. It can be 1 to 128 characters long.
- The tag value can contain only digits, letters, and these special characters: _-.:/=+@. It can be 1 to 256 characters long.

Step 8 Click **OK**.

The parameter is modified.

----End

6.6.4 Viewing Parameter Details

Scenarios

To view parameter details, version history, sensitive parameter values, and decrypted data, perform the following operations:

Viewing Parameter Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Routine O&M** module, click **Parameter Center**.

Step 4 Select the parameter to be viewed and click its name.

If the parameter type is encrypted text, click 👁 next to the parameter value to view the sensitive parameter value, and click **Viewing Decrypted Data** to view the parameter values of all versions.

----End

6.7 OS Version Change

6.7.1 Overview

Background

OS Version Change allows you to change the host OS version. You can create an OS version change task to batch upgrade hosts. Each OS version change task generates an upgrade service ticket. You can view the upgrade progress of each instance in the service ticket and retry or roll back the upgrade as required.

Constraints

Currently, only Red Hat Linux is supported. Only ECSs and IDC offline resources are supported. Only minor version upgrades are allowed (upgrade path: From Red Hat 7.4/7.6 to Red Hat 7.9). The architecture type can only be x86_64. Batching is not supported.

6.7.2 Creating an OS Version Change Task

Scenarios

You can choose **Resource O&M** > **Automatic O&M** in the navigation pane. On the displayed page, click the **OS Version Change** card and create an OS version change task. After the task is created, a service ticket for upgrading the OS version is generated.

The OS version change feature is billed on a pay-per-use basis. You can create OS version change tasks as required. For details, see **Billing Mode**.

Creating an OS Change Task

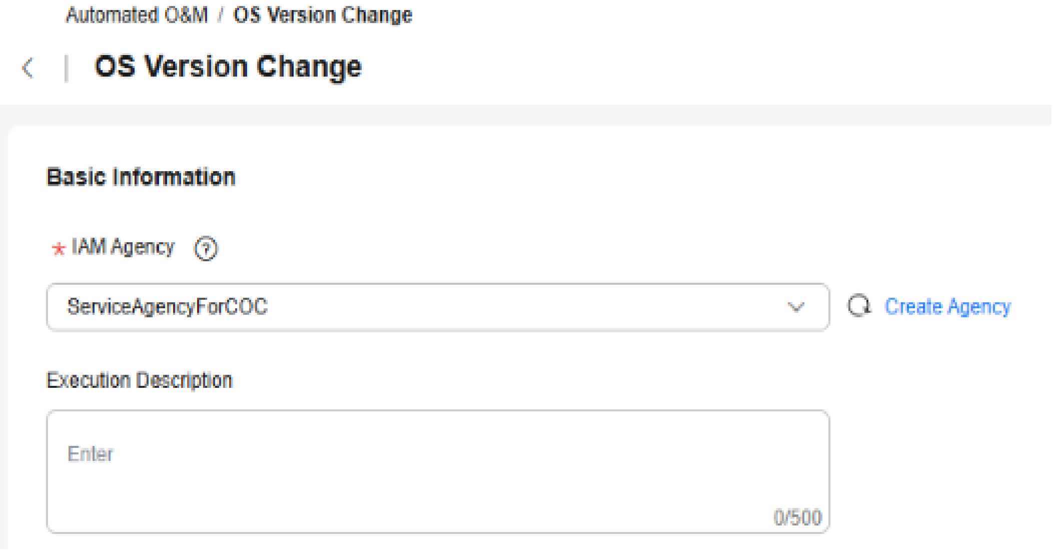
Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.

Step 3 In the **Advanced O&M** module, click **OS Version Change**.

Step 4 Set the basic information.

Figure 6-10 Configuring basic parameters



Automated O&M / OS Version Change

OS Version Change

Basic Information

* IAM Agency: ServiceAgencyForCOC

Execution Description: Enter

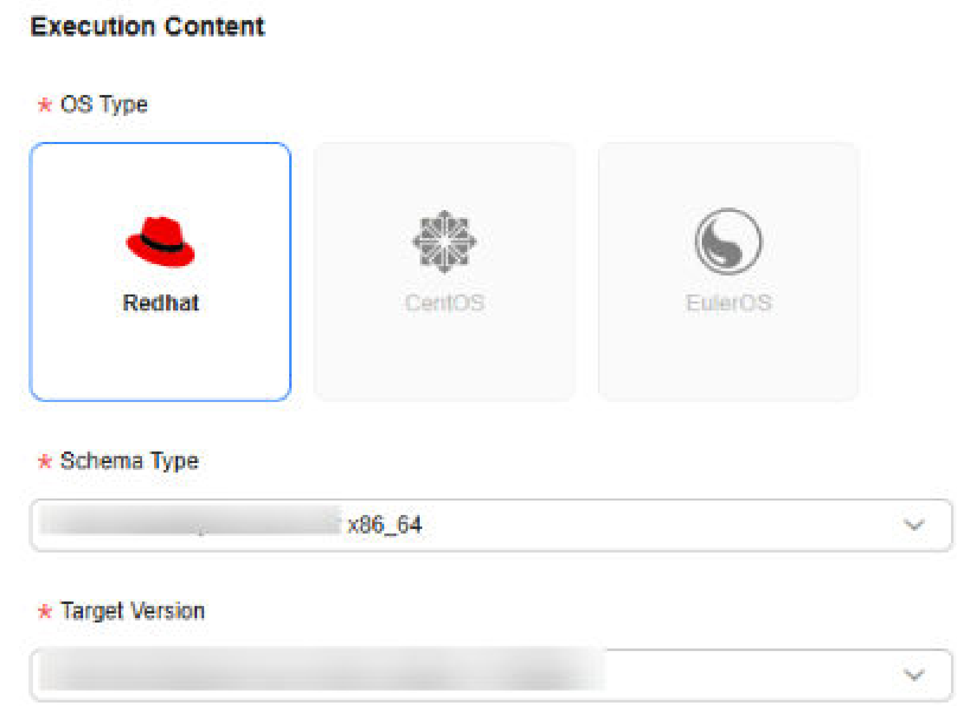
Table 6-38 Basic information parameters

Parameter	Description	Example Value
IAM Agency	(Mandatory) Scope of permissions that can be used on COC to execute jobs.	ServiceAgencyForCOC
Execution Description	(Optional) Description of the job to be executed.	-

Step 5 Specify **OS Type**, **Schema Type**, and **Target Version**.

- **OS Type**: Select the type of the OS you want to use for the target version. Currently, only Red Hat type is supported.
- **Architecture Type**: Select the CPU architecture type you want to use in the target version.
- **Target Version**: Select the target version.

Figure 6-11 Configuring execution content



Execution Content

* OS Type

* Schema Type

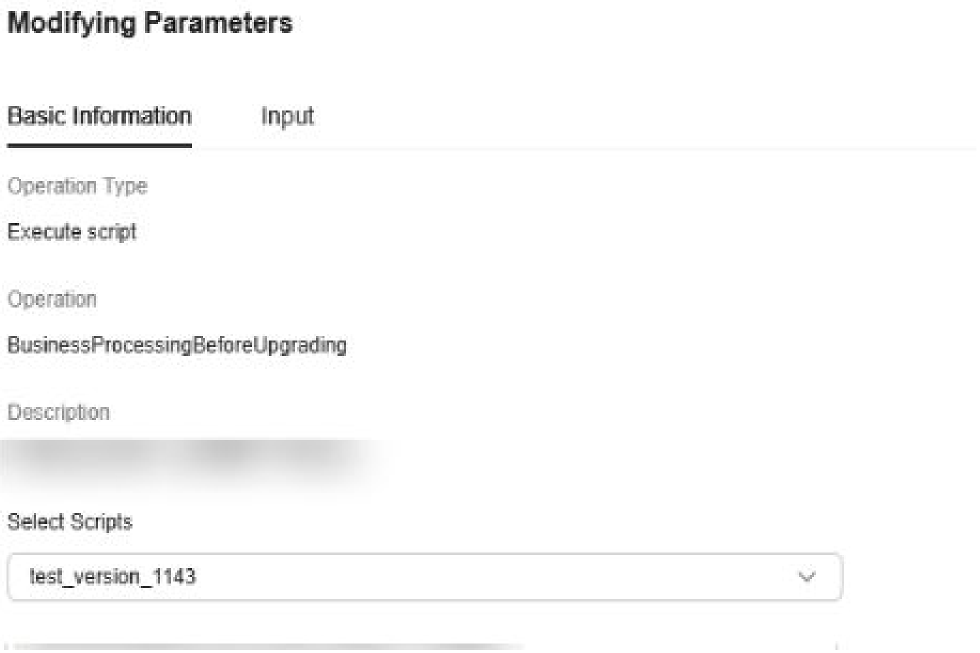
x86_64

* Target Version

Step 6 Set the OS upgrade procedure.

- The following 11 steps have been preset in the system: **BusinessProcessingBeforeUpgrading User-defined**, **PreparationBeforeUpgrading**, **CheckBeforeUpgrading**, **BackupBeforeUpgrading**, **UpgradeOS**, **RebootOS**, **Sleep-20s**, **WaitingForOSReboot**, **SystemProcessingAfterUpgrading**, **BusinessProcessingAfterUpgrading User-defined**, and **BusinessVerificationAfterUpgrading User-defined**.
- **BusinessProcessingBeforeUpgrading User-defined**, **BusinessProcessingAfterUpgrading User-defined**, and **BusinessVerificationAfterUpgrading User-defined** support user-defined configurations. You can click **Modify** under each step to go to the **Modify Parameter** drawer on the right. You can select a customized script on the **Basic Information** tab page. On the **Input** tab page, modify the input parameters. Other steps do not support user-defined configuration.

Figure 6-12 Custom parameters



Modifying Parameters

Basic Information | Input

Operation Type

Execute script

Operation

BusinessProcessingBeforeUpgrading

Description

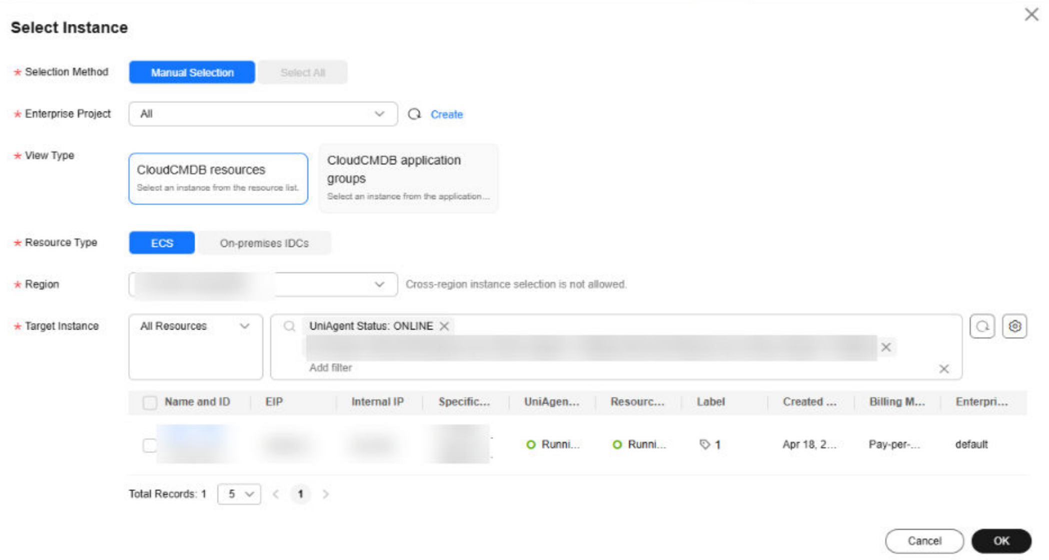
[redacted]

Select Scripts

test_version_1143

Step 7 Click **Add Instance** and set instance information.

Figure 6-13 Adding an instance



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All — Create

* View Type:
- CloudCMDB resources — Select an instance from the resource list.
- CloudCMDB application groups — Select an instance from the application...

* Resource Type: ECS | On-premises IDCs

* Region: [redacted] — Cross-region instance selection is not allowed.

* Target Instance: All Resources — UniAgent Status: ONLINE [redacted] Add filter

Name and ID	EIP	Internal IP	Specific...	UniAgen...	Resourc...	Label	Created ...	Billing M...	Enterpri...
[redacted]	[redacted]	[redacted]	[redacted]	Runni...	Runni...	1	Apr 18, 2...	Pay-per-...	default

Total Records: 1 5 < 1 >

Cancel OK

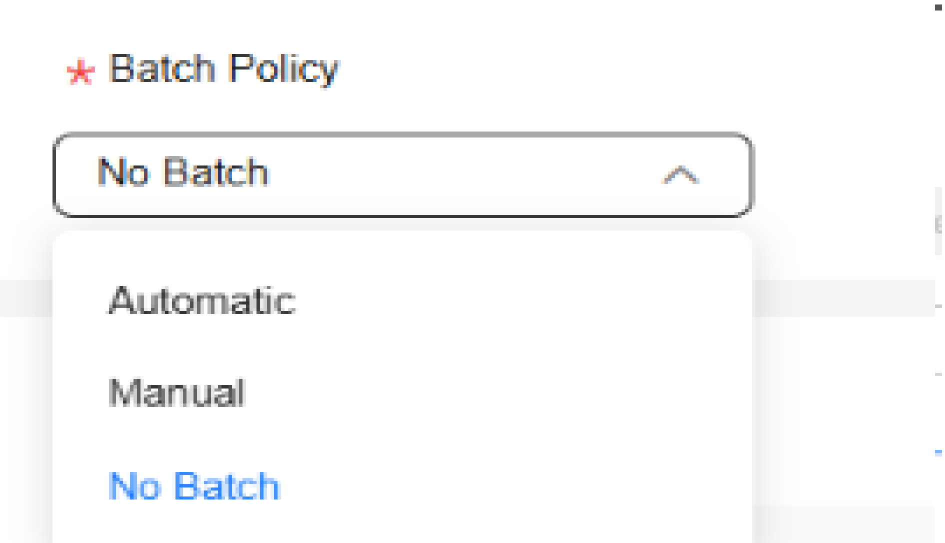
Table 6-39 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. **Select All** is not enabled. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● **Select All**: Automatically select all instances based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project. You can select **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	Select a resource type. The default value is used and cannot be changed.	ECS
Region	Select an execution region. The target DB instance cannot be selected across regions.	CN North-Beijing4
Target Instance	Set filter criteria in the filter box and select the filtered instances manually or automatically.	Select the required instance.

Step 8 Select a batch policy.

- **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
- **Manual**: You can manually create multiple batches and add instances to each batch as required.
- **No Batch**: All instances will be executed in the same batch.

Figure 6-14 Selecting a batch policy



Step 9 (Optional) Set global parameters.

Click **Modify** to modify the global parameters related to the OS version change.

Step 10 Click **OK**, confirm the execution information, and click **OK** again.

Step 11 The OS version change service ticket page is displayed. You can perform the following operations:

- Retry: If the service ticket status is abnormal, you can retry at the instance level and re-execute the current failed step.
- Rollback: If the service ticket status is abnormal or complete, you can create an OS rollback task. After the task is created, an OS rollback service ticket is generated.

----End

7 Faults

7.1 Fault Diagnosis

7.1.1 Overview

The fault diagnosis tool helps you check the status of ECSs, RDS DB, DCS, DMS, and ELB instances, detect potential problems in a timely manner, and provide professional rectification suggestions and solutions for abnormal metrics. In this way, you can effectively manage resources and enjoy better cloud migration experience.

NOTE

The diagnosis metrics vary depending on the cloud service resource type. For details about the diagnosis result, see the service ticket details.

Core Features

- Diversified diagnosis metrics: The diagnosis metrics cover commonly used inspection items of each cloud service instance, meeting routine diagnosis requirements.
- Professional repair suggestions: The diagnosis tool provides professional repair suggestions for abnormal items in the diagnosis result to improve your governance efficiency.
- One-click batch diagnosis: Cloud service instances of the same type can be selected in batches for quick diagnosis.

Typical Scenarios

Routine inspection: O&M personnel conduct routine inspections on resources and periodically execute batch diagnosis tasks to proactively identify risks in advance.

In the event of faults such as incidents or alarms, when the faulty instance is known, you can utilize the COC fault diagnostic tool for targeted in-depth diagnosis on the instance to identify and resolve faults at the instance level.

7.1.2 ECS Diagnosis

Scenarios

Backed by Huawei Cloud's accumulated expertise and detection algorithms, ECS diagnostic tool collects a small amount of guest OS data to help you quickly learn server statuses and provides troubleshooting methods.

Precautions

The UniAgent status of the target instance must be **Running**. For details about UniAgent operations, see **3.6 Configuring a UniAgent**.

The ECS diagnosis plug-in can only be used for some OSs. For details, see the following table.

Table 7-1 OSs supported by the ECS diagnosis plug-in

VM Architecture	OS Type		Supported by holmes-agent (Y/N)
x86	Huawei Cloud EulerOS	Huawei Cloud EulerOS 2.0 Standard Edition 64-bit (40 GB)	Y
	CentOS	CentOS 7.9	Y
		CentOS 8.0	Y
		CentOS 8.2 64-bit	Y
		CentOS 7.8	Y
		CentOS 7.7	Y
		CentOS 7.6	Y
		CentOS 7.5	Y
		CentOS 7.4	Y
		CentOS 7.3	Y
		CentOS 7.2	Y
		CentOS 6.10	N
	Ubuntu	Ubuntu 20.04 server 64-bit	Y
		Ubuntu 22.04 server 64-bit	Y
		Ubuntu 18.04 server 64-bit	Y
		Ubuntu 16.04 server 64-bit	Y
	EulerOS	EulerOS 2.5 64-bit	Y

VM Architecture	OS Type		Supported by holmes-agent (Y/N)
	Debian	Debian 9.0.0 64-bit	Y
		Debian 8.8.0 64-bit	Y
		Debian 8.2.0 64-bit	Y
		Debian 12.0.0 64-bit	N
		Debian 11.1.0 64-bit	Y
		Debian 10.0.0 64-bit	Y
	OpenSUSE	openSUSE 15.0 64-bit	Y
	AlmaLinux	AlmaLinux 9.0 64-bit	N
		AlmaLinux 8.4 64-bit	N
		AlmaLinux 8.3 64-bit	N
	Rocky Linux	Rocky Linux 9.0 64-bit	N
		Rocky Linux 8.5 64-bit	N
		Rocky Linux 8.4 64-bit	N
	CentOS Stream	CentOS Stream 9 64-bit	Y
		CentOS Stream 8 64-bit	Y
	CoreOS	CoreOS 2079.4.0 64-bit	N
	openEuler	openEuler 22.03 64-bit	Y
		openEuler 20.03 64-bit	Y
	Others	FreeBSD 11.0-RELEASE 64-bit	N
Arm	Huawei Cloud EulerOS	Huawei Cloud EulerOS 2.0 Standard Edition 64-bit (40 GB)	Y
	Ubuntu	Ubuntu 18.04 server 64-bit	Y
	CentOS	CentOS 7.6 64-bit with Arm	N
	EulerOS	EulerOS: 2.8 64-bit with Arm	N
	Debian	Debian 10.2.0 64-bit with Arm	N
	Kylin OS	Kylin Linux Advanced Server for Kunpeng V10	N
	openEuler	openEuler 20.03 64-bit with Arm	N

VM Architecture	OS Type		Supported by holmes-agent (Y/N)
Windows	Windows2012	Windows Server 2012 R2 Datacenter 64-bit English	N
		Windows Server 2012 R2 Standard 64-bit English	N
		Windows Server 2012 R2 Datacenter 64-bit Chinese	N
		Windows Server 2012 R2 Standard 64-bit Chinese	N
	Windows2016	Windows Server 2016 Datacenter 64-bit English (40 GB)	Y
		Windows Server 2016 Standard 64-bit English (40 GB)	Y
		Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	Y
		Windows Server 2016 Standard 64-bit Chinese (40 GB)	Y
	Windows2019	Windows Server 2019 Datacenter 64-bit English (40 GB)	Y
		Windows Server 2019 Standard 64-bit English (40 GB)	Y
		Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	Y
		Windows Server 2019 Standard 64-bit Chinese (40 GB)	Y
	Windows2022	Windows Server 2022 Datacenter 64-bit Chinese (40 GB)	Y
		Windows Server 2022 Standard 64-bit Chinese (40 GB)	Y

VM Architecture	OS Type		Supported by holmes-agent (Y/N)
		Windows Server 2022 Datacenter 64-bit English (40 GB)	Y
		Windows Server 2022 Standard 64-bit English (40 GB)	Y

ECS Diagnosis

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Trouble Diagnosis**.

Step 3 Click **Diagnose Now** on the **Diagnose ECS** card.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 7-2 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong

Parameter	Description	Example Value
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Select **I agree to install the plug-in and collect data based on the Guest OS Diagnosis Service Frontend Data Collection License.** and click **OK**.

Step 6 Click **OK**.

After the diagnosis is complete, view the diagnosis report.

----End

7.1.3 Diagnosing RDS DB Instances

Scenarios

By analyzing memory usage, disk performance metrics, and slow SQL data, you can quickly understand the overall running status of RDS and acquire troubleshooting suggestions.

Precautions

RDS diagnosis can be performed only for instances.

Diagnosing RDS DB Instances

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Trouble Diagnosis**.

Step 3 Click **Diagnose Now** on the **Diagnose RDS** card.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 7-3 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	RDS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Click **OK**.

After the diagnosis is complete, view the diagnosis report.

----End

7.1.4 Diagnosing DCS Instances

Scenarios

By collecting and analyzing metrics such as flow control, memory usage, and command duration statistics, you can quickly learn about the overall usage of DCS and acquire troubleshooting methods.

Precautions

DCS diagnosis can be performed for Redis instances in the last seven days. The diagnosis time spans only 10 minutes.

Diagnosing DCS Instances

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Trouble Diagnosis**.

Step 3 Click **Diagnose Now** on the **Diagnose DCS** card.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 7-4 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	DCS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Modify the diagnosis time range in the diagnosis configuration area.

Step 6 Click **OK**.

After the diagnosis is complete, view the diagnosis report.

----End

7.1.5 Diagnosing DMS Instances

Scenarios

By collecting memory and CPU usage and analyzing message congestion and traffic, you can quickly learn about the overall usage of DMS and acquire troubleshooting suggestions.

Precautions

DMS diagnosis can be performed only for Kafka instances.

Diagnosing DMS Instances

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Trouble Diagnosis**.

Step 3 Click **Diagnose Now** on the **Diagnose DMS** card.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 7-5 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	DMS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Select the consumer group and topic in the diagnosis configuration area.

Step 6 Click **OK**.

After the diagnosis is complete, view the diagnosis report.

----End

7.1.6 Diagnosing ELB Instances

Scenarios

ELB diagnosis helps you detect abnormal backend servers and provides rectification suggestions, improving load balancing efficiency.

Precautions

ELB diagnosis can be performed only for backend servers that have been associated with listeners.

Diagnosing ELB Instances

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Trouble Diagnosis**.

Step 3 Click **Diagnose Now** on the **Diagnose ELB** card.

Step 4 Click **Add** and configure the parameters on the **Select Instance** dialog box.

Table 7-6 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. ● **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**. ● Auto select all: This option is not supported currently.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. ● **CloudCMDB resources**: Select an instance from the resource list. ● **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The default value is used and cannot be changed.	ELB
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

Step 5 Select the server in the diagnosis configuration area.

Step 6 Click **OK**.

After the diagnosis is complete, view the diagnosis report.

----End

7.2 Alarms

7.2.1 Overview

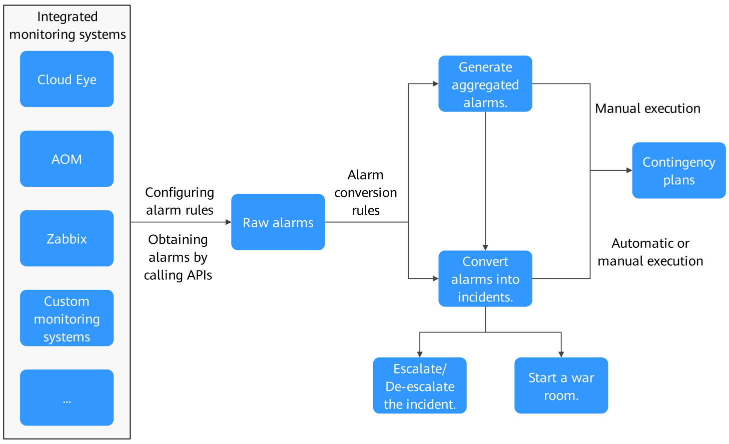
You can use collect, aggregate, and convert alarm data, and configure and manage alarm rules.

Core Features

- **Integrating alarm sources to generate raw alarms**: This function can integrate multiple existing or third-party monitoring systems (such as Cloud Eye, AOM, and Prometheus) and collect scattered alarm data from services to generate raw alarms. You can enable or disable existing alarm sources or connect to third-party monitoring systems on the **integration management** page.
- **Generating aggregated alarms based on transfer rules**: You can set **alarm conversion rules** to aggregate multiple raw alarms that match a specific rule into one alarm, which is called an aggregated alarm.
- **Handling aggregated alarms and restoring resources and applications**: For aggregated alarms, you can convert them to incident tickets, or execute scripts and jobs to clear the alarms, and automatically notify the corresponding owner. Aggregated alarms reduce repeated alarms and avoid alarm storms, improving alarm handling efficiency.
- **Alarm rule management**: This function helps you efficiently create and manage alarm rules. It provides the alarm rule configuration capability across accounts and regions, helping you improve the batch configuration efficiency. Currently, alarm rules can be configured only for Cloud Eye alarms.

Note that the initial aggregated alarm is the active alarm. After you handle the aggregated alarm, convert it to an incident, or clear the alarm, it will be moved to the historical alarm list.

Figure 7-1 Alarm management process


Integrated monitoring systems
Cloud Eye
AOM
Zabbix
Custom monitoring systems
...
Configuring alarm rules
Obtaining alarms by calling APIs
Raw alarms
Alarm conversion rules
Generate aggregated alarms.
Convert alarms into incidents.
Manual execution
Contingency plans
Automatic or manual execution
Escalate/ De-escalate the incident.
Start a war room.

7.2.2 Handling Alarms

Scenarios

After an aggregated alarm is generated, you can quickly handle it on COC and apply the response solution using jobs or scripts.

Precautions

Only the owner can handle the current alarm.

Handling Alarms

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**.

Step 3 Choose **Aggregated Alarms** > **Unhandled Alarms**.

Step 4 Select the alarm to be handled and choose **More** > **Handle** in the **Operation** column.

Step 5 Configure information in **Task Type**.

- If you select **Contingency Plans**, select the corresponding contingency plan from the drop-down list. If there is no desired contingency plan, click **Create**. For details, see **Creating a Custom Contingency Plan**.
  - If you select a document-based contingency plan, you can view the name and description of the contingency plan step. No operation is required.

  - – If you select an automatic contingency plan, you need to set a contingency plan to be executed. Based on the handling mode (custom script, public script, custom job, or public job), perform the remaining steps by referring to **Executing a Custom Script**, **Executing a Public Script**, **Executing a Custom Job**, or **Executing a Public Job**.
- If you select **Scripts**, perform subsequent steps by referring to **6.2.5 Executing Custom Scripts** or **6.2.6 Executing Public Scripts**.
- If you select **Jobs**, perform the subsequent steps by referring to **6.3.6 Executing Custom Jobs** or **6.3.2 Executing Public Jobs**.

Step 6 Click **OK**.

The alarm is handled.

----End

7.2.3 Converting an Alarm to an Incident

Scenarios

After an aggregated alarm is generated, you can convert the aggregated alarm to an incident on COC. After the alarm is converted to an incident, an incident ticket is generated and the actual ticket number is displayed in the **Associated Event Ticket No.** column. You can click the ticket number to view its details. You can accept, reject, transfer, or handle the incident ticket.

Precautions

Only the owner of an alarm can convert the alarm to an incident.

Converting an Alarm to an Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**.

Step 3 Choose **Aggregated Alarms** > **Unhandled Alarms**.

Step 4 Select the alarm to be handled and click **Convert Alarms to Incidents** in the **Operation** column.

Step 5 Set parameters in **Convert Alarms to Incidents**.

Table 7-7 Parameters for converting an alarm to an incident

Parameter	Description
Enterprise Project	Select an enterprise project from the drop-down list.
Fault Occurrence Time	Enter the time when the fault occurs.
Application	Select a faulty application from the drop-down list.

Parameter	Description
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Service Interrupted	The options are **Yes** and **No**.
Incident Category	Select an incident category from the drop-down list.
Incident	Customize the incident name according to the naming rules.
Description	Describe the incident.

Step 6 Click **OK**.

The alarm is converted to an incident.

----End

7.2.4 Clearing Alarms

Scenarios

After an aggregated alarm is generated, it will be displayed on the **Unhandled Alarms** tab page. If the alarm has been handled or needs to be cleared for other reasons, you can clear the alarm on the **Unhandled Alarms** tab page. You can view the cleared aggregated alarm on the **Historical Alarms** tab page.

Precautions

Only the owner can clear current alarms.

Alarm data is retained for 31 days and will be automatically cleared, including data on the **Historical Alarms** tab page.

Clearing Alarms

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**.

Step 3 Choose **Aggregated Alarms** > **Unhandled Alarms**.

Step 4 Select the alarm to be cleared and click **Clear** in the **Operation** column.

Step 5 Set parameter for clearing the alarm.

Table 7-8 Parameters for clearing alarms

Parameter	Description
Service Interrupted	The options are **Yes** and **No**.
Fault Occurrence Time	This parameter is required only when **Service Interrupted** is set to **Yes**. Enter the time when the fault occurs.
Fault Recovery Time	This parameter is required only when **Service Interrupted** is set to **Yes**. Enter the time when the fault is rectified.
Remarks	(Optional) Enter remarks. The remarks can contain at most 100 characters, including letters, digits, and special characters.

NOTE

The time from the occurrence of a fault to the recovery of the fault is called the service interruption time. COC can automatically record the service interruption time entered in **Clearing alarms** in the SLO interruption record of the corresponding application. The procedure is as follows:

1. Create an SLA rule and set **Trigger Type** to **Alarm Ticket**. Choose the severity level and applications (including the aggregated alarm severity level and application).
2. Create an SLO rule and select applications (including the aggregated alarm application).
3. After an aggregated alarm is generated, if the severity and application match the SLA record settings, an SLA record is created.
4. Clear the aggregated alarm, enter the fault occurrence time and fault recovery time, generate an SLO interruption record, and view the interruption record in the **Operation** column of the corresponding SLO rule.

Step 6 Click **OK**.

The alarm is cleared.

----End

7.2.5 Viewing Historical Alarms

Scenarios

Historical alarms display cleared aggregated alarms. After an aggregated alarm is cleared, you can view the information and handling records of the aggregated alarm on the **Historical Alarms** tab.

Precautions

The system retains alarm data for 31 days. After this period, the data will be automatically deleted.

Viewing Historical Alarms

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**.

Step 3 Choose **Aggregated Alarms** > **Historical Alarms**.

View the integrated alarm list.

Step 4 Locate the target alarm and choose **More** > **History** in the **Operation** column.

View the historical records of the current alarm.

----End

7.2.6 Viewing Raw Alarms

Scenarios

Raw alarms are generated based on the alarm information collected from multiple existing or third-party monitoring systems (such as Cloud Eye, AOM, and Prometheus). The original alarm list displays the alarm source name, alarm status, alarm severity, alarm source, and associated application.

You can create an alarm conversion rule to aggregate one or more raw alarms into a single aggregated alarm. One original alarm can trigger multiple alarm conversion rules.

Precautions

By default, the page displays alarm information of the last 31 days. Expired alarms are automatically cleared.

Viewing Raw Alarms

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**.

Step 3 On the **Original Alarm** tab, click an alarm name.

View the original alarm details.

----End

7.3 Incident Management

7.3.1 Overview

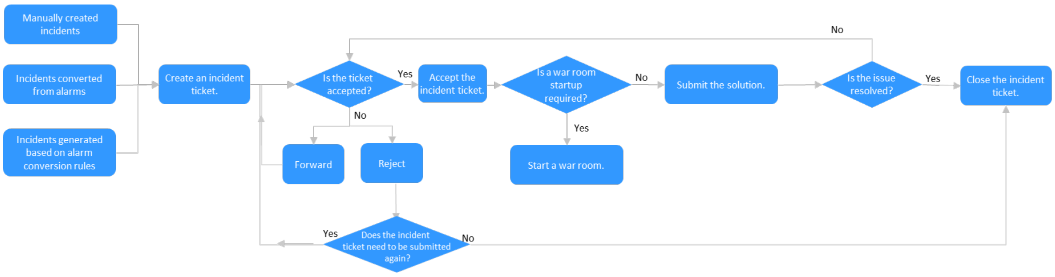
The incident management module manages all incidents of applications, including incident acceptance and rejection, ticket conversion, processing, and closing. Incidents can be generated based on alarm conversion rules, or created by users or based on alarms.

You can also configure SLA rules. For details about how to configure SLA rules, see **11.5 SLA Management**.

Incident Handling Process

- After an incident is created, it is in the unaccepted state. You can forward, reject, or accept the incident.
- After an incident ticket is rejected, it becomes the rejected state. The creator can close the incident or update the incident information and submit it again.
- After being accepted, an incident ticket is in the accepted state. You can perform operations such as incident handling, escalation and de-escalation, add remarks, and war room startup. After an incident ticket is processed, it becomes the resolved and to be verified state. You can perform the verification operation. If the verification is successful, the incident ticket becomes the completed state. If the verification fails, the incident ticket becomes the accepted state again.
- For details about how to customize incident levels, categories, review rules, and fault review rules, see **Basic Configuration - Incident Ticket Process**.

Figure 7-2 Incident management process


Manually created incidents
Incidents converted from alarms
Incidents generated based on alarm conversion rules
Create an incident ticket.
Is the ticket accepted?
Yes
No
Accept the incident ticket.
Is a war room startup required?
No
Yes
Submit the solution.
Is the issue resolved?
Yes
No
Close the incident ticket.
Forward
Reject
Start a war room.
Does the incident ticket need to be submitted again?
Yes
No

7.3.2 Creating an Incident Ticket

Scenarios

COC provides multiple methods to generate incidents to record faults. If converting aggregated alarms to incidents or automatically generating incidents from raw alarms doesn't meet your needs, you can manually create incidents.

Prerequisites

You have created an application by referring to **4 Application Management**.

Precautions

Create an incident service ticket.

Creating an Incident Ticket

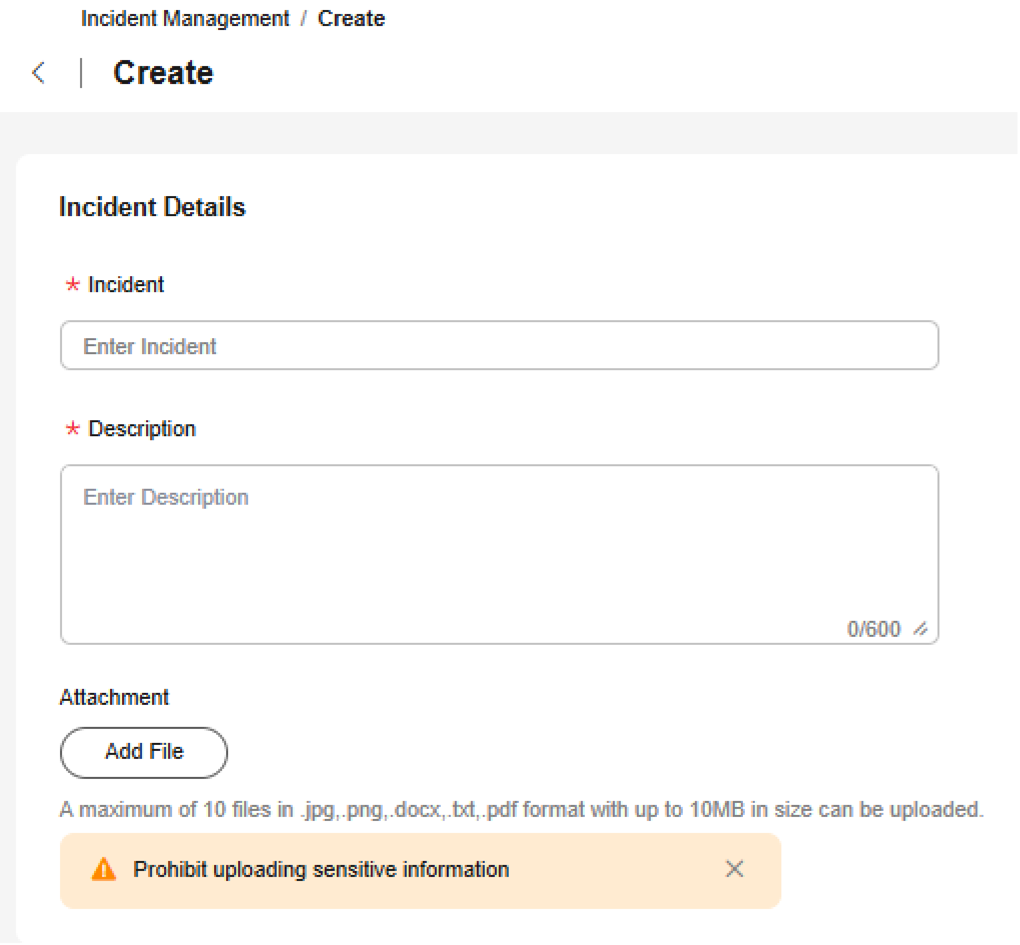
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 Click **Create** in the upper right corner.

Step 4 Set parameters.

Figure 7-3 Incident details



Incident Management / Create

Create

Incident Details

* Incident

Enter Incident

* Description

Enter Description

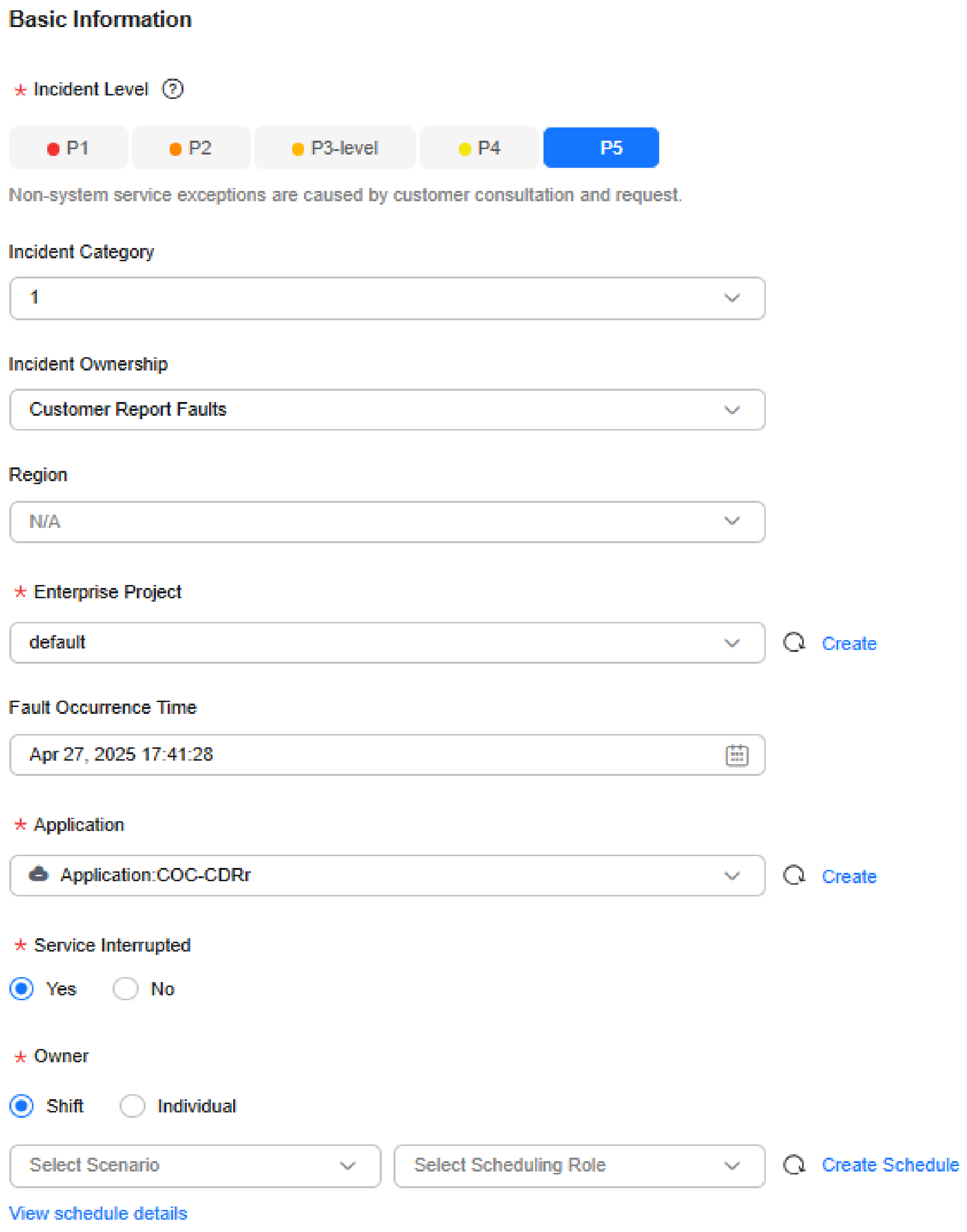
0/600

Attachment

A maximum of 10 files in .jpg,.png,.docx,.txt,.pdf format with up to 10MB in size can be uploaded.

