

Cloud Operations Center

User Guide

Issue 01
Date 2023-11-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 RBAC and ABAC Authorization Models..... | 1 |
| 1.1 Tutorials for RBAC..... | 1 |
| 1.2 Tutorials for ABAC..... | 3 |
| 2 Overview..... | 4 |
| 2.1 O&M Operations Center..... | 4 |
| 2.2 Resource Overview..... | 5 |
| 2.3 Resource Monitoring..... | 6 |
| 2.4 Application Monitoring..... | 7 |
| 2.5 Security Overview..... | 8 |
| 3 Application and Resource Management..... | 10 |
| 3.1 Resource Management..... | 10 |
| 3.1.1 Synchronizing Resources..... | 10 |
| 3.1.2 Performing Operations on a UniAgent..... | 12 |
| 3.1.3 Viewing Resource Details..... | 16 |
| 3.1.4 Viewing Resource Topologies..... | 18 |
| 4 Resource O&M..... | 20 |
| 4.1 Overview..... | 20 |
| 4.2 Patch Management..... | 20 |
| 4.2.1 Creating a Patch Baseline..... | 21 |
| 4.2.2 Scanning a Patch..... | 28 |
| 4.2.3 Repairing Patches..... | 32 |
| 4.2.4 Viewing the Patch Compliance Report Details..... | 34 |
| 4.3 Batch ECS operations..... | 35 |
| 4.3.1 Starting ECSs..... | 36 |
| 4.3.2 Stopping ECSs..... | 38 |
| 4.3.3 Restarting ECSs..... | 41 |
| 4.3.4 Reinstalling OSs..... | 43 |
| 4.3.5 Changing OSs..... | 46 |
| 4.4 Batch Operations on RDS Instances..... | 49 |
| 5 Automated O&M..... | 50 |
| 5.1 Script Management..... | 50 |
| 5.1.1 Creating a Custom Script..... | 50 |

| | |
|---|------------|
| 5.1.2 Managing Custom Scripts..... | 52 |
| 5.1.3 Executing Custom Scripts..... | 53 |
| 5.1.4 Executing Common Scripts..... | 56 |
| 5.2 Jobs..... | 59 |
| 5.2.1 Executing a Common Job..... | 59 |
| 5.2.2 Creating a Custom Job..... | 63 |
| 5.2.3 Managing Custom Jobs..... | 71 |
| 5.2.4 Executing a Custom Job..... | 72 |
| 5.2.5 Managing Tags..... | 76 |
| 5.3 Scheduled O&M..... | 77 |
| 5.3.1 Scheduled Task Management..... | 77 |
| 5.3.2 Scheduled Task Execution Records..... | 91 |
| 6 Parameter Management..... | 92 |
| 6.1 Parameter Center..... | 92 |
| 6.1.1 Creating a Parameter..... | 92 |
| 6.1.2 Modifying a Parameter..... | 96 |
| 6.1.3 Viewing Parameter Details..... | 97 |
| 6.2 Notification Rules..... | 98 |
| 6.2.1 Expiration Notification..... | 98 |
| 6.2.2 Unmodified Notifications..... | 99 |
| 7 Incident Management..... | 101 |
| 7.1 Incident Center..... | 101 |
| 7.1.1 Incidents..... | 101 |
| 7.1.2 Creating an Incident..... | 102 |
| 7.1.3 Handling an Incident..... | 103 |
| 7.1.3.1 Rejecting an Incident..... | 103 |
| 7.1.3.2 Resubmitting an Incident After Rejection..... | 104 |
| 7.1.3.3 Forwarding Incidents..... | 105 |
| 7.1.3.4 Handling Incidents..... | 107 |
| 7.1.3.5 Upgrading/Downgrading an Incident..... | 108 |
| 7.1.3.6 Adding Remarks..... | 110 |
| 7.1.3.7 Starting a WarRoom..... | 112 |
| 7.1.3.8 Handling an Incident..... | 113 |
| 7.1.3.9 Verifying Incident..... | 116 |
| 7.1.4 Incident History..... | 117 |
| 7.2 Alarms..... | 118 |
| 7.2.1 Viewing Alarms..... | 118 |
| 7.2.1.1 Handling Alarms..... | 119 |
| 7.2.1.2 Converting an Alarm to an Incident..... | 119 |
| 7.2.1.3 Clearing Alarms..... | 120 |
| 7.2.1.4 Historical Alarms..... | 120 |
| 7.2.2 Original Alarms..... | 121 |