Prohibit uploading sensitive information

Figure 7-4 Basic information



Basic Information

* Incident Level

● P1 ● P2 ● P3-level ● P4 P5

Non-system service exceptions are caused by customer consultation and request.

Incident Category: 1

Incident Ownership: Customer Report Faults

Region: N/A

* Enterprise Project: default

Fault Occurrence Time: Apr 27, 2025 17:41:28

* Application: Application:COC-CDRr

* Service Interrupted: ● Yes ○ No

* Owner: ● Shift ○ Individual

Table 7-9 Parameters for creating an incident ticket

Parameter	Description
Incident	Enter a custom incident name.
Description	Describe the incident.
Attachment	Click **Add File** to upload incident-related attachments. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.

Parameter	Description
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. Default incident levels: **P1**: Core service functions are unavailable, affecting all customers. **P2**: Core service functions are affected, affecting the core services of some customers. **P3**: An error is reported for non-core service functions, affecting some customer services. **P4**: Non-core service functions are faulty. The service latency increases, the performance deteriorates, and user experience decrease. **P5**: Non-core service exception occurs, which is customer consultation or request issue.
Incident Ownership	(Optional) Select the incident to which the ticket belongs from the drop-down list. ● Alarm detection ● Customer fault reporting ● Proactive O&M ● Other
Incident Category	(Optional) Select an incident category from the drop-down list.
Region	This parameter is optional. The default value is **N/A**. Select the region where the event occurs from the drop-down list.
Enterprise Project	Select an enterprise project from the drop-down list.
Fault Occurrence Time	Enter the time when the fault occurs.
Application	Select the application affected by the incident from the drop-down list.
Service Interrupted	The options are **Yes** and **No**.
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.

Step 5 Click **OK**.

The incident ticket is created.

----End

7.3.3 Rejecting an Incident Ticket

Scenarios

After an incident ticket is created, the incident handler can reject it if it is unreasonable or due to other reasons. If rejected, the incident creator can either modify and submit the incident ticket or close it.

Rejecting an Incident

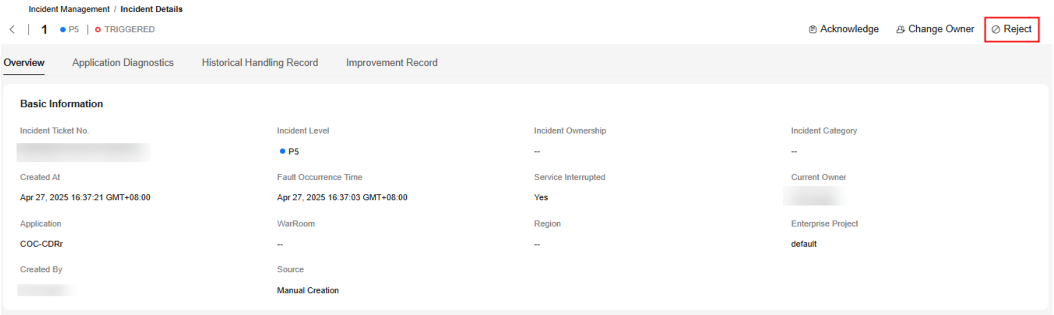
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Reject** in the upper right corner.

Figure 7-5 Rejecting an incident ticket

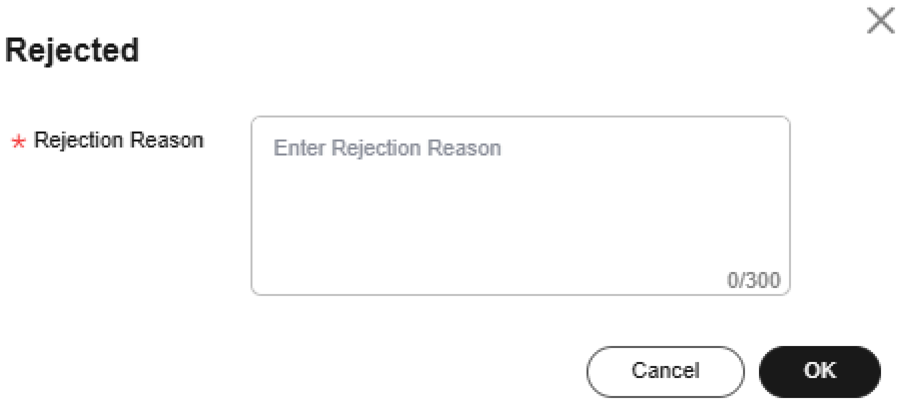


Basic Information

Incident Ticket No.: [redacted]
Incident Level: ● P5
Incident Ownership: --
Incident Category: --
Created At: Apr 27, 2025 16:37:21 GMT+08:00
Fault Occurrence Time: Apr 27, 2025 16:37:03 GMT+08:00
Service Interrupted: Yes
Current Owner: [redacted]
Application: COC-CDRr
WarRoom: --
Region: --
Enterprise Project: default
Created By: [redacted]
Source: Manual Creation

Step 5 Enter the rejection reason and click **OK**.

Figure 7-6 Entering the reason for rejecting the incident ticket



----End

7.3.4 Restarting an Incident

Scenarios

After an incident ticket is rejected, the incident applicant can edit and resubmit it.

Restarting an Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Re-opening** in the upper right corner.

Step 5 Set parameters for changing the incident ticket.

Table 7-10 Parameters for changing the incident ticket

Parameter	Description
Incident	Customize the incident name according to the naming rules.
Description	Describe the incident.
Attachment	Click **Add File** to upload incident-related attachments. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. **NOTE** The incident levels are defined as follows: **P1**: Core service functions are unavailable, affecting all customers. **P2**: Core service functions are affected, affecting the core services of some customers. **P3**: An error is reported for non-core service functions, affecting some customer services. **P4**: Non-core service functions are faulty. The service latency increases, the performance deteriorates, and user experience decrease. **P5**: Non-core service exception occurs, which is customer consultation or request issue.
Incident Category	(Optional) Select an incident category from the drop-down list.

Parameter	Description
Incident Ownership	(Optional) Select the incident to which the ticket belongs from the drop-down list. ● Alarm detection ● Customer fault reporting ● Proactive O&M ● Other
Region	(Optional) The default value is **N/A**. Select the region where the event occurs from the drop-down list.
Enterprise Project	Select an enterprise project from the drop-down list.
Fault Occurrence Time	Enter the time when the fault occurs.
Application	Select the application affected by the incident from the drop-down list.
Service Interrupted	The options are **Yes** and **No**.
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.

Step 6 Click **OK**.

The incident ticket is restarted. The incident status changes to unaccepted.

----End

7.3.5 Forwarding Incidents

Scenarios

If an incident belongs to another application or needs be handled by an O&M expert, you can forward the incident to the corresponding owner.

Forwarding Incidents

Step 1 Log in to **COC**.

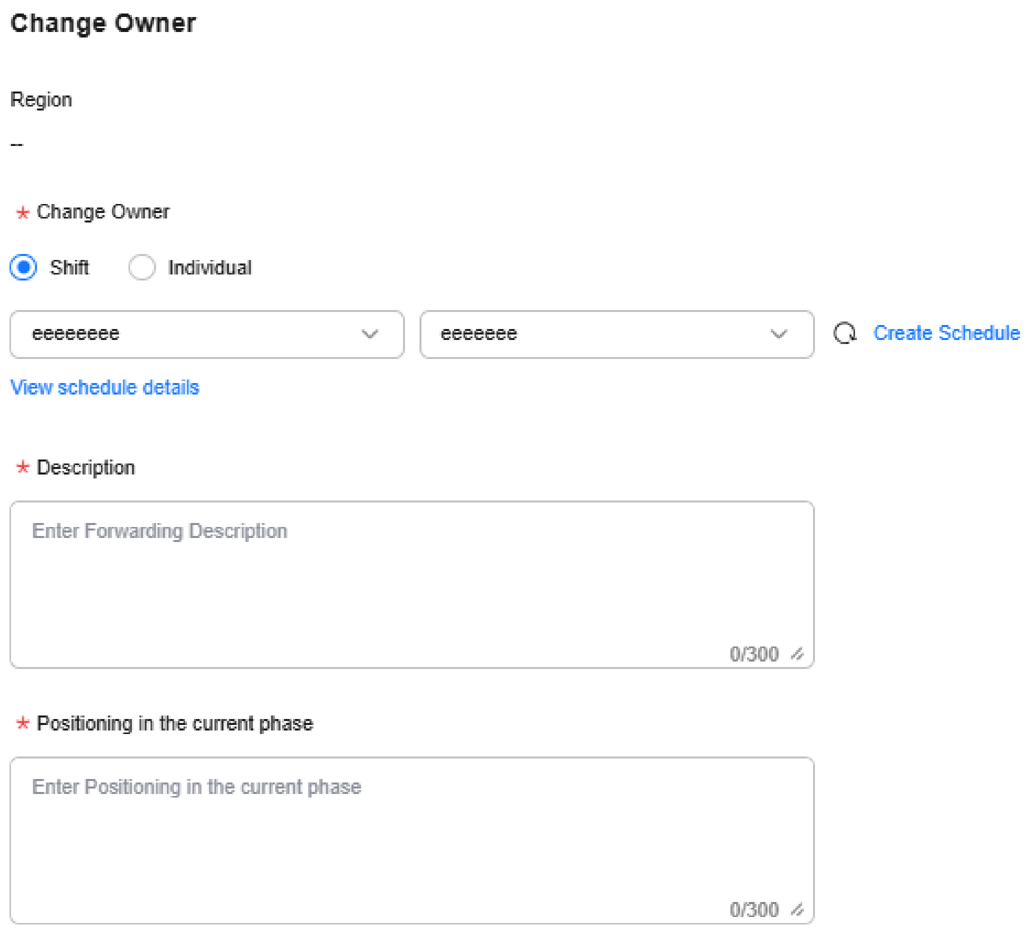
Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Change Owner** in the upper right corner.

Step 5 Set parameters.

Figure 7-7 Configuring the change owner



Change Owner

Region

--

* Change Owner

● Shift ○ Individual

eeeeeeee | eeeeeee

* Description

Enter Forwarding Description 0/300

* Positioning in the current phase

Enter Positioning in the current phase 0/300

Table 7-11 Parameters for changing the owner

Parameter	Description
Change Owner	Select **Shift** or **Individual**. - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. - **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.
Description	Enter description for changing the owner.
Positioning in the current phase	Provide information about positioning in the current phase.

Step 6 Click **OK**.

The incident owner is changed to the specified incident forwarding owner.

----End

7.3.6 Acknowledging an Incident

Scenarios

After an incident is created, the incident owner analyzes the incident. If the issue exists, the incident owner acknowledges and handles the incident.

Acknowledging an Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Acknowledge** in the upper right corner.

The incident status changes to **ACKNOWLEDGED**.

----End

7.3.7 Escalating and De-escalating Incident Tickets

Scenarios

If the incident level is inconsistent with the actual situation during incident handling, you can escalate or de-escalate the incident. Note: The incident level can be changed only after the incident is acknowledged. You can add an approval flow for incident downgrade. For details, see **Reviewing an Incident**. Once configured, the approver must approve or reject the incident downgrade request if it meets the conditions.

Escalating and De-escalating an Incident Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Upgrade and Downgrade** in the upper right corner.

Step 5 Set parameters.

Table 7-12 Parameters for escalating and de-escalating an incident ticket

Parameter	Description
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. **NOTE** Default incident levels: **P1**: Core service functions are unavailable, affecting all customers. **P2**: Core service functions are affected, affecting the core services of some customers. **P3**: An error is reported for non-core service functions, affecting some customer services. **P4**: Non-core service functions are faulty. The service latency increases, the performance deteriorates, and user experience decrease. **P5**: Non-core service exception occurs, which is customer consultation or request issue.
Description	Enter the service impact and reason for the escalation or de-escalation.

Step 6 Click **OK**.

The incident is escalated or de-escalated. If a downgrade approval flow is added for an incident, the approver must review the downgrade application that meets the conditions.

----End

7.3.8 Adding Remarks

Scenarios

When handling an incident, you can add remarks if needed.

Prerequisites

Remarks can be added only after an incident is acknowledged.

Adding Remarks

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Add Remark** in the upper right corner.

Step 5 Add remarks.

- **Remarks**: Enter remarks.

Step 6 Click **OK**.

The incident remarks are added.

----End

7.3.9 Starting a War Room

Scenarios

When handling an incident, if you determine the fault is a major one or affects a group, start a war room to address the issue and work with application experts to fix it quickly.

Precautions

If a group (WeCom, Lark, or DingTalk group) needs to be added when a war room is started, configure the following information:

- Configure applications by referring to **11.4 Managing Mobile Apps**.
- Configure the WeCom email address by referring to **11.1.1 Overview**.
- If **Shift** is selected, you need to **create a shift schedule** and **add O&M engineers to it**. Then the WeCom accounts will be added when the war room setup rule is met.

Starting a War Room

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Start WarRoom** in the upper right corner.

Step 5 Set parameters.

Table 7-13 Parameters for starting a war room

Parameter	Description
WarRoom Name	The default value is the incident ticket name. You can customize one.
WarRoom Description	Description of the war room.
WarRoom Management	Select a user from the drop-down list as the war room administrator.
Region	(Optional) Select a region for the war room from the drop-down list box. You can select multiple regions.
Enterprise Project	Select an enterprise project from the drop-down list.
Application	Select an affected application from the drop-down list. You can select multiple applications.

Parameter	Description
Mode of creating a group	The options are **Enterprise WeChat**, **DingTalk**, and **Lark**. Configure the application notification method in **Mobile App Management**. After the notification method is selected, the war room will add the scheduling personnel and participants to the corresponding group.
Shift	Select a value from the drop-down list box based on the configured shift scenario and role. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
Participant	Select a participant from the drop-down list. You can select multiple participants.

Step 6 Click **Submit**.

The war room is started.

----End

7.3.10 Handling an Incident

Scenarios

Once an incident is handled and the cause is found, you can quickly run the contingency plan, script, or job to fix the issue and record the details.

You can view the associated raw alarms in the incident details for the incident whose source is **alarm**.

Executing a Contingency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Select a value for the contingency plan.

- If you select **Contingency Plans**, select the corresponding contingency plan from the drop-down list box and click **Execute Contingency Plan**.

  Go to **5**.

  If there is no desired contingency plan, click **Create**. For details, see **Creating a Custom Contingency Plan**.

- If you select **Scripts**, select the desired script from the drop-down list and click **Execute Contingency Plan**.

  Go to **7**.

If there is no desired script, click **Create Scripts**. For details, see **6.2.3 Creating Custom Scripts**.

- If you select **Jobs**, select the desired job from the drop-down list and click **Execute Contingency Plan**.

  Go to **8**.

  If there is no desired job, click **Create jobs**. For details, see **6.3.4 Creating Custom Jobs**.

Step 5 Confirm the steps for contingency plan and click **OK**.

Step 6 Check the task type associated with the contingency plan.

- If the task type is **Scripts**, go to **7**.
- If the task type is **Jobs**, go to **8**.

Step 7 Set the execution script.

- **Script Input Parameters**: The parameter name and default value have been preset when you import a custom script.
- **Executed By**: **root** is set by default. It is the user who executes the script on a target instance node.
- **Timeout Interval**: **300** is set by default. It indicates the timeout interval for executing the script on a single target instance.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 7-14 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances you want to execute are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. If the number of failed hosts meets or exceeds this rate, the service ticket status changes to abnormal, and the ticket stops executing.
  - The success rate ranges from 0 to 100 and is accurate to one decimal place.

Skip step **8** and perform step **9**.

Step 8 Set parameters for executing a job.

- **Region**: Select the region where the target instance is located.
- **Target Instance Mode**: Select the execution mode of job step and target instances.
  - **Consistent for all steps**: All tasks are executed on the selected instance using the same batch policy.
  - **Unique for each step**: Tasks in one step are executed on the selected instance. Each step uses a batch policy.
  - **Unique for each task**: Set the target instance and batch policy for each task.
- **Job Execution Procedure**: Customize job details.
  - Click the job name. The **Modifying Parameters** drawer is displayed on the right.
  - Set **Input**, **Output**, and **Troubleshooting**.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 7-15 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All

Parameter	Description	Example Value
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	The default parameter cannot be modified and is determined by **Region** in **Execution Content**.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances you want to execute are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

Step 9 Click **OK**.

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    ii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

Setting Incident Handling Details

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Handle Incident** in the upper right corner and set parameters.

Table 7-16 Parameters for handling incidents

Parameter	Description
Incident Category	(Mandatory) Select an incident category from the drop-down list.
Service Interrupted	(Mandatory) The options are **Yes** and **No**.
Fault Occurred	Enter the time when the fault occurs. This parameter is mandatory when **Service Interrupted** is set to **Yes**.
Delimited Completion Time	Enter the issue or fault locating completion time.
Fault Recovery Time	Enter the fault recovery time. This parameter is mandatory when **Service Interrupted** is set to **Yes**.
Cause	Enter the cause for the incident.
Solution	Enter the solution for the incident.
Add File	Click **Add File** to upload incident-related attachments. You can upload maximum of 10 files, each no more than 10 MB. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF.

Step 5 Click **OK**.

Incident handling details are set.

----End

7.3.11 Verifying Incident

Scenarios

After handling an incident, check if the issue is fixed or the desired outcome is met and record the verification result in **Verify Incident Closure**. If you select **Unresolved**, reject the incident. When the incident is rejected, the handler must locate and handle the issue again.

Verifying Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click **Verify Incident Closure** in the upper right corner.

Step 5 Set parameters.

Table 7-17 Parameters for **Verify Incident Closure**

Parameter	Description
Verification Conclusion	The options are **Resolved** and **Unresolved**. If you select **Unresolved**, the incident will be rejected and the incident process status changes to **Pending**.
Description	Enter incident-related description.

Step 6 Click **OK**.

The incident is verified.

----End

7.3.12 Creating an Improvement Ticket For An Incident

Scenarios

If there are product or O&M improvement items during the handling of an incident ticket, you can create an improvement ticket to follow up the handling.

Prerequisites

An improvement ticket can be created only after the incident is accepted.

Creating an Improvement Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 On the **Pending** tab page, select the target incident ticket and click its title.

Step 4 Click ··· > **Create Improvement Ticket** or **Create Improvement Ticket** in the upper right corner.

Step 5 Set parameters.

Table 7-18 Parameters for creating an improvement ticket

Parameter	Description
Improvement Ticket	Name of the improvement ticket.
Application	Select an application for which the improvement is performed from the drop-down list.
Type	Select an improvement type from the drop-down list.
Improvement Owner	Select an owner from the drop-down list.
Improvement Acceptor	Select an acceptance user from the drop-down list.
Expected Completion	Enter the expected completion time. You can select a day. The time cannot be earlier than the current day.
Symptom	Enter the symptom related to the incident. The value can contain a maximum of 1,000 characters.
Improvement Ticket Closure Criteria	Enter the improvement closure criteria. The value can contain a maximum of 1,000 characters.

Step 6 Click **OK**.

The improvement ticket is created. On the incident details page, click **Improvement Record** to view the improvement ticket status and current owner. Click the improvement ticket name to go to the improvement management page and handle the improvement ticket.

----End

7.3.13 Managing Fault Review Tasks

Scenarios

After an incident is confirmed, a fault report is automatically created using fault review rules. We review the fault using this report to stop it from happening again. The fault review information includes more than 15 analysis items, such as fault symptom, fault impact, fault handling process, root cause analysis, solution, similar faults, and improvement measures.

By default, incidents of the P1, P2, P3, and P4 levels and incidents of all levels for which a war room is started need to be reviewed. This rule can be modified in **Fault Review Rules**.

Completing Fault Review

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 Click the **All incident Tickets** tab.

Step 4 Select the incident ticket to be reviewed and click **Fault Report** in the **Fault Report/Status** column.

The system automatically fills the basic information about the incident ticket in review report, such as the fault symptom, troubleshooting process, and fault cause. The information can be modified.

Step 5 Click **Edit Report** in the upper right corner.

Step 6 Set parameters in **Fault Information**.

Table 7-19 Fault parameters

Parameter	Description
Report Title	Customize the title of the fault report.
Responsible person for fault handling	Select the fault owner from the drop-down list.
Symptom	Enter the fault symptom. The value can contain a maximum of 1,000 characters.
Affected Customers	Enter the affected customer. The value can contain a maximum of 1,000 characters.
Affected Application	Enter how the application is affected. You can add and delete the affected application.

Step 7 Set parameters in **Process**.

Table 7-20 Parameters for the handling process

Parameter	Description
Procedure	Set the handling time and process description. You can add and delete a handling process.

Step 8 Set parameters in **Root cause analysis**.

Table 7-21 Parameters for a root cause analysis

Parameter	Description
Root cause analysis	Analyze the root cause for the fault. Click **Add File** to upload attachments related to root cause analysis. You can upload maximum of 10 files, each no more than 10 MB. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF.

Step 9 Set parameters in **Monitoring & Alerting**

Table 7-22 Parameters for monitoring alarms

Parameter	Description
Is it prioritized over customer discovery	The options are **Yes** and **No**.
Alarm Ticket ID	This parameter is mandatory when **Is it prioritized over customer discovery** is set to **Yes**. You can add or delete alarms.

Step 10 Set change parameters.

Table 7-23 Parameter changes

Parameter	Description
Change Involved	The options are **Yes** and **No**.
Change Ticket No.	This parameter is mandatory when **Change Involved** is set to **Yes**. You can add and delete change tickets.

Step 11 Set parameters in **Solution**.

Table 7-24 Solution parameters

Parameter	Description
Short term solution (how to recover from faults)	Enter the short-term solution to the fault. Click **Add File** to upload attachments related to the short-term solution. You can upload maximum of 10 files, each no more than 10 MB. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF.
Long term plan (how to avoid recurrence)	Enter the long-term solution to the fault. Click **Add File** to upload attachments related to the long-term solution. You can upload maximum of 10 files, each no more than 10 MB. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF.
Application Resilience Related Planning and Analysis	Enter the application resilience planning and analysis. Click **Add File** to upload attachments related to application resilience. You can upload maximum of 10 files, each no more than 10 MB. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF.

Step 12 Set a failure mode.

Table 7-25 Failure mode parameters

Parameter	Description
Is there a failure mode	The options are **Yes** and **No**.
Failure Modes	This parameter is mandatory when **Is there a failure mode** is set to **Yes**. You can add or delete failure modes.

Step 13 Set a contingency plan.

Table 7-26 Contingency plan parameters

Parameter	Description
Contingency Plan Available	The options are **Yes**, **No**, and **N/A**.
Contingency Plan	This parameter is mandatory when **Is there a failure mode** is set to **Yes**. Contingency plans can be added or deleted.

Step 14 Set parameters in **Failure Modes**.

Table 7-27 Parameters for failure modes

Parameter	Description
Is there a failure mode	The options are **Yes** and **No**.
Incident Ticket ID	This parameter is mandatory when **Is there a failure mode** is set to **Yes**. You can add or delete an incident.

Step 15 Set parameters for fault drills.

Table 7-28 Parameters for fault drills

Parameter	Description
Any Fault Drill Conducted	The options are **Yes**, **No**, and **N/A**.
Fault Drills	This parameter is mandatory when **Any Fault Drill Conducted** is set to **Yes**. You can add and delete drill tasks.

Step 16 Set parameters in **Improvement Measures**.

Table 7-29 Parameters for improvement measures

Parameter	Description
Product Improvement	Enter the product improvement details. You can create or delete product improvement tickets.
Operations Improvement	Enter the operations improvement details. You can create or delete operations improvement tickets.
Management Improvement	Enter the management improvement details. You can create or delete management improvement tickets.

Step 17 Click **OK**.

Step 18 Set **Fault review progress**.

- **Fault review progress**: The value can be **Reviewed**, **Reviewing in progress**, or **Not Reviewed**.

Step 19 Click **OK**.

The fault review is complete.

----End

7.3.14 Diagnosing Applications

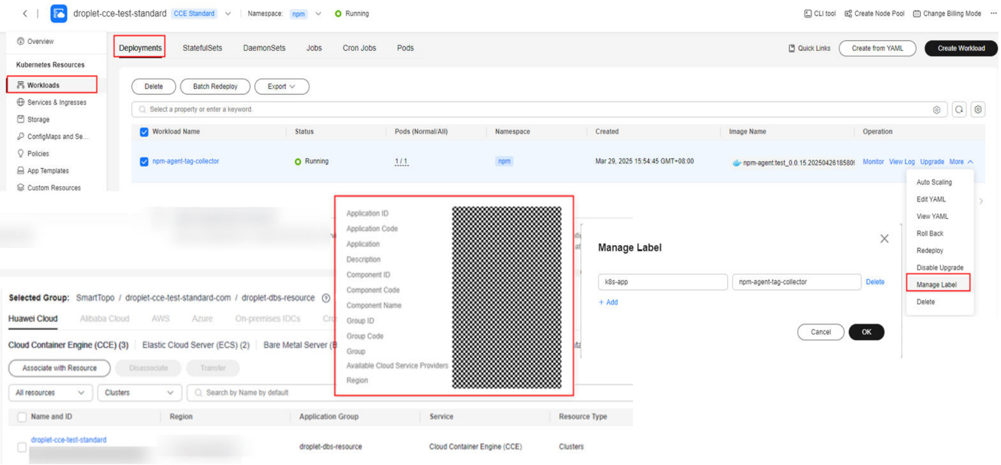
Scenarios

After an incident is created, you can use the full-link fault diagnosis function to quickly locate the root cause of the fault. You can view the relationship topology of the application layer, component layer, and resource layer for customer applications and abnormal data based on resources and application alarms. Capabilities of viewing core resource metrics and diagnosing instances are provided.

Prerequisites

- You have performed the operations described in **4.2 Creating an Application**, **4.12 Manually Associating Resources with an Application**, and **4.5 Managing Application Topologies** on CloudCMDB.
- CES has been connected. You can configure CES monitoring by referring to **Integration Management**.
- An incident ticket has been created.
- To display workload and POD information in a CCE cluster, you need to add label to workloads in CCE. (Only one CCE cluster resource can be added to each group. Otherwise, workload information is not displayed.)

Figure 7-8 Configuring CCE workload label



Diagnosing Applications

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 Click the **All incident Tickets** tab.

Step 4 Select the incident ticket to be diagnosed and its title.

Step 5 Click **Application Diagnosis**.

Step 6 Click the time box and set the fault occurrence time.

The time entered in the time box is the end time. The start time is one hour earlier than the end time. After the time is selected, the number of alarms for the application and its sub-applications in the selected time period is displayed on the application topology dashboard, and the application fault details are displayed on the details page on the right.

Step 7 (Optional) Select **Auto Refresh** and select a refresh frequency from the drop-down list.

After **Auto Refresh** is selected, the end time is updated to the current system time based on the refresh frequency.

Step 8 (Optional) If the application has sub-applications, click the target sub-application.

The application topology dashboard displays all components of the sub-application. The sub-application fault details are displayed on the details page on the right. You can switch to other sub-applications on the topology dashboard.

Step 9 Click a component under the application or its sub-application.

The application topology dashboard displays all resources of the component. The component fault details are displayed on the right details page. You can switch to other components on the topology dashboard. Metrics of core cloud services can be displayed. If APM is associated in application management, you can also view link-related metrics.

Step 10 Click **Alarm** on the right of the application topology.

View application alarms. Alarms generated within the time range on the right axis are displayed in the list. When you select a topology object on the left, its alarm information is automatically filtered.

Step 11 Click **Change** on the right of the application topology.

View application changes. Changes within the change time range on the right axis are displayed in the list.

Step 12 Click **Fault Diagnosis** on the right of the application topology.

View the fault diagnosis data for your resources. You can check DCS, RDS, DMS, ECS, and ELB resources. After a topology object is selected on the left, its diagnosis information is automatically filtered.

If no diagnosis task exists or you have created a new one, do the following:

1. Click **Create Diagnosis Task**.
2. Select a resource type and resource.
3. Click **OK**.
4. Read and agree to **Frontend Data Authorization Agreement on Guest OS Diagnosis Service**, and click **Agree**.

> NOTE
>
> You need to sign the agreement only if you select ECSs for fault diagnosis.

After the diagnosis is complete, click **View Details** on the right of the diagnosis result list to view the diagnosis report.

----End

7.3.15 Viewing Incident History

Scenarios

You can view the incident history to see the actions taken on a node during incident handling. This history shows the full incident handling process.

Viewing Incident History

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**.

Step 3 Click **All Incident Tickets**.

Step 4 Select the incident ticket to be viewed and click its title.

Step 5 Click **Historical Handling Record**.

----End

7.4 War Room Management

7.4.1 Overview

When a group or major fault occurs, a war room is set up to provide guidance for quick service recovery. It supports joint operations of O&M engineers, R&D team, and operations personnel for fault handling. You can add fault recovery members to the war room, send the fault progress to the personnel who are concerned about the fault in a timely manner, and use the application diagnosis and response plan to help quickly recover applications.

To set up a war room, you need to connect DingTalk, Lark, or WeCom to **Mobile App Management**.

Procedure

The war room handling process is as follows:

1. Start a war room on the incident handling page in the incident management module by referring to **7.3.9 Starting a War Room**.
2. Locate and rectify the fault by analyzing the fault impact scope and recovering all affected applications.

   If other applications are affected, add the applications by referring to **Adding an Affected Application**.

   You can quickly locate the root cause of the fault in **7.3.14 Diagnosing Applications** and rectify the fault in **9.3 Contingency Plans**. After the fault is rectified, change the application status to restored.
3. Check the fault rectification result and application status.

   Note: The fault can be rectified only after the status of all applications is changed to recovered.

   You can check the fault rectification result and application status through **application diagnosis**. After the fault is rectified, you need to enter basic fault information in the **fault information modification** module.
4. Close the war room after the fault is rectified.

   Note: You can close the war room only after entering all the mandatory information in the **fault information modification** module.

Notes:

- If you need to add members to the group during troubleshooting, see **7.4.5 Adding Engineers to War Rooms**.
- During troubleshooting, if you need to send a notification of the troubleshooting progress to related personnel, see **7.4.6 Updating Progress Notices**.
- If improvement items are identified for some products, O&M, or management during troubleshooting, you can create an improvement ticket and handle the ticket by referring to **7.5.2 Managing Improvement Tickets**.

Prerequisites

There is an incident ticket being handled and **a war room has been started** on the incident handling page.

7.4.2 Viewing the Statuses of War Rooms

Scenarios

After a war room is started, you need to view and update the war room status during fault handling. In this way, you can record the time when a fault is rectified and learn about the fault handling progress. A war room can be in the statuses of **Start**, **Demarcate and Rectify the Fault**, **Confirm Fault Recovery**, and **Finish**.

Viewing the Status of a War Room

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

You can view war rooms on the displayed page.

Step 3 Click the title of the war room you want to view.

The war room details page is displayed. You can view the status of the war room in the upper right corner of the page.

⚠ CAUTION

- Before the fault is rectified, ensure that the affected application is in the restored state.
- Before closing a war room, ensure that the fault information of the war room has been entered.

----End

7.4.3 Modifying Fault Information

Scenarios

Fault information in the war room module records the fault occurrence time, rectification time, impacts, and causes.

You can modify fault information during war room startup, fault demarcation and rectification, and fault rectification.

Modifying Fault Information

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Click **Modify** in the upper right corner.

Step 5 Set **Modify Fault Information**.

Table 7-30 Parameters for modifying fault information

Parameter	Description
Region	(Optional) Select a region from the drop-down list. Multiple regions can be selected. If no region is selected, **Default** is displayed, indicating that no region is required.
Fault Occurred	Enter the time when the fault occurs. The default value is the time when the war room is created. The fault occurrence time cannot be later than the war room creation time.
Fault Recovered	(Optional) This parameter is mandatory when the fault has been rectified. The fault rectification time cannot be earlier than the war room creation time.
Fault Impact	(Optional) This parameter is mandatory when the fault has been rectified. Enter the fault impact. The value can contain a maximum of 250 characters.
Fault Cause	(Optional) This parameter is mandatory when the fault has been rectified. Enter the fault cause. The value can contain a maximum of 250 characters.

Step 6 Click **OK**.

The fault information is modified.

----End

7.4.4 Managing Affected Applications

Scenarios

If an application is affected when a fault occurs, you can add the affected application in the war room details. You can use the application diagnosis function to check affected application details and execute contingency plans to quickly restore applications.

Adding an Affected Application

You can add affected applications when starting war rooms, locating faults, and rectifying faults.

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Click **Add Affected Application**.

Step 5 Set parameters for adding an affected application.

Table 7-31 Parameters for adding an affected application

Parameter	Description
Affected Application	Select an affected application from the drop-down list.
Start Time	Enter the time when the application starts to be affected. The default value is the time when the war room is created. The start time cannot be later than the war room creation time.
Recovery Time	(Optional) Enter the application recovery time. The recovery time cannot be earlier than the war room creation time.
Description	Enter the impact description of the application. The value can contain a maximum of 500 characters.

Step 6 Click **OK**.

The affected application is added. You can click **Affected Application** to view its alarms, incidents, and changes.

----End

Executing a Contingency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Select the application to be handled and click **Execute Plan**.

Step 5 If you select **Contingency Plans**, select the corresponding contingency plan from the drop-down list and click **Execute**.

If no appropriate contingency plans are available, create one. For details, see **Creating a Custom Contingency Plan**.

Step 6 Check the task type associated with the contingency plan.

- If the task type is **Scripts**, go to **7**.
- If the task type is **Jobs**, go to **8**.

Step 7 Set **Execute Scripts**.

- The parameter names and default values have been preset when the custom script is created.

- **Executed By**: **root** is set by default. It is the user who executes the script on a target instance node.
- **Timeout Interval**: **300** is set by default. It indicates the timeout interval for executing the script on a single target instance.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 7-32 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.
  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.
- **Suspension Policy**:
  - You can set the execution success rate. When the number of failed hosts reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
  - The success rate ranges from 0 to 100 and supports accuracy up to one decimal place.

Skip step 8 and perform step 9.

Step 8 Set **Execute Jobs**.

- **Region**: Select the region where the target instance is located.
- **Target Instance Mode**: Select the execution mode of job step and target instances.
  - **Consistent for all steps**: All tasks are executed on the selected instance using the same batch policy.
  - **Unique for each step**: Tasks in one step are executed on the selected instance. Each step uses a batch policy.
  - **Unique for each task**: Set the target instance and batch policy for each task.
- **Job Execution Procedure**: Customize job details.
  - Click the job name. The **Modifying Parameters** drawer is displayed on the right.
  - Set **Input**, **Output**, and **Troubleshooting**.
- **Target Instance**: Click **Add** and set **Select Instance**.

Table 7-33 Instance parameters

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	The default parameter cannot be modified and is determined by **Region** in **Execution Content**.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	-

- **Batch Policy**: Select **Automatic**, **Manual**, or **No Batch**.
  - **Automatic**: The selected instances to be executed are automatically divided into multiple batches based on the preset rule.

  - **Manual**: You can manually create multiple batches and add instances to each batch as required.
  - **No Batch**: All instances will be executed in the same batch.

Step 9 Click **OK**.

Step 10 Perform the following operations to check whether a service ticket execution is complete.

- For the service tickets that are being executed:
  - If you want to pause the next batch when the current batch is executed, click **Pause** in the upper right corner.
  - If you want to continue the paused batch, click **Continue** in the upper right corner.
  - If you want to stop the service ticket that is about to be executed or is abnormal, click **Forcibly End**.
- For the service tickets that are executed:
  - If some or all instance tasks in the service tickets are executed abnormally:
    i. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Retry** in the **Operation** column.
    ii. Click the **Abnormal** tab in the **Execution Information** area. Locate an abnormal batch and click **Cancel** in the **Operation** column.
  - If all instance tasks in the service tickets are executed successfully, no more operation is needed.

----End

Diagnosing Applications

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to diagnose.

Step 4 Select the application to be handled and click **Application Diagnosis**.

Step 5 Click the time box and set the fault occurrence time.

The time entered in the time box is the end time. The start time is one hour earlier than the end time. After the time is selected, the number of alarms for the application and its sub-applications in the selected time period is displayed on the application topology dashboard, and the application fault details are displayed on the details page on the right.

Step 6 (Optional) Select **Auto Refresh** and select a refresh frequency from the drop-down list.

After **Auto Refresh** is selected, the end time is updated to the current system time based on the refresh frequency.

Step 7 (Optional) If the application has sub-applications, click the target sub-application.

The application topology dashboard displays all components of the sub-application. The sub-application fault details are displayed on the details page on the right. You can switch to other sub-applications on the topology dashboard.

Step 8 Click a component under the application or its sub-application.

The application topology dashboard displays all resources of the component. The component fault details are displayed on the right details page. You can switch to other components on the topology dashboard. Metrics of core cloud services can be displayed. If APM is associated in application management, you can also view link-related metrics.

Step 9 Click **Alarm** on the right of the application topology.

View application alarms. Alarms generated within the time range on the right axis are displayed in the list. When you select a topology object on the left, its alarm information is automatically filtered.

Step 10 Click **Change** on the right of the application topology.

View application changes. Changes within the change time range on the right axis are displayed in the list.

Step 11 Click **Fault Diagnosis** on the right of the application topology.

View the fault diagnosis data for your resources. You can check DCS, RDS, DMS, ECS, and ELB resources. After a topology object is selected on the left, its diagnosis information is automatically filtered.

If no diagnosis task exists or you have created a new one, do the following:

1. Click **Create Diagnosis Task**.
2. Select a resource type and resource.
3. Click **OK**.
4. Read and agree to **Frontend Data Authorization Agreement on Guest OS Diagnosis Service**, and click **Agree**.

   📖 NOTE

   You need to sign the agreement only if you select ECSs for fault diagnosis.

After the diagnosis is complete, click **View Details** on the right of the diagnosis result list to view the diagnosis report.

----End

7.4.5 Adding Engineers to War Rooms

Scenarios

To quickly rectify a fault, you can add the fault recovery engineers to a war room or you can notify them through phone calls or SMS messages. After adding them to a war room, you can set the administrator, fault recovery owner, and fault recovery engineers.

The administrator is the engineer who creates the war room.

Adding Engineers to a War Room

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Click **Invite** on the right.

Step 5 Set parameters for inviting members.

Table 7-34 Parameters for inviting members

Parameter	Description
Attendance Mode	(Optional) Set this parameter to **WeCom**, **Lark,** or **DingTalk**. After you select an attendance mode, the corresponding notification mode is automatically selected. You need to configure the application on the **mobile app management** page and configure the email address of the application on the **personnel management** page.
Notification Mode	(Optional) Set this parameter to **SMS** or **Phone**. You can select multiple options. The value can be **WeCom**, **Lark**, or **DingTalk**. The notification mode is automatically selected when you select an attendance mode. For details about how to configure user information, see **11.1 O&M Engineer Management**.
O&M Roles	(Optional) Select a role from the drop-down list. You can select multiple shifts. After a shift is selected, all members in the shift are automatically selected. For details about how to configure a shift, see **11.2 Shift Schedule Management**.
O&M Engineers	(Optional) Select a user from the drop-down list. Multiple options can be selected.

Step 6 Click **Add to WarRoom**.

Members are added.

----End

Setting Member Roles

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Click ⌄ next to **Members**.

Step 5 Select the user to be modified and click ⋮ on the right.

Step 6 Set member roles.

Table 7-35 Member role description

Member Role	Description
Administrator	The administrator can be handed over to other members without roles. The war room administrator is a hidden administrator. Even if other members are set as administrators, the war room administrator still has the permission to manage members.
Fault Recovery Owner	You can set a member without a role as a fault recovery owner. The fault recovery owner can be canceled by the administrator but cannot be removed.
Fault Recovery Engineer	You can set a member without a role as a fault recovery engineer. The fault recovery engineer can be canceled or removed by the administrator.
Member Without a Role	You can set a member as an administrator, fault recovery owner, or fault recovery engineer. The member without a role can be removed by the administrator.

----End

7.4.6 Updating Progress Notices

Scenarios

When a fault occurs or is handled, the progress notice is synchronized to related personnel in a timely manner. People who are concerned about the fault can quickly learn the fault progress.

Updating a Progress Notice

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the title of the war room you want to modify.

Step 4 Click **Update Notice** on the right.

Step 5 Set parameters on the displayed page.

Table 7-36 Parameters for updating progress notices

Parameter	Description
Notification Template	The options are **First Notification**, **Progress Notification**, and **Fault Recovery Notification**.
Content	Enter the content based on the selected notification template. The value can contain a maximum of 1,000 characters.

Step 6 Click **OK**.

The notice is updated. The latest notice is displayed in the **Progress Notice** area.

Step 7 Click **Release**.

Step 8 Set parameters for releasing a notice.

Table 7-37 Parameters for releasing a notice

Parameter	Description
Notice Topic	Customize the notice topic.
Recipient	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. Click **Create Shift** to configure the shift. For details, see **11.2 Shift Schedule Management**. ● **Individual**: Select an individual that you want to notify. Click **Synchronize** to configure users. For details, see **11.1 O&M Engineer Management**.
Sending Mode	The options are **WeChat**, **SMS**, **Lark**, and **DingTalk**. Before setting this parameter, configure WeCom, Lark, and DingTalk in **11.4 Managing Mobile Apps**.
Content	The content cannot be modified. The content is the latest notice content.

Step 9 Click **OK**.

The notice is released.

----End

7.4.7 Creating War Room Rules

Scenarios

When a war room is created, the system matches a rule based on the region, application, and incident level, and adds related engineers to a group. The engineers responsible for fault rectification can receive a notification and rectify the fault in a timely manner.

Creating a War Room Rule

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the **WarRoom Rules** tab.

Step 4 Click **Create WarRoom Rule** in the upper right corner.

Step 5 Set parameters for creating a war room rule.

Table 7-38 Parameters for creating a war room rule

Parameter	Description
Rule	Customize the rule name.
Region	(Optional) Select a region from the drop-down list. Multiple regions can be selected. If no region is selected, **Default** is displayed, indicating that no region is required.
Application	Select an application from the drop-down list. Multiple applications can be selected.
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. Multiple options can be selected. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Group	(Optional) Select a shift role. The shift members are automatically added to the third-party application group when the war room is started. For details about how to configure a shift, see **11.2 Shift Schedule Management**. For details about how to configure mobile apps, see **11.4 Managing Mobile Apps**.

Step 6 Click **OK**.

The war room rule is created. War room creation logic: The region, application, and incident level of the war room rule are matched with those of the incident. The group members are added to the war room and mobile app.

----End

Modifying a War Room Rule

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom**.

Step 3 Click the **WarRoom Rules** tab.

Step 4 Locate the rule you want to modify and click **Modify** in the **Operation** column.

Step 5 Set parameters for modifying a war room rule.

Table 7-39 Parameters for modifying a war room rule

Parameter	Description
Rule	Customize the rule name.
Region	(Optional) Select a region from the drop-down list. Multiple regions can be selected. If no region is selected, **Default** is displayed, indicating that no region is required.
Application	Select an application from the drop-down list. Multiple applications can be selected.
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. Multiple options can be selected. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Group	(Optional) Select a shift role. The shift members are automatically added to the third-party application group when the war room is started. For details about how to configure a shift, see **11.2 Shift Schedule Management**. For details about how to configure mobile apps, see **11.4 Managing Mobile Apps**.

Step 6 Click **OK**.

The war room rule is modified.

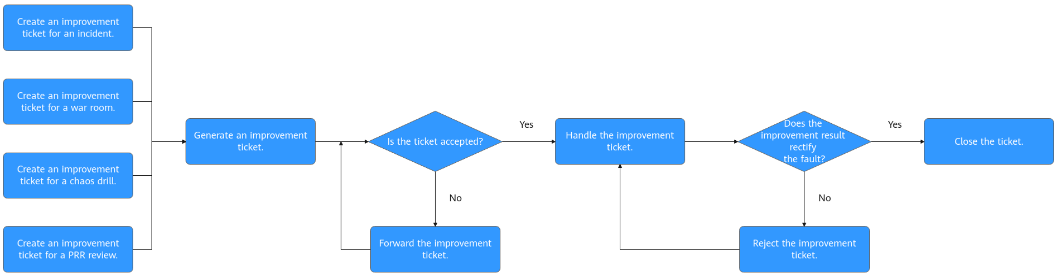
----End

7.5 Improvement Ticket Management

7.5.1 Overview

You can trace and close the products, O&M, and management improvement items identified during troubleshooting through improvement tickets. For O&M improvement items, for example, you need to configure alarm rules for an application in a specific scenario to detect software product exceptions in a timely manner. Improvement tickets can be created during incident handling, war room operations, chaos drills, and PRRs.

Figure 7-9 Improvement ticket management process


Create an improvement ticket for an incident.
Create an improvement ticket for a war room.
Create an improvement ticket for a chaos drill.
Create an improvement ticket for a PRR review.
Generate an improvement ticket.
Is the ticket accepted?
Yes
No
Forward the improvement ticket.
Handle the improvement ticket.
Does the improvement result rectify the fault?
Yes
No
Reject the improvement ticket.
Close the ticket.

7.5.2 Managing Improvement Tickets

Scenarios

You can create improvement tickets for incidents, war rooms, chaos drills, and PRRs, accept the tickets, and complete the improvement tasks within an expected time. If you find you are not the handling owner of the improvement tickets, you can forward the tickets to the owner. After the improvement items are completed, they can be closed only after they are verified by the verification owner.

Prerequisites

You have created improvement tickets for incidents, war rooms, chaos drills, or PRRs.

Handling Improvement Tickets

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**.

Step 3 On the **Pending** tab page, locate the target improvement ticket and click its title.

Step 4 Click **Process** in the upper right corner.

Step 5 Set **Handle Ticket**.

Table 7-40 Parameters for handling improvement tickets

Parameter	Description
Cause of Issue	Enter the cause of the issue. The value can contain a maximum of 1,000 characters.
Improvement Measures	Enter detailed improvement measures. The value can contain a maximum of 1,000 characters.

Step 6 Click **OK**.

The improvement ticket is handled.

----End

Forwarding an Improvement Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**.

Step 3 On the **Pending** tab page, locate the target improvement ticket and click its title.

Step 4 Click **Forwarding** in the upper right corner.

Step 5 Set parameters on the displayed page.

Table 7-41 Parameters for forwarding improvement tickets

Parameter	Description
Application	Select the application involved in the improvement ticket from the drop-down list.
Receiving Owner	Select the target owner from the drop-down list.

Step 6 Click **OK**.

The improvement ticket is forwarded.

----End

Verifying an Improvement Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**.

Step 3 On the **Pending** tab page, locate the target improvement ticket and click its title.

Step 4 Click **Verify** in the upper right corner.

Step 5 Set parameters on the displayed page.

Table 7-42 Parameters for verifying the conclusion

Parameter	Description
Improvement Ticket Verification	The options are **Pass** and **Reject**.
Reason of Rejection	This parameter is mandatory only when **Improvement Ticket Verification** is set to **Reject**. Enter the reason of rejection.

Step 6 Click **OK**.

The improvement ticket is verified.

----End

Viewing the Improvement Ticket History

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**.

Step 3 On the **Pending** tab page, locate the target improvement ticket and click its title.

Step 4 Click **Improvement History**.

The improvement history is displayed.

----End

7.6 Issue Ticket Management

7.6.1 Overview

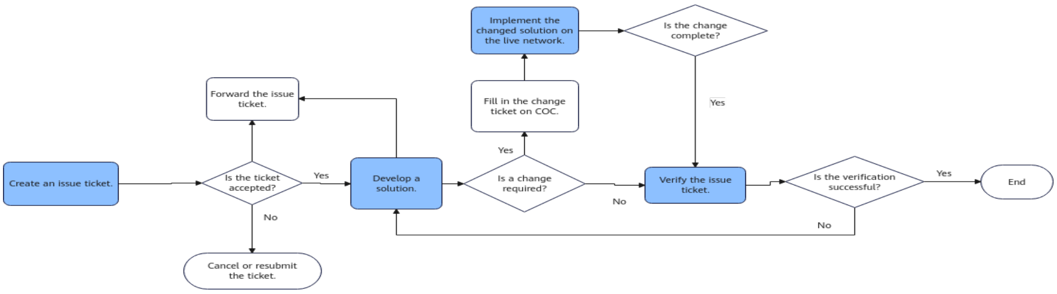
You can discover, record, and resolve product function defects and poor performance during software product use. This function is to reduce the number of product or service faults on the live network, improve the quality of services, products, or applications, and prevent problems from recurring. In this module, the whole lifecycle of issues tickets is managed, including ticket creation, acceptance, rejection, transferring, handling, and closure. Issue tickets can be created manually or through northbound APIs.

You can also configure SLA rules. For details about how to configure SLA rules, see **11.5 SLA Management**.

Issue Management Process

- After the issue ticket is created, the status is **Not accepted**. You can accept or reject the ticket, or transfer it to the owner.
- After the issue ticket is accepted, its status becomes **Locate the solution**. You can enter the issue locating result, transfer the ticket to the owner, escalate or de-escalate the ticket, or suspend it.
- After an issue ticket is suspended, it needs to be reviewed by the creator. After the ticket is approved, the status of the issue ticket changes to **Suspend**. You can manually cancel the suspension or the suspension is automatically canceled when the specified time arrives.
- When you enter the locating result, if you select change-required, the ticket status is **To be implemented on the live network**. You need to associate it with a change ticket and the change ticket has the backfilling result. In this way, the issue ticket can be transferred to the next step.
- If an issue ticket does not require change or the issue ticket has a change result, the ticket status is **To be verified**. The creator confirms whether the issue is resolved or not. If the issue is not resolved, the creator can reject the ticket.

Figure 7-10 Issue management process


Create an issue ticket.
Is the ticket accepted?
Yes
No
Forward the issue ticket.
Cancel or resubmit the ticket.
Develop a solution.
Is a change required?
Yes
No
Fill in the change ticket on COC.
Implement the changed solution on the live network.
Is the change complete?
Yes
Verify the issue ticket.
Is the verification successful?
Yes
No
End

7.6.2 Creating Issue Tickets

Scenarios

If you find any defects or poor performance in the software products, you can create an issue ticket to trace the issue.

To set notifications for issue tickets, you need to configure notification rules on the notification management page. For details, see **11.3 Managing Notifications**. Set notification type to issue notification.

Prerequisites

You have created an application by referring to **4 Application Management**.

Creating an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 Click **Create Issue Ticket** in the upper right corner.

Step 4 Configure related parameters on the displayed page.

Table 7-43 Parameter description

Parameter	Description
Issue Title	Customize the issue title.
Issue Description	Description of the issue symptoms and impacts on the live network.
Attachment	Click **Add File** to upload issue-related attachments. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.
Region	(Optional) The default value is **N/A**. Select the region where the incident occurs from the drop-down list. Multiple regions can be selected.

Parameter	Description
Enterprise Project	Select an enterprise project from the drop-down list.
Issue Source	(Optional) The options are **incident**, **alarms**, **WarRoom**, and **Proactive O&M discovery**. Select the source of the issue. If you select **incident**, **alarms**, or **WarRoom**, you need to associate the corresponding service ticket.
Source Ticket No.	This parameter needs to be set only when you select **incident**, **alarms**, or **WarRoom**. Click **Associated Ticket No.** and select the corresponding ticket.
Occurrence Time	(Optional) Enter the time when the issue occurs.
Issue Application	Select the issue application from the drop-down list.
Issue Level	The value can be **Critical**, **Major**, **Minor**, or **Prompts**. ● **Critical**: The system or application breaks down, stops, or suspends, causing data loss. Main functions are unavailable, or the module or related modules are abnormal. ● **Major**: Some main functions of the system are unavailable, data cannot be saved, and secondary functions of the system are unavailable. The fault is limited to the module. As a result, the module functions are invalid or the module exits abnormally. ● **Minor**: Secondary functions are not completely implemented but are not affected, for example, the prompt information is inaccurate, the user interface is poor, the operation time is long, and some module functions are invalid. ● **Prompts**: Minor software defects that cause inconvenience or trouble to operators but do not affect the operation and execution of functions.
Type of Issue	Select the issue type from the drop-down list.
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.

Step 5 Click **OK**.

After the issue ticket is created, the status is **Not accepted**.

----End

7.6.3 Rejecting Issues Tickets

Scenarios

If the issue submitted by the creator is not an issue or for other reasons, the issue ticket can be rejected. After the issue ticket is rejected, the creator can modify and submit the issue ticket again or cancel the issue ticket. After the issue ticket is submitted again, the handler needs to continue to locate and resolve the issue.

Rejecting an Issues Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Reject** in the upper right corner.

Step 5 Enter the reason and click **OK**.

The status of the issue ticket is **Rejected**.

----End

7.6.4 Resubmitting Issue Tickets

Scenarios

After an issue ticket is rejected, the applicant can resubmit the ticket after confirming that the issue needs to be addressed and modifying the ticket content.

Resubmitting an Issue Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Modify** in the upper right corner.

Step 5 Set parameters for modifying an issue ticket.

Table 7-44 Parameters for modifying an issue ticket.

Parameter	Description
Issue Title	Customize the issue title.
Issue Description	Description of the issue symptoms and impacts on the live network.

Parameter	Description
Attachment	Click **Add File** to upload issue-related attachments. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.
Region	(Optional) The default value is **N/A**. Select the region where the incident occurs from the drop-down list. Multiple regions can be selected.
Enterprise Project	Select an enterprise project from the drop-down list.
Issue Source	(Optional) The options are **incident**, **alarms**, **WarRoom**, and **Proactive O&M discovery**. Select the source of the issue. If you select **incident**, **alarms**, or **WarRoom**, you need to associate the corresponding service ticket.
Source Ticket No.	This parameter needs to be set only when you select **incident**, **alarms**, or **WarRoom**. Click **Associated Ticket No.** and select the corresponding ticket.
Occurrence Time	(Optional) Enter the time when the issue occurs.
Issue Application	Select the issue application from the drop-down list.
Issue Level	The value can be **Critical**, **Major**, **Minor**, or **Prompts**. ● **Critical**: The system or application breaks down, stops, or suspends, causing data loss. Main functions are unavailable, or the module or related modules are abnormal. ● **Major**: Some main functions of the system are unavailable, data cannot be saved, and secondary functions of the system are unavailable. The fault is limited to the module. As a result, the module functions are invalid or the module exits abnormally. ● **Minor**: Secondary functions are not completely implemented but are not affected, for example, the prompt information is inaccurate, the user interface is poor, the operation time is long, and some module functions are invalid. ● **Prompts**: Minor software defects that cause inconvenience or trouble to operators but do not affect the operation and execution of functions.
Type of Issue	Select the issue type from the drop-down list.

Parameter	Description
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.

Step 6 Click **OK**.

After the issue ticket is resubmitted, the status is **Not accepted**.

----End

7.6.5 Cancelling Issue Tickets

Scenarios

After an issue ticket is created, you can cancel the ticket if it is not an issue or for other reasons. Before canceling an issue ticket, you need to reject it. Accepted issue tickets cannot be canceled.

Cancelling an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Cancel** in the upper right corner.

Step 5 Enter the reason and click **OK**.

The issue ticket status is **Canceled**.

----End

7.6.6 Forwarding Issue Tickets

Scenarios

During the issue ticket processing, if you find that the issue needs to be accepted by other O&M experts, you can forward the issue ticket to the corresponding owner.

Forwarding an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Forwarding Owner** in the upper right corner.

Step 5 Set **Forwarding Owner**.

Table 7-45 Parameters for forwarding an issue ticket

Parameter	Description
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.
Description	Enter the forwarding description.

Step 6 Click **OK**.

The issue ticket is forwarded. The owner of the issue ticket is the forwarding owner you set.

----End

7.6.7 Accepting Issue Tickets

Scenarios

After the issue ticket is created, the owner analyzes the actual situation of the issue. If the issue is valid, the owner accepts the issue ticket and handles it further to close the issue ticket.

Accepting an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Accept** in the upper right corner.

After the issue ticket is accepted, the status of the ticket is **Locate the solution**.

----End

7.6.8 Escalating and De-escalating Issue Tickets

Scenarios

After an issue ticket is submitted, if the issue handler thinks that the current issue level is improper, the handler can escalate or de-escalate the issue ticket. The escalation or de-escalation process can be configured by referring to **11.7.3.3 Managing Issue Review Tasks**.

Escalating and De-escalating an Issue Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Upgrade and Downgrade** in the upper right corner.

Step 5 Set parameters on the displayed page.

Table 7-46 Parameters for de-escalating and escalating an issue ticket

Parameter	Description
Issue Level	The value can be **Critical**, **Major**, **Minor**, or **Prompts**. ● **Critical**: The system or application breaks down, stops, or suspends, causing data loss. Main functions are unavailable, or the module or related modules are abnormal. ● **Major**: Some main functions of the system are unavailable, data cannot be saved, and secondary functions of the system are unavailable. The fault is limited to the module. As a result, the module functions are invalid or the module exits abnormally. ● **Minor**: Secondary functions are not completely implemented but are not affected, for example, the prompt information is inaccurate, the user interface is poor, the operation time is long, and some module functions are invalid. ● **Prompts**: Minor software defects that cause inconvenience or trouble to operators but do not affect the operation and execution of functions.
Description	Enter the detailed escalation and de-escalation description. The description can contain a maximum of 300 characters.

Step 6 Click **OK**.

The issue ticket is escalated or de-escalated. The escalation or de-escalation does not need to be approved.

----End

7.6.9 Suspending Issue Tickets

Scenarios

After an issue ticket is accepted, the ticket creator needs to provide data or other information in the fault locating phase, and approve the change tickets during issue ticket implementation phase. The ticket handler can suspend an issue ticket. By default, a suspended issue ticket needs to be approved by the creator. For details about how to modify the approval process, see **11.7.3.3 Managing Issue Review Tasks**.

Suspending an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Suspend** in the upper right corner.

Step 5 Set parameters for suspending an issue ticket.

Table 7-47 Parameters for suspending an issue ticket

Parameter	Description
Estimated Recovery Time	Enter the estimated recovery time.
Description	Enter the detailed suspension description. The description can contain a maximum of 300 characters.

Step 6 Click **OK**.

After the issue ticket is suspended, the issue ticket handling duration stops being calculated until the issue ticket is resumed.

----End

Approving a Suspended Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **All Issues** tab page, locate the target issue ticket and click its title.

Step 4 Click **Approve**

Step 5 Set parameters on the displayed page.

- **Passed or Not**: **Passed** or **Not Passed**.
- **Review Comment**: Enter review comments. The value can contain a maximum of 1,024 characters.

Step 6 Click **OK**.

The suspended issue ticket is approved. If the suspension is approved, the status of the ticket is suspended. If the suspension is not approved, the status of the ticket is the status when the suspension is initiated.

----End

Resuming a Suspended Issue Ticket

Only the issue ticket creator can suspend and resume an issue ticket.

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **All Issues** tab page, locate the target issue ticket and click its title.

Step 4 Click **Resume** in the upper right corner.

The suspended issue ticket is resumed.

----End

7.6.10 Locating Issue Tickets and Developing Solutions

Scenarios

After an issue ticket is accepted, you need to analyze the ticket, provide the locating result, and develop a solution.

Locating an Issue Ticket and Developing a Solution

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Positioning solution** in the upper right corner.

Step 5 Set **Positioning solution**.

Table 7-48 Parameters for positioning solutions

Parameter	Description
Issue Application	The application selected during issue ticket creation is used by default. Select the issue application from the drop-down list.

Parameter	Description
Common Issue	The options are **Yes** and **No**.
Issue Version	(Optional) Enter a correct version number.
Region	(Optional) The region selected during issue ticket creation is used by default. Select the region where the incident occurs from the drop-down list. Multiple regions can be selected. This parameter is mandatory if you select **Need** for **Whether the live network needs to be changed**
Root Cause Classification	Select a root cause category from the drop-down list.
Root cause analysis	Enter the root cause analysis of the issue ticket The value can contain a maximum of 1,000 characters.
Solution	Enter a solution to the issue ticket. The value can contain a maximum of 1,000 characters.
Whether the live network needs to be changed	The options are **Need** and **Not Need**. ● **Need**: The ticket is in the to-be-implemented status and needs to be associated with a change ticket. ● **Not Need**: The ticket is in the to-be-verified status.

Step 6 Click **OK**.

After developing a solution for the issue ticket, if you select **Need** for **Whether the live network needs to be changed**, the status of the issue ticket is **To be implemented on the live network**. If you select **Not Need** for **Whether the live network needs to be changed**, the status of the issue ticket is **To be verified**.

----End

7.6.11 Implementing Changes on the Live Network

Scenarios

On the **Positioning solution** page, if you select **Need** for **Whether the live network needs to be changed**, the issue ticket will be in the **To be implemented on the live network** status. At this point, you need to change the region where the issue ticket is belongs. The issue ticket is resolved only after the change is completed.

Prerequisites

On the **Positioning solution** page, you have selected **Need** for **Whether the live network needs to be changed**. The issue ticket is in the **To be implemented on the live network** status.

Implementing Changes on the Live Network

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Live network implementation** in the upper right corner.

Step 5 Set **Live network implementation**.

- If the region needs to be changed, click **Associated Change Order** in the **Operation** column. For details about operations on change tickets, see **8 Change Management**.
- If the region does not need to be changed, click **No change required** in the **Operation** column.
- You can add a region or delete an existing region.

Step 6 Click **Implement completed**.

After the live network implementation is completed, the ticket status changes to **To be verified**.

----End

7.6.12 Verifying Issue Tickets

Scenarios

After the issue ticket is handled, the issue ticket creator needs to verify whether the issue ticket is resolved. If the ticket is not resolved, the handler needs to relocate the issue ticket and develop a solution. If the ticket is resolved, it can be closed.

Verifying an Issue Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **Pending** tab page, locate the target issue ticket and click its title.

Step 4 Click **Verify** in the upper right corner.

Step 5 Set **Validate**.

- **Passed or Not**: **Passed** or **Not Passed**.
- **Validation Description**: Enter the verification description. The description can contain a maximum of 300 characters.

Step 6 Click **OK**.

The issue ticket is verified. If the verification is passed, the issue ticket status is **Completed**. If the verification fails, the status is **Locate the solution**.

----End

7.6.13 Viewing Handling History of Issue Tickets

Scenarios

If you have any questions about handling issue tickets or entering basic information during tracing issue tickets, you can view the handing history.

Viewing Handling History of an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 3 On the **All Issues** tab page, locate the target issue ticket and click its title.

Step 4 Click the **Handle Record** tab.

The issue handling history is displayed.

----End

7.7 Alarm Conversion Rule Management

7.7.1 Overview

Alarm conversion rules eliminate duplicate raw alarms, allowing you to set specific triggers and conditions that convert raw alarms into aggregated alarms or incidents. Each alarm conversion rule can be assigned to shifts or owners to implement accurate notification. In addition, during the process of alarm-to-incident, alarms can be converted to an incident for automatic fault rectification.

7.7.2 Creating an Alarm Conversion Rule

Scenarios

You can use an alarm conversion rule to configure incident and alarm rules based on service requirements. You can use an alarm conversion rule to convert raw alarms into aggregated alarms or incidents.

Prerequisites

Before configuring an alarm conversion rule, ensure that the monitoring system for which the forwarding rule you want to configure has been connected to **Data Sources**.

Constraints and Limitations

- After an incident is generated based on an alarm conversion rule, if the incident meets another alarm conversion rule before it is completed or closed, the new incident will no longer be generated. This rule is enabled by default and can be disabled.

- If you receive no raw alarms within the corresponding time window for generating aggregated alarms using alarm conversion rules, the system considers the alarms generated in the previous window period as historical alarms (that is, the current alarm status is set to **Handled** by default).

Creating an Alarm Conversion Rule

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Click **Add Rule** in the upper right corner.

If the information in the two alarm conversion rules is similar, click **Copy** in the **Operation** column of the forwarding rule you want to copy to quickly create a forwarding rule.

Step 4 Set the basic information.

Table 7-49 Basic information parameters

Parameter	Description
Rule	Specify the name of the alarm conversion rule you want to create.
Region	(Optional) Select a region from the drop-down list. If no region is selected, **default** is displayed, indicating that no region is required.
Enterprise Project	Select an enterprise project from the drop-down list.
Application	Select an application from the drop-down list.

Step 5 Set a trigger rule.

Table 7-50 Parameters for configuring a trigger rule

Parameter	Description
Trigger Type	The options are **Incident** and **Alarm**. ● **Incident**: An incident ticket is generated. The on-duty personnel need to handle the incident as soon as possible and continuously track the incident until it is closed. ● **Alarm**: Alarms are generated and are manually or automatically based on contingency plans.

Parameter	Description
Data Source	Select a data source. A data source is the system where raw alarms are from. Before configuring alarm rules, ensure that alarm data has been integrated and enabled. When all conditions of a rule are met, the alarm conversion rule is triggered. For details about how to set data sources, see **7.7.2 Creating an Alarm Conversion Rule**.
Triggering Conditions	Select the key, comparison method, and value for the trigger criteria. A maximum of five trigger criteria can be added. For details about how to set the keys, see **Table 7-51**.
Trigger Criteria	Select a trigger rule.
Incident Level	This parameter is required only when **Trigger Type** is set to **Incident**. The options are **P1**, **P2**, **P3**, **P4**, and **P5**. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Silence Rule	This parameter is required only when **Trigger Type** is set to **Incident**. Enable or disable this rule as required. After an incident is generated based on the alarm conversion rule, a new incident will be generated if the trigger criteria are met before the incident is completed or closed.
Alarm Severity	This parameter is required only when **Trigger Type** is set to **Alarm**. The value can be **Critical**, **Major**, **Minor**, or **Warning**.

Table 7-51 Key parameters for the trigger criteria

Key Parameter	Description	Alarm Field from Cloud Eye	Alarm Field from AOM
alarmId	Alarm ID	alarm_id	id
alarmName	Alarm name	alarm_name	**event_name** in the metadata
alarmLevel	Alarm severity. The options are **Critical**, **Major**, **Minor**, and **Warning**.	AlarmLevel	event_severity

Key Parameter	Description	Alarm Field from Cloud Eye	Alarm Field from AOM
time	Time when an alarm is generated	time	starts_at
nameSpace	Service namespace	namespace	namespace
region	Region	**Region** in **template_variable**	/
application	Application name	/	/
resourceName	Resource name	**ResourceName** in **template_variable**	**resource_id** in the metadata
resourceId	Resource ID	**ResourceId** in **template_variable**	/
alarmDesc	Alarm description	**AlarmDesc** in **template_variable**	/
URL	Raw alarm URL	**Link** in **template_variable**	/
alarmStatus	Alarm status. The value can be **alarm** (active alarm) or **ok** (alarm handled).	alarm_status	/
alarmSource	Alarm source name. For example, if an alarm is reported from Cloud Eye, the value of this field is **CES**.	/	/

Key Parameter	Description	Alarm Field from Cloud Eye	Alarm Field from AOM
additional	Additional alarm information. Format: **additional.***xxx*.	Except the preceding parameters, other parameters are contained in this parameter and are represented by **additional.***xxx*. For more information about fields on Cloud Eye, click **here**.	Except the preceding parameters, other parameters are contained in this parameter and are represented by additional.xxx. For more information about fields on AOM, click **here**.

Step 6 Set the contingency plan.

Table 7-52 Contingency plan parameters

Parameter	Description
Task Type	The options are **Contingency plan**, **Script**, and **Job**.
Automatic Execution	Determine whether to automatically execute what you have selected. Automatic contingency plans, scripts, and jobs can be automatically executed. ● If you select **Automatic Execution**, **Parameter Mapping** will be displayed. The system automatically executes tasks based on the trigger criteria and settings. The parameter value, region ID, and target instance must be in the format of **$***{}*. You need to use this expression to parse the corresponding value. For details, see **Example of Automatic Parameter Execution**. ● If you deselect **Automatic execution**, you can click the link on the left to manually execute the task.

Step 7 Set **Assignment Details**.

Table 7-53 Parameters for configuring a ticket dispatch rule

Parameter	Description
Owner	Select **Shift** or **Individual**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an owner. For details about how to configure an owner, see **11.1 O&M Engineer Management**.

Step 8 Click **OK**.

The alarm conversion rule is created.

----End

Example of Automatic Parameter Execution

The parameter value, region ID, and target instance are in the format of ${}. You need to use this expression to parse the corresponding value.

Example:

Alarm information:

{

"alarmId": "al1696664837170EWbvx24kW",

"alarmName": "alarm-4z39coctest1007",

......

"URL": "https://console.***.com/ces/?region=***#/alarms/detail?alarmId=al16849986549022X5Vp4pxr",

"additional": {

"dimension": "instance_id:29d99a09-2d15-4ced-8723-6e94ae1c1472",

......

},

......

}

- To obtain the value of **alarmId** in the current alarm information, use the following expression:
  ```
  ${currentAlarm.alarmId}
  ```
- To obtain the UUID of **instance_id** from the **additional.dimension** string, use the following expression:
  ```
  ${string.substring(currentAlarm.additional.dimension,
  string.indexOf(currentAlarm.additional.dimension, 'instance_id:') + 12)}
  ```

Alternatively, use the following content:

```
${string.substring(currentAlarm.additional.dimension, 12)}
```

- To obtain the region ID of cn-north-7 from the URL string, use the following expression:

```
${string.substring(currentAlarm.URL, string.indexOf(currentAlarm.URL, 'region=') + 7,
string.indexOf(currentAlarm.URL, '#/alarms'))}
```

In the expression, **currentAlarm.** is a fixed prefix, which indicates that the data is obtained from the current alarm data.

7.7.3 Managing Alarm Conversion Rules

Scenarios

After an alarm conversion rule is created, if you want to disable, enable, modify, copy, or delete the rule, perform the operations in this section.

Disabling an Alarm Conversion Rule

Step 1 Log in to COC.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Select the rule to be disabled and click **Disable** in the **Operation** column.

Step 4 Click **OK**.

The alarm conversion rule is disabled.

----End

Enabling an Alarm Conversion Rule

Step 1 Log in to COC.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Select the rule you want to enable and click **Enable** in the **Operation** column.

Step 4 Click **OK**.

The alarm conversion rule is enabled.

----End

Modifying an Alarm Conversion Rule

Step 1 Log in to COC.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Locate the action you want to modify and click **More** in the **Operation** column and choose **Modify**.

Step 4 The parameters for creating an alarm conversion rule are similar to those for creating an alarm conversion rule. For details, see **7.7.2 Creating an Alarm Conversion Rule**.

Step 5 Click **OK**.

The alarm conversion rule is modified.

----End

Copying an Alarm Conversion Rule

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Select the rule to be disabled and click **Copy** in the **Operation** column.

Step 4 The parameters for creating an alarm conversion rule are similar to those for creating an alarm conversion rule. For details, see **7.7.2 Creating an Alarm Conversion Rule**.

Step 5 Click **OK**.

The alarm conversion rule is copied.

----End

Deleting an Alarm Conversion Rule

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Alarm Conversion Rules**.

Step 3 Locate the action you want to review and click **More** in the **Operation** column and choose **Delete**.

Step 4 Click **OK**.

The alarm conversion rule is deleted.

----End

7.8 Data Source Management

7.8.1 Overview

You can quickly integrate with existing or external monitoring systems (such as Huawei Cloud Cloud Eye and AOM) with ease for centralized alarm management. Each monitoring system employs distinct integration access keys for seamless interconnectivity.

After the monitoring systems are integrated, you can view alarm information in raw alarms. After **alarm conversion rules** are configured, alarm information can be converted to incidents or aggregated alarms.

7.8.2 Integrating a Monitoring System

Scenarios

Each monitoring system is independent integrated into COC. For details, see the integration process description.

Integrating a Monitoring System

- **This part describes how to integrate Huawei Cloud and open-source monitoring systems to COC.**

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Data Sources**.

Step 3 On the displayed page, locate the monitoring system you want to integrate into COC based on service requirements and click **Integrate**.

The detailed system integration procedure is displayed. The integration procedure varies depending on the monitoring system.

Step 4 Click **Submit**.

After the integration is confirmed, the status of the monitoring source changes to **Enabled** in the **Integrated** area on the **Data Sources** page.

Step 5 Complete monitoring system integration based on the integration procedure corresponding to the specific monitoring system.

----End

- **This part describes how to integrate monitoring systems except those mentioned in the above part into COC.**

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Data Sources**.

Step 3 On the **Data Sources** page, in the **To Be Integrated** area, locate **Other Monitoring Systems**, and click **Integrate**.

The detailed integration access procedure is displayed.

Step 4 Enter the short name and full name of the monitoring system you want to integrate and click the button for confirming the integration.

Step 5 Integrate a Huawei-built monitoring system.

Currently, alarm management data can be ingested using the POST method. For details, see .

Step 6 Check whether the integration is successful.

In the navigation pane on the left, choose **Fault Management** > **Data Sources**. In the **Integrated** area, check whether the status of the monitoring system you integrated is **Enabled**. If it is, the integration is successful.

NOTICE

A maximum of five monitoring systems can be integrated for customized integration. If the integration is incorrect, disable it and then delete it.

----End

Enabling and Disabling a Monitoring System

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Data Sources**.

Step 3 Slider on or off the **Enable** or **Disable** feature toggle of an integrated monitoring source.

Enable or disable an integrated monitoring system as required.

----End

Updating an Integration Sign

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Data Sources**.

Step 3 Click the monitoring system you want to update.

Step 4 Click ↻ on the right of the integration sign.

The integration sign is updated.

----End

8 Change Management

8.1 Overview

Change management is used to manage change tasks on COC. This feature aims to build secure production capabilities throughout the lifecycle of O&M operations, reducing change risks. This module provides capabilities such as the change calendar, change center, change configurations, and change control.

Change calendar: displays the data of manually created change requests in a calendar view for you to check the change distribution by status.

Change center: manages change processes using change tickets, covering **change request**, **review**, and **execution**. It provides a unified management platform for change personnel and change management personnel.

Change configurations: enable configurations for changes in the change center and basic configuration change capabilities such as configuration review. You can customize a review process for change requests and specify reviewers based on service requirements.

Change control: When changing resources, you can only execute scripts, jobs, or query accounts and passwords if you use a service ticket to request privilege escalation. This ensures that the operator and operation object of a change ticket match the actual resources you want to change, limiting the permissions of the operator for enhanced security.

8.2 Creating a Change Ticket

Scenarios

If an application requires changes, you can create a change ticket to record the change scope and solution. You can upload a detailed change solution or implement the change by executing jobs.

Prerequisites

1. You have created an application by referring to **4 Application Management**.
2. You have created a reviewer shift schedule by referring to **11.2.1 Overview**.

Precautions

Confirm the content of change ticket and apply for the change based on the actual change requirement.

Creating a Change Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Click **Create Change Ticket** in the upper right corner.

Step 4 Configure the basic information.

- **Title**: Customize the title of the change ticket.
- **Description**: Describe the change. Enter a maximum of 4,096 characters.

Step 5 Set **Change Configuration**.

Table 8-1 Changing configuration parameters

Parameter	Description	Example Value
Change Type	The options are **Regular** and **Urgent**. ● Regular changes are non-emergency changes that can be requested, evaluated, reviewed, sorted, planned, tested, and implemented using regular procedures. ● Emergent changes are unplanned changes that are proposed because the production environment is unavailable or the changes cannot be evaluated and approved in time through the normal process, or to meet urgent service requirements.	Regular
Level	The options are **A**, **B**, **C**, and **D** (A > B > C > D).	A
Scenario	Select a change scenario from the drop-down list.	API change
Application	Select a change application, a sub-application, a group, and a component from the drop-down lists as required. Multiple sub-applications, groups, and components can be selected.	N/A
Region	Select a region from the drop-down list. Multiple options can be selected.	CN-Hong Kong

Parameter	Description	Example Value
Selected Change Scope	Configure the change region corresponding to the sub-application, group, and component.	N/A

Step 6 Configure **Change Plan**.

Set the change plan for the selected regions.

Table 8-2 Change plan parameters

Parameter	Description
Planned Change Time	Select a time range for the plan change.
Change Implementer	Select a change implementation user. Multiple users can be selected.
Change Coordinator	(Optional) Select a user as the change cooperation. Multiple users can be selected.

Step 7 Configure information in **Task Type**.

- **Task Type**: Select **Jobs** or **Change guidelines**.
- If **Task Type** is set to **Jobs**, configure other parameters by referring to **Table 8-3**.

Table 8-3 Job parameters

Parameter	Description
Task Type	Select the job you want to execute from the drop-down list.
Region	Select a region from the drop-down list.
Target Instance Mode	This parameter is only required for some jobs. You can select the execution methods for job steps and target instances. – **Consistent for all steps**: All tasks are executed on the selected instance using the same batch policy. – **Unique for each step**: Tasks in one step are executed on the selected instance. Each step uses a batch policy.
Job Execution Procedure	This parameter is required for some jobs. You can customize job details. – Click a job name. The drawer for modifying parameters is displayed on the right. – Set **Input**, **Output**, and **Troubleshooting**.

Parameter	Description
Global Parameters	This parameter is required for some jobs. You can set global parameters.
Target Instance	This parameter is required for some jobs. Click **Add Instance** and set **Select Instance**. For details about how to set the parameters, see **Table 8-4**.
Batch Policy	This parameter is required for some jobs. You can select **Automatic**, **Manual**, or **No Batch**. – **Automatic**: The selected instances you want to execute are automatically divided into multiple batches based on the preset rule. – **Manual**: You can manually create multiple batches and add instances to each batch as required. – **No Batch**: All instances to be executed are in the same batch.

Table 8-4 Parameters for selecting an instance

Parameter	Description	Example Value
Selection Method	Select an instance selection method. – **Manual Selection**: Manually select an instance based on **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and **Target Instance**.	Manual Selection
Enterprise Project	Select an enterprise project from the drop-down list. You can choose **All**.	All
View Type	Select a view type. – **CloudCMDB resources**: Select an instance from the resource list. – **CloudCMDB application groups**: Select an instance from the application group list.	CloudCMDB resources
Resource Type	The value can be **ECS** or **BMS**.	ECS
Region	Select a region from the drop-down list.	CN-Hong Kong
Target Instance	Set filter criteria in the filter box and select the filtered instances.	N/A

- If **Task Type** is set to **Change guidelines**, see **Table 8-5** to set required parameters.

Table 8-5 Parameter description for the change task that is based on change guidelines

Parameter	Description
Task Type	Click **Add File** to upload the files related to the change guidelines. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.

Step 8 Click **Submit**.

Step 9 Click **OK**.

The change ticket is created. Choose **Change Ticket Management** > **Change Center**. Switch to the **Created by Me** tab page to view the created change ticket.

----End

8.3 Reviewing a Change Ticket

Scenarios

After a change ticket is created, you need to perform the following operations to approve or reject the change ticket.

Reviewing a Change Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Assess the **Pending** tab page, select the change ticket you need to review and click **Deal** in the **Operation** column.

Step 4 Click **Review**.

Step 5 Configure the review parameters.

- **Approve or Not**: The options are **Approve** and **Reject**.
- **Review Comment**: Enter the review comments.

Step 6 Click **OK**.

The change ticket review is complete

----End

8.4 Handling and Closing a Change Ticket

Scenarios

After a change ticket is approved, implement the change within the specified time window according to the change solution. After the change is implemented, fill in the change result and fill in the verification report.

Handling and Closing a Change Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Assess the **Pending** tab page, select the change ticket you need to handle and click **Deal** in the **Operation** column.

Step 4 Conduct changes based on the change solution type.

- If the change task type is set **Jobs**, click **Execute Job**.
- If the change task type is set to **change guidelines**, implement the change according to the steps mentioned in the change guidelines.

Step 5 Click **Start Change**.

Wait until the change is complete.

Step 6 After the change is complete, click **End**.

Step 7 Set parameters for filling in the change result.

Table 8-6 Parameters for successful change results

Parameter	Description
Change Result	Select **Success**.
Change Verification	The options are **Verification within the change time window** and **The change time window cannot be verified**.
Verification Report or Verification Description	Click **Add File** to upload the verification report or verification description file. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.
Remarks	(Optional) Description of the change result. Enter 0 to 256 characters.

Table 8-7 Parameters for failed change results

Parameter	Description
Change Result	Select **Failed**. This parameter covers situations like change rollbacks, service interruptions due to changes, and incidents triggered by changes.
Whether to monitor discovery	The options are **Yes** and **No**.
Rollback Succeeded	The options are **Rollback succeeded** and **Rollback failed**.
Rollback Time	Set the rollback time.
Change Failure Type	Select a failure type. ● Dependent service issue ● Change Quality Issues ● Change Tool Issues ● Change Implementation Issues ● Change Solution Issues ● Other Issues
Failure Cause Description	Describes the cause of the change failure. Enter 0 to 256 characters.
Verification Report or Verification Description	Click **Add File** to upload the verification report or verification description file. A maximum of 10 files can be uploaded. The supported file types are JPG, PNG, DOCX, TXT, and PDF. The size of a single file cannot exceed 10 MB.

Step 8 Click **OK**.

The change ticket is closed and the change is complete.

----End

8.5 Managing Change Review Tickets

Scenarios

To create a change ticket, you need to configure the review process and reviewer from the change type and change level dimensions based on service requirements.

Creating a Review Configuration

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Click **Create Review Configurations** in the upper right corner.

Step 4 Set parameters for creating a review configuration.

Table 8-8 Parameters for creating a review configuration task

Parameter	Description
Change Type	The options are **Regular** and **Urgent**. Only one change type can be configured each time.
Level	The options are **A**, **B**, **C**, and **D** (A > B > C > D). You can select multiple change levels at the same time.
Review Configurations	Select a value from the drop-down list box based on the configured shift scenario and role. For details about how to configure a shift, see **11.2 Shift Schedule Management**. A shift role becomes active only after a reviewer is assigned. Without a reviewer, the change request cannot be submitted. **Review Rule**: The options are **One-member Approval** and **All-member Approval**. You can add up to five levels of reviews.

Step 5 Click **OK**.

The review configuration task is created.

----End

Modifying a Review Configuration

Only the creator and management account can modify review configurations.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Locate the action you want to review and click **Modify** in the **Operation** column.

Step 4 Set parameters for modifying a review configuration.

Table 8-9 Parameters for modifying review configurations

Parameter	Description
Change Type	The options are **Regular** and **Urgent**. Only one change type can be configured each time.