| | |
|---|------------|
| 7.3 WarRoom..... | 122 |
| 7.3.1 WarRoom Status..... | 122 |
| 7.3.2 Fault Information..... | 123 |
| 7.3.3 Affected Application Management..... | 123 |
| 7.3.4 WarRoom Members..... | 125 |
| 7.3.5 Progress Notification..... | 125 |
| 7.3.6 Adding a WarRoom Initiation Rule..... | 126 |
| 7.3.7 Modifying a WarRoom Rule..... | 127 |
| 7.4 Forwarding Rules..... | 128 |
| 7.4.1 Overview..... | 128 |
| 7.4.2 Forwarding rules..... | 128 |
| 7.5 Integration Management..... | 132 |
| 7.5.1 Overview..... | 132 |
| 7.5.2 Integration Management..... | 132 |
| 8 Change Management..... | 135 |
| 8.1 Change Center..... | 135 |
| 8.1.1 Creating a Change Ticket..... | 135 |
| 8.2 Change Configuration..... | 137 |
| 8.2.1 Configuring Approval Settings..... | 137 |
| 9 Resilience Center..... | 139 |
| 9.1 Chaos Drills..... | 139 |
| 9.1.1 Overview..... | 139 |
| 9.1.2 Fault Type..... | 139 |
| 9.1.3 Drill Plan..... | 141 |
| 9.1.4 Drill Tasks..... | 143 |
| 9.1.5 Drill Report..... | 161 |
| 9.2 Emergency Plan..... | 164 |
| 9.3 Improvement Task..... | 169 |
| 9.3.1 Overview..... | 170 |
| 9.3.2 Improvement Task Management..... | 170 |
| 9.4 PRR Review..... | 174 |
| 9.4.1 Overview..... | 174 |
| 9.4.2 PRR Template Management..... | 174 |
| 9.4.3 PRR Management..... | 178 |
| 10 Task Management..... | 187 |
| 10.1 Execution Records..... | 187 |
| 10.1.1 Script Tickets..... | 187 |
| 10.1.2 Job Tickets..... | 189 |
| 10.1.3 Patch Tickets..... | 191 |
| 10.1.4 Resource Operation Tickets..... | 192 |
| 10.2 To-do Center..... | 194 |

| | |
|--|------------|
| 11 Basic Configurations..... | 202 |
| 11.1 O&M Engineer Management (COC)..... | 202 |
| 11.1.1 O&M Engineer Management Overview..... | 202 |
| 11.1.2 O&M Engineer Management Usage..... | 202 |
| 11.2 Shift Schedule Management..... | 206 |
| 11.2.1 Overview..... | 206 |
| 11.2.1.1 Creating a Schedule..... | 207 |
| 11.2.1.2 Adding O&M Engineers..... | 208 |
| 11.2.1.3 Managing O&M Engineers..... | 214 |
| 11.2.2 Managing Scheduling Scenarios..... | 217 |
| 11.2.3 Managing Scheduling Roles..... | 223 |
| 11.3 Notification Management..... | 224 |
| 11.4 Mobile Application Management | 230 |
| 11.5 SLA Management..... | 232 |
| 11.5.1 Custom SLA..... | 232 |
| 11.5.2 Common SLA..... | 239 |
| 11.5.3 Managing SLA Records..... | 241 |
| 12 Viewing Logs..... | 243 |

1 RBAC and ABAC Authorization Models

1.1 Tutorials for RBAC

This topic 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 users only the permissions required to perform a given task based on their job responsibilities.
- Entrust an account or cloud service to perform efficient O&M on your COC resources.

If your account does not require individual IAM users, skip this topic.

This section describes the workflow for granting permissions to users.

Prerequisites

Learn about [the permissions supported by COC](#). To grant permissions for other services, learn about all [system-defined permissions](#).