Parameter	Description
Level	The options are **A**, **B**, **C**, and **D** (A > B > C > D). You can select multiple change levels at the same time.
Review Configurations	Select a value from the drop-down list box based on the configured shift scenario and role. For details about how to configure a shift, see **11.2 Shift Schedule Management**. A shift role becomes active only after a reviewer is assigned. Without a reviewer, the change request cannot be submitted. **Review Rule**: The options are **One-member Approval** and **All-member Approval**. You can add up to five levels of reviews.

Step 5 Click **OK**.

The review configurations are modified.

----End

Deleting a Review Configuration

Only the creator and management account of a review configuration can delete it.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**.

Step 3 Locate the action you want to review and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

The review configuration is deleted.

----End

8.6 Configuring Change Control

Scenarios

You can configure whether to enable privilege escalation using a service ticket based on application scenarios. Currently, privilege escalation using incidents, war rooms, and change tickets are supported.

Prerequisites

To enable change control, you need to apply for the IAM permission. The action IDs are as follows:

Permissions required by policies, system-defined policies, and custom policies:

"iam:roles:listRoles",

"iam:permissions:grantRoleToAgency",

"iam:permissions:grantRoleToAgencyOnDomain",

"iam:roles:createRole",

"iam:groups:listGroups",

"iam:permissions:listRoleAssignments",

"iam:permissions:grantRoleToGroupOnDomain",

"iam:permissions:revokeRoleFromGroupOnDomain",

"iam:permissions:revokeRoleFromGroupOnDomain",

"iam:roles:deleteRole",

"iam:roles:updateRole"

Permissions required by identity policies, system-defined identity policies, and custom identity policies:

"iam:policies:createV5",

"iam:policies:listV5",

"iam:groups:attachPolicyV5",

"iam:groups:detachPolicyV5",

"iam:policies:deleteV5",

"iam:policies:listVersionsV5",

"iam:policies:createVersionV5",

"iam:policies:deleteVersionV5"

Precautions

1. By default, the change control policy generated by COC can only be bound to user groups for further permissions granting. Do not use the policy for other purposes.
2. You can click the editing button of actions on the related COC page to determine whether to control functions corresponding to the actions. Note that all operations must be performed on COC. Do not directly edit the policy.
3. If you enabled the feature of privilege escalation using service tickets, you need to bind the policy to your account. To disable this policy, you need to unbind the policy from your user group first.
4. During service ticket privilege escalation, the system needs to verify the region, application, and service ticket status of the resources required. If a resource does not belong to any region or application, the system does not verify the resource but will display all service tickets of the user. Verification requirements on service tickets are as follows.
   - Incident ticket status verification:

i. P1, P2, P3, and P4 incident tickets must be in the accepted state.

ii. The privilege escalation application must be the same as the one in the incident ticket analysis and handling phase.

iii. The privilege escalation operator must be the current owner in the incident analysis and handling phase.

iv. The privilege escalation region must be the same as the region specified in the incident ticket.

– War room status verification:

i. A war room must be in the started or fault demarcation phase.

ii. The privilege escalation application must be in the list of applications affected by the war room.

iii. The privilege escalation operator must be the fault rectification owner, a fault rectification member, or the administrator of the war room.

– Change ticket status verification:

i. The region and application for the privilege escalation must be the same as those specified in the change ticket.

ii. The privilege escalation operator must be the implementer of the change ticket.

iii. The current operation time must be within the planned implementation time window of the change ticket. (The current operation time must be later than the planned start time and earlier than the planned end time.)

iv. You must click **Change Start** for a change ticket.

NOTICE

After service ticket privilege escalation is enabled, the northbound interface becomes unavailable. For example, if a script is executed to enable service ticket privilege escalation, the northbound script interface cannot be used.

Configuring Change Control

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Change Ticket Mgmt** > **Change Control**.

Step 3 Click **Enable Service Ticket Authorization**.

Service ticket authorization is disabled by default and can be enabled or disabled. After this function is enabled, all actions performed on the COC platform will be displayed in the list.

Step 4 Locate the action you want to modify and click **Modify** in the **Operation** column.

Only actions whose value of the **Interconnected** column is **Yes** can be modified.

Step 5 Set parameters in **Modify Service Ticket Type**.

Table 8-10 Parameters for modifying a service ticket type

Parameter	Description
Enable Service Ticket Authorization	Options: **Enable** and **Disable**. **Enable** indicates that privilege escalation is required. **Disable** indicates that privilege escalation is not required for all accounts in this scenario.
Ticket Type	The options are **Change ticket**, **Incident ticket**, and **War room**. Multiple options can be selected.
Automatic Ticket Creation	The options are **Yes** and **No**.

Step 6 Click **Correlation Policy** under **Enable Service Ticket Authorization**.

Step 7 Set **Correlation Policy**.

Table 8-11 Parameters for adding a policy

Parameter	Description
Add to User Group	Select a user group. Multiple options can be selected. Add the automatic COC policies to the user group of the account.

Step 8 Click **OK**.

The change control configuration is complete.

----End

8.7 Viewing the Change Calendar

Scenarios

After a change ticket is created, you can view the distribution and details of the change ticket in the change calendar by month or day. The detailed operations are as follows:

Viewing the Change Calendar

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Ticket Mgmt** > **Change Calendar**.

- By default, the distribution of changes reviewed in the current month is displayed. You can click a change title to go to the corresponding change ticket details page.

- You can filter changes by change application, change level, status, and change title.
- To view the change information of a day, click the corresponding date.

NOTE

- Change tickets in the **Pending review**, **Pending implementation verification**, **Successful**, **Failed**, and **Canceled** states are displayed in the change calendar.
- By default, the change application and title are displayed in the change calendar. Different colors indicate different change status.
- Rules for sorting change tickets:
  - The sorting based on the cross-day duration is used preferentially, with longer cross-day duration yielding higher ranking
  - The change plan with an earlier start time ranks higher.
  - If the change plans start at the same time, the one created first ranks higher.

----End

9 Resilience Center

9.1 Chaos Drills

9.1.1 Overview

With the transformation from traditional IT infrastructure O&M to cloud service O&M, traditional O&M methods face challenges such as complex inter-service invoking, fast application iteration, massive O&M objects, and complex non-linearity systems. Service downtime will bring huge economic losses and reputational damage to the company.

Chaos engineering is introduced to the O&M process. Through periodic simulation, system weaknesses (such as software bugs, solution design defects, and fault recovery process points) can be identified before problems occur on the live network, and system availability problems can be detected and resolved in a timely manner, continuously improve application resilience and build O&M confidence. For unavoidable scenarios (such as hardware faults, abnormal server power-off, and network device board faults), formulate a contingency plan for quick fault recovery in advance.

COC allows you to perform automatic chaos drills covering from risk identification, emergency plan management, fault injection, and review and improvement. Based on years of best practices of Huawei Cloud SRE in chaos drills, customers can proactively identify, mitigate, and verify risks of cloud applications, continuously improving the resilience of cloud applications.

Image and Disruptor Version Support Statement

Currently, the chaos drill feature supports probe attack objects such as Elastic Cloud Servers (ECSs), FlexusL instances, and Bare Metal Servers (BMSs), and provides corresponding resource and network disruptors for you to drill. Probe disruptors include disruptors for practicing, host resources, host processes, and host network modules. By integrating disruptor modules and functions, you can accurately simulate faults in the actual environment and detect system availability issues as early as possible, continuously improving application resilience.

The following table lists the ECSs, FlexusL, and BMSs image versions and supported probe tools.

⚠ CAUTION

CentOS 6.10 images and earlier versions do not support some probe disruptors because the system does not have the shared libraries (GLIBC_2.14 and GLIBCXX_3.4.15) required for running corresponding probe packages.

Table 1 lists the probe disruptors supported by each ECS image version.

Table 9-1 ECS and disruptor compatibility list

Disruptor		Supported Image Version	Description
Disruptors for practicing	Qualifying practice	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
Host resources	CPU usage increase	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Memory usage increase	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Disk usage increase	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-

Disruptor		Supported Image Version	Description
	Disk I/O pressure increase	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
Host process	Process ID exhaustion	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	The process IDs of the EulerOS image are used up. The protection mechanism may be triggered, causing the kernel to restart. As a result, the drill fails.
	Killing a process/ Continuously killing a process	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
Host network	Network latency	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Network packet loss	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Network error packets	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-

Disruptor		Supported Image Version	Description
	Duplicate packets	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Network packet disorder	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Network disconnection	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	NIC break-down	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	If the NIC becomes faulty, the UniAgent may go offline. As a result, the UniAgent information cannot be received, and the page fails to be displayed.
	DNS tempering	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-

Disruptor		Supported Image Version	Description
	Port occupation	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Server disconnection	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	If the server becomes fault, the UniAgent may go offline. As a result, the UniAgent information cannot be received, and the page fails to be displayed.
	NIC bandwidth limiting	CentOS 7.2, CentOS 7.6, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-
	Connection exhaustion	CentOS 7.2, CentOS 7.6, CentOS 7.9, CentOS 8.2, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, EulerOS 2.2, EulerOS 2.5, EulerOS 2.9, EulerOS 2.10, Debian 8.2.0, Debian 8.8.0, Debian 9.0.0, Debian 11.1.0, and Huawei Cloud EulerOS 2.0	-

Table 9-2 lists the probe disruptors supported by each BMS image version.

Table 9-2 Bare metal server image and tool compatibility list

Disruptor		Supported Image Version
Disruptors for practicing	Qualifying practice	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3

Disruptor		Supported Image Version
Host resources	CPU usage increase	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Memory usage increase	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Disk usage increase	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Disk I/O pressure increase	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
Host process	Process ID exhaustion	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Killing a process/ Continuously killing a process	CentOS 7.4, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
Host network	Network latency	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Network packet loss	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Network error packets	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Duplicate packets	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Network packet disorder	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	Network disconnection	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	NIC break-down	CentOS 7.3, CentOS 7.9, Ubuntu 16, Ubuntu 1804, and EulerOS 2.3
	DNS tempering	CentOS 6.9, CentOS 7.9, Ubuntu 16, Ubuntu 1804, EulerOS 2.3, and EulerOS 2.9
	Port occupation	CentOS 6.9, CentOS 7.9, Ubuntu 16, Ubuntu 1804, EulerOS 2.3, and EulerOS 2.9

Disruptor		Supported Image Version
	Server disconnection	CentOS 6.9, CentOS 7.9, Ubuntu 16, Ubuntu 1804, EulerOS 2.3, and EulerOS 2.9
	NIC bandwidth limiting	CentOS 6.9, CentOS 7.4, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, EulerOS 2.3, and EulerOS 2.9
	Connection exhaustion	CentOS 7.4, CentOS 7.9, Ubuntu 16.04, Ubuntu 18.04, EulerOS 2.3, and EulerOS 2.9

Table 9-3 lists the probe disruptors supported by each FlexusL image.

Table 9-3 FlexusL instance images and probe tool compatibility list

Disruptor		Supported Image Version
Disruptors for practicing	Qualifying practice	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
Host resources	CPU usage increase	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Memory usage increase	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Disk usage increase	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Disk I/O pressure increase	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
Host process	Process ID exhaustion	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Killing a process/ Continuously killing a process	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
Host network	Network latency	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Network packet loss	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0

Disruptor		Supported Image Version
	Network error packets	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Duplicate packets	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Network packet disorder	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Network disconnection	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	NIC break-down	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	DNS tempering	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Port occupation	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Server disconnection	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	NIC bandwidth limiting	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0
	Connection exhaustion	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, and Debian 11.1.0

9.1.2 Creating and Managing Failure Modes

Scenarios

A failure mode refers to a specific type of problem or failure status that may occur during application running. Build a rich failure mode library and formulate corresponding prevention and recovery measures to help design a more highly available application system. By identifying potential faults, you can perform routine drills to verify whether the fault recovery measures and fault impacts meet the expectations and prepare for better response to various challenges. You can analyze the possible fault points of an application, create a failure mode by describing the fault occurrence conditions, fault symptoms, and customer impacts, and apply the failure mode to routine chaos drills.

Precautions

Verify that the enterprise project, application, event level, and scenario category of the failure mode are correct.

Creating a Failure Mode

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 On the **Failure Modes** tab page, click **Create Failure Mode**.

Step 4 Set parameters for creating a failure mode.

Table 9-4 Parameters for creating a failure mode

Parameter	Description
Failure Mode	Custom failure mode name

Parameter	Description
Scenario Category	The options are **Node**, **Cluster**, **Network**, **DR**, **Container**, and **Service and Data**. ● **Node**: The CPU or memory of the host is overloaded, or the process is faulty. As a result, services are abnormal, for example, the CPU or memory is overloaded, or the process status is abnormal. ● **Cluster**: Simulate abnormal scenarios by increasing the pressure or performing an active/standby cluster switchover, for example, increasing the pressure of the container cluster and performing an active/standby switchover in the database cluster. ● **Network**: Inject network faults to hosts or clusters to verify the DR capability of your service. Such faults include packet loss, network latency, and intermittent disconnection at the link layer. ● **DR**: Simulate inter-region network exceptions or service unavailability in a single region to verify the self-recovery capabilities of services. ● **Container**: Simulate process and resource faults and network attacks on container instances, such as CPU and memory pressure increase, network attacks, system OOM, or process killing. ● **Service and data**: Simulate service exceptions caused by database or file exceptions, such as database table deletion and database unavailability.
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. By default, P1 incidents are the most critical, while P5 incidents are the least severe.

Parameter	Description
Source	The options are **Failure modes detected proactively** and **Existing failure modes**. ● **Proactive analysis**: Proactively analyze risks in the application architecture and running environment to form a failure mode. ● **Existing faults**: A failure mode is formed based on the analysis of existing faults and incidents.
Alarm ID	(Optional) ID of the alarm that is triggered when a fault occurs.
Attack Scenario	(Optional) Select an attack scenario from the drop-down list. A maximum of 10 attack scenarios can be selected.
Enterprise Project	Select the enterprise project to which the failure mode resource belongs from the drop-down list.
Application	Select the application to which the drill target belongs from the drop-down list.
Contingency Plan Available	This feature toggle can be enabled or disabled.
Contingency Plan Available	This parameter is mandatory when **Contingency Plan Available** is enabled. Select a contingency plan from the drop-down list. If no best-fit contingency plans are available, create one. For details, see **Creating a Custom Contingency Plan**.
Occurrence Conditions	Enter the conditions under which the fault may occur. The value can contain a maximum of 1,024 characters.
Fault Symptom	Enter the possible service symptom when the fault occurs. The value can contain a maximum of 1,024 characters.

Parameter	Description
Impact on Customer	Failure impact on customers. The value can contain a maximum of 1,024 characters.

Step 5 Click **OK**.

The failure mode is created.

----End

Cloning a Failure Mode

Only excellent failure modes can be cloned. For details about the excellent failure modes, see pre-defined failure modes on COC.

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Choose **Failure Modes** > **Excellent Failure Mode Cases**.

Step 4 Locate the failure mode you want to clone and click **Clone** in the **Operation** column.

Step 5 Set parameters for cloning a failure mode.

Table 9-5 Parameters for cloning a failure mode

Parameter	Description
Failure Mode	Custom failure mode name

Parameter	Description
Scenario Category	The options are **Node**, **Cluster**, **Network**, **DR**, **Container**, and **Service and Data**. ● **Node**: The CPU or memory of the host is overloaded, or the process is faulty. As a result, services are abnormal, for example, the CPU or memory is overloaded, or the process status is abnormal. ● **Cluster**: Simulate abnormal scenarios by increasing the pressure or performing an active/standby cluster switchover, for example, increasing the pressure of the container cluster and performing an active/standby switchover in the database cluster. ● **Network**: Inject network faults to hosts or clusters to verify the DR capability of your service. Such faults include packet loss, network latency, and intermittent disconnection at the link layer. ● **DR**: Simulate inter-region network exceptions or service unavailability in a single region to verify the self-recovery capabilities of services. ● **Container**: Simulate process and resource faults and network attacks on container instances, such as CPU and memory pressure increase, network attacks, system OOM, or process killing. ● **Service and data**: Simulate service exceptions caused by database or file exceptions. Such faults include packet loss, network latency, and intermittent disconnection at the link layer.
Incident Level	The options are **P1**, **P2**, **P3**, **P4**, and **P5**. By default, P1 incidents are the most critical, while P5 incidents are the least severe.
Source	The options are **Failure modes detected proactively** and **Existing failure modes**. ● **Proactive analysis**: Proactively analyze risks in the application architecture and running environment to form a failure mode. ● **Existing faults**: A failure mode is formed based on the analysis of existing faults and incidents.
Alarm ID	(Optional) ID of the alarm that is triggered when a fault occurs.
Attack Scenario	(Optional) Select an attack scenario from the drop-down list. A maximum of 10 attack scenarios can be selected.
Enterprise Project	Select the enterprise project to which the failure mode resource belongs from the drop-down list.

Parameter	Description
Application	Select the application to which the drill target belongs from the drop-down list.
Contingency Plan Available	This feature toggle can be enabled or disabled.
Contingency Plan Available	This parameter is mandatory when **Contingency Plan Available** is enabled. Select a contingency plan from the drop-down list. If no best-fit contingency plans are available, create one. For details, see **Creating a Custom Contingency Plan**.
Occurrence Conditions	Enter the conditions under which the fault may occur. The value can contain 1 to 1,024 characters.
Fault Symptom	Enter the possible service symptom when the fault occurs. The value can contain 1 to 1,024 characters.
Impact on Customer	Failure impact on customers. The value can contain 0 to 1,024 characters.

Step 6 Click **OK**.

The failure mode is cloned.

----End

9.1.3 Creating and Managing Drill Plans

Scenarios

You can schedule failure modes using drill plans. When creating a drill plan, you can specify the executor and planned drill time. The executor creates a drill task when receiving a service ticket and associate the drill task with a failure mode and a region.

Precautions

You do not need to specify the enterprise project to which a drill plan belongs. The enterprise project must be the same as that associated with the failure mode.

Creating a Drill Plan

Step 1 Log in to **COC**.

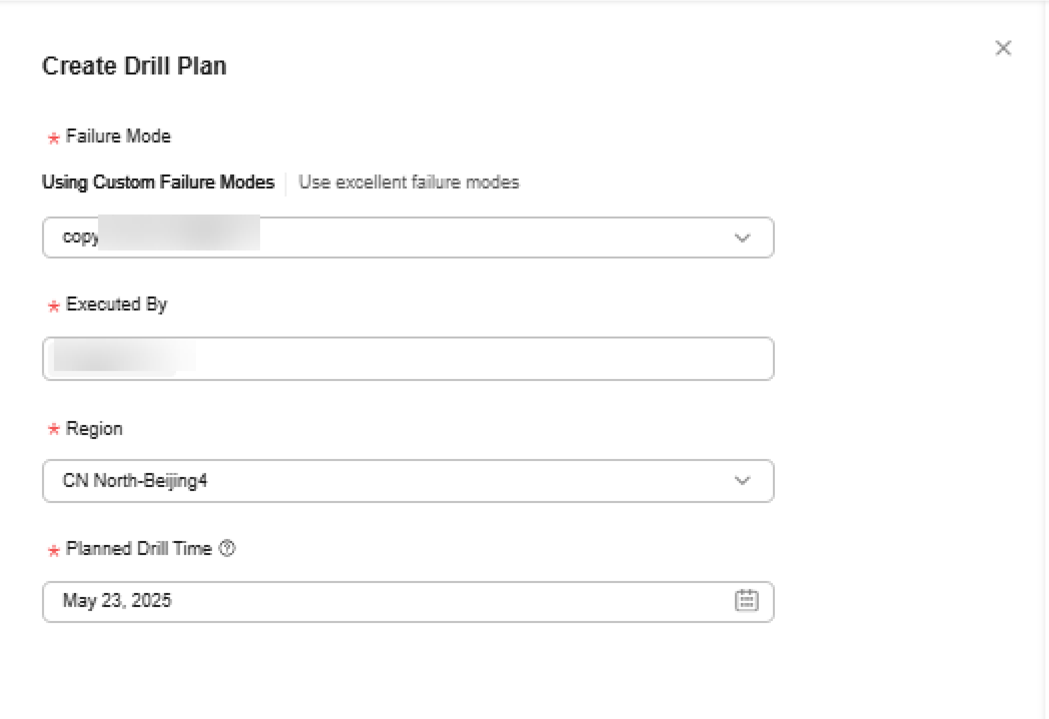
Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Plans** tab.

Step 4 Click **Create Drill Plan**.

Step 5 Set parameters for creating a drill plan.

Figure 9-1 Creating a drill plan



Create Drill Plan

* Failure Mode

Using Custom Failure Modes | Use excellent failure modes

copy[redacted]

* Executed By

[redacted]

* Region

CN North-Beijing4

* Planned Drill Time

May 23, 2025

Table 9-6 Parameters for creating a drill plan

Parameter	Description
Failure Mode	The options are **Use custom failure mode** and **Use preset failure mode**. Select a failure mode from the drop-down list box.
Executor	Select the user who performs the drill from the drop-down list.
Region	Select a region from the drop-down list.
Planned Drill Time	Set the end date of the drill. The executor must complete the drill before the planned drill time.
Enterprise Project	This parameter is mandatory when **Failure Mode Name** is set to **Use preset failure mode**. Select the enterprise project to which the drill belongs from the drop-down list.

Step 6 Click **OK**.

The drill plan is created.

----End

Cancelling a Drill Plan

Only tickets in the pending state can be canceled. Only the creator can perform this operation.

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Plans** tab.

Step 4 Locate the drill plan you want to cancel, click **More** and choose **Cancel** in the **Operation** column.

Step 5 Click **Cancel**.

The drill plan is canceled.

----End

Accepting a Drill Plan Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Plans** tab.

Step 4 Locate the drill plan you want to accept and click **Accept** in the **Operation** column.

The **Create Drill Task** page is displayed. For details, see **Creating a Drill Task**.

----End

9.1.4 Creating and Managing Drill Tasks

Scenarios

Drill tasks allow you to simulate software or hardware faults to test the system's fault recovery capability. Drill task operations include managing chaos drill tasks, viewing drill records, and creating drill tasks. Setting a drill task include setting the basic information, adding an attack task group, selecting an attack task, and selecting an attack scenario. In addition, a drill task involves monitoring task configuration and post-drill review and improvement. This ensures that an excellent optimization policy can be applied when the system is under various pressures.

Automatic Task Termination Mechanism

- Automatic termination upon timeout: If a drill task fails and you do not manually close the task within 48 hours, the system automatically terminates the drill task.

- Automatic termination upon exceptions: During the drill, if a pod exception (for example, the pod has been deleted) is detected or a resource O&M ticket is manually closed, the system automatically terminates the current task immediately.

Creating a Drill Task

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

Step 4 Click **Create Task**.

You can also use the drill plan ticket accepting function to access the page for creating a drill task. For details, see **9.1.3 Creating and Managing Drill Plans**.

Step 5 Configure the basic information.

Table 9-7 Parameters in the basic information

Parameter	Description	Example Value
Drill Task	Name of the drill task. Set it according to the naming rules.	test-drill
Expected Recovery Duration (Minutes)	Expected time from the fault occurrence to the fault recovery, in minutes. Expected time for an application to automatically recover to the normal state during emergency plan execution after a fault is injected. This time does not affect the drill task.	3

Step 6 Click **Add Attack Task**.

By default, there is one attack task group. You can click **Add Task Group** to add a task group. After adding an attack task, you can click **Add Attack Task** to add another attack task.

NOTE

- Tasks in different task groups are executed in serial mode, and tasks in the same task group are executed in parallel mode.
- Currently, multiple fault injection operations on the same resource in a task group are not supported.

1. Set parameters for adding an attack task.
   - To add an existing task, click **Select from Existing**, select the existing task, and click **OK**.
   - To add a new attack task, perform the follow-up steps.

Table 9-8 Parameters for adding an attack task

Parameter	Description	Example Value
Vendor	Select a cloud vendor type.	Huawei Cloud
Source of Attack Target	Select the source of the target instance. You can select attack targets by selecting instances, pods, or a specified number of targets if CCE instances are used.	Elastic Cloud Server (ECS)
Attack Task	Customize the name of the attack task based on the naming rule.	test-attacktask
Attack Target	Select the target instance.	-

2. Click **Next**.
3. Set parameters for selecting an attack scenario.

   For details, see **9.1.7 Attack Scenarios**.

Table 9-9 Parameters for selecting an attack scenario

Parameter	Description	Example Value
Attack Type	Attack scenarios are classified based on attack scenario types.	Host Resource
Attack Scenario	Select an attack scenario.	CPU usage increase
Attack Parameters	Configure attack parameters based on attack scenarios.	CPU Usage (%): 80 Fault Duration (s): 60

4. Click **Next**.
5. (Optional) Set **Configure Monitoring Tasks**.

Table 9-10 Parameters for configuring a monitoring task

Parameter	Description
Steady-State Metrics	Select the target resource, performance metric, lower limit, and upper limit from the drop-down lists one by one. If a service can perform well and stably when a performance monitoring metric is set to a certain value range, this metric is called stable-status metric. If this metric value is not in that value range before a drill, the drill will be canceled.

Parameter	Description
Metric	Select the target resource, monitoring metric, lower limit, and upper limit from the drop-down lists one by one. These service metrics monitor the corresponding service data during fault drills. If the value of such a metric is within the allowed value range, the service is normal. Otherwise, you can determine whether to stop a drill.
Automatic Rollback	Select whether to enable automatic rollback. Fault injection is automatically rolled back and restored to the status before fault injection. Automatic rollback cannot be configured for some disruptors for fault drills that do not support fault termination. If the value of a steady-state metric is not within the stable value range during a drill, the corresponding fault injection automatically stops after automatic rollback is enabled.

6. Click **Finish**. The attack task is added.

Step 7 Click **OK**.

----End

Modifying a Drill Task

Modify the created drill task. If a drill record has been generated for the drill task, the drill task cannot be modified.

Step 1 Log in to COC.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

Step 4 Locate the drill task you want to modify and click **More** in the **Operation** column and choose **Modify**.

Step 5 Modify the drill task based on the requirement scenario.

- Click **Add Task Group**.
- Click **Add Attack Task**.
- Click **Delete** in the row of a task to delete the attack task.

Step 6 Click **OK**.

The drill task is modified.

----End

Deleting a Drill Task

Delete a created drill task. If a drill record has been generated for the drill task, the drill task cannot be deleted. If a drill plan is associated with the drill task, the drill task cannot be deleted.

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

Step 4 Locate the drill task you want to delete and click **More** in the **Operation** column and choose **Delete**.

Step 5 Click **OK**.

The drill task is deleted.

----End

Starting a Drill Task

Start a drill task.

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

Step 4 Locate the drill task you want to start and click **Start** in the **Operation** column.

Step 5 Click **OK**.

The drill starts. On the drill details page, you can view the attack progress, including installing probes, performing drills, and clearing the environment. The system automatically performs the drill task. The execution time depends on the attack time of the disruptor.

⚠ CAUTION

In the probe installation step, a probe will be installed on the target machine. The probe runs in the system to receive disruptor commands for attack, query, and clearance. After the drill is complete or terminated, the environment clearing step stops all operations in the system and is removed.

Step 6 For drill execution, the following operations are supported:

- **Terminate**: During a drill, click **Terminate** in the upper right corner to stop the task to be executed or the task that is abnormal.
- **Retry**: If some or all attack tasks fail to check instances, install probes, clear environments, or perform steady-state detection, or the drill times out, expand the failed attack task and click **Retry** to retry the task.
- **Skip**: If some or all attack tasks fail to be executed during the drill, expand a failed attack task and click **Skip** to skip the task and execute the next task.

- **Details**: Expand an attack task and click Details to view the attack details.

NOTE

Description of the drill details page:

- The drill record module displays attack task details, including the attack task progress, task information, and execution time.
- The attack details module displays the attack status of instances in the application of the current task. BMSs, FlexusL (HCSS) instances, and CSS instances are not supported.
- The monitoring details module displays real-time monitoring data of attack targets. You need to configure a drill monitoring task when creating an attack task.

----End

Viewing Drill Records

View the drill records of a drill task. A drill task that has not been drilled does not contain drill record.

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

Step 4 Locate the target drill task and click **Drill Record** in the **Operation** column.

The basic information about the drill task includes the drill task name, drill task ID, attack details, and failure mode. All drill records include the drill record ID, execution status, executor, drill start time, and drill end time.

Step 5 Locate the drill record to be viewed and click **View Progress** in the **Operation** column.

View the attack progress and attack details of the current drill task.

Step 6 Click **Drill Report** on the right.

Create or view a drill report. For details, see **9.1.5 Creating a Drill Report**.

----End

9.1.5 Creating a Drill Report

Scenarios

After a drill task is complete, you can directly create a report if necessary. After a report is created, you can export the report as a PDF file and send it to related personnel. The entire process is flexible and efficient, meeting the requirements of the entire process from production to format fixing.

You can modify the actual fault recovery duration, create improvement tickets, and view fault records in a drill report so that you can comprehensively record and manage drill activities and results.

The drill report consists of the following modules:

- Recovery capability scoring module: You can modify the actual recovery duration. The system automatically generates a recovery capability score.

- Basic information module: displays basic information about a drill task, including the drill task name, drill report ID, drill start time, end time, drill executor, drill duration, and expected fault recovery duration (minutes).
- Drill process module: displays drill task cards.
- Attack task group module: displays attack task details, including attack targets, steady-state metrics, and monitoring metrics.

  The list of selected instances is displayed for attack targets. Line charts are displayed for steady-state metrics and monitoring metrics. If no data is available, **No data available** is displayed.
- Improvement item module: You can create improvement tickets. The improvement details are displayed by default, including the processing and verification information.

Creating a Drill Report

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Resilience Center** > **Chaos Drills**.

Step 3 Click the **Drill Tasks** tab.

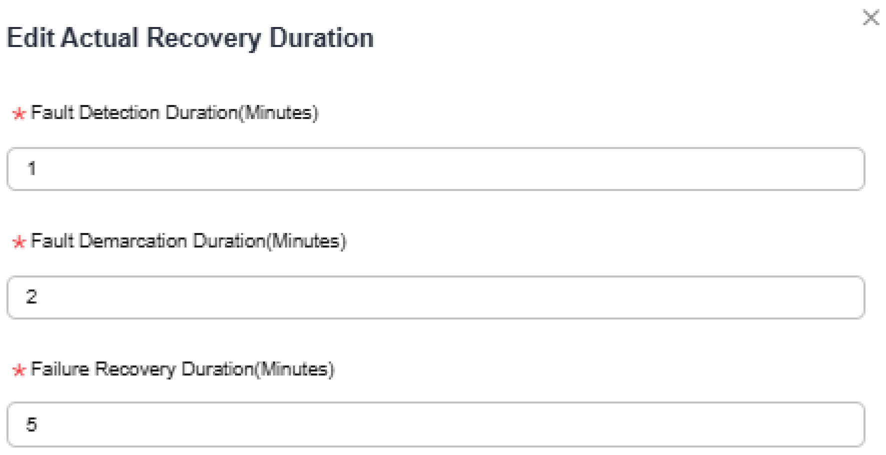
Step 4 Locate the target drill task and click **Drill Record** in the **Operation** column.

Step 5 Select a target drill record and click **Generate Report** in the **Operation** column.

Step 6 Click **Edit Duration** to change the actual recovery duration.

Actual recovery duration: indicates the actual time required for an application to automatically recover to the normal state or achieve recovery through the execution of a contingency plan after a fault is injected.

Figure 9-2 Changing the actual recovery duration



Edit Actual Recovery Duration

* Fault Detection Duration(Minutes)

1

* Fault Demarcation Duration(Minutes)

2

* Failure Recovery Duration(Minutes)

5

Table 9-11 Parameters for modifying the actual restoration duration

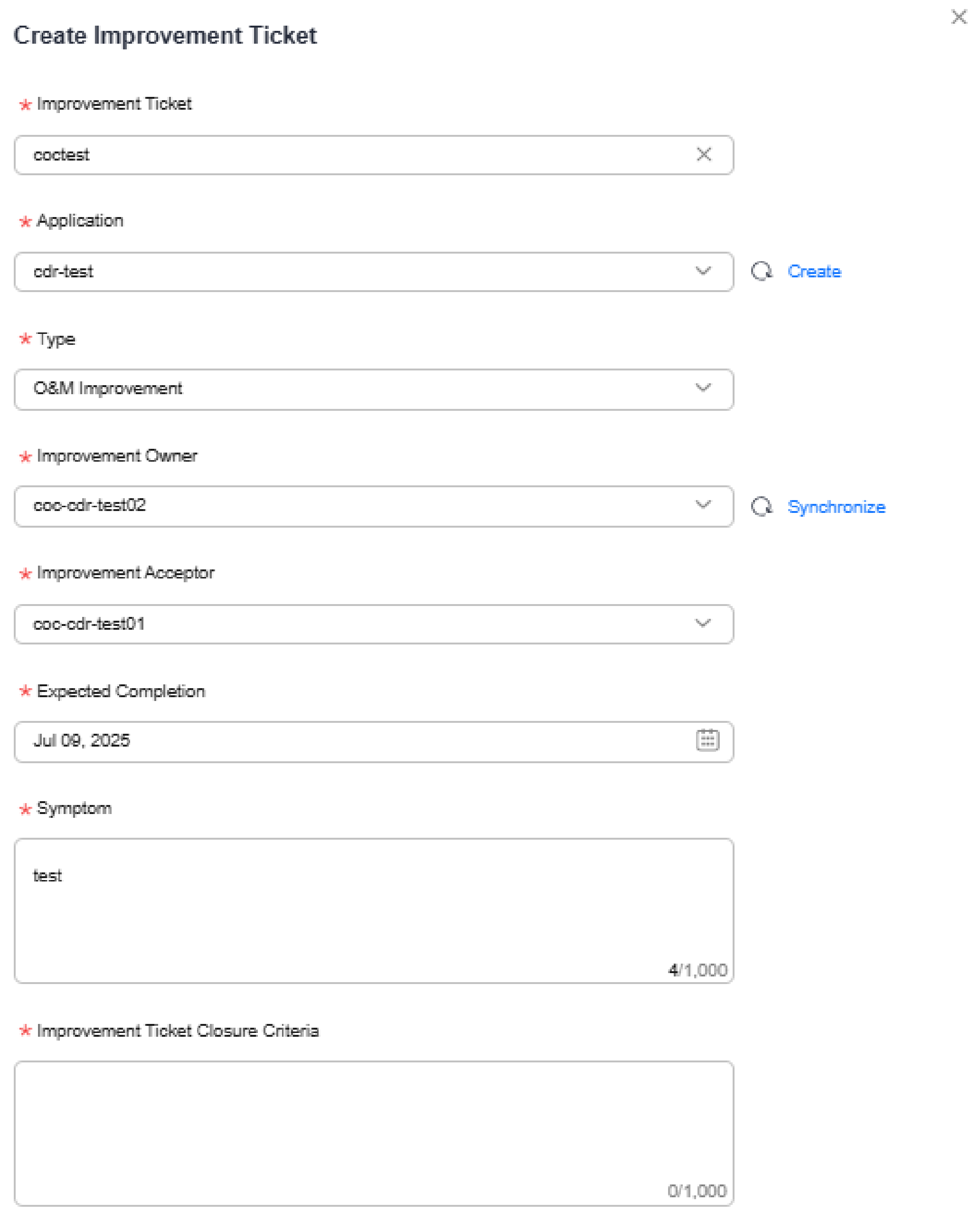
Parameter	Description
Fault Detection Duration (Minutes)	Enter the fault detection duration. Duration from the time when the fault injection is complete to the time when the fault alarm is received.
Fault Demarcation Duration (Minutes)	Enter the fault demarcation duration. Duration from the time when an alarm is reported to the time when the fault demarcation is complete
Fault Recovery Duration (Minutes)	Enter the fault recovery duration. Time from fault demarcation to fault recovery.

Step 7 Click **OK**.

After the actual recovery duration is changed, the system automatically generates a recovery capability score.

Step 8 Click **Create Improvement Ticket**. In the dialog box that is displayed, set the improvement ticket information.

Figure 9-3 Creating an improvement ticket



Create Improvement Ticket

* Improvement Ticket: coctest
* Application: cdr-test
* Type: O&M Improvement
* Improvement Owner: coc-cdr-test02
* Improvement Acceptor: coc-cdr-test01
* Expected Completion: Jul 09, 2025
* Symptom: test
* Improvement Ticket Closure Criteria:

Table 9-12 Parameters for creating an improvement ticket

Parameter	Description
Improvement Ticket	Name of an improvement ticket. Name of an improvement ticket. The name can contain a maximum of 64 characters, including letters, digits, hyphens (-), underscores (_), and spaces. It cannot start or end with a space.
Application	Select an application for which the improvement is performed from the drop-down list.

Parameter	Description
Type	Select an improvement type from the drop-down list. The options are **Product**, **O&M**, **Management**, and **Monitoring & alerting**.
Improvement Owner	Select an owner from the drop-down list.
Improvement Acceptor	Select an acceptance user from the drop-down list.
Expected Completion	Enter the expected completion time (accurate to day). The selected date cannot be earlier than today.
Symptom	Enter the incident-related problem symptom. Enter a maximum of 1,000 characters.
Improvement Ticket Closure Criteria	Enter the improvement closure criteria. Enter a maximum of 1,000 characters.

Step 9 Click **OK**.

After the ticket is created, the improvement item list is expanded by default, including the processing information and verification information.

----End

Other Operations

Table 9-13 Operation description

Function	Description
Export Report	On the drill report page, click **Export Report** in the upper right corner to download the PDF file of the current page.
Refresh	On the drill report page, click **Refresh** in the upper right corner to refresh the current page.
View Report	On the drill records page, locate the row that contains the target drill record and click **View Report** in the **Operation** column.

9.1.6 Creating a Custom Fault

Scenarios

You can create a failure mode to perform routine drills for potential faults and verify whether the fault recovery measures and fault impact meet the expectation. This helps you better prepare for various challenges.

Precautions

A custom fault is determined by the script you compiled. Therefore, when scripts are used to attack ECSs, exceptions such as high resource usage and network faults may occur. As a result, the status of the UniAgent installed on the ECSs may change to offline or abnormal. Exercise caution when performing this operation.

Creating a Custom Fault

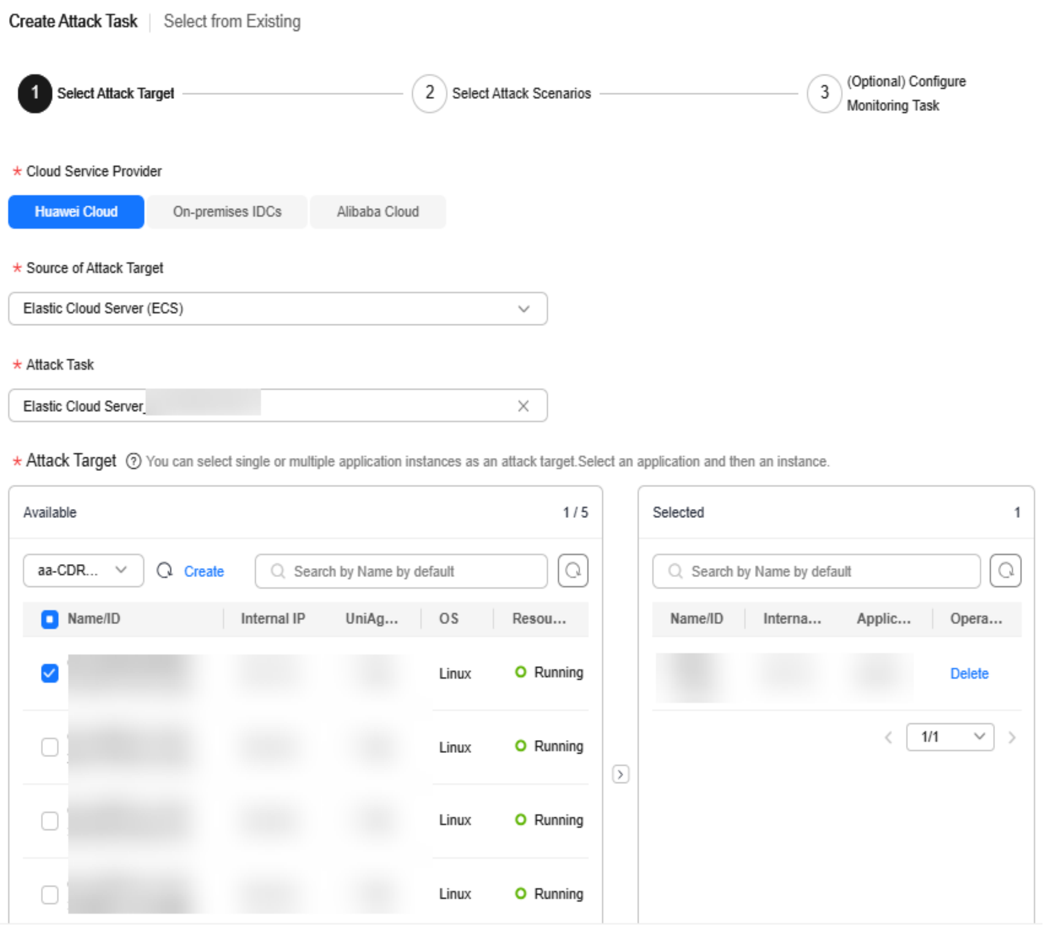
Create a drill task for a custom fault attack scenario on COC.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click the **Drill Tasks** tab and create an attack task by referring to **9.1.4 Creating and Managing Drill Tasks**.

Step 3 Enter the attack task name, select Elastic Cloud Server (ECS) as **Source of Attack Target**, and click **Next**.

Figure 9-4 Selecting ECS as the attack target source



* Cloud Service Provider: Huawei Cloud

* Source of Attack Target: Elastic Cloud Server (ECS)

* Attack Task: Elastic Cloud Server_

* Attack Target ⓘ You can select single or multiple application instances as an attack target.Select an application and then an instance.

Available 1 / 5

aa-CDR... Search by Name by default

	Name/ID	Internal IP	UniAg...	OS	Resou...
☑				Linux	Running
□				Linux	Running
□				Linux	Running
□				Linux	Running

Selected 1

Search by Name by default

Name/ID	Interna...	Applic...	Opera...
			Delete

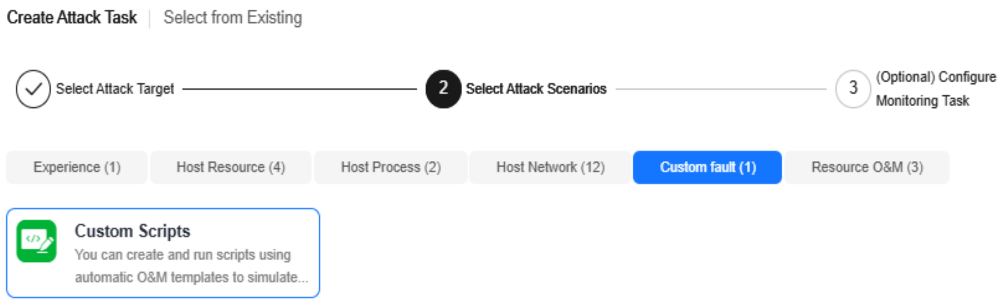
1/1

Step 4 On the **Select Attack Scenario** procedure, click **Custom fault**, and then **Custom Scripts**.

- If a user-defined fault script exists, you can select an existing script. In this case, go to **Step 6**.

- If no user-defined fault script has been created or the existing script does not apply to the current scenario, perform step **Step 5** to create a script.

Figure 9-5 Selecting **custom fault** as the attack scenario



You can create and run scripts using automatic O&M templates to simulate...

Step 5 To create a custom fault script, click **Scripts**. The **Automated O&M** > **Scripts** page is displayed. Click **Create Script**. For details about how to create a script, see section **6.2.3 Creating Custom Scripts**. For details about the script specifications, see the following code:

```
#!/bin/bash
set +x

function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}

function inject_fault()
{
    echo "inject fault"
}

function check_fault_status()
{
    echo "check fault status"
}

function rollback()
{
    echo "rollback"
}

function clean()
{
    echo "clean"
}

case "$ACTION" in
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
```

```
  *)
     usage
;;
esac
```

You are advised to define a custom fault script based on the preceding script specifications. In the preceding specifications, you can define the fault injection function, fault check function, fault rollback function, and environment clearing function by compiling customized content in the **inject_fault()**, **check_fault_status()**, **rollback()** and **clean()** functions.

According to the preceding specifications, there are two mandatory script parameters: Whether other script parameters are included depends on your script content.

Table 9-14 Mandatory parameters for customizing a fault script

Parameter	Value	Description
ACTION	inject_fault	Drill operation action. The value is automatically changed by the system background in different drill phases. The options are as follows: ● **inject_fault**: The drill is in the fault injection phase. ● **check_fault_status**: The drill is in the fault query phase. ● **rollback**: The drill is in the phase of canceling the fault injection. ● **clean**: The drill is in the environment clearing phase.
CAN_ROLLBACK	false	Whether rollback is supported. The options are as follows: ● **true**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is executed. ● **false**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is not executed.

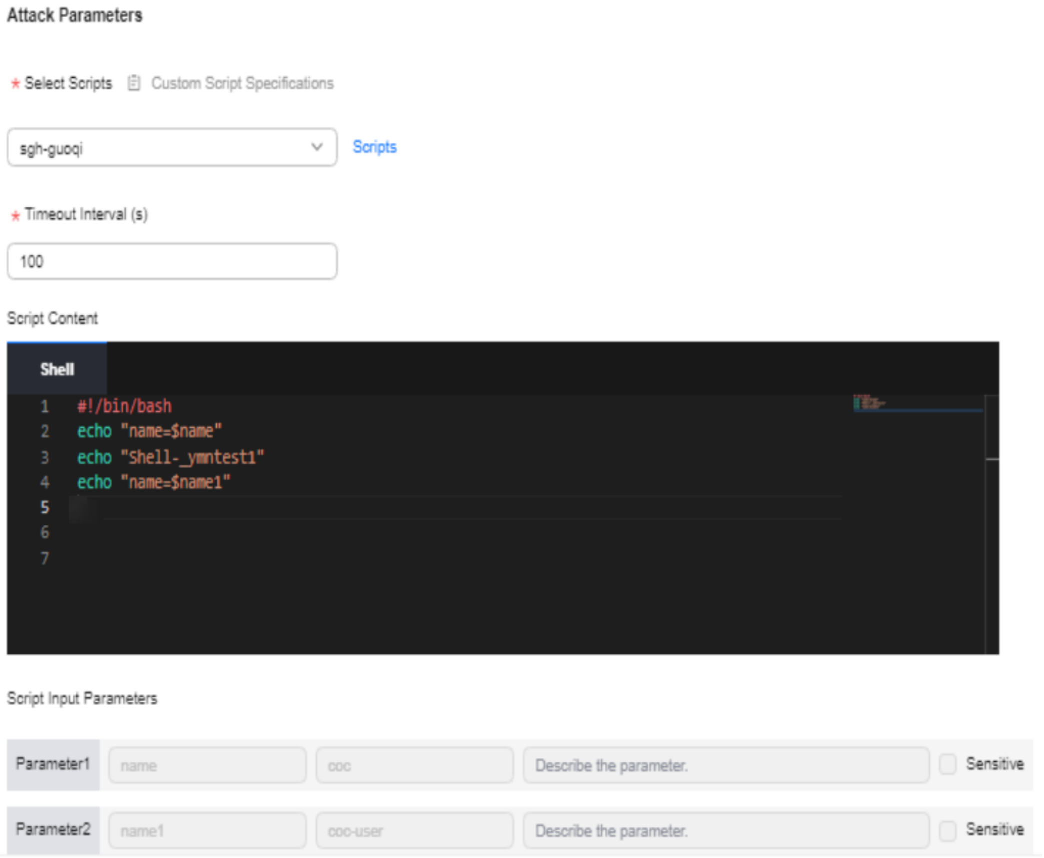
NOTE

In the **inject_fault** function, add a label indicating that the fault injection is successful, and check whether the label exists in the **check_fault_status** function.

- If it does, the **check_fault_status** function can return normally (for example, **exit 0**).
- If it does not, the **check_fault_status** function can return an exception (for example, **exit 1**).

Step 6 If you already have a custom script, you can select the script by its name from the drop-down list. After the script is selected, the corresponding script content and parameters are automatically displayed on the tab page.

Figure 9-6 Selecting a custom script



Attack Parameters

* Select Scripts

sgh-guoqi

* Timeout Interval (s)

100

Script Content

```
#!/bin/bash
echo "name=$name"
echo "Shell-_ymtest1"
echo "name=$name1"
```

Script Input Parameters

Parameter1	name	coc	Describe the parameter.	□ Sensitive
Parameter2	name1	coc-user	Describe the parameter.	□ Sensitive

Step 7 Set the timeout interval and click **Next**.

Timeout Interval: specifies the maximum time allowed for executing a script. **Note: The timeout interval must be longer than the actual script execution time. It is recommended that the timeout interval be at least 30 seconds longer than the actual script execution time**.

Step 8 Complete the remaining steps by referring to **9.1.4 Creating and Managing Drill Tasks**. Then, you can create a drill task whose attack scenario is set to **Custom fault**.

----End

Custom Script Example

The following is an example of a customized script.

The file content is listed as follows:

```
#!/bin/bash
set +x
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:~/bin
export PATH


function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}
```

```
function inject_fault()
{
    echo "============start inject fault============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
        mkdir -p "${SCRIPT_PATH}/${DIR_NAME}"
        echo "mkdir ${SCRIPT_PATH}/${DIR_NAME} successfully"
    fi

    cd "${SCRIPT_PATH}/${DIR_NAME}"

    if [ ! -f ${FILE} ]; then
        touch "${FILE}"
        echo "create tmp file ${FILE}"
        touch inject.log
        chmod u+x "${FILE}"
        chmod u+x inject.log
    else
        echo "append content">${FILE}
    fi
    echo "successfully inject">${FILE}
    echo "============end inject fault============"
}

function check_fault_status()
{
    echo "============start check fault status============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
        echo "inject has been finished"
        exit 0
    fi
    cd "${SCRIPT_PATH}/${DIR_NAME}"
    SUCCESS_FLAG="successfully inject"

    if [ -f ${FILE} ]; then
        if [[ "$(sed -n '1p' ${FILE})" = "${SUCCESS_FLAG}" ]]; then
            echo "fault inject successfully"
        else
            echo "fault inject failed"
            exit 1
        fi
    else
        echo "inject finished"
        exit 0
    fi
    sleep ${DURATION}
    echo "============end check fault status============"
}

function rollback()
{
    echo "============start rollback============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end rollback============"
}

function clean()
{
    echo "============start clean============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end clean============"
}

case "$ACTION" in
```

```
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
    *)
        usage
;;
esac
```

The input parameters of the script are described as follows:

Table 9-15 Script input parameters of the customized script example

Parameter	Value	Description
ACTION	inject_fault	Drill operation action
CAN_ROLLBACK	false	Rollback is not supported.
SCRIPT_PATH	/tmp	Root directory of the custom fault log
DIR_NAME	test_script	Parent directory of the custom fault log
FILE	test.log	Custom fault log name
DURATION	10	Duration of a simulated custom fault, in seconds. (This parameter does not take effect when it is placed in the **inject_fault** function.)

- In the sample **inject_fault** function, the injected fault is to **create a {FILE} file and add content to the {FILE} file**. If **successfully inject** is entered in the {FILE} file, the fault injection is successful.
- In the example, the **check_fault_status** function checks whether the file specified in *{FILE}* exists. If no, the fault may have been rectified. In this case, **exit 1** is returned. If yes, check whether the label indicating that the fault injection is successful exists. If the label exists, the fault injection is successful. Here, **sleep {DURATION}** is used to simulate the fault duration. If the label does not exist, the fault injection fails.

9.1.7 Attack Scenarios

Scenarios

Chaos drills support multiple attack scenarios, including disruptors for practicing, host resources, host processes, host networks, user-defined faults, and resource O&M. By integrating disruptor modules and functions, you can accurately simulate faults in the actual environment and identify system availability issues as early as possible, continuously improving application resilience. IPv6 fault drills of ECSs, BMSs, and on-premises IDC devices are supported. The drills of host network disruptors help you quickly master fault locating and emergency response capabilities in IPv6 networking environments, ensuring high network availability and security.

Constraints and Limitations

- FlexusL instance (HCSS) scenario: A drill task can be executed only on a single FlexusL host. High availability (HA) is not supported.
- Cloud Container Engine (CCE) scenario: The Kubernetes version supported by the drill task must be the same as that supported by CCE. For details, see **Kubernetes Version Policy**.

Attack Scenario Description

Table 9-16 Attack scenario description

Source of Attack Target	Attack Scenario		Description
ECSs	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. Drills cannot be terminated in an emergency scenario.
		Process killing	Kill processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.
		NIC bandwidth limiting	Limit the NIC bandwidth, support multiple NICs. The drill can be terminated in an emergency scenario.
		Connection exhaustion	Create a large number of socket connections to the specified server end (combination of the IP address and port number) to exhaust the connections. As a result, normal requests of the node cannot connect to the server (the requests of other nodes on the server may also be affected). The drill can be terminated in an emergency scenario.
	Customizing a fault	Customizing a script	Users can create scripts using automated O&M scripts and run the scripts to simulate faults. The drill can be terminated in an emergency scenario.
	Resource O&M	Device startup	Start ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
		Device shutdown	Shut down ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
		Device restart	Restart ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
BMSs	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. The drill cannot be terminated in an emergency scenario.
		Process killing	Kill processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.

Source of Attack Target	Attack Scenario		Description
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.
	Resource O&M	Device startup	Start ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
		Device shutdown	Shut down ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Device restart	Restart ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
FlexusL instances (HCSS)	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. The drill cannot be terminated in an emergency scenario.
		Process killing	Kill HCSS processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.

Source of Attack Target	Attack Scenario		Description
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.
	Resource O&M	Device startup	Start ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Device shutdown	Shut down ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
		Device restart	Restart ECSs, BMSs, and Flexus instances in batches. Status may not be synchronized in a timely manner. The drill can be terminated in an emergency scenario.
CCE nodes	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. The drill cannot be terminated in an emergency scenario.
		Process killing	Kill processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		NIC bandwidth limiting	Limit the NIC bandwidth, support multiple NICs. The drill can be terminated in an emergency scenario.
		Connection exhaustion	Create a large number of socket connections to the specified server end (combination of the IP address and port number) to exhaust the connections. As a result, normal requests of the node cannot connect to the server (the requests of other nodes on the server may also be affected). The drill can be terminated in an emergency scenario.
CCE pods	Pod resources	Increases pod CPU usage	Simulate a pod CPU usage surge. Ensure the attack target is writable. If it is not, the drill will fail. If the drill fails, you can use the emergency termination function.
		Pod memory usage increase	Simulate a pod memory usage surge. Ensure the attack target is writable. If it is not, the drill will fail. In this case, you can use the emergency termination function.
		Pod disk I/O pressure	Continuously simulates I/O reads and writes. The drill can be terminated in an emergency scenario.
		Pod disk usage increase	Writes large files to a specified directory to simulate the pressure increase of the Kubernetes container file system. The drill can be terminated in an emergency scenario.
	Pod process	Forcible pod stopping	Forcibly stop a pod. The drill cannot be terminated in an emergency scenario.
		Forcibly killing containers in a pod	Forcibly kill containers in a pod. The drill cannot be terminated in an emergency scenario.
	Pod network	Pod network latency	Simulate a network fault that incurs the network latency increase in a pod. Drills can be terminated in an emergency scenario. Drills cannot be terminated when the latency reaches 30,000 ms.

Source of Attack Target	Attack Scenario		Description
		Pod network packet loss	Simulate a network fault that incurs packet loss in a pod. Drills can be terminated in an emergency scenario.
		Pod network interruption	Simulate a network disconnection between a POD and other IP addresses. The drill can be terminated in an emergency scenario. To interrupt an established persistent connection, select all directions as the directions to be interrupted.
		Pod network packet disorder	Simulate packet disorder generated on a link due to a pod network fault. Drills can be terminated in an emergency scenario.
		Duplicate pod network packets	Simulate duplicate packets generated on a link due to a pod network fault. Drills can be terminated in an emergency scenario.
		Pod DNS tampering	If the address mapping of the domain name is tampered with in the pod, ensure that the running user of the attack target is root. Otherwise, the drill will fail due to insufficient permission. The drill can be terminated in an emergency scenario.
		Pod port masking	Simulate disabling of a pod port. The drill can be terminated in an emergency scenario.
		Pod network isolation	Simulate the scenario where access from a pod to another IP address networks is directly rejected. The drill can be terminated in an emergency scenario. If you need to reject established persistent connections, select **All** for **Direction**.
RDS instances	Instances	RDS active/standby switchover	Only MySQL and PostgreSQL engines in HA mode are supported. This operation is not allowed during creating and restarting instances, upgrading databases, recovering and modifying ports, as well as creating and deleting accounts. Active/standby switchover cannot change the IP address of the internal network of an instance. The drill cannot be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Stopping an RDS instance	Stop both the primary and read-only instances. After the fault duration ends, start the instance. The drill can be terminated in an emergency.
DCS instances	Instances	DCS active/standby switchover	Switch the primary and standby DB instance nodes. This operation is supported only for primary/standby DB instances. The drill cannot be terminated in an emergency scenario.
		DCS instance restart	Restart a running DCS instance. If you clear data of a Redis 4.0, 5.0, or 6.0 instance, the cleared data cannot be restored. Exercise caution when performing this operation. The drill cannot be terminated in an emergency scenario.
		Powering off a DCS AZ	All nodes in the AZ are powered off centrally. The drill cannot be terminated in an emergency scenario. This disruptor is not supported in some areas.
CSS instances	Instances	Restarting a CSS cluster	Restart the CSS cluster that is in the available status. During the restart, Kibana and Cerebro may fail to be accessed. The drill cannot be terminated in an emergency scenario.
DDS instances	Instances	Forcibly promoting a standby node to primary	Supported forcible promotion of standby nodes to primary for backup sets, shards, and config nodes. However, there is a risk of failure when the primary/standby latency is large. The drill cannot be terminated in an emergency scenario.
IDC offline resource VMs	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. The drill cannot be terminated in an emergency scenario.
		Process killing	Kill processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.

Source of Attack Target	Attack Scenario		Description
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.
		NIC bandwidth limiting	Limit the NIC bandwidth, support multiple NICs. The drill can be terminated in an emergency scenario.
		Connection exhaustion	Create a large number of socket connections to the specified server end (combination of the IP address and port number) to exhaust the connections. As a result, normal requests of the node cannot connect to the server (the requests of other nodes on the server may also be affected). The drill can be terminated in an emergency scenario.
Alibaba Cloud server	Disruptors for practicing	Qualifying practice	You can familiarize yourself with the chaos engineering process without worrying real faults.
	Host resources	CPU usage increase	Simulate CPU usage surge. The drill can be terminated in an emergency scenario.
		Memory usage increase	Simulate the memory usage surg. The drill can be terminated in an emergency scenario.

Source of Attack Target	Attack Scenario		Description
		Disk usage increase	Simulate the disk usage surge. The drill can be terminated in an emergency scenario.
		Disk I/O pressure increase	Continuously read and write files to increase disk I/O pressure. The drill can be terminated in an emergency scenario.
	Host process	Process ID exhaustion	The system process IDs (PIDs) are exhausted. The drill cannot be terminated in an emergency scenario.
		Process killing	Kill processes repeatedly during the fault duration. The drill can be terminated in an emergency scenario. After the emergency termination or drill is complete, the drill system does not start the processes. The service needs to ensure that the processes are restored.
	Host network	Network latency	Simulate network faults to increase link latency. The drill can be terminated in an emergency scenario.
		Network packet loss	Simulate network faults to cause packet loss on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet loss rate is 100%.
		Network error packets	Simulate network faults to cause error packets on links. The drill can be terminated in an emergency scenario. The drill cannot be terminated when the packet error rate reaches 100%.
		Duplicate packets	Simulate duplicate packets generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network packet disorder	Simulate packet disorder generated on a link due to a network fault. The drill can be terminated in an emergency scenario.
		Network disconnection	Simulate the network disconnection between nodes. The drill can be terminated in an emergency scenario. Do not enter the IP addresses of the drill system and UniAgent server. Otherwise, the drill may fail. To interrupt an established persistent connection, select **All** for the interruption direction.

Source of Attack Target	Attack Scenario		Description
		NIC break-down	Simulate the NIC break-down scenario. The NIC may fail to be started after the NIC breaks down due to different network configurations of hosts. Therefore, prepare a contingency plan for network recovery. The drill cannot be terminated in an emergency scenario.
		DNS tempering	Tamper with the domain name address mapping. The drill can be terminated in an emergency scenario.
		Port occupation	Simulate the scenario where network ports of the system are occupied (a maximum of 100 ports can be occupied). The drill can be terminated in an emergency scenario.
		Server disconnection	Simulate the scenario where the entire server is disconnected, reject all TCP, UDP, and ICMP data packets, and open only ports 22, 8002, 39604, 33552, 33554, 33557, 32552, 32554, and 32557. The drill can be terminated in an emergency scenario.
		NIC bandwidth limiting	Limit the NIC bandwidth, support multiple NICs. The drill can be terminated in an emergency scenario.
		Connection exhaustion	Create a large number of socket connections to the specified server end (combination of the IP address and port number) to exhaust the connections. As a result, normal requests of the node cannot connect to the server (the requests of other nodes on the server may also be affected). The drill can be terminated in an emergency scenario.

Customizing a Fault

Users can create scripts using automated O&M scripts and run the scripts to simulate faults. The drill can be terminated in an emergency scenario.

⚠ CAUTION

A custom fault is determined by the script you compiled. Therefore, when scripts are used to attack ECSs, exceptions such as high resource usage and network faults may occur. As a result, the status of the UniAgent installed on the ECSs may change to offline or abnormal. Exercise caution when performing this operation.

For details about the custom script specifications, see the following code:

```
#!/bin/bash
set +x

function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}

function inject_fault()
{
    echo "inject fault"
}

function check_fault_status()
{
    echo "check fault status"
}

function rollback()
{
    echo "rollback"
}

function clean()
{
    echo "clean"
}

case "$ACTION" in
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
    *)
        usage
;;
esac
```

You are advised to define a custom fault script based on the preceding script specifications. In the preceding specifications, you can define the fault injection function, fault check function, fault rollback function, and environment clearing function by compiling customized content in the **inject_fault()**, **check_fault_status()**, **rollback()** and **clean()** functions.

According to the preceding specifications, there are two mandatory script parameters: Whether other script parameters are included depends on your script content.

Table 9-17 Mandatory parameters for customizing a fault script

Parameter	Value	Description
ACTION	inject_fault	Drill operation action. The value is automatically changed by the system background in different drill phases. The options are as follows: ● **inject_fault**: The drill is in the fault injection phase. ● **check_fault_status**: The drill is in the fault query phase. ● **rollback**: The drill is in the phase of canceling the fault injection. ● **clean**: The drill is in the environment clearing phase.
CAN_ROLLBACK	false	Whether rollback is supported. The options are as follows: ● **true**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is executed. ● **false**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is not executed.

NOTE

In the **inject_fault** function, add a label indicating that the fault injection is successful, and check whether the label exists in the **check_fault_status** function.

- If the label exists, the **check_fault_status** function can return normally (for example, exit 0).
- If the label does not exist, the **check_fault_status** function will return an abnormality (for example, exit 1).

Custom Script Example

The following is an example of a customized script.

The script content is as follows:

```
#!/bin/bash
set +x
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:~/bin
export PATH


function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}

function inject_fault()
{
    echo "============start inject fault============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
```

```
        mkdir -p "${SCRIPT_PATH}/${DIR_NAME}"
        echo "mkdir ${SCRIPT_PATH}/${DIR_NAME} successfully"
    fi

    cd "${SCRIPT_PATH}/${DIR_NAME}"

    if [ ! -f ${FILE} ]; then
        touch "${FILE}"
        echo "create tmp file ${FILE}"
        touch inject.log
        chmod u+x "${FILE}"
        chmod u+x inject.log
    else
        echo "append content">${FILE}
    fi
    echo "successfully inject">${FILE}
    echo "============end inject fault============"
}

function check_fault_status()
{
    echo "============start check fault status============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
        echo "inject has been finished"
        exit 0
    fi
    cd "${SCRIPT_PATH}/${DIR_NAME}"
    SUCCESS_FLAG="successfully inject"

    if [ -f ${FILE} ]; then
        if [[ "$(sed -n '1p' ${FILE})" = "${SUCCESS_FLAG}" ]]; then
            echo "fault inject successfully"
        else
            echo "fault inject failed"
            exit 1
        fi
    else
        echo "inject finished"
        exit 0
    fi
    sleep ${DURATION}
    echo "============end check fault status============"
}

function rollback()
{
    echo "============start rollback============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end rollback============"
}

function clean()
{
    echo "============start clean============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end clean============"
}

case "$ACTION" in
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
```

```
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
    *)
        usage
;;
esac
```

The input parameters of the script are as follows:

Table 9-18 Script input parameters of the customized script example

Parameter	Value	Description
ACTION	inject_fault	Drill operation action
CAN_ROLLBACK	false	Rollback is not supported.
SCRIPT_PATH	/tmp	Root directory of the custom fault log
DIR_NAME	test_script	Parent directory of the custom fault log
FILE	test.log	Custom fault log name
DURATION	10	Duration of a simulated custom fault, in seconds. (This parameter does not take effect when it is placed in the **inject_fault** function.)

NOTE

- In the sample **inject_fault** function, the injected fault is to **create a {FILE} file and add content to the {FILE} file**. If **successfully inject** is entered in the {FILE} file, the fault injection is successful.
- In the example, the **check_fault_status** function checks whether the {FILE} file exists. If no, the fault may have been rectified. In this case, **exit 1** is returned. If yes, check whether the label indicating that the fault injection is successful exists. If the label exists, the fault injection is successful. Here, **sleep {DURATION}** is used to simulate the fault duration. If the label does not exist, the fault injection fails.

9.2 Drill Templates

9.2.1 Overview

A drill template is designed for building, managing, and optimizing fault drills. It contributes a systematic process to improve the efficiency of drill lifecycle management to some extend. This drill template helps you quickly create a specific fault drill, covering the entire process including creation, maintenance, and update. You will conduct a real, effective, and reusable drill on your system.

Core Features

- Out-of-the-box standardized design
  - There are multiple preset templates designed for typical scenarios (such as cross-AZ DR and data storage exception scenarios). You can use the templates to create drill tasks.
  - You can customize scenarios based on the existing ones to meet your specific service requirements like special service process and customized risk situations.
- Scenario library for actual requirements
  - Built-in industry-typical scenario library: covers common service scenarios (such as high system resource usage and automatic traffic switchover) and contingency plan scenarios (such as data storage exceptions and environment overload in the microservice architecture).
  - Scenario-based tag management: improves co-work efficiency using templates filtered by template name and description.

Core Advantages

Table 9-19 Core advantages

Item	Description
High efficiency	● The scenario setup time is reduced, and the template can be reused over 80%. ● The standardized process shortens the drill preparation and improves the execution efficiency.
Accessible for all	● Scenario configuration can be completed through visualized GUIs and wizard-based operations without professional technical background. ● Beginners can quickly get started.

Item	Description
Scenario validity	● The templates are designed based on actual service requirements and history cases. The drill content is close to actual scenarios. ● The templates can be verified from multiple dimensions (such as risk coverage and process rationality) to improve the practice value.
Flexibility and scalability	● Customized scenarios can meet differentiated requirements. ● The existing systems (such as the emergency management platform and training system) can be interconnected for data exchange.
Knowledge accumulation	● The scenario library records enterprise-specific best practices which forms organization-level knowledge assets. ● The version management function facilitates experience inheritance and continuous optimization.

Typical Scenarios

- Enterprise emergency drills: Quickly enable contingency plans when you need to respond to cyber security attacks, handle production incidents, and more.
- Compliance drills: Customize scenarios (such as data privacy protection) based on regulatory requirements to ensure that drills comply with industry specifications.
- Routine drills: Perform chaos drills regularly based on different template scenarios to identify and avoid live network problems.

9.2.2 Viewing a Drill Template

Scenarios

There are several frequently-used drill templates in the template list. You can filter them by drill name and description (case insensitive).

Viewing Drill Template Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Drill Templates**.

Step 3 Click the target template card in the list. The template details page is displayed.

For details about the template information, see **9.2.4 Drill Template Description**.

----End

9.2.3 Creating a Drill Task Using a Template

Scenarios

You can use a drill template to create a drill task in a specific scenario.

Creating a Drill Task Using a Template

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Drill Templates**.

Step 3 Create a drill task in either of the following ways:

- Select the required template based on **9.2.4 Drill Template Description** and click **Create Task** on the template card.
- Select the required template based on **9.2.4 Drill Template Description**, click the template card to go to the **Template Details** page, and click **Create Task** in the upper right corner.

Step 4 Configure the basic information.

Table 9-20 Basic information parameters

Parameter	Description	Example Value
Drill Task	Name of the drill task. Set it according to the naming rules.	Test-Drill
Expected Recovery Duration (Minutes)	Expected time from the fault occurrence to the fault recovery, in minutes. Expected time for an application to automatically recover to the normal state during contingency plan execution after a fault is injected. This time does not affect the drill task.	3

Step 5 In the task group that contains scenario and parameters, locate the scenario and add an attack target for the task.

1. Click **Select** under **Attack Target**.
2. **Cloud Service Provider** and **Source of Attack Target** are selected based on the preset value of the scenario.
3. In the **Attack Target** table, the instances that do not support the current weapon are dimmed. After you select an existing task, change the cloud server provider, or change the source of the attack target, the preset weapon information will be cleared. For details, see **Creating a Drill Task Using a Template**.

4. After you select an attack target and click **Next**, the corresponding weapon is selected based on the target scenario. The preset value of the attack parameter is the data in the template.
5. (Optional) Set **Configure Monitoring Tasks**.

Table 9-21 Parameters for configuring a monitoring task

Parameter	Description
Steady-State Metrics	Select the target resource, performance metric, lower limit, and upper limit from the drop-down lists one by one. If a service can perform well and stably when a performance monitoring metric is set to a certain value range, this metric is called steady-state metric. If this metric value is not in that value range before a drill, the drill will be canceled. If the value of the steady-state metric is not within the stable value range during a drill, the corresponding fault injection automatically stops after automatic rollback is enabled.
Metric	Select the target resource, monitoring metric, lower limit, and upper limit from the drop-down lists one by one. These service metrics monitor the corresponding service data during fault drills. If the value of such a metric is within the allowed value range, the service is normal. Otherwise, you can determine whether to stop a drill.
Automatic Rollback	Select whether to enable automatic rollback. Fault injection is automatically rolled back and restored to the status before fault injection. Automatic rollback cannot be configured for some fault drill weapons that do not support fault termination.

6. Click **Finish**. The attack task is added.

Step 6 (Optional) Click **Add Attack Task**.

Attack tasks are preset in the template. You can add an attack task as required. Click **Add Task Group**. After adding an attack task, you can click **Add Attack Task** to add another one.

NOTE

- Tasks in different task groups are executed in serial, and tasks in the same task group are executed in parallel.
- Currently, multiple fault injection operations on the same resource in a task group are not supported.

- To add an existing task, click **Select from Existing**, select the existing task, and click **OK**.

- To add a new attack task, perform the follow-up steps.
  a. Set the attack target.

Table 9-22 Attack target parameters

Parameter	Description	Example Value
Cloud Service Provider	Select a cloud service vendor type.	Huawei Cloud
Source of Attack Target	Select the source of the target instance. You can select attack targets by selecting instances, pods, or a specified number of targets if CCE instances are used.	ECS
Attack Task	Customize the name of the attack task based on the naming rule.	test-attacktask
Attack Target	Select a target instance.	-

  b. Click **Next**.

  c. Set parameters for selecting an attack scenario.

  For details, see **9.1.7 Attack Scenarios**.

Table 9-23 Attack scenario parameters

Parameter	Description	Example Value
Attack Type	Attack scenarios are classified based on attack scenario types.	Host resources
Attack Scenario	Customize the name of the attack task based on the naming rule.	CPU usage increase
Attack Parameters	Configure attack parameters based on attack scenarios.	CPU usage (%): 80 Fault duration (s): 60

  d. Click **Next**.

  e. (Optional) Set **Configure Monitoring Tasks**.

Table 9-24 Parameters for configuring a monitoring task

Parameter	Description
Steady-State Metrics	Select the target resource, performance metric, lower limit, and upper limit from the drop-down lists one by one. If a service can perform well and stably when a performance monitoring metric is set to a certain value range, this metric is called steady-state metric. If this metric value is not in that value range before a drill, the drill will be canceled. If the value of the steady-state metric is not within the stable value range during a drill, the corresponding fault injection automatically stops after automatic rollback is enabled.
Metric	Select the target resource, monitoring metric, lower limit, and upper limit from the drop-down lists one by one. These service metrics monitor the corresponding service data during fault drills. If the value of such a metric is within the allowed value range, the service is normal. Otherwise, you can determine whether to stop a drill.
Automatic Rollback	Select whether to enable automatic rollback. Fault injection is automatically rolled back and restored to the status before fault injection. Automatic rollback cannot be configured for some fault drill weapons that do not support fault termination.

f. Click **Finish**. The attack task is added.

Step 7 If a preset scenario in the template is not required, click **Delete** next to the task. This step is optional.

Step 8 Click **OK**.

After a drill task is created, choose **Resilience Center** > **Chaos Drills** > **Drill Tasks** to view the task and start the drill by referring to **Starting a Drill Task**.

----End

9.2.4 Drill Template Description

In this section, you will find a standard drill template library covering multiple scenarios, including 12 types of core templates, such as emergency handling, process deduction, and contingency plan practice.

All templates are designed based on industry best practices and have complete structure and reusable content. There are standard frameworks such as drill background, process nodes, roles and responsibilities. You can modify scenario parameters, risk elements, and handling procedures based on actual requirements. The instructions and error-prone prompts can help you customize your drill tasks efficiently using these templates.

Table 9-25 Drill template description

Template Name	Description	Label	Level	Task Group Name	Attack Scenario
Cross-AZ DR	This drill simulates how a DR failover is performed for the target service and its antecedent middleware when an AZ is faulty or the network is abnormal in the DR deployment architecture.	DR	Advanced	Cross-AZ DR	Server disconnection
					Powering off a DCS AZ
Initial Chaos Drill	This is essential for beginners to experience the chaos drill process.	Nodes	Basic	Initial Chaos Drill	Qualifying practice
High System Resource Usage	This drill specifies the system resource usage to test the service performance in high pressure scenarios. When host resources are insufficient, you can handle the problem in advance.	Nodes	Medium	Disk Stress	Disk usage increase
				Memory Stress	Memory usage increase
				CPU Stress	CPU usage increase
HPA Configuration in Kubernetes	In the cloud native architecture, auto scaling is an important feature. This drill simulates scale-up after pod resource usage (such as memory) increases in a short period of time and scale-down after resource usage decreases.	Containers and clusters	Advanced	HPA Configuration in Kubernetes	Pod memory usage increase

Template Name	Description	Label	Level	Task Group Name	Attack Scenario
Data Storage Exception	Generally, service records are stored on the host or middleware where the service is located. Logs are stored on the disk of the host, and data is stored on the middleware such as DDS. This drill simulates the scenario where the ECS disk I/O is high and the primary/standby switchover is performed.	Services and data	Medium	Data Storage Exception	Disk I/O pressure increase
					Forcibly promoting a standby node to primary
Automatic Pod Recovery and Scheduling	Kubernetes schedules workloads based on pods. When workloads are generated, the scheduler automatically allocates pods in the workloads. For example, the scheduler distributes pods to nodes that have enough resources.	Clusters	Medium	Automatic Pod Recovery and Scheduling	Memory usage increase
					Forcible pod stopping
Network Instability Affecting Service Performance	This drill injects a network delay to the NIC of the service host to simulate the impact on services when the network is unstable.	Networks	Medium	Network Instability Affecting Service Performance	Network latency

Template Name	Description	Label	Level	Task Group Name	Attack Scenario
Environment Overload in the Microservice Architecture	Microservices are the mainstream architecture. The core value of microservices is to shorten the service release period and ensure reliable system operation. However, microservices also bring many challenges, such as how to locate and rectify faults in the microservice architecture. This drill simulates overloaded nodes of multiple microservices for your reference.	DR	Medium	Environment Overload in the Microservice Architecture	CPU usage increase
					Connection exhaustion
					Process killing
Abnormal Server Power-off	This drill simulates whether services can be recovered with no data loss after a server is powered off. In this drill, you can use the corresponding preset contingency plan to recover services after a node is powered off.	Services and data	Medium	Abnormal Server Power-off	Device shutdown
Data Loss in Service Middleware Cache	In large-scale concurrent data query scenarios where high data query efficiency is required, Redis has become an essential service for internet applications due to its significant speed advantages over traditional databases. However, it may face issues related to data consistency and reliability. This chaos drill aims to verify whether service operations remain normal after clearing Redis data.	DR	Medium	Data Loss in Service Middleware Cache	DCS instance restart

Template Name	Description	Label	Level	Task Group Name	Attack Scenario
Misoperations in the Host Configuration File	It is a high risk for O&M personnel to directly perform black screen operations on the service host. If the permission of the service configuration file is directly modified, the service process may not be able to read or write the file. This chaos drill uses a custom script to perform operations (modifying or removing permissions) on the host configuration file. You can use the prepared contingency plan to recover the service.	Services and data	Medium	Misoperations in the Host Configuration File	Custom scripts
Automatic Workload Switchover	FlexusL instances are new-generation out-of-the-box lightweight application cloud servers designed for developers and small- and medium-sized enterprises. You can deploy databases or service applications on FlexusL instances. This drill simulates service workload switchover when processes disappear and database nodes are disconnected.	Networks	Advanced	Automatic Workload Switchover	Process killing Network disconnection

Helpful Links

- Attack Scenarios
- Viewing a Drill Template

9.3 Contingency Plans

9.3.1 Overview

You can create contingency plans for potential system failures in **Resilience Center** of COC. These contingency plans can help you to restore services after a fault occurs. You can log in to COC, choose **Resilience Center** > **Contingency Plans**. On the displayed page, you can create a contingency plan as needed by configuring basic information, selecting a handling method (such as **scripts** or

jobs), and associating the contingency plan with the corresponding scripts or jobs. Also, you can check, modify, or delete created contingency plans.

9.3.2 Creating and Managing Custom Contingency Plans

Scenarios

You can create a customized contingency plan for faults that may occur in the system. If a fault occurs, you can rectify the fault by referring to the created contingency plan.

Creating a Custom Contingency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Contingency Plans**.

Step 3 On the **Customized Plan** tab page, click **Create** in the upper right corner.

Step 4 Set **Basic Information**.

Table 9-26 Basic information parameters

Parameter	Description
Contingency Plan Name	Enter a contingency plan name.
Enterprise Project	Select the enterprise project to which the contingency plan belongs from the drop-down list.
Application	Select the application to which the contingency plan belongs from the drop-down list.
Recovery Duration	Enter the expected fault recovery duration, in minutes.
Version	Enter the contingency plan version number.
Summary	Enter the main information about the contingency plan. The information can contain a maximum of 1,024 characters.

Step 5 Set **Troubleshooting**.

- **Contingency Plan Type**: **Automation Plan** or **Document Plan**.
  - **Automation Plan**: A contingency plan that can rectify faults using scripts and jobs.
  - **Document Plan**: A contingency plan that requires manual intervention to rectify faults.
- **Handling Method**: **Scripts** or **Jobs**. If you choose **Document Plan**, you can also select **Not Involved**.
  - **Scripts**: Select a script from the drop-down list. You can select a custom script or common script.

  - **Jobs**: Select a job from the drop-down list. You can select a custom job or public job.
  - **Not Involved**: This option can be selected only for a document plan. Scripts or jobs are not involved.
- **Step Name**: Enter the step name. It is mandatory only for a document plan. If you set **Handling Method** to **Scripts** or **Jobs**, the script or job name will be automatically entered.
- **Step Description**: Enter the step description. It is mandatory only for a document plan. The description cannot exceed 3 MB.

You can add more steps to a document plan. A maximum of 20 steps are supported.

Step 6 Click **OK**.

The contingency plan is created.

----End

Modifying a Custom Contingency Plan

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resilience Center** > **Contingency Plans**.

Step 3 On the **Customized Plan** tab page, locate the contingency plan to be modified and click **Modify** in the **Operation** column.

The parameters are the same as those for creating a contingency plan. For details, see **Creating a Custom Contingency Plan**.

Step 4 Click **OK**.

The customized contingency plan is modified.

----End

Deleting a Custom Contingency Plan

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resilience Center** > **Contingency Plans**.

Step 3 On the **Customized Plan** tab page, locate the contingency plan to be deleted and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

The customized contingency plan is deleted.

----End

9.3.3 Viewing and Cloning a Public Contingency Plan

Scenarios

Public contingency plans are predefined plans provided by COC. You can only read and use these plans. The **Public Plan** page provides basic public contingency plans. You can clone public plans to create public contingency plans.

Viewing Public Contingency Plan Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Contingency Plans**.

Step 3 On the displayed page, click the **Public Plan** tab.

Step 4 Locate the public contingency plan you want to view and click its name.

----End

Cloning a Public Contingency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Contingency Plans**.

Step 3 On the displayed page, click the **Public Plan** tab.

Step 4 Locate a public contingency plan and click **Clone** in the **Operation** column.

Step 5 The parameters are the same as those for creating a custom contingency plan. For details, see **Creating a Custom Contingency Plan**.

Step 6 Click **OK**.

The public contingency plan is cloned.

----End

9.4 PRR Management

9.4.1 Overview

Production Readiness Review (PRR).

PRR provides the baselines for service availability and operations capabilities from dimensions such as SLI/SLO, redundancy, disaster recovery, overload control, fault management, change capability, operations, and secure production. It allows the frontend personnel to perform requirement planning, design, and development, as well as the production admission review before service rollout.

PRR ensures that the product initiation, design, and rollout processes meet the specified quality standards and requirements. You can view the PRR list and perform related operations. The main functions of PRRs include initiating PRRs and managing PRR templates.

You can click **Initiate PRR** to enter the PRR initiation page. Enter the basic information such as the review name, description, application name, and application owner, and specify the corresponding PRR template and check item information. During a PRR, you can upload self-check materials and record the review minutes after the review is complete. You can create improvement items for check items that need to be improved.