Example Workflow

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.](#)
Create a user on the IAM console and add the user to the group created in 1.
3. [Log in](#) and verify permissions.
 - Log in to COC, access the **Overview** page, and click **Create Task** in the upper right corner to create a to-do task. If a to-do task fails to be created (assume that you have only the **COC ReadOnlyAccess** permission), the **COC ReadOnlyAccess** permission has taken effect.

- Log in to COC, access the **Overview** page, and click **Create Task** in the upper right corner to create a to-do task. If a to-do task is created (assume that you have only the **COC FullAccess** permission), the **COC FullAccess** permission has taken effect.
4. Custom policies can be created to supplement the system-defined policies of COC. For the actions supported for custom policies, see [Policies](#) and [Actions](#). To create a custom policy, choose either visual editor or JSON.
- 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

- 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 "Deny" permissions must be used together with other policies. 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 a custom policy containing multiple actions:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
```



```
"Action": [  
  "coc:document:create",  
  "scm:cert:complete"  
]  
}  
]  
}
```

1.2 Tutorials for ABAC

N/A

2 Overview

In the overview module, you can create O&M tasks and view information about resource health, resource monitoring, security statuses, O&M capabilities, and system bulletins.

2.1 O&M Operations Center

You can create, follow up, and close O&M to-do tasks.

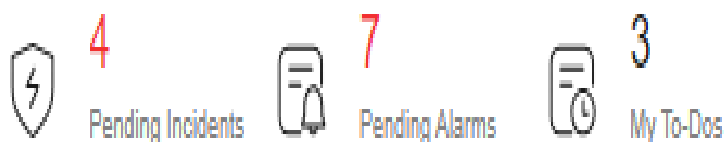
Scenarios

Create, follow up, and close O&M to-do tasks on Cloud Operations Center.

Procedure

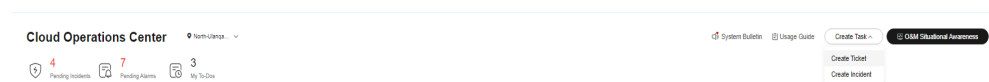
- Step 1** Log in to [COC](#).
- Step 2** On the **Overview** page of COC, you can view the number of incidents to be handled, alarms to be handled, and your to-do tasks in the upper left part of the page.

Figure 2-1 Statistical quantity



- Step 3** Click the **Create Task** button, and choose **Create Ticket**.

Figure 2-2 Creating a to-do task



Step 4 Click **Create Incident**.

Figure 2-3 Creating an incident