PRR Template Management

The PRR template is a tool used for PRRs. It contains check item information in three phases: product initiation, product design, and product rollout. You can customize a PRR template on the PRR template management page. In addition, you can initiate a PRR based on the existing template to start the review process. PRR template management is a part of the PRR management function.

PRR Management

The PRR management list displays basic information about all PRRs, including the review name, review progress, application, status, number of issue tickets, number of war rooms, and expected completion time. In addition, you can click the PRR name in the list to go to the review details page and view the review details, including the review progress details and improvement items. The PRR list is a part of the PRR management function. It enables you to effectively track and manage the entire PRR process.

9.4.2 Managing PRR Templates

Scenarios

Create, modify, delete, and view PRR templates. You can customize a PRR template on the PRR template management page.

Creating a PRR Template

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 Click the **PRR Template Management** tab.

Step 4 Click **Formulate Template**.

Step 5 Set the basic information.

Table 9-27 Basic information parameters

Parameter	Description
Template	Name of a PRR template.
Template Description	Enter the detailed description of the PRR template.

Parameter	Description
Application Category	The options are **Core application** and **Non-core application**. Application category to which the PRR template belongs, which is user-defined.
PRR Check Items	Check items in the product initiation, product design, and product rollout phases defined in the PRR template in advance

Step 6 Set **PRR Check Items**.

PRR check items are the check items in the product initiation, product design, and product rollout phases defined in advance

- Select a PRR check item. Click **Add Check Item**. You can select **Select from the System** or **Custom Add**.
  - **Select from the System**: Select the predefined check items provided by COC. Multiple check items can be selected. Expand the check items and add metrics.
  - **Custom Add**: Customize the check name and click **Adding Customized Indicator** to set the evaluation details.

⚠ CAUTION

If an A-level check item fails, the PRR fails.

Step 7 Click **OK**.

The PRR template is created.

----End

Modifying a PRR Template

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 Click the **PRR Template Management** tab.

Step 4 Select the PRR template you want to modify and click **Modify** in the **Operation** column.

Step 5 The parameters are similar to those for creating a PRR template. For details, see **Creating a PRR Template**.

Step 6 Click **OK**.

The PRR template is modified.

----End

Deleting a PRR Template

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 Click the **PRR Template Management** tab.

Step 4 Locate the PRR template you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The PRR template is deleted.

----End

Initiating a PRR Based on a Template

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 Click the **PRR Template Management** tab.

Step 4 Locate the PRR template you want to review and click **Initiate PRR Review using a Template** in the **Operation** column.

Select this template to start a PRR. For details about how to start a PRR, see **Initiating a PRR**.

----End

9.4.3 Managing PRRs

Scenarios

You can manage the process from project initiation to product rollout through a PRR. A PRR is based on the PRR template. The PRR management list displays the basic information about all PRRs. You can view the review progress details and improvement items.

Initiating a PRR

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, click **Initiate PRR**.

Step 4 Configure the basic information.

Table 9-28 Basic information parameters

Parameter	Description
PRR Name	Name of a PRR template.
PRR Description	Enter the detailed description of the PRR.
Application	Select the application to which the PRR belongs from the drop-down list.
Owner	The preset value is the current user and cannot be changed. Owner of the application to which the PRR belongs
Application Description	Enter the detailed description of the application to which the PRR belongs.
Application Category	The options are **Core application** and **Non-core application**. Application category to which the PRR belongs. The application category corresponds to different PRR templates.
Template	Select a PRR template from the drop-down list.
Review Phase	Select the review phase for which the PRR needs to be initiated. Multiple review phases can be selected.
Expected Completion	Set the expected PRR completion time.

Step 5 Set **PRR Check Items**.

Based on the PRR template selected in the basic information, the check items required for the self-check before the review of the template will be displayed. Fill in the check items for PRR and modify the self-check result as required.

Table 9-29 PRR check item parameters

Parameter	Description
Self-Check Result	The options are **Passed** and **Not passed**. Select self-check results of check items. (If an A-level check item fails, the self-check cannot be initiated.) The self-check results are automatically displayed in automatic evaluation mode.

Parameter	Description
Violated Item	Enter details about the non-compliant items. If a check item fails, the information about the item that does not meet the requirements is displayed. If you select the automatic evaluation method, you can view details about the items that do not meet the requirements.
Conference Initiator	The preset value is the current user and cannot be changed. Initiator of the PRR conference.
Participant	Select participants of the PRR from the drop-down list. Multiple participants can be selected.
Minutes Recorded By	Select the meeting minutes taker of the PRR meeting from the drop-down list.
Add self-check materials	Click **Add self-check material** to upload self-check documents before review. A maximum of one file can be uploaded. The file type can be .docx, .pdf, or .pptx. The size of the file you want to upload cannot exceed 10 MB.

Step 6 Click **OK**.

The PRR is initiated. After the PRR is initiated, the PRR status changes to **To be input**. After the PRR, the meeting minutes recorder records the PRR conclusion. For details, see **Inputting the PRR Conclusion**.

----End

Viewing PRR Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR you want to view, and click the PRR name.

Go to the PRR details page and view the PRR details.

----End

Downloading PRR Details in PDF

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR you want to view, and click its name.

On the PRR details page, the PRR report can be downloaded in the upper right corner.

----End

Inputting the PRR Conclusion

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR you want to input, and click **Input** in the **Operation** column.

Step 4 Click **Input PRR Conclusion**.

Step 5 Set parameters for inputting the PRR conclusion.

Table 9-30 Parameters for imputing the PRR conclusion

Parameter	Description
Review Result	The options are **Passed** and **Not passed**. Select the self-check result of the check item. If the check item whose necessity is A fails, the review result is failed.
Violated Item in Review	Enter details about the items that do not meet the review requirements. If a check item fails, the information about the item that does not meet the requirements is displayed.
Improvement Service Ticket	Click **Create Improvement Item** to create an improvement ticket for the check items to be improved. For details about the parameters, see **Table 9-31**.
Add Meeting Minutes	Click **Add Meeting Minutes** to upload PRR conclusion documents. A maximum of one file can be uploaded. The file type can be .docx, .pdf, or .pptx. The size of the file you want to upload cannot exceed 10 MB.

Table 9-31 Parameters for creating an improvement ticket

Parameter	Description
Improvement Task	Name of an improvement ticket.
Application	Select an application for which the improvement is performed from the drop-down list.
Type	Select an improvement type from the drop-down list.
Improvement Owner	Select an owner from the drop-down list.
Improvement Acceptor	Select an acceptance user from the drop-down list.
Expected Completion	Enter the expected completion time. You can select a day. The time cannot be earlier than the current day.
Symptom	Enter the incident-related problem symptom. The value can contain a maximum of 1,000 characters.
Improvement Ticket Closure Criteria	Enter the improvement closure criteria. The value can contain a maximum of 1,000 characters.

Step 6 Click **OK**.

Enter the PRR conclusion. If any check item whose **Necessity** is **A** fails, the overall review result will be Failed. In this case, you need to perform the review again until the review is passed. Then, you can **review the conclusion**.

----End

Reviewing PRR Conclusions

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR you want to review and click **Review** in the **Operation** column.

Step 4 Set the review conclusion.

- **Review Result**: The options are **Passed** and **Not passed**.
- **Description**: Enter the review comment only when the review comment is **Not passed**.

Step 5 Click **OK**.

Review the PRR conclusion.

----End

Continuing a PRR

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR task you want to continue and click **Continue** in the **Operation** column.

You can continue to start the PRR of the next phase only after the PRR of the current phase is approved.

The parameter information is basically the same as that of initiating a PRR review. For details, see **Initiating a PRR**.

Step 4 Click **OK**.

Complete the review and continue.

----End

Canceling a PRR

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **PRRs**.

Step 3 On the **PRR List** tab page, locate the PRR task you want to cancel and click **Cancel** in the **Operation** column.

Step 4 Click **OK**.

The review is canceled.

----End

9.5 Architecture Design

9.5.1 Overview

You can draw an overall architecture for an application. The service automatically calculates the SLO value of the architecture by analyzing how business units connect in series or parallel. You can quickly identify architecture weaknesses based on the calculated SLO value and adjust the number and layout of resource instances. You do not need to know the calculation details or worry about if there is any calculation error from data deviation or complex formulas.

In this module, you can manage application architectures. After you click an architecture name, you will be redirected to the page for drawing and governing architectures. On that page, you can draw an architecture and evaluate its SLO value.

Concepts

Service level objectives (SLOs) can be understood as the proportion of time that a system can provide services in the life cycle. Both availability and maintainability of the service need to be considered.

Service Level Indicators (SLIs) are the specific measurements used to trace progress toward SLOs. They quantitatively measure a specific aspect of a service from the perspective of users. For example, if you have a website service, the SLI might be page loading time, request success rate, request delay, and traffic. If any indicator exceeds the normal range, the system is considered unable to provide services. The SLO value of the system decreases as the system fails to provide services for a longer time.

Service Level Agreements (SLAs) are formal, legally binding agreements between a service provider and its users, outlining the details of service, responsibilities and obligations of both parties, and liabilities for breach of these agreements. SLOs are typically included as part of quality standards in these agreements.

9.5.2 Managing Deployment Architectures

Scenarios

You can create, modify, delete, view, copy, and export deployment architectures. You can use deployment architectures to draw and govern the architecture.

Creating a Deployment Architecture

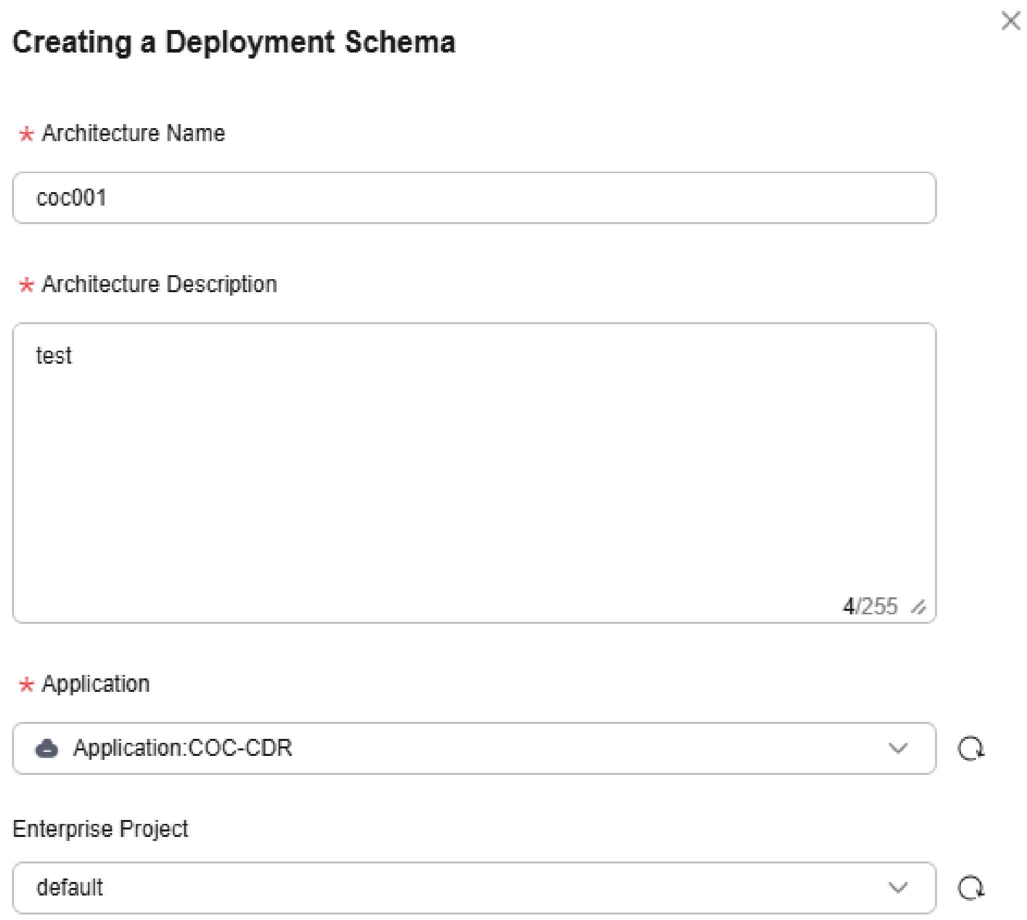
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Click **Create Deployment Architecture**.

Step 4 Configure the basic information.

Figure 9-7 Configuring basic architecture information



Creating a Deployment Schema

* Architecture Name

coc001

* Architecture Description

test

4/255

* Application

Application:COC-CDR

Enterprise Project

default

Table 9-32 Basic information parameters

Architecture Name	Name of the deployment architecture
Description	Description of the deployment architecture.
Application	Select the application to which the architecture belongs from the drop-down list. After an architecture is created, its associated applications cannot be modified.
Enterprise Project	Select the enterprise project to which the deployment architecture belongs from the drop-down list.

Step 5 Click **OK**.

The deployment architecture is created.

----End

Modifying a Deployment Architecture

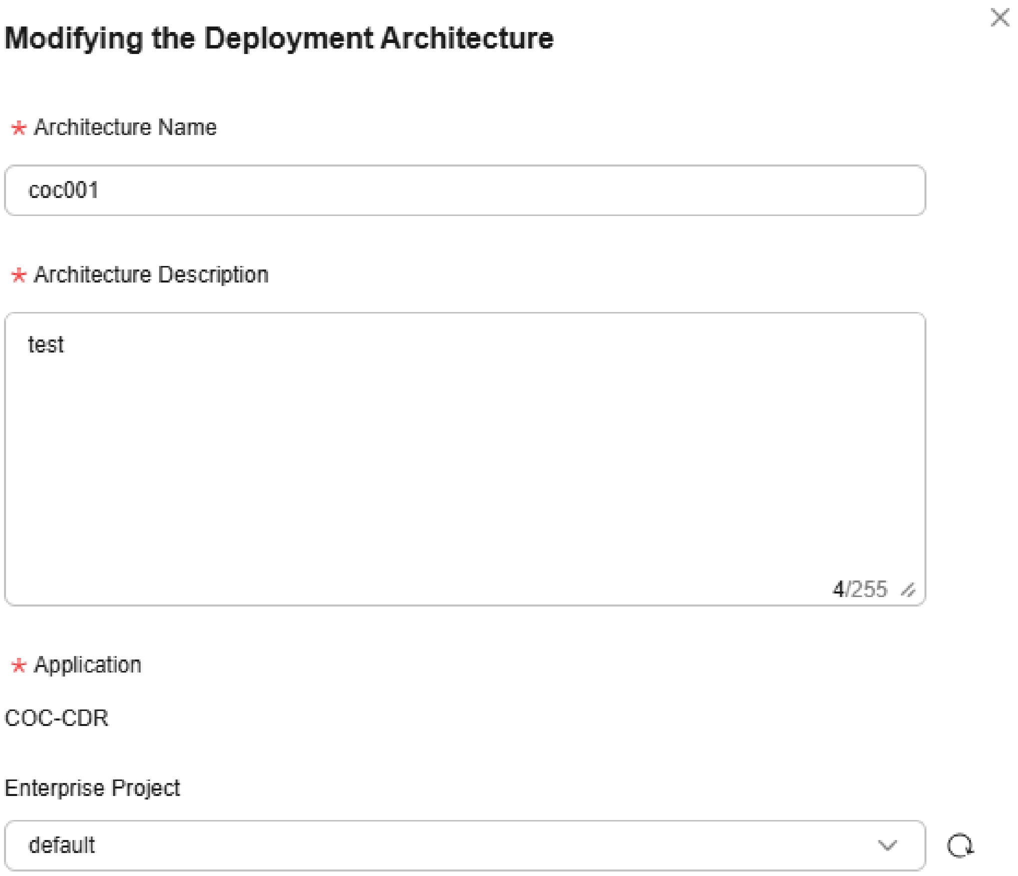
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Locate the target deployment architecture and click **Modify** in the **Operation** column.

Step 4 The parameters are the same as those for creating a deployment architecture. For details, see **Table 9-32**.

Figure 9-8 Modifying a deployment architecture



Modifying the Deployment Architecture

* Architecture Name

coc001

* Architecture Description

test

4/255

* Application

COC-CDR

Enterprise Project

default

Step 5 Click **OK**.

Step 6 The deployment architecture is modified.

----End

Deleting a Deployment Architecture

Step 1 Log in to **COC**.

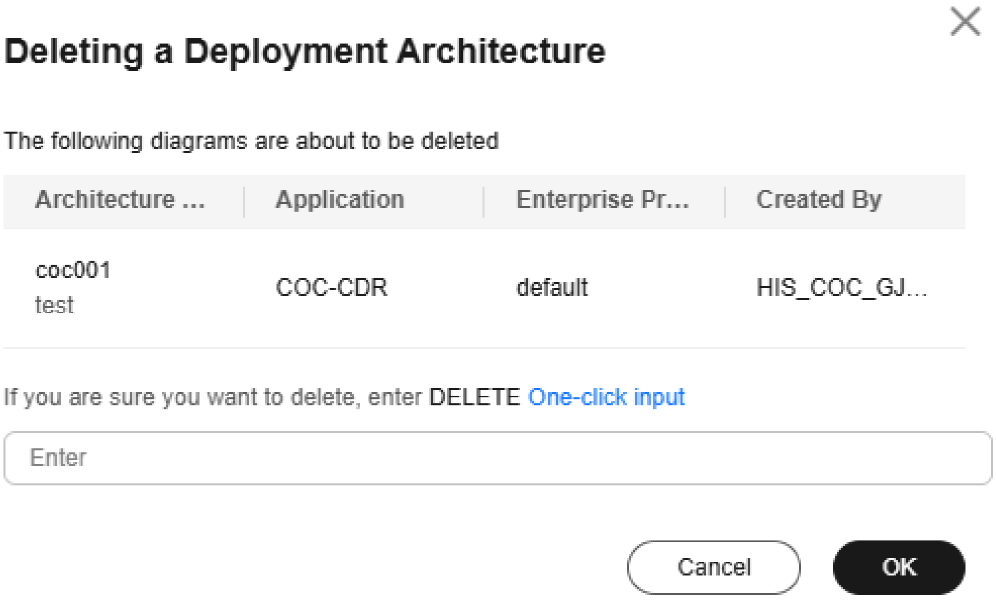
Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Locate the target deployment architecture and click **Delete** in the **Operation** column.

Step 4 In the displayed dialog box, enter **DELETE** and click **OK**.

The deployment architecture is deleted.

Figure 9-9 Deleting a deployment architecture



Deleting a Deployment Architecture

The following diagrams are about to be deleted

Architecture ...	Application	Enterprise Pr...	Created By
coc001 test	COC-CDR	default	HIS_COC_GJ...

If you are sure you want to delete, enter DELETE One-click input

----End

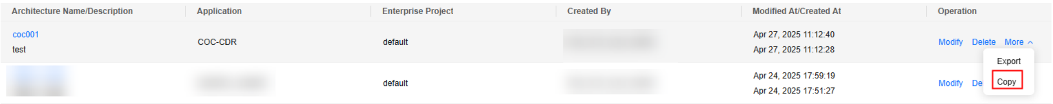
Copying a Deployment Architecture

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Locate the target deployment architecture and choose **More** > **Delete** in the **Operation** column.

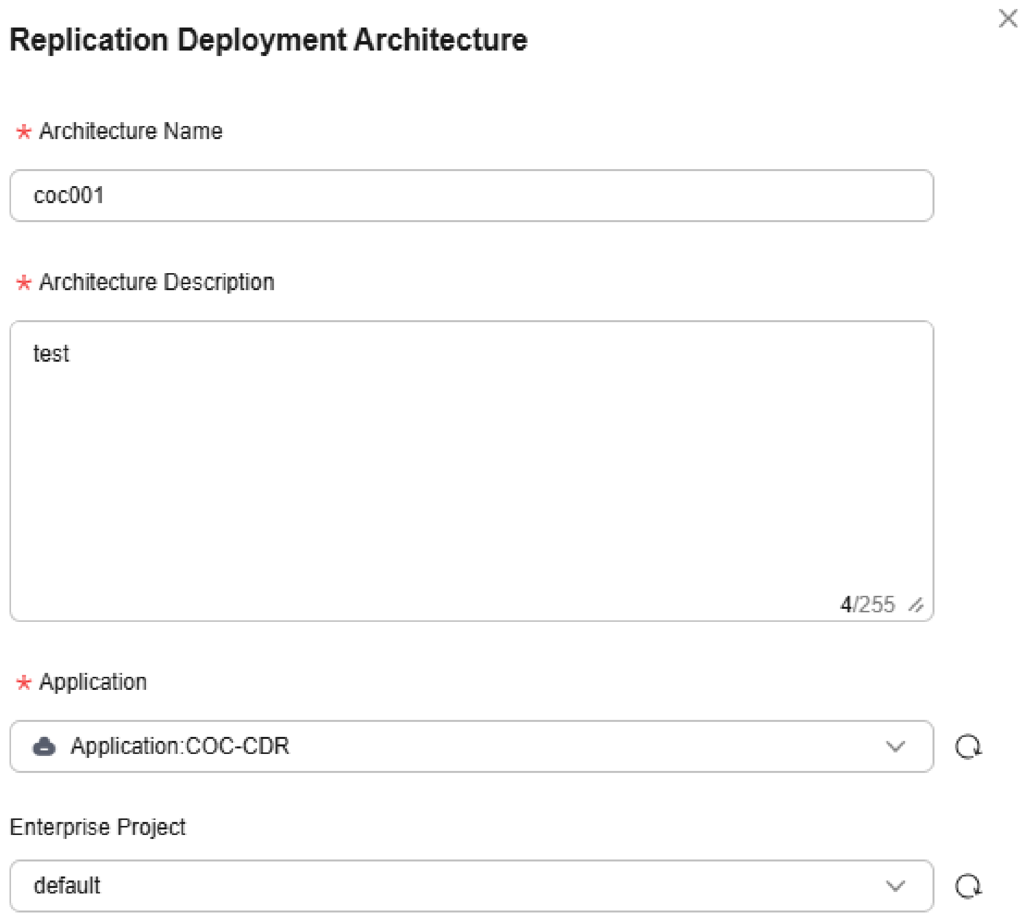
Figure 9-10 Copying a deployment architecture



Architecture Name/Description	Application	Enterprise Project	Created By	Modified At/Created At	Operation
coc001 test	COC-CDR	default	[redacted]	Apr 27, 2025 11:12:40 Apr 27, 2025 11:12:28	Modify Delete More
[redacted]	[redacted]	default	[redacted]	Apr 24, 2025 17:59:19 Apr 24, 2025 17:51:27	Modify De

Step 4 The parameters are the same as those for creating a deployment architecture. For details, see **Table 9-32**.

Figure 9-11 Configuring basic parameters



Replication Deployment Architecture

* Architecture Name

coc001

* Architecture Description

test

4/255

* Application

Application:COC-CDR

Enterprise Project

default

Step 5 Click **OK**.

The deployment architecture is copied.

----End

Exporting a Deployment Architecture

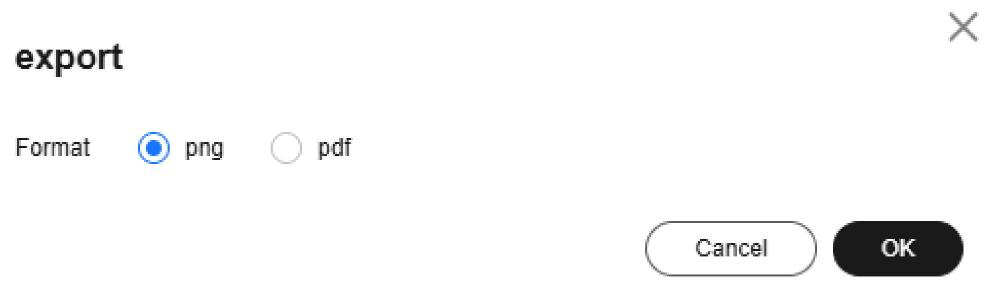
Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Locate the target deployment architecture and choose **More** > **Export** in the **Operation** column.

Step 4 Select the format to be exported.

Figure 9-12 Exporting a deployment architecture



Format ● png ○ pdf

Step 5 Click **OK**.

The deployment architecture is exported.

----End

9.5.3 Drawing and Governing Deployment Architectures

Scenarios

You can draw an application architecture using basic canvas elements such as border, element node, and edge. After saving the architecture, you can view the architecture details on the **Architecture Governance** page. On that page, you can view all architectures and SLO values. You can also modify the deduction item configurations of an application, and re-evaluate SLO values of the architecture.

Drawing a Deployment Architecture

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Click the name of the target deployment architecture in the **Architecture Name/ Description** column. The **Architecture Governance** page is displayed.

Step 4 Click **Architecture Drawings**.

Step 5 Draw an architecture.

- Select a diagram element in the left list and drag it to the canvas.

Table 9-33 Diagram elements

Element Type	Description	Example Value
Border	A border is used to wrap canvas elements that need to be connected in parallel. You can double-click a border to configure the parallel relationship.	Basic Diagram Elements > Border

Element Type	Description	Example Value
Element node	An element node represents a specific cloud service. Each element node has an SLO value.	Compute > Elastic Cloud Server
Edge	An edge represents a serial relationship between canvas elements. Only one edge can be dragged out to connect to another element on a canvas, and can be connected by only one edge.	-

- Drag an edge from one element to connect to another element in the canvas to establish a serial relationship between elements.
- Drag a border from the diagram element list on the left to the canvas and use another element to establish a parallel relationship in it. This element can be a nested border or an element node.
- Double-click the border to be connected in parallel and configure parameters on the displayed page.

Table 9-34 Basic parameters

Parameter	Description
Enable parallel configuration	Whether to enable parallel configuration. If this parameter is enabled, the current border is enabled for parallel configuration.

Parameter	Description	
Redundancy mode	Voting decision-making: In a K-out-of-N system, when N parallel nodes work at the same time, they share workloads evenly to ensure that at least K nodes are running normally. That is, the system can tolerate a maximum of N – K node failures. By default, K is set to 1, ensuring that at least one parallel node is running normally. In this case, the nodes are fully parallel, and the SLO availability calculation yields a probability of ≥ 1. For other values of K, the SLO availability calculation results in a probability of ≥ K.	● Number of votes (K): The redundancy mode of voting decision-making ensures that at least K parallel nodes are normal. The default value is 1. ● Number of active nodes: N parallel nodes that work at the same time in the redundancy mode of voting decision-making.
	N + M active/standby: N active nodes and M standby nodes. Only when one of the active nodes is faulty, the standby nodes start to work.	● Number of active nodes: N active nodes in N + M active/standby redundancy mode. ● Number of standby nodes: M standby nodes in N + M active/standby redundancy mode.
	N + 1 redundancy: N + 1 parallel nodes work at the same time and share even workloads. That is, at least N parallel nodes are normal, and the system can work properly only when there is no more than one faulty parallel node.	Number of active nodes: N parallel nodes working at the same time in N + 1 redundancy mode.

Parameter	Description
Active/standby mode in the border	The border can function as the active or standby node in the N + M active/standby redundancy mode. The options are as follows: ● Active ● Standby
Active/Standby mode of a diagram element node	The diagram element node functions as the active or standby node in the N + M active/standby redundancy mode. The options are as follows: ● Active ● Standby

Step 6 Click **Save**.

The architecture drawing is complete.

----End

Governing a Deployment Architecture

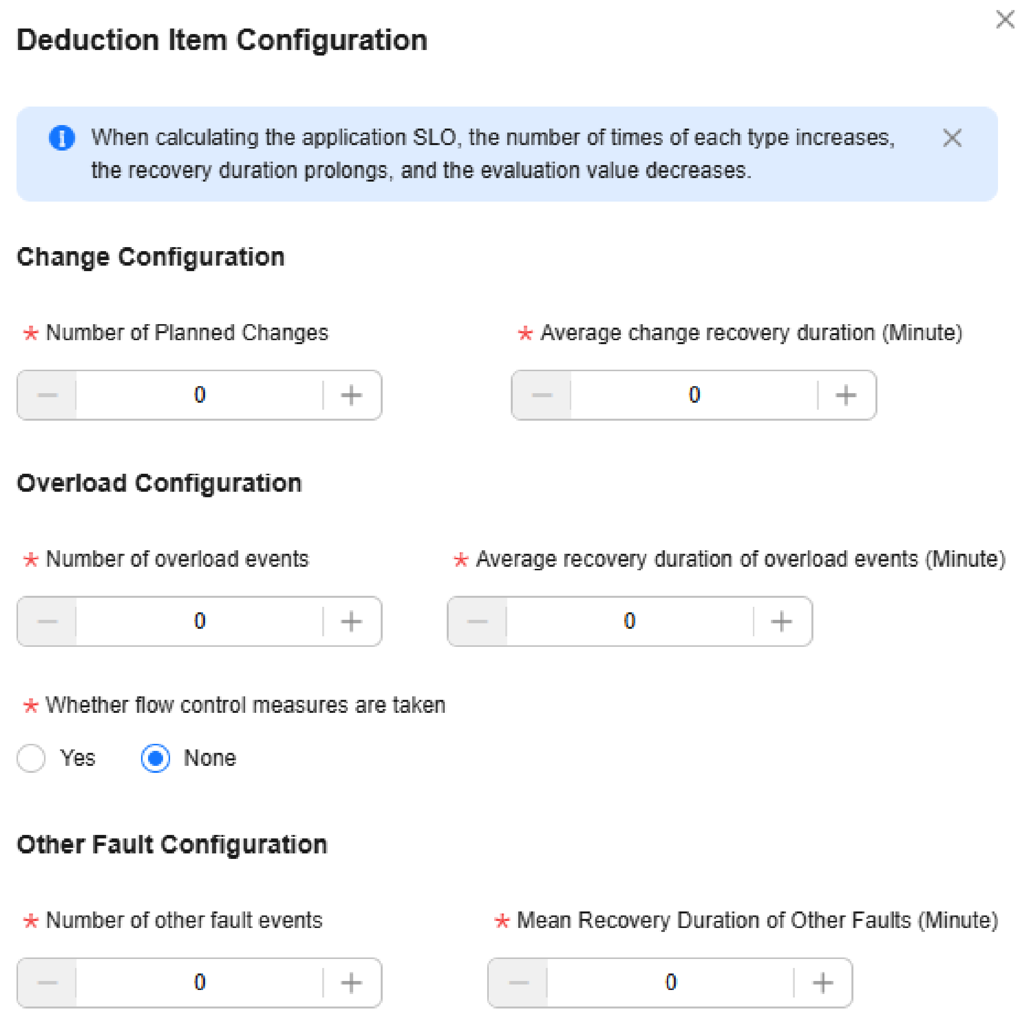
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resilience Center** > **Architecture Design**.

Step 3 Click the name of the target deployment architecture in the **Architecture Name/ Description** column. The **Architecture Governance** page is displayed.

Step 4 Click **Deduction Item Configuration** and configure the parameters on the displayed page. If you set a larger number for parameters, the SLO value you calculated for the architecture will be a smaller one.

Figure 9-13 Configuring deduction items



Deduction Item Configuration

When calculating the application SLO, the number of times of each type increases, the recovery duration prolongs, and the evaluation value decreases.

Change Configuration

* Number of Planned Changes: 0

* Average change recovery duration (Minute): 0

Overload Configuration

* Number of overload events: 0

* Average recovery duration of overload events (Minute): 0

* Whether flow control measures are taken

○ Yes ● None

Other Fault Configuration

* Number of other fault events: 0

* Mean Recovery Duration of Other Faults (Minute): 0

Table 9-35 Parameters for deduction item configuration

Parameter	Description
Number of Planned Changes	Number of plan changes within one year.
Average change recovery duration (Minute)	Average recovery duration of each change within one year, in minutes.
Number of overload events	Number of overload incidents that may occur within one year.
Average recovery duration of overload incidents (Minute)	Average recovery duration of each overload incident within one year, in minutes.

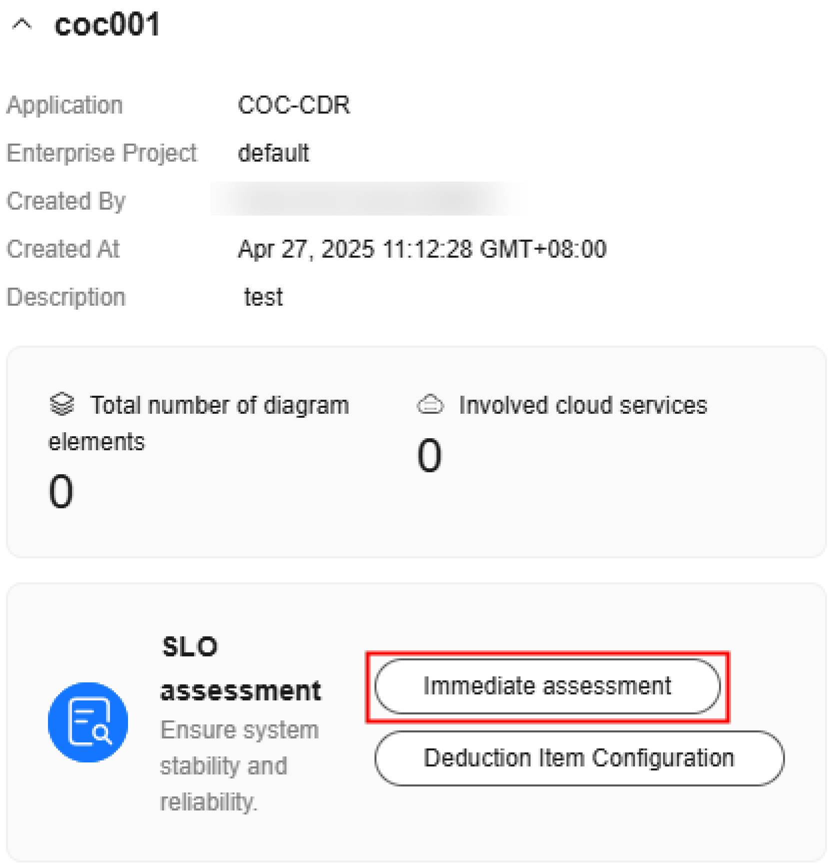
Parameter	Description
Whether flow control measures are taken	Flow control switch. If you set this parameter to **Yes**, the **Number of overload events** and **Average recovery duration of overload events (Minute)** parameters are invalid and their values are the default value 0.
Number of other fault events	Number of other fault incidents that may occur within one year.
Mean Recovery Duration of Other Faults (Minute)	Average recovery duration of other fault incidents within one year, in minutes.

Step 5 Click **OK**.

Step 6 Click **Immediate assessment** to re-evaluate the SLO value of the architecture.

The architecture is governed.

Figure 9-14 Evaluating an architecture



coc001

Application COC-CDR

Enterprise Project default

Created By [redacted]

Created At Apr 27, 2025 11:12:28 GMT+08:00

Description test

Total number of diagram elements 0

Involved cloud services 0

SLO assessment

Ensure system stability and reliability.

----End

10 Task Management

10.1 Execution Records

10.1.1 Viewing a Script Service Ticket

Scenarios

After a script is executed, a script service ticket record is generated to record the script execution results. To trace and record the execution objects and results of the script, you can use the script service ticket function.

Viewing the Execution Records of a Script Service Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click the **Script Tickets** tab.

Step 4 Click a script name.

Step 5 Perform the following operations based on the service ticket status:

- **Abnormal**: Click **Forcibly End** in the upper right corner to end the service ticket.
- **Executing**: Click **Pause** or **Forcibly End** in the upper right corner to pause or stop the script ticket.
- **Paused**: Click **Continue** or **Forcibly End** in the upper right corner to continue or stop the service ticket.

----End

10.1.2 Viewing a Job Service Ticket

Scenarios

After a job is executed, a service ticket record is generated to record the job execution result. To monitor and record the execution objects and results of the job, you can use the job service ticket function.

Viewing the Execution Records of a Job Service Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click the **Job Tickets** tab.

Step 4 Locate the target ticket and clone or tag the job ticket.

- Cloning a job ticket: Locate a job ticket, click **Clone** in the **Operation** column.

  On the job execution page, execute the job again by referring to **6.3.6 Executing Custom Jobs**.

- Tagging a job ticket: Locate a job ticket, and modify the tag of the ticket by referring to **6.3.7 Managing Jobs Using Tags**.

Step 5 Click the job name.

Step 6 Perform the following operations based on the service ticket status:

- **Abnormal**: Click **Forcibly End** in the upper right corner to end the service ticket.
- **Executing**: Click **Forcibly End** in the upper right corner to end the service ticket.
- **Paused**: Click **Forcibly End** in the upper right corner to end the service ticket.

----End

10.1.3 Viewing a Patch Service Ticket

Scenarios

After a patch scanning or repair task is executed, a patch service ticket record is generated to record the patch execution result. To monitor and record the execution objects and results of a patch scan and repair task, you can use the patch service ticket function.

Viewing the Execution Records of a Patch Service Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click the **Patch Tickets** tab.

Step 4 Click a patch ID.

Step 5 Perform the following operations based on the service ticket status:

- **Abnormal**: Click **Forcibly End** in the upper right corner to end the service ticket.
- **Executing**: Click **Pause** or **Forcibly End** in the upper right corner to pause or terminate the service ticket.
- **Paused**: Click **Continue** or **Forcibly End** in the upper right corner to continue or terminate the service ticket.
- **Completed**: Click **Compliance Report** in the upper right corner to view the patch service ticket result.

----End

10.1.4 Viewing an OS Version Change Ticket

Scenarios

After an OS version is changed, an OS version change record that contains the execution results of this change will be generated. You can use the OS version change service ticket function to monitor and record the OS version change objects and execution results.

Viewing the Execution Records of an OS Version Change Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click **OS Version Change Tickets**.

Step 4 Click the ticket ID to enter the ticket details page.

Step 5 Perform the following operations based on the service ticket status:

- If the service ticket status is failed, click **Retry** to execute the OS version change service ticket again.
- If the service ticket status is failed, click the rollback button to roll back the ticket to the source version.

----End

10.1.5 Viewing a Resource Operation Ticket

Scenarios

After a batch operation is performed on resources such as ECSs, RDS DB instances, FlexusL instances, and BMSs in batches, a service ticket is generated for you to record the batch operation results. If you want to monitor and record the execution objects and results of a batch resource operation, you can use the resource operation ticket function.

Viewing the Execution Records of a Resource Operation Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click **Resource Operation Tickets**.

Step 4 Locate the target ticket and click the resource operation ID.

Step 5 Perform the following operations based on the service ticket status:

- **Abnormal**: Click **Forcibly End** in the upper right corner to terminate the service ticket.
- **Executing**: Click **Pause** or **Forcibly End** in the upper right corner to pause or terminate the service ticket.
- **Paused**: Click **Continue** or **Forcibly End** in the upper right corner to continue or terminate the service ticket.

----End

10.1.6 Viewing a Diagnosis Service Ticket

Viewing the Execution Records of a Diagnosis Service Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click the **Diagnose Ticket** tab.

Step 4 Locate the target ticket and click the service ticket ID.

Step 5 Perform the following operations based on the service ticket status:

- **Failed**: Click **Retry** on the left to perform the failed resource operation again.
- **Executing**: Click **Stop** to terminate the ticket.

----End

10.1.7 Viewing a Quick Configuration Ticket

Scenarios

Choose **Overview** in the navigation pane. In the **Quick Configuration Center** area, click the **Cloud Service Configurations** tab, and click **Cloud Eye**. After a cloud service configuration task is added, a quick configuration ticket record is generated for you to record the new configuration result. If you want to monitor and learn about the target objects and configuration results of quick configuration tasks, you can use the quick configuration ticket feature.

Viewing the Execution Records of a Quick Configuration Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Task Management** > **Execution Records**.

Step 3 Click the **Quick Configuration Tickets** tab.

Step 4 Locate the target ticket, and click the ticket ID.

Step 5 Perform the following operations based on the service ticket status:

- **Abnormal**: Click **Forcibly End** in the upper right corner to terminate the service ticket.
- **Executing**: Click **Pause** or **Forcibly End** in the upper right corner to pause or terminate the service ticket.
- **Paused**: Click **Continue** or **Forcibly End** in the upper right corner to continue or terminate the service ticket.
- **Completed**: Click **Compliance Report** in the upper right corner to view the patch service ticket result.

----End

10.2 To-Do Center

10.2.1 Overview

The to-do center is used to record and track daily to-do tasks to remind you of the tasks.

In the COC to-do center, you can create a to-do task and assign it to a specified engineer for processing. You can set the deadline and enter the recommended solution for the to-do task. After the to-do task is created, the owner can be notified by SMS messages or emails.

In addition to the preceding functions, you can set tags and add attachments when creating a to-do task.

After a to-do task is created, the owner can handle and close the to-do task.

10.2.2 Creating a To-Do Task

Scenarios

You can create a to-do task and assign it to a specified engineer, set the deadline, and enter the recommended solution for the task. After the to-do task is created, the owner can be notified by SMS messages or emails. When creating a to-do task, you can also set tags and add attachments.

Precautions

Only the to-do tasks of the current login account (the creator or owner) are displayed. The to-do tasks of other sub-accounts are not displayed.

Creating a To-Do Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **To-Do Center**.

Step 3 Click **Create** in the upper right corner.

Step 4 Set parameters for creating a to-do task.

Table 10-1 Parameters for creating a to-do task

Parameter	Description
Ticket	Name of a custom to-do task. - The name can contain a maximum of 255 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). - The name must start with a letter or digit. - The name cannot end with a decimal point.
Description	Enter the background and purpose of the to-do task. The description can contain a maximum of 1,000 characters, including letters, digits, and special characters.
Type	The options are **Scheduled Events**, **Risk warning**, and **Other**.
Severity	The value can be **Critical**, **Major**, **Minor**, or **Suggestion**.
Owner	Select **Shift** or **Individual**. - **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. - **Individual**: Select an owner. For details about how to configure a recipient, see **11.1 O&M Engineer Management**
Notification Mode	Select a notification channel from the drop-down list box. - **Default**: Same as that selected in the reviewer subscription function. For details about how to set the default notification mode, see **Selecting a Notification Method**. - **SMS, WeCom**, **DingTalk**, **Lark**, and **Email**: Notifications are sent based on the information reserved by the reviewer. For details about how to set the reviewer information, see **Modifying Personnel Information**. - **No notification**: The system does not notify any recipient.
Ticket Deadline	Configure the end time of the to-do task.
Label	(Optional) Select an existing label or enter a new label and press **Enter** to create a tag.

Parameter	Description
Recommended Solution	Enter a recommended solution. The value can contain a maximum of 1,000 characters, including letters, digits, and special characters. Click **Add File** to upload files related to the recommended solution. A maximum of one file no more than 50 MB can be uploaded. Only the following file formats are supported: JPG, PNG, DOCX, TXT, and PDF. **CAUTION** Attachments can be downloaded when you view to-do tasks. However, the download traffic is limited. The traffic limiting policy is that the interval between two download operations must be 5 seconds.

Step 5 Click **OK**.

The to-do task is created.

----End

10.2.3 Managing a To-Do Task

Scenarios

After a to-do task is created, the owner can handle and close the to-do task.

Precautions

You can handle only the to-do tasks whose owner or creator is yourself.

Handling a To-Do Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **To-Do Center**.

Step 3 Click the **Pending** tab.

Step 4 Locate a to-do task and click the task name.

Step 5 Click **Handle** in the upper right corner.

The to-do task is handled.

----End

Canceling a To-Do Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **To-Do Center**.

Step 3 Click the **Created by Me** tab.

Step 4 Locate the to-do task you want to cancel and click the task name.

Step 5 Click **Cancel** in the upper right corner.

Step 6 Enter the cancellation reason and click **OK**.

The to-do task is canceled.

----End

Closing a To-Do Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Task Management** > **To-Do Center**.

Step 3 Click the **Handled by Me** tab.

Step 4 Locate the to-do task you want to close and click the task name.

Step 5 Click **Close** in the upper right corner.

Step 6 Enter the closure description and click **OK**.

The to-do task is closed.

----End

11 Basic Configurations

11.1 O&M Engineer Management

11.1.1 Overview

You can centrally manage O&M engineers on COC using this feature. On the **O&M Engineer Management** page, you can manage users who log in through different login methods, including IAM users, IAM federated users, and IAM Identity Center users. Data on the **O&M Engineer Management** page is the basic user data of COC and is available for authorized users to use the basic functional modules such as to-do task creation, scheduled O&M, notification management, and incident center. **Table 1** lists the user types and their sources on the **O&M Engineer Management** page.

Table 11-1 User types and their sources on the O&M Engineer Management page

User Type	User Data Source
Common IAM user	Synchronized from IAM
IAM Federated User (IAM User SSO)	Synchronized from IAM
IAM federated user (Virtual User SSO)	Manually added on the O&M engineer page
IAM Identity Center	Synchronized from IAM Identity Center

- On the **O&M Engineer Management** page, you can manually select users you want to edit, delete, and configure subscription information for.
- If you edit the information of an existing user, the system will select a notification method to notify the user by mobile number, email address, WeCom, Lark, or DingTalk.

NOTE

If you log in as an IAM user, COC can only synchronize personnel information to the administrator account (including the organization administrator and IAM delegated administrator). The IAM user cannot perform operations under any member account. If you need to perform COC operations (such as executing scripts and jobs) under a member account, **specify a delegated administrator** for it in the organization service.

11.1.2 Managing O&M Engineers

Scenarios

O&M Engineer Management collects statistics on users and basic information under the current Huawei Cloud account. You can modify user information, such as modifying contact information and setting notification methods. The procedure is as follows.

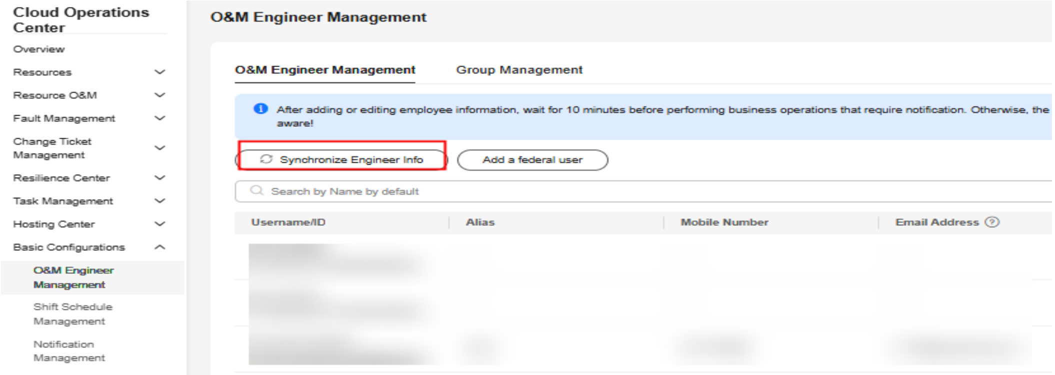
Synchronizing O&M Engineer Information

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click **Synchronize Engineer Info**.

Figure 11-1 Synchronizing information about O&M engineers



After adding or editing employee information, wait for 10 minutes before performing business operations that require notification. Otherwise, the aware!

----End

Adding a Federated User

If you log in to the system as an IAM virtual user via SSO, you need to manually add the username to use COC functions. For details about the data source types of each login user, see **O&M Engineer Overview**.

Step 1 Log in to **COC**.

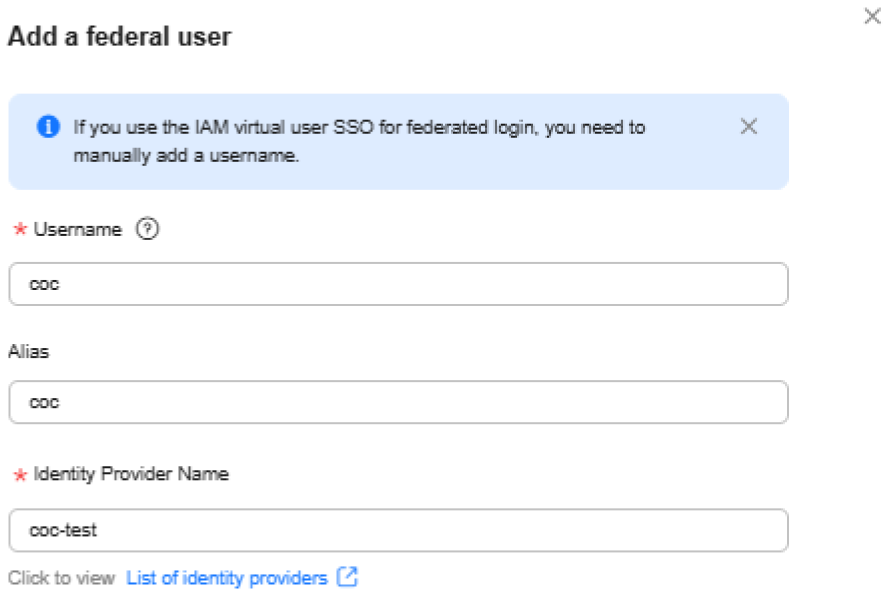
Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click **Add Federated User** in the upper left corner.

Step 4 Set the parameters in the **Add Federated User** dialog box.

- **Username**: username displayed on Huawei Cloud, which is configured in the IAM identity transition rule.
- **Alias**: Alias of the current user.
- **Identity Provider Name**: name of the user identity provider in IAM.

Figure 11-2 Adding a federated user



Add a federal user

If you use the IAM virtual user SSO for federated login, you need to manually add a username.

* Username: coc

Alias: coc

* Identity Provider Name: coc-test

Click to view List of identity providers

Step 5 Click **OK**. The federated user is added.

----End

Modifying Personnel Information

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Locate the user you want to modify and click **Modify** in the **Operation** column.

Step 4 Set the parameters for modifying the user information.

- **Alias**: Alias of the current user.
- **Mobile Number**: The mobile number of the current user.
- **Email Address**: The Email address of the current user.
- **WeCom**: The webhook address of the WeCom group chatbot.
- **DingTalk**: The webhook address of the DingTalk group chatbot.
- **DingTalk Key**: When a user adds a custom robot to a DingTalk group, the user can select **Add Endorsement** to verify the generated signature key.
- **Lark**: The webhook address of the robot customized for the Lark group chat.

NOTE

The usage of the communication methods in the personnel information:

After the communication methods are modified and saved, the system background subscribes to the corresponding notification methods for sending notifications to users in other scenarios.

- **Mobile Number**: After the mobile number is saved, the system subscribes to the message and voice services of SMN and send the subscription information to the user's mobile phone by message. Users need to manually confirm the subscriptions to make them take effect.
- **Email Address**: After the Email address is saved, the system subscribes to the Email service of SMN and send the subscription information to users by Email. Users need to manually confirm the subscriptions to make them take effect.
- **WeCom** can be used without subscription.
- **DingTalk** can be used without subscription.
- **DingTalk Key**: When a message is sent to DingTalk, DingTalk verifies the key. The message can be sent only when the key is correct.
- **Lark**: After you fill in and save the configuration, you can use Lark without creating a subscription.

Notes:

- The current version supports the following notification methods: SMS messages, WeCom, voice calls, DingTalk, Lark, and emails. WeCom, Lark, voice call notifications, and DingTalk are in the open beta test (OBT) phase and can be used only after you apply for the OBT permission. For details about how to apply for the OBT permission, see the message bar in the **O&M Engineer Management** page.
- After the configurations for the WeCom, Lark, and DingTalk notification methods are saved, the system can use them without subscription.
- After the subscription is manually confirmed, the subscription status is automatically synchronized 10 minutes later. The corresponding notifications can be used only after the synchronization is successful.

Step 5 Click **OK**.

The user information is modified.

----End

Deleting Information About a User

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Locate the user to be deleted and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

The user information is deleted.

----End

Selecting a Notification Method

Subscriptions let you select your preferred notification methods. If a user does not confirm the subscription message within 48 hours, the subscription confirmation link becomes invalid. After the subscription expires, the user can initiate a subscription again on the **O&M Engineer Management** page.

Step 1 Log in to **COC**.

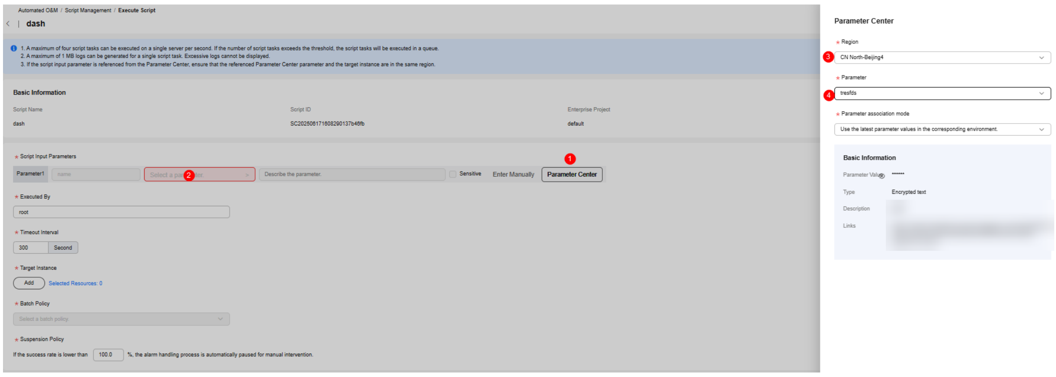
Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 On the displayed page, select the target engineer and click **Subscribe** in the **Operation** column.

Step 4 In the displayed dialog box, select the desired notification method and click **OK**.

- After you click **Subscribe**, you can select a notification method in the displayed dialog box.
- If the subscription of a notification method has been confirmed, its option will be unavailable in the **Pull Subscription** dialog box.
- If a user has confirmed the subscription of all notification methods, the **Subscription** button in the **Operation** column on the page is unavailable.

Figure 11-3 Subscription request



Automated O&M / Script Management / Execute Script

dash

1. A maximum of four script tasks can be executed on a single server per second. If the number of script tasks exceeds the threshold, the script tasks will be executed in a queue.
2. A maximum of 1 MB logs can be generated for a single script task. Excessive logs cannot be displayed.
3. If the script input parameter is referenced from the Parameter Center, ensure that the referenced Parameter Center parameter and the target instance are in the same region.

Basic Information

Script Name	Script ID	Enterprise Project
dash	SC202506171608290137b46fb	default

* Script Input Parameters

Parameter1 | name | Select a parameter. | Describe the parameter. | □ Sensitive | Enter Manually | Parameter Center

* Executed By: root

* Timeout Interval: 300 Second

* Target Instance: Add | Selected Resources: 0

* Batch Policy: Select a batch policy.

* Suspension Policy: If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Parameter Center

* Region: CN North-Beijing4

* Parameter: tresfds

* Parameter association mode: Use the latest parameter values in the corresponding environment.

Basic Information

Parameter Value: ******

Type: Encrypted text

Description: [redacted]

Links

----End

11.1.3 Managing Notification Groups

Scenarios

You can select a notification mode on the **Notification Management** and **SLA Management** pages to send different alarms, incidents, changes, and SLA warnings to different groups.

Constraints and Limitations

- A maximum of 10,000 groups can be added to a tenant account, and a maximum of 500 members can be added to each group.
- A maximum of 10 groups can be selected for a single notification.
- The group name can contain a maximum of 128 characters.

Creating a Notification Group

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click the **Manage Notification Group** tab.

Step 4 Click **Create Notification Group**.

Step 5 Set the basic information by referring to **Table 11-2**.

Table 11-2 Parameters for creating a notification group

Parameter	Description
Notification Group	Name of the notification group.
Notification Group Member	Select notification group members from the drop-down list. Multiple members can be selected. The data comes from O&M engineer management.
Webhook URL	Webhook address of the notification group. ● Select the group type. The options are WeCom Group, DingTalk Group, Lark Group, and HTTP/HTTPS Group. If you want to notify a third-party platform, select HTTP/HTTPS group. ● Enter the webhook address. The address must be configured on notification apps such as WeCom and DingTalk. The value is in URL format.
Description	(Optional) Enter the description of the notification group.

Step 6 Click **OK**.

----End

Subscribing to a Notification Group

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click the **Manage Notification Group** tab.

Step 4 In the notification group list, select the target personnel and click **Subscribe** in the **Operation** column.

Complete the subscription.

----End

Modifying a Notification Group

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click the **Manage Notification Group** tab.

Step 4 In the notification group list, select the notification group to be modified and click **Edit** in the **Operation** column.

Step 5 Select notification group members from the drop-down list. Multiple members can be selected. The data comes from O&M engineer management.

Step 6 Click **OK**.

----End

Deleting a Notification Group

Deleted notification groups cannot be recovered.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click the **Manage Notification Group** tab.

Step 4 In the notification group list, select the notification group to be deleted and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

----End

11.2 Shift Schedule Management

11.2.1 Overview

You can customize a unified, multi-dimensional, and multi-form personnel management system on COC. This function is widely used in scenarios where owners are involved, such as service review and service ticket transfer. You can manage **scheduling scenarios** on the shift schedule management page and add personnel on the **O&M Personnel Management** page to configure roles in shifts.

- To configure or obtain personnel in a shift, go to the **Shift Schedule Management** page to configure or query the shift roles.
- Created shift schedules can be directly used to configure personnel parameters when using O&M service modules such as alarm conversion rules, incident center, automated O&M, notification management, and change ticket management.

Shift Scenarios

A shift scenario indicates a type of shifts. When creating a shift scenario, you need to specify the scheduling type and dimension. The scheduling type varies according to your selection.

For example, change review can be defined as a shift scenario, which indicates this shift is dedicated for change ticket review. The shift type (non-fixed shift or fixed shift) and dimension (application-based scheduling or global scheduling) are determined based on your service requirements.

Shift Roles

A shift role is the minimum unit for setting a shift schedule. Multiple roles can be created in a shift scenario, and each role can be attached to multiple personnel.

Based on the example of the change review shift scenario, you can configure shift roles based on the actual roles in your business process. Assume that a change ticket needs to be reviewed by the business director, SRE, and department leader in sequence, you can configure these three shift roles.

11.2.2 Creating Shift Schedules

Scenarios

In scenarios for handling incident and change tickets, you need to select an owner in a shift. You can create shift scenarios and roles to manage personnel.

Creating a Shift Schedule

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 On the displayed page, click **Create Schedule** in the upper right corner.

Step 4 Set the shift scenario.

- **Select from Existing**: Select an existing shift scenario and add a shift role. You can view the roles in the scenario.
- **New Scenario**: Create and configure a new shift scenario.

Table 11-3 Parameters for creating a scenario

Parameter	Description
Scenario Name	Name of a customized shift scenario.
Shift Type	The options are **Non-fixed shift (Monday-Sunday)** and **Fixed shift**. – **Non-fixed shift (Monday–Sunday)**: Engineers work different shifts depending on the schedule. – **Fixed**: Engineers work within fixed working hours.

Parameter	Description
Scheduling Dimension	The options are **Application** and **Global**. – **Application**: The schedule is created for an application in a specific region (optional). – **Global**: The schedule is globally used regardless of applications.
Scenario Description	(Optional) Enter the detailed description of the shift scenario.

Step 5 Set the scheduling role.

Table 11-4 Parameters for setting a scheduling role.

Parameter	Description
Name	Role name that you can customize.
Description	(Optional) Enter the detailed description of the role.
Add Role	Click **Add Role** to add roles.

Step 6 Click **OK**.

Access the newly created schedule. Click **Schedule**. The method of adding engineers varies according to the scheduling mode and dimension. For details, see **11.2.3 Adding Shift Personnel**.

----End

11.2.3 Adding Shift Personnel

Prerequisites

Before adding shift personnel to your schedule, you need to add them to a list on the **O&M Engineer Management** page, and then create a shift scenario and roles.

Scenarios

The methods of adding personnel vary depending on shift methods and dimensions. Click the links in the following table to see detailed procedures.

Schedule Type	Fixed Shifts	Non-fixed Shift (Monday to Sunday)
Global	Adding personnel to a **global schedule of fixed shifts**	Adding personnel to a **global schedule of non-fixed shifts**

Schedule Type	Fixed Shifts	Non-fixed Shift (Monday to Sunday)
Application-specific	Adding personnel to an **application-specific schedule of fixed shifts**	Adding personnel to an **application-specific schedule of non-fixed shifts**

Global Schedule of Fixed Shifts

Application scenario: These schedules are applied to all applications. Shift personnel are fixed in a day.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Global+ fixed** is displayed next to the scenario name.)

Step 4 Select a shift role from the drop-down list on the right.

Step 5 Click **Schedule** to add personnel for scheduling.

Step 6 Select a user from the drop-down list. Multiple users can be selected.

Step 7 Click **OK**.

Personnel for scheduling are added.

----End

Global Schedule of Non-fixed Shifts

Application scenario: These schedules are applied to all applications. Personnel work in non-fixed shifts.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Global + fixed (Monday–Sunday)** is displayed next to the scenario name.)

Step 4 Click **Schedule** to add personnel for scheduling.

Step 5 Set parameters for adding personnel for scheduling.

- **Start Time**: Select the start date. The schedule starts at 00:00 on the selected date.
- **End Time**: Select the end date. The schedule ends at 23:59 on the selected date.
- **Shift Number**: Select the number of shifts in each day.

A maximum of five shifts can be selected at a time. You need to specify the start and end time of each shift and set the owners of specific roles for each shift.

You can select multiple owners for each shift.

Step 6 Click **OK**.

Personnel for scheduling are added. After a schedule is added, you can select a schedule scenario and time segment on the Schedule page to view the personnel in the schedule.

----End

Application-specific Schedule of Fixed Shifts

Application scenario: These schedules are applied to specific applications. Shift personnel are fixed in a day.

Prerequisites: An application has been created on the **Mobile App Management** page.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Application+ fixed** is displayed next to the scenario name.)

You can quickly filter regions and applications from the drop-down lists in the upper right corner.

NOTE

You can switch between regions to view the shifts of the same application in different regions. You can leave the region blank if there are no regional differences.

Step 4 Locate the application you want to modify and click **Modify** in the **Operation** column.

Step 5 Select one or multiple personnel.

Step 6 Click **OK**.

Personnel for scheduling are added. After the schedule is added, you can view the personnel in the schedule on the schedule page.

----End

Application-specific Schedule of Non-fixed Shifts

Application scenario: These schedules are applied to specific applications.

Prerequisites: An application has been created on the **Mobile App Management** page.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Application+ fixed (Monday–Sunday)** is displayed next to the scenario name.)

You can quickly filter regions, applications, and time segments from the drop-down lists in the upper right corner.

NOTE

You can switch between regions to view the shifts of the same application in different regions. You can leave the region blank if there are no regional differences.

Step 4 Click **Schedule**.

Step 5 Set parameters for adding personnel for scheduling.

- **Region**: (Optional) Region where the schedule is applied. You can select multiple regions.
- **Application**: Application where this schedule is applied. You can select multiple applications.
- **Start Time**: Select the start date. The schedule starts at 00:00 on the selected date.
- **End Time**: Select the end date. The schedule ends at 23:59 on the selected date.
- **Shift Number**: Select the number of shifts in each day.

Step 6 Click **OK**.

Personnel for scheduling are added. After the schedule is added, you can view the personnel in the schedule on the schedule page.

----End

11.2.4 Managing Shift Personnel

Scenarios

When the personnel in a shift change, you can modify or delete the information about the changes. The method of changing the personnel varies according to the scenario.

Global Schedule of Fixed Shifts

CAUTION

After a global shift role is deleted, it cannot be restored. Check whether the shift role or scenario is referenced. If yes, the review process will be interrupted or the service ticket will fail to be dispatched after the deletion. If no, there are no impacts.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Global+ fixed** is displayed next to the scenario name.)

Step 4 Locate the application for which shift personnel you want to delete and click **Delete** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

The selected personnel are deleted.

----End

Global Schedule of Non-fixed Shifts

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Global + fixed (Monday–Sunday)** is displayed next to the scenario name.)

Step 4 Click **Clear**.

- **Start Time**: Select the start date. The schedule starts at 00:00 on the selected date.
- **End Time**: Select the end date. The schedule ends at 23:59 on the selected date.
- **Schedule Role**: Select the shift roles you want to clear.

Step 5 Click **OK**.

The corresponding personnel are cleared.

----End

Application-specific Schedule of Fixed Shifts

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Application+ fixed** is displayed next to the scenario name.)

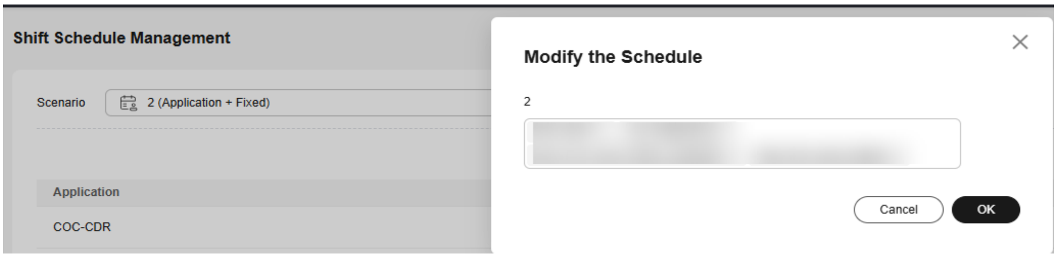
You can quickly filter regions and applications from the drop-down lists in the upper right corner.

NOTE

You can switch between regions to view the shifts of the same application in different regions. You can leave the region blank if there are no regional differences.

Step 4 Locate the application for which you want to modify the shift personnel and click **Modify** in the **Operation** column.

Figure 11-4 Modifying shift personnel



Step 5 Add or delete a shift personnel.

Step 6 Click **OK**.

The selected personnel are modified.

----End

Application-specific Schedule of Non-fixed Shifts

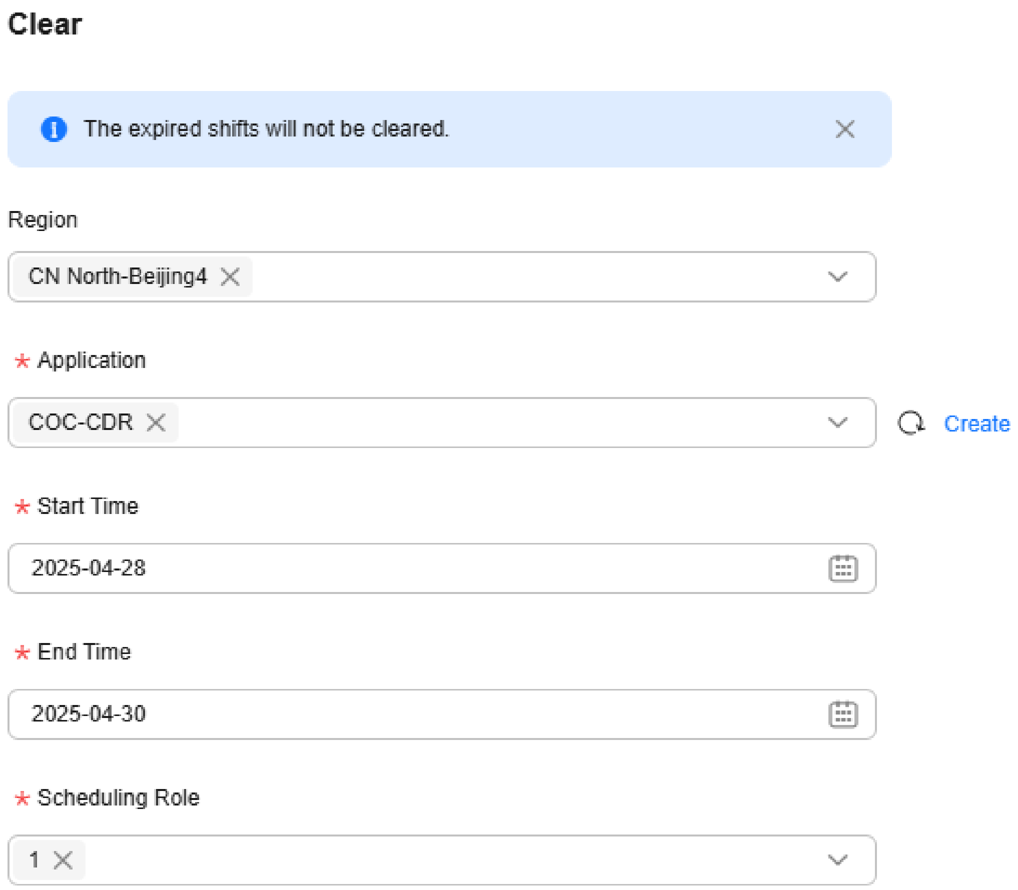
Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Select a created shift scenario from the drop-down list in the upper part. (**Application+ fixed (Monday–Sunday)** is displayed next to the scenario name.)

Step 4 Click **Clear**.

Figure 11-5 Clear shift personnel



Clear

The expired shifts will not be cleared.

Region: CN North-Beijing4

* Application: COC-CDR

* Start Time: 2025-04-28

* End Time: 2025-04-30

* Scheduling Role: 1

- **Region**: (Optional) Region where the schedule is applied. You can select multiple regions.
- **Application**: Application where this schedule is applied. You can select multiple applications.
- **Start Time**: Select the start date. The schedule starts at 00:00 on the selected date.
- **End Time**: Select the end date. The schedule ends at 23:59 on the selected date.
- **Schedule Role**: Select the shift roles you want to clear.

Step 5 Click **OK**.

The corresponding personnel are cleared.

----End

11.2.5 Managing Shift Scenarios

Scenarios

After a schedule is created, you can add, delete, modify, and query shift scenarios and roles.

Creating a Shift Scenario

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Click **Scenario Management** in the upper right corner.

Step 4 Click **Create Schedule** in the upper right corner.

Step 5 Set the parameters for creating a shift scenario.

Table 11-5 Parameters for creating a shift scenario

Parameter	Description
Scenario Name	Name of a customized shift scenario.
Shift Type	The options are **Non-fixed shift (Monday-Sunday)** and **Fixed shift**. ● **Non-fixed shift (Monday–Sunday)**: Engineers work different shifts depending on the schedule. ● **Fixed**: Engineers work within fixed working hours.
Scheduling Dimension	The options are **Application** and **Global**. ● **Application**: The schedule is created for an application in a specific region (optional). ● **Global**: The schedule is globally used regardless of applications.
Scenario Description	(Optional) Enter the detailed description of the shift scenario.

Step 6 Click **OK**.

The shift scenario is created.

----End

Creating a Shift Role

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Click **Scenario Management** in the upper right corner.

Step 4 Locate the shift scenario for which you want to create a shift role and click **Create Scheduling Role** in the **Operation** column.

Step 5 Set the parameters for creating a shift role.

Table 11-6 Parameters for creating a shift scenario

Parameter	Description
Name	Role name that you can customize.
Scenario	The preset value is the selected shift scenario and cannot be changed.
Description	(Optional) Enter the detailed description of the role.

Step 6 Click **OK**.

The shift role is created.

----End

Modifying a Shift Scenario

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Click **Scenario Management** in the upper right corner.

Step 4 Locate the shift scenario you want to modify and click **Modify** in the **Operation** column.

Step 5 Set the parameters for modifying a shift scenario.

Table 11-7 Parameters for modifying a shift scenario

Parameter	Description
Scenario Name	Name of a customized shift scenario.
Shift Type	The preset value is the selected shift type and cannot be changed.
Scheduling Dimension	The preset value is the selected dimension and cannot be changed.
Scenario Description	(Optional) Enter the detailed description of the shift scenario.

NOTE

The shift type and scheduling dimension in a scenario cannot be modified. You can create a schedule to specify the shift type and dimension you need as described in **Creating a Schedule**.

Step 6 Click **OK**.

The shift scenario is modified.

Step 7 Click ⌄ on the left of the scenario name.

Step 8 Locate the role you want to modify and click **Modify** in the **Operation** column.

Step 9 Set the parameters for modifying a shift role.

Table 11-8 Parameters for modifying a shift scenario

Parameter	Description
Name	Role name that you can customize.
Scenario	The preset value is the selected shift scenario and cannot be changed.
Description	(Optional) Enter the detailed description of the role.

Step 10 Click **OK**.

The shift role is modified.

----End

Deleting a Shift Scenario

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 3 Click **Scenario Management** in the upper right corner.

Step 4 Locate the shift scenario you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The scheduling scenario is deleted.

NOTE

A scheduling scenario can be deleted only when no scheduling role is used in that scheduling scenario.

Step 6 Click ⌄ on the left of the scenario name.

Step 7 Locate the role you want to delete and click **Delete** in the **Operation** column.

Step 8 Click **OK**.

The role in the shift scenario is deleted.

----End

11.3 Managing Notifications

Overview

- You can use notification templates for changes, incidents, issues, and alarms with various notification modes in different service scenarios and process phases. You can subscribe to notifications as required to avoid missing important information.
- When an incident ticket, issue ticket, alarm ticket, or change ticket is generated, the system uses the configured notification rules to match the incident, issue, alarm, or change. It then parses the notification rule to obtain the recipients, notification content, and notification mode, and finally sends out the appropriate notifications. Notification modes are classified into incident, issue, change, and alarm notifications.
- The system provides multiple built-in notification templates for the preceding O&M service tickets. You can select a notification template based on your scenario.

Creating a Notification Rule

Create a notification rule. After an incident, issue, or change ticket matches the corresponding rule, a notification is automatically sent.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Notification Management**.

Step 3 Click **Create Notification** in the upper right corner.

Step 4 Set parameters for creating a notification.

Table 11-9 Parameters for creating a notification

Parameter	Description
Name	Notification name that you can customize.
Type	The options are **Incident notification**, **Issue notification**, **Change notification**, and **Alarm notification**.
Template	Select a notification template from the drop-down list. Multiple templates can be selected. Notification content templates are preset by the system. The template list varies depending on the notification type. After a template is selected, the notification template details are displayed.

Parameter	Description
Notification Scope	Select a notification scope from the drop-down list. You can select multiple notification scopes by application. When you select a service, such as Service A, and the incident ticket also indicates Service A without considering other matching rules, the subscription instance will take effect and notifications will be sent based on that subscription instance.
Recipient	The options are **Ticket owner**, **Ticket creator**, **Shift**, **Individual**, and **Group**. Multiple options can be selected at a time. Set the objects to be notified and send notifications to the corresponding recipients. ● **Ticket creator**: This parameter is not required if you need to notify users of an alarm. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an individual that you want to notify. For details about how to configure a recipient, see **11.1 O&M Engineer Management** ● **Group**: Select a group you want to send notifications to and specify target group members as the recipients. You can also specify the service ticket owner as the recipient. If you do not specify the service ticket owner or other group members as the recipients, all of them in the group will be selected by default. For details about how to configure a group, see **11.1 O&M Engineer Management**
Notification Rule: Level	(Optional) Select a notification level from the drop-down list. Multiple options can be selected.
Notification Rule: Incident Category	(Optional) Select a notification type from the drop-down list. Multiple options can be selected. This parameter is not required if you need to notify users of an alarm.
Notification Rule: Source	(Optional) Select a notification ticket source from the drop-down list. Multiple options can be selected.
Notification Rule - Region	(Optional) Select a notification ticket region from the drop-down list. Multiple options can be selected.
Notification Mode	You can select **All**, **SMS**, **Phone Call**, **Lark**, **WeCom**, **DingTalk**, or **Email**. Multiple options can be selected. Before setting this parameter, configure WeCom, Lark, and DingTalk in **11.4 Managing Mobile Apps**.

⚠ CAUTION

In the shift scenario, duplicated personnel will be removed. However, if multiple persons use the same mobile number, multiple same notifications are sent, which is the same as the notification logic in individual scenario.

Notification rule example: If the value of rule *A* is set to *a*, in an incident ticket, the value of rule *A* is *a*, not considering other matching rules, the subscription instance will take effect and a notification is sent based on the subscription instance. However, if the value of rule *A* in the incident ticket is *b*, the subscription instance will not take effect, and no notification is sent.

If no rule value is set in a rule, the rule will not be matched. For example, if no value is configured for rule *A*, the notification instance takes effect without matching rule *A*, not considering other matching rules. If rule *A* changes, the notification instance still takes effect without matching rule *A*.

After a notification is created, it is enabled by default.

Step 5 Click **OK**.

The notification is created.

----End

Modifying a Notification

Modify an existing notification information.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Notification Management**.

Step 3 Locate the notification you want to modify and click **Modify** in the **Operation** column.

The parameters are similar to those for creating an emergency notification scheme. For details, see **Creating a Notification Rule**.

Step 4 Click **OK**.

The notification is modified.

----End

Deleting a Notification

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Notification Management**.

Step 3 Locate the notification you want to delete and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

The notification is deleted.

----End

Enabling or Disabling a Notification

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Notification Management**.

Step 3 Locate the notification you want to enable or disable and click **Enable** or **Disable** in the **Operation** column.

Step 4 Click **OK**.

The notification is enabled or disabled.

NOTE

The notification instance statuses include **Enabled** (in green) and **Disabled** (in red).

----End

Other Notification Features

The following notification features are not displayed on the page:

1. Notification deduplication

   When an incident ticket or a change ticket triggers multiple notifications, and the recipients or other factors of these notifications are the same, the notification module deduplicates the recipients, ensuring that a recipient receives only one notification when an incident or change ticket is generated.

11.4 Managing Mobile Apps

Scenarios

You can manage configurations of third-party mobile apps and configure parameters for a war room when an incident requires the war room on a third-party mobile app.

Viewing Mobile Apps

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Mobile App Management**.

If the current tenant has been bound to a WeChat account, the binding information is displayed. If the current tenant is not bound to a WeChat account, the page for adding a WeChat key is displayed.

NOTE

Currently, WeCom, Lark, and DingTalk are supported.

----End

Adding a Mobile App

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Mobile App Management**.

Step 3 Select the mobile app you want to enable and click the button for enabling the application now.

Step 4 Set parameters for enabling an app.

Table 11-10 Parameters for enabling an app

Parameter	Description
Enterprise ID	To obtain the company ID, click **My Company** in the top menu. In the left navigation pane, choose **Company Information**.
Enterprise Key	Log in to the WeCom management backend and click **App Management** on the top menu. In the left navigation pane, choose **Apps**. Under **Self-built**, select the app you created.
Address Book Key	Log in to the WeCom management backend and click **App Management** on the top menu. In the left navigation pane, choose **Apps**. Under **Self-built**, select the app you created.
Service ID	Log in to the WeCom management backend, choose **App Management**. Obtain the agent ID.

Table 11-11 Parameters for enabling DingTalk

Parameter	Description
Client ID	Log in to the DingTalk open platform, go to the application development module, and find the DingTalk application. In the credential and basic information area, obtain the client ID.
Client Secret	Log in to the DingTalk open platform, go to the application development module, and find the DingTalk application. In the credential and basic information area, obtain the client secret.
Group Template ID	Log in to the DingTalk Open platform, go to the Open Capabilities module, access the scenario group page, and find the group template. Then, obtain the group template ID.

Parameter	Description
Robot ID	Log in to the DingTalk Open platform, go to the Open Capabilities module, access the scenario group page, and find the robot option. Then, obtain the group robot ID.
Service ID	Log in to the DingTalk open platform, go to the application development module, and find the DingTalk application. In the credential and basic information area, obtain the Agent ID.

Table 11-12 Parameters for enabling Lark

Parameter	Description
App ID	Log in to the Lark developer backend, go to the enterprise-built application module, and find the Lark application. In the credentials and basic information area, obtain the app ID.
App Secret	Log in to the Lark developer backend, go to the enterprise-built application module, and find the Lark application. In the credentials and basic information area, obtain the app secret.
Service ID	Log in to the Lark developer backend, go to the enterprise-built application module, and find the Lark application. In the credentials and basic information area, obtain the app ID.

Step 5 Click **OK**.

The mobile app is enabled.

----End

Changing the Mobile App Key

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Mobile App Management**.

Step 3 Locate the mobile app whose key you want to change and click the button for changing the key.

Step 4 Set parameters for changing the key.

Table 11-13 Parameters for modifying information about a WeCom account

Parameter	Description
Enterprise ID	The value cannot be changed.

Parameter	Description
Enterprise Key	Log in to the WeCom management backend and click **App Management** on the top menu. In the left navigation pane, choose **Apps**. Under **Self-built**, select the app you created.
Address Book Key	Log in to the WeCom management backend and click **App Management** on the top menu. In the left navigation pane, choose **Apps**. Under **Self-built**, select the app you created.
Service ID	Log in to the WeCom management backend, choose **App Management**. Obtain the agent ID.

Table 11-14 Parameters for modifying information about a DingTalk account

Parameter	Description
Client ID	The value cannot be changed.
Client Secret	Log in to the DingTalk open platform, go to the application development module, and find the DingTalk application. In the credential and basic information area, obtain the client secret.
Group Template ID	Log in to the DingTalk Open platform, go to the Open Capabilities module, access the scenario group page, and find the group template. Then, obtain the group template ID.
Robot ID	Log in to the DingTalk Open platform, go to the Open Capabilities module, access the scenario group page, and find the robot option. Then, obtain the group robot ID.
Service ID	Log in to the DingTalk open platform, go to the application development module, and find the DingTalk application. In the credential and basic information area, obtain the Agent ID.

Table 11-15 Parameters for modifying information about a Lark account

Parameter	Description
App ID	The value cannot be changed.
App Secret	Log in to the Lark developer backend, go to the enterprise-built application module, and find the Lark application. In the credentials and basic information area, obtain the app secret.
Service ID	Log in to the Lark developer backend, go to the enterprise-built application module, and find the Lark application. In the credentials and basic information area, obtain the app ID.

Step 5 Click **OK**.

The mobile app key is changed.

----End

Deleting a Mobile App

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Mobile App Management**.

Step 3 Select the mobile app you want to delete and click **Delete**.

Step 4 Click **OK**.

The mobile app is deleted.

----End

11.5 SLA Management

11.5.1 Overview

Service Level Agreement (SLA) is generally used to measure the service quality in the industry. It defines the quality standard, delivery method, and acceptable performance level of a service. The SLA management function of COC provides the service ticket validity period management capability. When a service ticket triggers an SLA rule, COC records the SLA trigger details for the service ticket and notifies the corresponding users to follow up and handle the service ticket in a timely manner.

SLA functions:

- Customers can customize SLAs or use public SLA rules preset by COC.
- Four trigger scenarios are supported: incident tickets, alarm tickets, to-do tasks, and issue tickets.
- You can set SLA targets (a service ticket must be completed within a specified period of time). When a service ticket triggers a rule, the system notifies the specified personnel in a specified method and supports continuous notification.
- You can set SLA warning targets. When an SLA is about to be broken, the system sends a notification at a specified time in advance.
- You can view SLA records, including key information such as the service ticket ID, SLA status, and SLA rule.