----End

2.2 Resource Overview

You can view statistics about purchased resources, including ECSs, EIPs, and cloud databases.

Scenarios

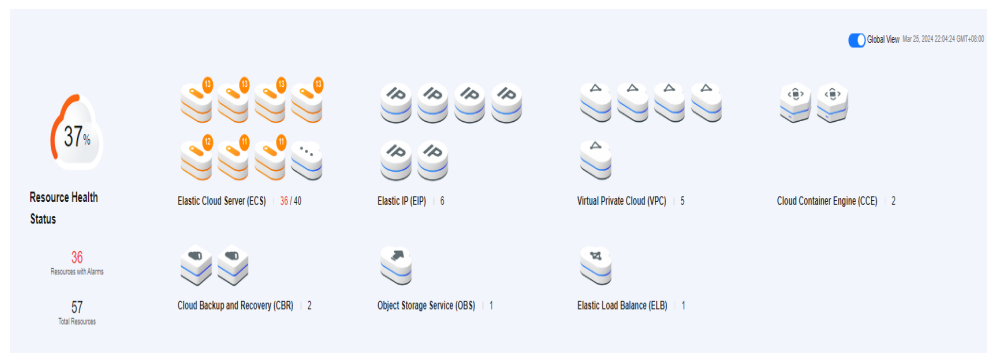
View resources (including ECSs, EIPs, and cloud databases) on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 On the **Overview** page of COC, you can view required resource information.

Figure 2-4 Resource information



Step 3 Enable the **Global View** feature toggle to view resource information of all regions.

Step 4 Click  to query all resource information of the corresponding resource type.


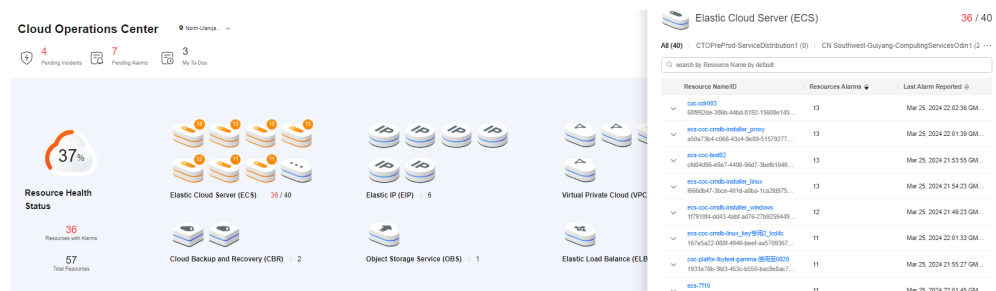
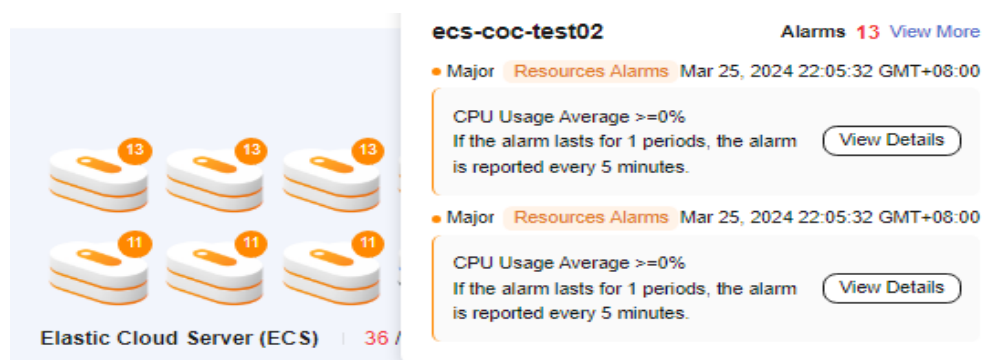
Step 5 In the global view, click  to query all resource information of the corresponding resource type in different regions.

Figure 2-5 Resources in different regions



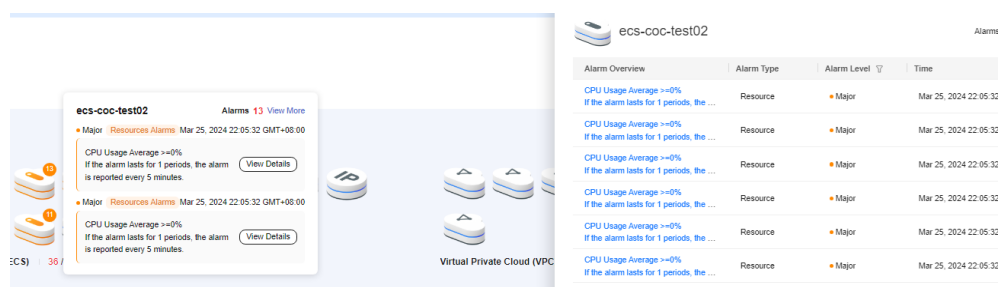
Step 6 Move your cursor to resources that are marked by alarms to view alarm details of the resources.

Figure 2-6 Alarm information



Step 7 Click **View More** to view more alarms.

Figure 2-7 More alarm information



Step 8 Click the refresh icon in the upper right corner to refresh resource and alarm information.

----End

2.3 Resource Monitoring

You can view resources monitored by CES.

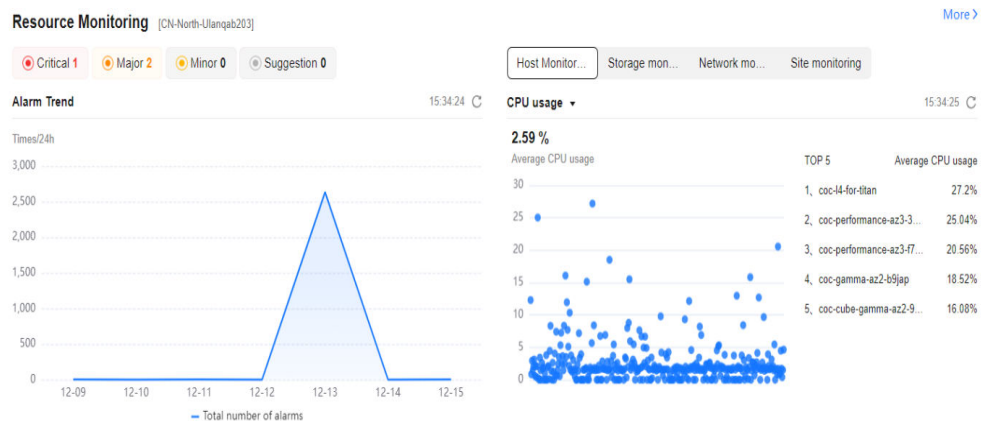
Scenarios

View resources monitored by CES on COC.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** On the **Overview** page of COC, you can view metric information monitored by CES.

Figure 2-8 CES monitoring information



- Step 3** Click **Storage Monitoring**, **Network Monitoring**, and **Site Monitoring** to view different monitoring information.
 - Step 4** Click **More** to access the CES page and view the original monitoring information.
- End

2.4 Application Monitoring

You can view custom application monitoring information.

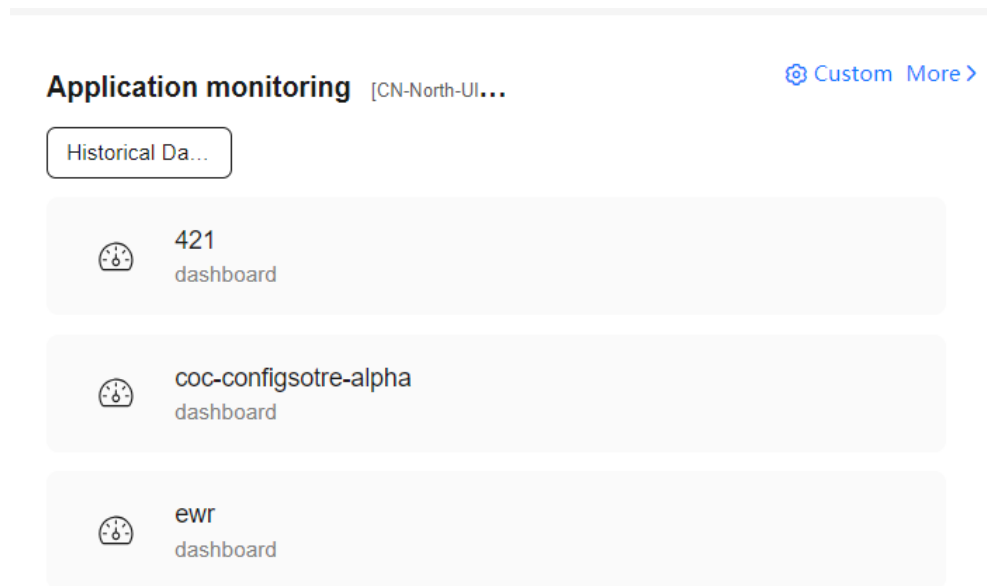
Scenarios

View the information on the dashboard of Application Operations Management (AOM) on COC.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** On the **Overview** page of COC, you can view monitoring information of applications.

Figure 2-9 Application monitoring information



----End

2.5 Security Overview

You can view the security monitoring information from SecMaster.