NOTE

- After an SLA is created or modified, the SLA takes effect for the service tickets that enter the SLA workflow later but does not take effect for the service tickets that are already in the SLA workflow.
- Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

11.5.2 Managing Custom SLAs

Scenarios

You can customize SLA target rules and warning rules for service tickets based on service requirements to standardize ticket owners' operations such as timely response and handling of service tickets.

Precautions

The SLA list displays only the custom SLAs created by the current tenant account and its subaccounts.

Creating a Custom SLA

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 On the **Custom SLAs** tab page, click **Create SLA** in the upper right corner.

Step 4 Set parameters for creating an SLA.

Table 11-16 Parameters for creating an SLA

Parameter	Description
SLA Name	Specify an SLA name based on naming rules.
Description	(Optional) Description of an SLA.
Trigger Type	The options are **Incident ticket**, **Alarm ticket**, **To-do task**, and **Issue ticket**.
Level	Select the level of the service ticket to be triggered. Multiple levels can be selected.
Application	Select the application to which the service ticket belongs. Multiple applications can be selected. This parameter is not required for to-do tasks.
Rule Settings	Select the rule type you want to set and click **Modify** in the **Operation** column. For details about the parameters, see **Table 11-17**.
Available Duration	The options are **24/7** and **Other**. Set the time by week. SLA records are generated for service tickets generated in the time period where the SLA has not taken effect. SLA calculation starts when the effective time arrives.

Table 11-17 Parameters for setting rules

Parameter	Description
SLA Target	After this function is enabled, you can set the target time. A maximum of 60 days can be set.
Recipient	The options are **Ticket owner**, **Shift**, **Individual**, and **Group**. Multiple options can be selected. By default, **Ticket owner** is selected. Set the objects to be notified and send notifications to the corresponding users. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select an individual that you want to notify. For details about how to configure a recipient, see **11.1 O&M Engineer Management** ● **Group**: Select a notification group. For details about how to configure a notification group, see **Notification Group Management**. – Select a group: Select the group type and group name. The group type can be WeCom, DingTalk, Lark, or HTTP/HTTPS groups. – (Optional) Select a group member to be notified: Select a user.
Notification Mode	Select a notification method from the drop-down list. Notification method can be used only when the notification object is a service ticket owner, shift, or individual. ● **Default**: Select any notification method you have subscribed to. If you have not subscribed to any notification method, you cannot receive notifications. ● **SMS and Email**: After a notification method is selected, the notification is sent based on the information reserved by the reviewer. For details about how to set the reviewer information, see **Modifying Personnel Information**. ● **No notification**: The system does not notify any recipient.
Continuous Notification	The options are **Yes** and **No**.
SLA Warning	This parameter can be set only when the SLA target is enabled. After the SLA target is enabled, the SLA warning time is set.
Warning Recipient	This parameter can be set only when **SLA Warning** is enabled. Select warning recipients from the drop-down list. The options are service ticket owner, shift, individual, and group. Multiple options are supported. By default, **Ticket owner** is selected.

Parameter	Description
Warning Notification Method	This parameter can be set only when **SLA Warning** is enabled. You can select a warning notification method from the drop-down list. This parameter is used only when the recipient is the service ticket owner, a shift, or an individual.
Notify Escalation	This parameter can be set only when the SLA target is enabled. After the SLA target is enabled, the time for escalating the notification can be configured. Click the button for adding an escalation rule to add more escalation rules. A maximum of five rules can be added.
Recipient	You can set this parameter only when the notification escalation function is enabled. Select a recipient from the drop-down list. The options are **Ticket owner**, **Shift**, **Individual**, and **Group**. Multiple options can be selected at a time. By default, **Ticket owner** is selected.
Notification Mode	You can set this parameter only when the notification escalation function is enabled. Select a notification method from the drop-down list. This parameter is used only when the recipient is the service ticket owner, a shift, or an individual.

Step 5 Click **OK**.

The SLA is created.

NOTE

- Only custom SLAs can be created. The public SLA is automatically preset in the system. Tenants can only enable, disable, and view the public SLA.
- After an SLA is created or modified, the SLA takes effect for the service tickets that enter the SLA workflow later but does not take effect for the service tickets that are already in the SLA workflow.
- SLA templates with the same SLA type, application, and importance cannot be created repeatedly.

----End

Enabling or Disabling a Custom SLA

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 On the **Custom SLAs** tab page, select the SLA you want to enable or disable and click **Enable** or **Disable** in the **Operation** column.

Step 4 Click **OK**.

The SLA is enabled or disabled.

NOTE

- After an SLA is created, it is disabled by default. You need to enable it manually.
- When multiple SLA rules match a new service ticket, the priority of the custom SLA is higher than that of the common SLA, and the priority of some applications is higher than that of all applications.
- By default, common SLA is disabled. After you click **Enable**, SLA management is enabled for the ticket.

----End

Modifying a Custom SLA

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 On the **Custom SLAs** tab page, locate the SLA you want to modify and click **Modify** in the **Operation** column.

Set parameters on the displayed page. The parameters are the same to those for creating an SLA. For details, see **Creating a Custom SLA**.

Step 4 Click **OK**.

The SLA is modified.

NOTE

- Only custom SLAs in the **Disable** state can be modified.
- After an SLA is modified, enable it. The new SLA applies only to new tickets that enter the process. Existing tickets remain under the old SLA.

----End

Deleting a Custom SLA

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 On the **Custom SLAs** tab page, locate the SLA you want to delete and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

The SLA is deleted.

NOTE

Only custom SLA templates in the **Disabled** state can be deleted.

----End

11.5.3 Managing Public SLAs

Scenarios

Public SLAs are preset by the system and can be used out of the box. By default, public SLAs are disabled. You can enable or disable public SLAs based on service requirements.

Enabling or Disabling Public SLAs

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 Click the **Public SLAs** tab.

Step 4 Locate the public SLA you want to enable or disable and click **Enable** or **Disable** in the **Operation** column.

Step 5 Click **OK**.

The public SLA is enabled or disabled.

----End

11.5.4 Viewing SLA Records

Scenarios

If there is an SLA rule for this account and the SLA rule is triggered by a service ticket, a record is generated on the SLA record page. You can view the SLA record details, such as the service ticket ID, SLA status, and SLA rule (public SLA or custom SLA).

Viewing SLA Records

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLA Management**.

Step 3 Click the **SLA-based Tickets** tab.

Step 4 Locate the SLA-based ticket you want to view and click **SLA Template** in the SLA column.

View the corresponding SLA template.

Step 5 Locate the SLA record you want to view and click the service ticket name.

View SLA record details.

NOTE

- The **SLA Status** column in the **SLA Information** table on the **SLA Record Details** page is strongly associated with the SLA rule configured during SLA template creation. If a service ticket status keeps for a duration that exceeds the specified duration set in the SLA rule, the status automatically changes to **Has Broken**.
- Duration is closely related to the status change of the ticket.

----End

11.6 SLO Management

11.6.1 Overview

Service Level Object (SLO) is a common metric in the industry. The actual SLO value is calculated as follows: Actual SLO value = 1 – (Application unavailability duration/Total application duration) × 100%. Generally, the SLO value indicates the quality level of a service or application.

On COC, O&M service tickets, such as war rooms, alarm tickets, and incident tickets (incident tickets whose **Service Interruption Attribute** is **Yes**), affect the SLO. COC automatically calculates the SLO and provides data for the SLO dashboard.

11.6.2 Configuring an SLO

Scenarios

You can configure an SLO based on service requirements and view the configured SLO, including the configured Service Level Indicator (SLI) and SLO interruption records.

Creating an SLO

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Click **Create SLO** in the upper right corner.

Step 4 Set parameters for creating an SLO.

Table 11-18 Parameters for creating an SLO

Parameter	Description
Application	Select an application from the drop-down list.
SLO	Enter the SLO value. The unit is %.

Step 5 Click **OK**.

The SLO is created.

----End

Modifying an SLO

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO you want to modify and click **More** in the **Operation** column and choose **Modify**.

Step 4 Set parameters for creating an SLO.

Table 11-19 Parameters for modifying an SLO target

Parameter	Description
Application	The value cannot be changed.
SLO	Enter the SLO value. The unit is %.

Step 5 Click **OK**.

The SLO is modified.

----End

Deleting an SLO

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO you want to delete and choose **More** > **Delete** in the **Operation** column.

Step 4 Click **OK**.

The SLO is deleted.

----End

11.6.3 Configuring SLO Metrics

Scenarios

On this page, you can add, modify, delete, and view SLO metrics.

Metrics are classified into request SLIs and instance-based SLIs. After the configuration is complete, you can manually add the metrics in **11.6.4 Viewing SLO Interruption Records**.

Adding an SLO Metric

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO metric you want to configure and click **Configure Metric** in the **Operation** column.

Step 4 Click **Add SLI Metric**.

Step 5 Set parameters for configuring an SLI.

Table 11-20 Parameters for configuring an SLI

Parameter	Description
Metric Type	The options are **Request SLI Metric** and **Instance SLI Metric**.
SLI Metric Name	Specify an SLI name based on naming rules.
SLI Metric Description	Enter the detailed description of the SLI.
Definition of Unavailable	Select the comparison mode, parameter value, and parameter unit. The parameter is unavailable when it meets the conditions.

Step 6 Click **OK**.

Step 7 Click **OK**.

The SLO metric is added.

----End

Modifying an SLO Metric

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO metric you want to configure and click **Metric Configuration** in the **Operation** column.

Step 4 Locate the metric you want to modify and click **Modify** in the **Operation** column.

Step 5 Set parameters for configuring an SLI.

Table 11-21 Parameters for configuring an SLI

Parameter	Description
Metric Type	The options are **Request SLI Metric** and **Instance SLI Metric**.

Parameter	Description
SLI Metric Name	Specify an SLI name based on naming rules.
SLI Metric Description	Enter the detailed description of the SLI.
Definition of Unavailable	Select the comparison mode, parameter value, and parameter unit.

Step 6 Click **OK**.

Step 7 Click **OK**.

The SLO metric is modified.

----End

Deleting an SLO Metric

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO metric you want to configure and click **Configure Metric** in the **Operation** column.

Step 4 Locate the metric you want to delete and click **Modify** in the **Operation** column.

Step 5 Click **OK**.

The SLO metric is deleted.

----End

11.6.4 Viewing SLO Interruption Records

Scenarios

On this page, you can view, add, and modify SLO interruption records.

You can add SLO interruption records from five sources: SLIs, war rooms, alarm tickets, incident tickets, and other. If SLA records are available and there are service interruptions, interruption records are automatically generated for alarm and incident tickets. For details about the rule examples, see the alarm ticket SLO interruptions in **7.2.4 Clearing Alarms**. However, the interruption records for the other three types can only be manually added.

You can also modify the SLO interruption record. This enables automatic calculation of the unavailability duration by modifying the unavailability start and end time in the interruption record.

Adding an SLO Interruption Record

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO metric you want to view and click **Interruption Record** in the **Operation** column.

Step 4 Click **Add Interruption Record** in the upper left corner.

Table 11-22 Parameters for adding an interruption record

Parameter	Description
Source	The options are **SLI metric**, **War room**, **Alarm ticket**, **Incident ticket**, and **Other**.
Metric/Ticket No./Other	Select a metric, ticket number, or other sources based on the source.
Region	Select the region where the interruption occurs from the drop-down list.
Unavailability Start Time and End Time	Enter the start time and end time of the interruption.
Description	Enter the detailed description of the interruption record.

Step 5 Click **OK**.

The interruption record is added.

----End

Modifying an Interruption Record

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **SLO Management**.

Step 3 Locate the SLO metric you want to view and click **Interruption Record** in the **Operation** column.

Step 4 Locate the interruption record to be modified and click **Modify** in the **Operation** column.

Table 11-23 Parameters for modifying an interruption record

Parameter	Description
Unavailability Start Time and End Time	Enter the start time and end time of the interruption.

Parameter	Description
Description	Enter the detailed description of the interruption record.

Step 5 Click **OK**.

The interruption record is modified.

Step 6 Locate the interruption record you want to view and click **Correct Record** in the **Operation** column.

Details about the interruption record are displayed.

----End

11.7 Process Management

11.7.1 Overview

You can customize the incident process, issue process, and change scenario. You can use the customized process management configuration for the fault management and change management modules as needed. The following table lists the processes that can be configured.

Table 11-24 Process management scenarios

Level-1 Category	Level-2 Category	Scenario
Incident Process	Incident Level	A maximum of five incident levels can be set. You can modify the incident level name, description, and whether to enable the incident level.
	Incident Category	You can enable or disable incident categories, and add, delete, or modify custom incident categories (preset incident categories are not supported).
	Incident Review	You can customize review rules for incident de-escalation and suspension scenarios.
	Fault Review	You can customize incident fault review rules.
Issue Process	Issue Level	A maximum of four issue levels can be set. You can modify the issue level name, description, and whether to enable the issue level.

Level-1 Category	Level-2 Category	Scenario
	Issue Category	You can enable or disable issue categories, and add, delete, or modify custom issue categories (preset issue categories are not supported).
	Issue Review	You can customize review rules for issue suspension and issue level adjustment scenarios.
Change Scenario	Change Scenario	You can enable or disable change scenarios and add, delete, modify, enable, or disable subnodes. Custom change scenarios can be added, deleted, or modified. Preset scenarios cannot be deleted or modified.

11.7.2 Incident-related Operations

11.7.2.1 Managing Incident Levels

Scenarios

If the incident level name description provided by the system does not comply with the incident level and description defined in the service process, you can change the incident level and modify the description. Once the information is modified, the latest defined level is displayed on the incident ticket creation page.

Changing an Incident Level

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Level** tab.

Step 4 Locate the incident level you want to change and click **Change** in the **Operation** column.

Step 5 Set parameters for changing the incident level.

Table 11-25 Parameters for changing the incident level

Parameter	Description
Incident Level - Chinese Name	Enter the name of the incident level in the Chinese environment.
Incident Level - English Name	Enter the name of the incident level in the English environment.

Parameter	Description
Level Color	Select the color corresponding to the current incident level.
Description - Chinese	Enter the detailed description of the incident for the Chinese environment.
Description - English	Enter the detailed description of the incident for the English environment.

Step 6 Click **OK**.

The incident level is changed.

Step 7 Locate the incident level you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable the incident level. Once the incident level is disabled, the current incident level will become unavailable.

----End

11.7.2.2 Managing Incident Categories

Scenarios

If the incident category name provided by the system does not match the incident category defined in the service process, you can change the incident category. After the incident category is changed, you can view the latest incident category on the incident creation page.

Creating an Incident Category

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Category** tab.

Step 4 Click **Create Incident Category**.

Table 11-26 Parameters for creating an incident category

Parameter	Description
Incident Category - Chinese Name	Enter the name of the incident category in the Chinese environment.
Incident Category - English Name	Enter the name of the incident category in the English environment.
Description - Chinese	Enter the detailed description of the incident category for the Chinese environment.

Parameter	Description
Description - English	Enter the detailed description of the incident category for the English environment.

Step 5 Click **OK**.

The incident category is created.

----End

Changing an Incident Category

The preset incident category cannot be changed.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Category** tab.

Step 4 Locate the incident category you want to change and click **Change** in the **Operation** column.

Step 5 Set parameters for changing the incident category.

Table 11-27 Parameters for changing the incident category

Parameter	Description
Incident Category - Chinese Name	Enter the name of the incident category for the Chinese environment.
Incident Category - English Name	Enter the name of the incident category for the English environment.
Description - Chinese	Enter the detailed description of the incident category for the Chinese environment.
Description - English	Enter the detailed description of the incident category for the English environment.

Step 6 Click **OK**.

The incident category is changed.

Step 7 Locate the incident category you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable an incident category. After an incident category is disabled, it cannot be used.

----End

Deleting an Incident Category

The preset incident category cannot be deleted.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Category** tab.

Step 4 Locate the incident category you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The incident category is deleted.

----End

11.7.2.3 Managing Incident Review Tasks

Scenarios

The system provides the default incident suspension and de-escalation processes. You can customize the incident suspension and de-escalation review processes. After the processes are modified, you can initiate requests and review the processes on the incident handling page.

- The created incident ticket process takes effect only after the incident de-escalation and review process configurations take effect.
- Incidents in the handled state can be escalated, de-escalated, or suspended.
- Before closing an incident, close the escalation, de-escalation, and suspension e-flows.
- Incident escalation does not need to be reviewed.

Viewing an Incident Review Task

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Approval** tab.

Step 4 Select the incident review task you want to view and click **View Details** in the **Operation** column.

View review configuration details.

----End

Enabling or Disabling an Incident Review Task

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Approval** tab.

Step 4 Locate the incident review task you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable the incident review task. If the incident review task is disabled, the current incident review task is unavailable.

----End

Creating an Incident Review Task

Only one review scenario can be available. If there is already a same review scenario, the review scenario cannot be created.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Approval** tab.

Step 4 Click **Create Incident Review**.

Step 5 Set parameters for configuring a review task.

Table 11-28 Parameters of review configurations

Parameter	Description
Review Scenario	The options are **Incident de-escalation** and **Incident suspension**. Select the scenario to which the incident review applies.
Incident Level	This parameter needs to be set only when the review scenario is incident de-escalation. The options are **P1**, **P2**, **P3**, **P4**, and **P5**. Multiple options can be selected. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Reviewer	The options are **Incident creator**, **Individual**, and **Shift**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Review Rule	The options are **One-member Approval** and **All-member Approval**.

Step 6 Click **OK**.

The incident review task is created.

----End

Modifying an Incident Review Task

Only the creator can review and modify incident review tasks.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Approval** tab.

Step 4 Locate the incident review task you want to modify and click **Change** in the **Operation** column.

Table 11-29 Parameters of review configurations

Parameter	Description
Review Scenario	The options are **Incident de-escalation** and **Incident Pause**. Select the scenario to which the incident review applies.
Incident Level	This parameter needs to be set only when the review scenario is incident de-escalation. The options are **P1**, **P2**, **P3**, **P4**, and **P5**. Multiple options can be selected. **P1** incidents are the most critical, while **P5** incidents are the least severe.
Reviewer	The options are **Incident creator**, **Individual**, and **Shift**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Review Rule	The options are **One-member Approval** and **All-member Approval**.

Step 5 Click **OK**.

The incident review task is modified.

----End

Deleting an Incident Review Task

Only the creator can review and delete incident review tasks.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab and click the **Incident Approval** tab.

Step 4 Locate the incident review task you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The incident review task is deleted.

----End

11.7.2.4 Managing Fault Review Tasks

Scenarios

After an incident passes the verification, a fault report is automatically generated based on the fault review rules. If the current fault review rules do not meet the actual service requirements, perform the following operations to adjust the fault review rules:

Enabling or Disabling a Rule

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab page and click the **Fault Review** tab.

Step 4 Locate the rule you want to enable or disable and click the feature flag to enable or disable the rule.

Enable or disable the rule. Once the rule is disabled, it will become unavailable.

----End

Modifying a Rule

NOTE

Only the management account can modify review rules.

Default Rule:

- P1, P2, P3, P4, and P5 incidents for which war rooms are set up need to be reviewed.
- P1, P2, P3, and P4 incidents for which no war rooms are set up need to be reviewed.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Incident Process** tab page and click the **Fault Review** tab.

Step 4 Locate the rule you want to modify and click **Modify** in the **Operation** column.

Step 5 Set the incident level.

Select the incident level for fault review. Multiple levels can be selected. The options are **P1**, **P2**, **P3**, **P4**, and **P5**. The preset value is **P1** (most serious) and P5 (most moderate).

Step 6 Click **OK**.

The fault review rule is modified.

----End

11.7.3 Issue Process-related Operations

Scenarios

In actual services, the issue level, type, de-escalation, and suspension are different from the default enumerated values or processes. You can modify the issue level and category, and customize the review configurations for issue de-escalation and suspension.

11.7.3.1 Managing Issue Levels

Changing an Issue Level

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Level** tab.

Step 4 Locate the issue level you want to change and click **Change** in the **Operation** column.

Step 5 Set parameters for changing the incident level.

Table 11-30 Parameters for changing an issue level

Parameter	Description
Issue Level - Chinese Name	Enter the name of the issue level in the Chinese environment.
Issue Level - English Name	Enter the name of the issue level in the English environment.
Level Color	Select the color corresponding to the current issue level.
Description - Chinese	Enter the detailed description of the issue level for the Chinese environment.
Description - English	Enter the detailed description of the issue level for the English environment.

Step 6 Click **OK**.

The issue level is changed.

Step 7 Locate the issue level you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable the issue level. After the issue level is disabled, it will become unavailable.

----End

11.7.3.2 Managing Issue Types

Creating an Issue Type

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Type of Issue** tab.

Step 4 Click **Create Issue Type**.

Table 11-31 Parameters for creating an issue type

Parameter	Description
Issue Type - Chinese Name	Enter the name of the issue type in the Chinese environment.
Issue Type - English Name	Enter the name of the issue type in the English environment.
Description - Chinese	Enter the detailed description of the issue type for the Chinese environment.
Description - English	Enter the detailed description of the issue type for the English environment.

Step 5 Click **OK**.

The issue type is created.

----End

Changing an Issue Type

A preset issue type cannot be changed.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Type of Issue** tab.

Step 4 Locate the issue type you want to change and click **Change** in the **Operation** column.

Step 5 Set parameters for changing the incident type.

Table 11-32 Parameters for changing the issue type

Parameter	Description
Issue Type (Chinese)	Enter the name of the issue type in the Chinese environment.

Parameter	Description
Issue Type (English)	Enter the name of the issue type in the English environment.
Description - Chinese	Enter the detailed description of the issue type for the Chinese environment.
Description - English	Enter the detailed description of the issue type for the English environment.

Step 6 Click **OK**.

The issue type is changed.

Step 7 Locate the issue type you want to enable or disable and click the feature flag to enable or disable feature.

Adjust the enabling/disabling status of the issue type. After the issue type is disabled, it cannot be used.

----End

Deleting an Issue Type

A preset issue type cannot be deleted.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Type of Issue** tab.

Step 4 Locate the issue type you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The issue type is deleted.

----End

11.7.3.3 Managing Issue Review Tasks

Constraints and Limitations

- An issue ticket process takes effect only after the issue de-escalation and suspension review processes take effect.
- After an issue ticket is accepted, it can be escalated, de-escalated, or suspended.
- Before closing an issue ticket, close the escalation, de-escalation, and suspension e-flows.
- Escalation of an issue ticket does not need to be reviewed.

Viewing an Issue Review Task

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Review** tab.

Step 4 Locate the issue review task you want to view and click **View Details** in the **Operation** column.

View review configuration details.

----End

Enabling or Disabling an Issue Review Task

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Review** tab.

Step 4 Locate the issue review task you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable the issue review task. If the issue review task is disabled, the issue review task is unavailable.

----End

Creating an Issue Review Task

Only one review scenario can be available. If there is already a same review scenario, the review scenario cannot be created.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Review** tab.

Step 4 Click **Create Issue Review**.

Step 5 Set parameters for creating an issue review task.

Table 11-33 Parameters for creating an issue review task

Parameter	Description
Review Scenario	The options are **De-escalation** and **Suspension**. Select the scenario to which the issue review applies.
Issue Level	This parameter needs to be set only when the review scenario is issue de-escalation. The options are **Critical**, **Major**, **Minor**, and **Warning**. Multiple options can be selected.

Parameter	Description
Reviewer	The options are **Issue creator**, **Individual**, and **Shift**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.
Review Rule	The options are **One-member Approval** and **All-member Approval**.

Step 6 Click **OK**.

The issue review task is created.

----End

Modifying an Issue Review Task

Only issue review task creators can modify issue review tasks.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Review** tab.

Step 4 Locate the issue review task you want to change and click **Change** in the **Operation** column.

Table 11-34 Parameters for modifying an issue review task

Parameter	Description
Review Scenario	The options are **De-escalation** and **Suspension**. Select the scenario to which the issue review applies.
Issue Level	This parameter needs to be set only when the review scenario is issue de-escalation. The options are **Critical**, **Major**, **Minor**, and **Warning**. Multiple options can be selected.
Reviewer	The options are **Issue creator**, **Individual**, and **Shift**. ● **Shift**: Select a scenario and role from the drop-down lists based on the configured values. For details about how to configure a shift, see **11.2 Shift Schedule Management**. ● **Individual**: Select a reviewer. For details about how to configure a reviewer, see **11.1 O&M Engineer Management**.

Parameter	Description
Review Rule	The options are **One-member Approval** and **All-member Approval**.

Step 5 Click **OK**.

The issue review task is modified.

----End

Deleting an Issue Review Task

Only issue review task creators can and delete issue review tasks.

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Access the **Issue Process** tab page and click the **Issue Review** tab.

Step 4 Locate the issue review task you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The issue review task is deleted.

----End

11.7.4 Managing Change Scenarios

Scenarios

The preset change scenario fields in change management are different from those used in actual services. You can change the enumerated values of change scenarios.

Enabling or Disabling a Change Scenario

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Click the **Change Scenario** tab.

Step 4 Locate the change scenario you want to enable or disable and click the feature flag to enable or disable feature.

Enable or disable the change scenario. If the change scenario is disabled, the scenario becomes unavailable.

----End

Creating a Change Scenario

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Click **Change Scenario**.

Step 4 Click **Create Change Scenario**.

Step 5 Set parameters for creating a change scenario.

Table 11-35 Parameters for creating a change scenario

Parameter	Description
Change Scenario - Chinese Name	Enter the name of the change scenario for the Chinese environment.
Change Scenario - English Name	Enter the name of the change scenario for the English environment.
Description - Chinese	Enter the detailed description of the change scenario in the Chinese environment.
Description - English	Enter the detailed description of the change scenario in the English environment.
Parent Node ID	(Optional) Enter the change scenario ID. If you enter a parent node ID, the scenario is added under the corresponding parent node. If you do not enter a parent node ID, the scenario is added as a parent node. Currently, only one layer of subnodes is supported.

Step 6 Click **OK**.

The change scenario is created.

----End

Modifying a Change Scenario

A preset change scenario cannot be modified.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Click **Change Scenario**.

Step 4 Locate the change scenario you want to modify and click **Modify** in the **Operation** column.

Table 11-36 Parameters for modifying a change scenario

Parameter	Description
Change Scenario - Chinese Name	Enter the name of the change scenario for the Chinese environment.
Change Scenario - English Name	Enter the name of the change scenario for the English environment.
Description - Chinese	Enter the detailed description of the change scenario in the Chinese environment.
Description - English	Enter the detailed description of the change scenario in the English environment.
Parent Node ID	The value cannot be changed.

Step 5 Click **OK**.

The change scenario is modified.

----End

Deleting a Change Scenario

A preset change scenario cannot be deleted.

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**.

Step 3 Click **Change Scenario**.

Step 4 Locate the change scenario you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK**.

The change scenario is deleted.

----End

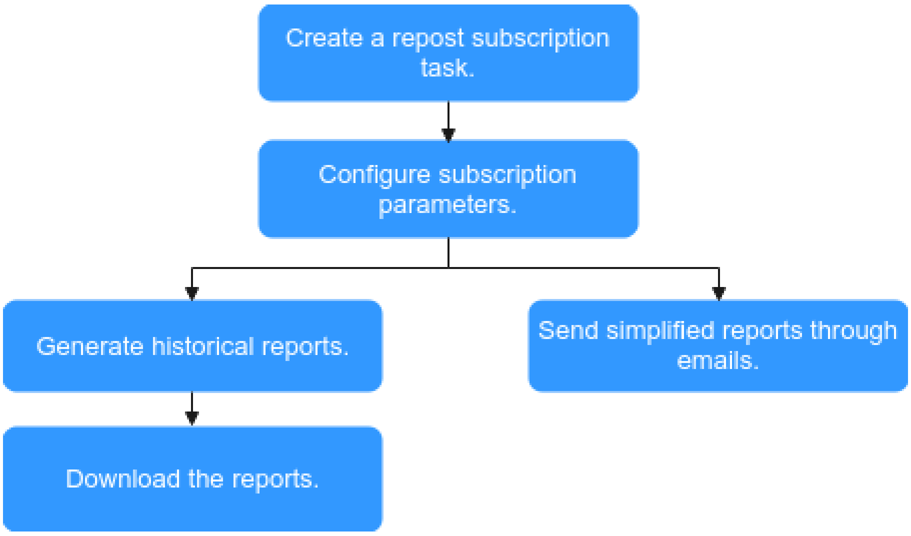
11.8 Report Subscription

11.8.1 Overview

The report subscription function is used by O&M personnel to collect O&M data and report service statuses. It provides automatic and periodic O&M data statistics reports. This feature addresses the issues of inefficiency in traditional manual collection and sorting of O&M data, as well as the high labor costs associated with statistical analysis.

The report data comes from the **O&M BI** dashboards delivered by COC. When creating a subscription report, you can set subscription parameters such as the report sending frequency, report content, and recipients. Then, recipients can periodically receive the subscribed report in their email addresses. You can also view and download historical reports on the report subscription page.

Figure 11-6 Report subscription process


Create a repost subscription task.
Configure subscription parameters.
Generate historical reports.
Send simplified reports through emails.
Download the reports.

11.8.2 Managing Report Subscription Tasks

Scenarios

When you need to collect statistics on O&M data for service reporting, you can create, modify, and delete custom subscription reports as required, and view historical subscription reports that are periodically generated.

Constraints and Limitations

When you create or modify a subscription task, a maximum of 50 recipients, 50 regions, and 10 applications can be selected.

Prerequisites

- Ensure that you have enabled the O&M BI function in the **Package Management** module in the navigation pane on the left. For details, see **Billing Items**.
- You need to modify and subscribe to the email contact information of the personnel on the **Personnel Management** page.

Creating a Subscription Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Report Subscription**.

Step 3 Click **Create Subscription Task** in the upper right corner.

Step 4 Set the basic information about the report subscription by referring to **Table 11-37**.

Table 11-37 Parameters for creating a subscription task

Parameter	Description
Subscription Name	Customize a subscription task name.
Sending Frequency	The options are **Daily**, **Weekly**, and **Monthly**. ● **Daily**: At 03:30 every day, the system automatically sends an O&M report of a previous day by default. ● **Weekly**: At 03:30 every Monday, the system automatically sends an O&M report of the previous week by default. ● **Monthly**: At 03:30 on the first day of each month, the system automatically sends an O&M report of the previous month by default.
Recipient	Select the person who receives the report. Multiple options can be selected. By default, all personnel are selected.
Report Content	The options are **Select All**, **O&M Overview**, **Change**, **Fault Management**, **Alarm**, **SLO**, and **PRR**. Multiple options can be selected.
Region	Select the region where the report data is from. Multiple options can be selected.
Application	Select the application to which the report data belongs. Multiple options can be selected.

Step 5 Click **OK**.

----End

Modifying a Subscription Task

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Report Subscription**.

Step 3 Locate the subscription task for which you want to modify the shift personnel and click **Modify** in the **Operation** column.

Step 4 Modify the basic information about the report subscription by referring to **Table 11-37**.

Table 11-38 Parameters for modifying a subscription task

Parameter	Description
Subscription Name	Customize a subscription task name.

Parameter	Description
Sending Frequency	The options are **Daily**, **Weekly**, and **Monthly**. ● **Daily**: At 03:30 every day, the system automatically sends an O&M report of a previous day by default. ● **Weekly**: At 03:30 every Monday, the system automatically sends an O&M report of the previous week by default. ● **Monthly**: At 03:30 on the first day of each month, the system automatically sends an O&M report of the previous month by default.
Recipient	Select the person who receives the report. Multiple options can be selected. By default, all personnel are selected.
Report Content	The options are **Select All**, **O&M Overview**, **Change**, **Fault Management**, **Alarm**, **SLO**, and **PRR**. Multiple options can be selected.
Region	Select the region where the report data is from. Multiple options can be selected.
Application	Select the application to which the report data belongs. Multiple options can be selected.

Step 5 Click **OK**.

----End

Deleting a Subscription Task

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Report Subscription**.

Step 3 Locate the subscription task you want to delete and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

----End

Viewing Historical Reports

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Report Subscription**.

Step 3 Select the subscription task whose reports you want to view and click **Historical Reports** in the **Operation** column.

Step 4 Select the report you want to view and click **Download Report** in the **Operation** column to go to a new tab page to view the report content.

Step 5 Click **Download Report** in the upper right corner to download the report in PDF format to the local PC.

----End

12 Viewing Logs

COC Operations That Can Be Audited

With Cloud Trace Service (CTS), you can record operations associated with COC for later query, audit, and backtracking. **Table 12-1** lists the key operations.

Table 12-1 Key COC operations recorded by CTS

Action	Resource	Trace
Creating a war room	War rooms	createWarRoom
Creating a war room initiation rule	MeetingRule	createMeetingRule
Deleting a war room initiation rule	MeetingRule	deleteMeetingRule
Modifying a war room initiation rule	MeetingRule	updateMeetingRule
Modifying war room information	War rooms	modifyWarRoomInfo
Sending notifications using war room	NotificationBriefing	sendNotificationBriefing
Adding war room members	War rooms	addWarRoomMember
Removing a war room member	War rooms	deleteWarRoomMember
Creating the war room affected applications	ImpactApplication	createImpactApplication
Modifying the war room affected applications	ImpactApplication	updateImpactApplication
Deleting the war room affected applications	ImpactApplication	deleteImpactApplication

Action	Resource	Trace
Executing actions	Ticket	actionTicket
Creating a service ticket	Ticket	createTicket
Modifying a service ticket	Ticket	updateTicket
Deleting a service ticket	Ticket	deleteTicketInfo
Uploading an attachment	Attachment	uploadFileTicket
Downloading files	Attachment	downloadFileTicket
Updating the integration configuration key	IntegrationConfig	updateIntegrationConfig-Key
Accessing integration	IntegrationConfig	accessIntegrationConfig
Disabling Integration	IntegrationConfig	disableIntegrationConfig
Enabling integration	IntegrationConfig	enableIntegrationConfig
Canceling integration	IntegrationConfig	removeIntegrationConfig
Creating an alarm conversion rule	TransferRule	createTransferRules
Modifying an alarm conversion rule	TransferRule	updateTransferRules
Deleting an alarm conversion rule	TransferRule	deleteTransferRules
Disabling an alarm conversion rule	TransferRule	disableTransferRules
Enabling an alarm conversion rule	TransferRule	enableTransferRules
Unsubscription	NotificationRule	disableNotificationRule
Subscription	NotificationRule	enableNotificationRule
Creating a subscription	NotificationRule	createNotificationRule
Deleting a subscription	NotificationRule	deleteNotificationRule
Modifying subscription information	NotificationRule	updateNotificationRule
Creating a scheduling scenario	ScheduleScene	createSceneOncall
Deleting a scheduling scenario	ScheduleScene	deleteSceneOncall

Action	Resource	Trace
Updating a scheduling scenario	ScheduleScene	updateSceneOncall
Creating a shift role	ScheduleRole	createRoleOncall
Updating a shift role	ScheduleRole	updateRoleOncall
Deleting a shift role	ScheduleRole	deleteRoleOncall
Deleting a fixed shift engineer	ScheduleUser	deleteGlobalFixed
Adding a user to the global fixed shift	ScheduleUser	createGlobalFixed
Updating fixed shift personnel	ScheduleUser	updatePersonnelsOncall
Clearing shifts with one click	ScheduleUser	batchDeleteShift
Creating shift agents in batches	ScheduleUser	batchCreateShift
Updating the shift schedule personnel of a specific day	ScheduleUser	UpdateUserShift
Creating scheduling scenarios and roles	ScheduleRole	createRoleOncall
Creating a custom script	Document	createJobScript
Deleting a custom script	Document	deleteJobScript
Modifying a customized script	Document	editJobScript
Approving a custom script	Document	approveJobScript
Executing a custom script	Document	executeJobScript
Operating the script service ticket	Job	jobScriptOrderOperation
Creating a custom job	Document	CreateRunbook
Deleting a custom job	Document	DeleteRunbook
Modifying a custom job	Document	EditRunbook
Approving a custom job	Document	ApproveRunbook
Executing a custom job	Job	ExecuteRunbook

Action	Resource	Trace
Executing a public job	Job	ExecutePublicRunbook
Operating the job service ticket	Job	OperateJobTicket

Viewing Logs

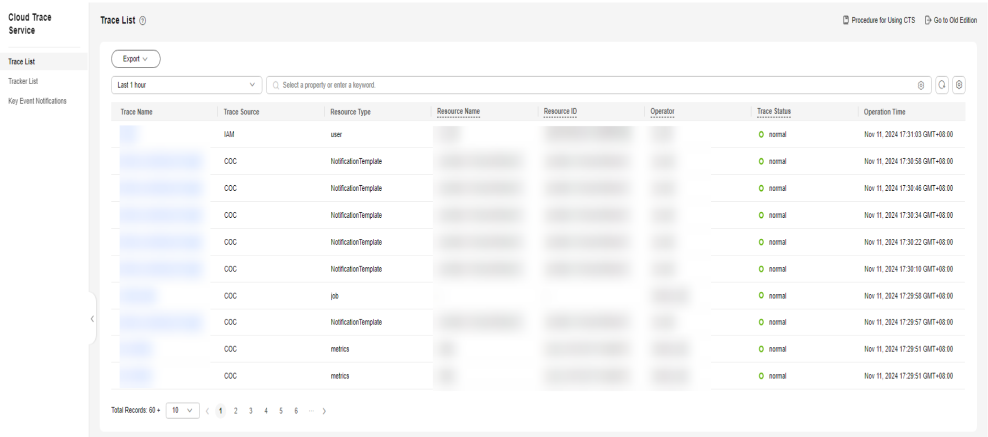
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Choose **Management & Governance** > **Cloud Trace Service**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Specify filter criteria as needed.

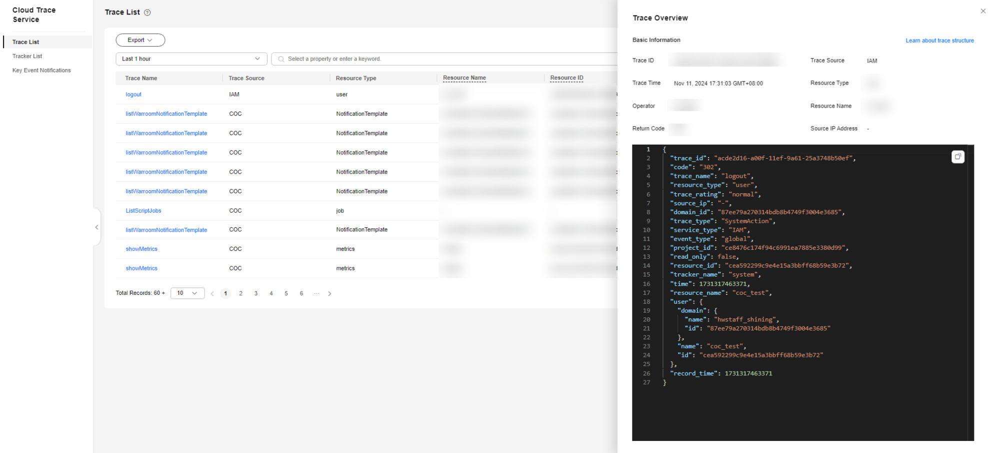
Figure 12-1 CTS events



Trace Name	Trace Source	Resource Type	Resource Name	Resource ID	Operator	Trace Status	Operation Time
[redacted]	IAM	user	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:31:03 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:58 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:46 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:34 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:22 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:10 GMT+08:00
[redacted]	COC	job			[redacted]	normal	Nov 11, 2024 17:29:58 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:57 GMT+08:00
[redacted]	COC	metrics	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:51 GMT+08:00
[redacted]	COC	metrics	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:51 GMT+08:00

Step 5 Select the trace to be viewed and click the trace name to expand the overview.

Figure 12-2 Trace overview



Trace Name	Trace Source	Resource Type	Resource Name	Resource ID
logout	IAM	user	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
ListScriptJobs	COC	job		
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
showMetrics	COC	metrics	[redacted]	[redacted]
showMetrics	COC	metrics	[redacted]	[redacted]

Total Records: 60 + 10 < 1 2 3 4 5 6 ··· >

Trace ID	[redacted]	Trace Source	IAM
Trace Time	Nov 11, 2024 17:31:03 GMT+08:00	Resource Type	[redacted]
Operator	[redacted]	Resource Name	[redacted]
Return Code	[redacted]	Source IP Address	-

```
{
  "trace_id": "acde2d16-a00f-11ef-9a61-25a3748b50ef",
  "code": "302",
  "trace_name": "logout",
  "resource_type": "user",
  "trace_rating": "normal",
  "source_ip": "-",
  "domain_id": "87ee79a270314bdb8b4749f3004e3685",
  "trace_type": "SystemAction",
  "service_type": "IAM",
  "event_type": "global",
  "project_id": "ce8476c174f94c6991ea7885e3380d99",
  "read_only": false,
  "resource_id": "cea592299c9e4e15a3bbff68b59e3b72",
  "tracker_name": "system",
  "time": 1731317463371,
  "resource_name": "coc_test",
  "user": {
    "domain": {
      "name": "hwstaff_shining",
      "id": "87ee79a270314bdb8b4749f3004e3685"
    },
    "name": "coc_test",
    "id": "cea592299c9e4e15a3bbff68b59e3b72"
  },
  "record_time": 1731317463371
}
```

----End