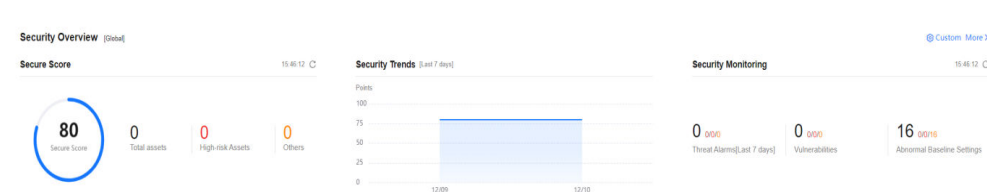
Scenarios

View the security monitoring information provided by SecMaster on COC.

Procedure

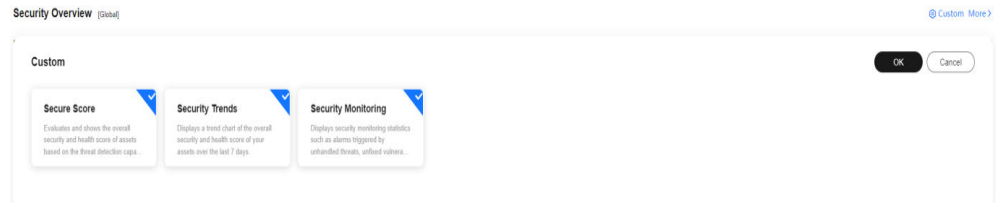
- Step 1** Log in to [COC](#).
- Step 2** On the **Overview** page of COC, you can view the security monitoring information provided by SecMaster.

Figure 2-10 Security monitoring information from SecMaster



- Step 3** Click **Custom Dashboard** to set the charts to display.

Figure 2-11 Customizing security monitoring dashboard



----End

3 Application and Resource Management

3.1 Resource Management

3.1.1 Synchronizing Resources

You can synchronize resources from resource management platforms. You filter resources by selecting filter criteria or setting the columns to display on the **Resources** tab page.

 **NOTE**

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.

Scenarios

Synchronize resources from other platforms to COC.

Precautions

After resource synchronization is triggered, wait until the synchronization task is executed. The synchronization duration depends on the total amount of resource data to be synchronized.

Procedure

Step 1 Log in to [COC](#).


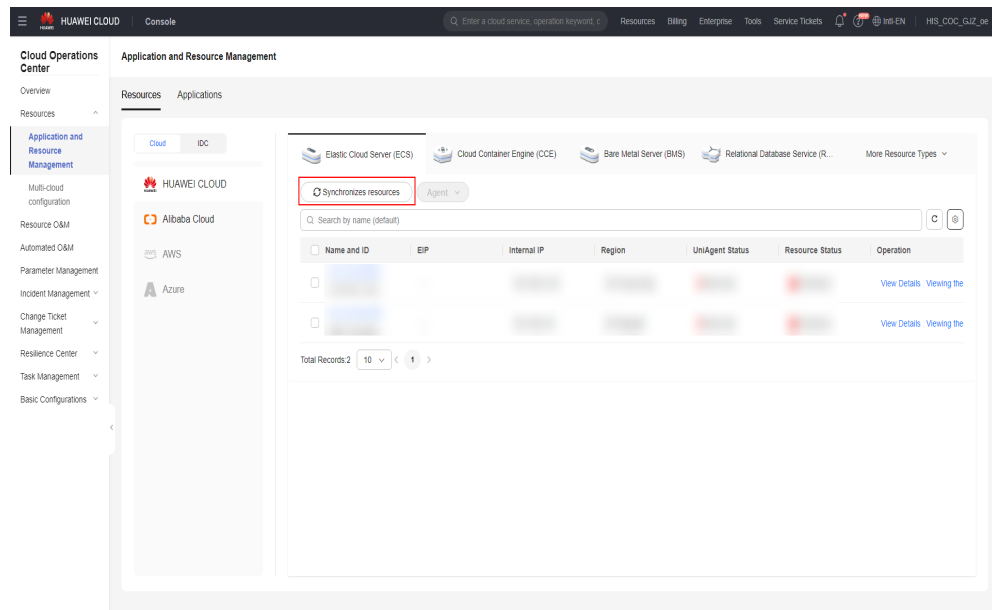
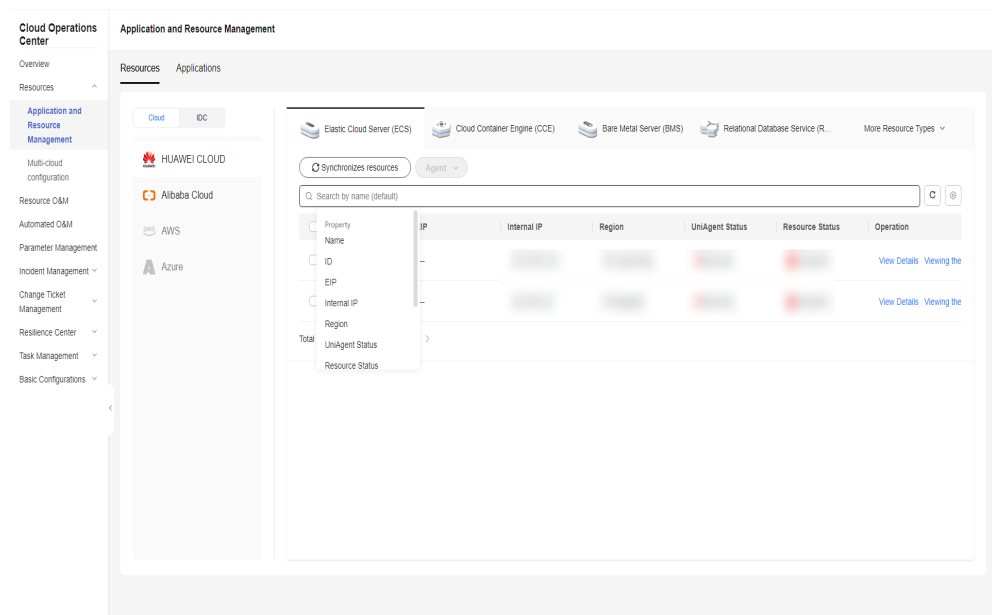
Step 2 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Resources** tab page, click  .

Figure 3-1 Synchronizing resources



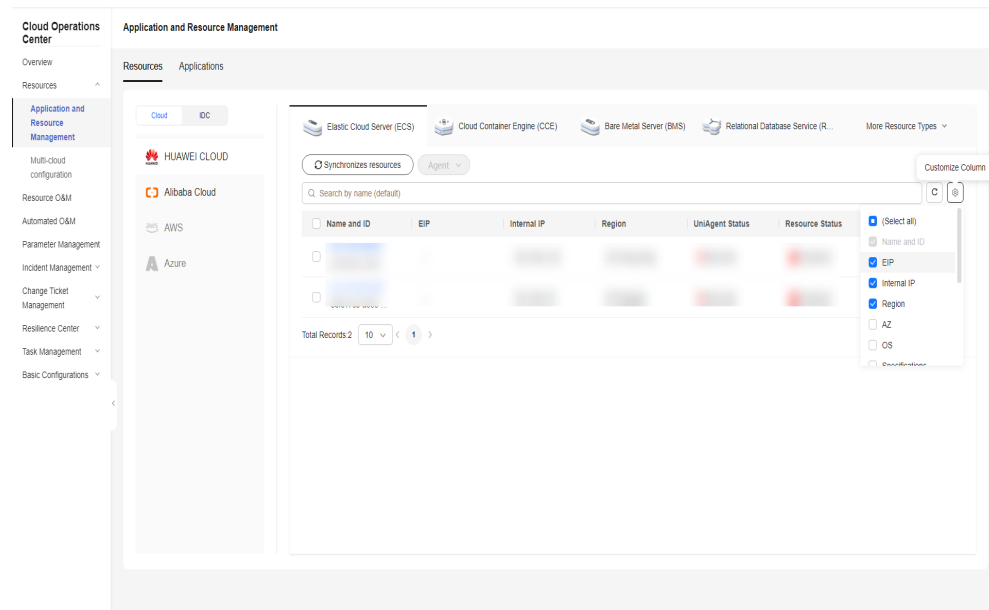
Step 3 In the search box on the **Resources** tab page, select filter criteria to quickly search for resources.

Figure 3-2 Filtering resources



Step 4 Click  to select the columns to display.

Figure 3-3 Column display control



----End

3.1.2 Performing Operations on a UniAgent

You can install, upgrade, and uninstall a UniAgent on corresponding nodes.

Scenarios

Install, upgrade, and uninstall a UniAgent on corresponding nodes on COC.

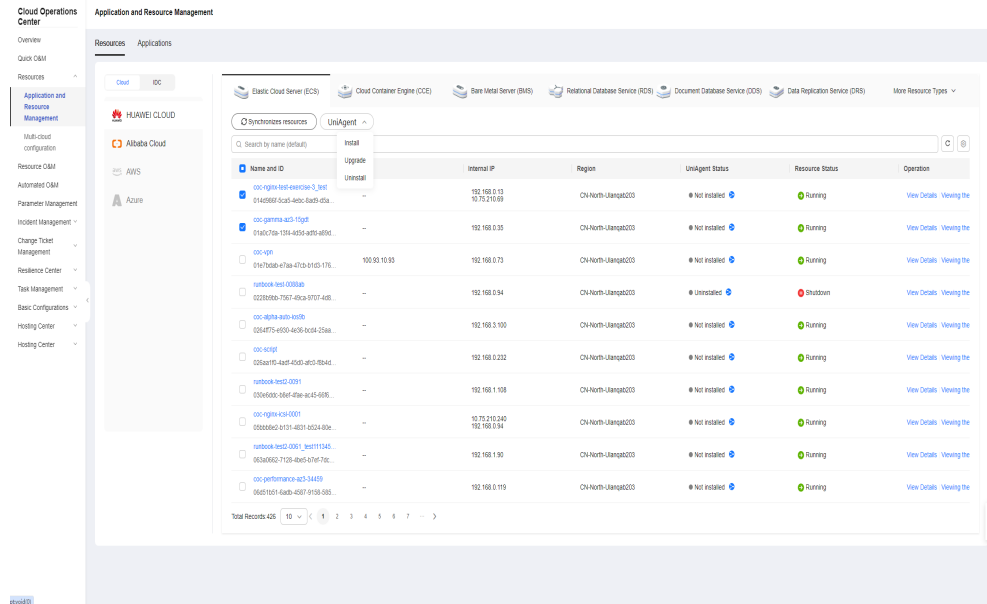
Precautions

Such operations cannot be performed on nodes where UniAgents are abnormal.

Procedure

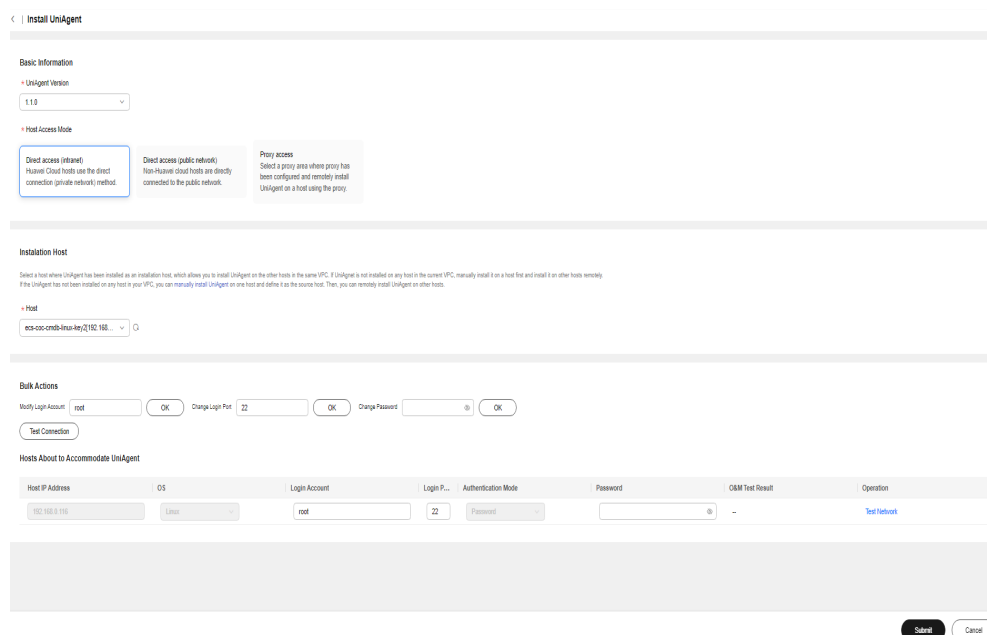
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the **Resources** tab page, select ECSs for which you want to install a UniAgent and click **UniAgent** and choose **Install**.

Figure 3-4 Installing a UniAgent



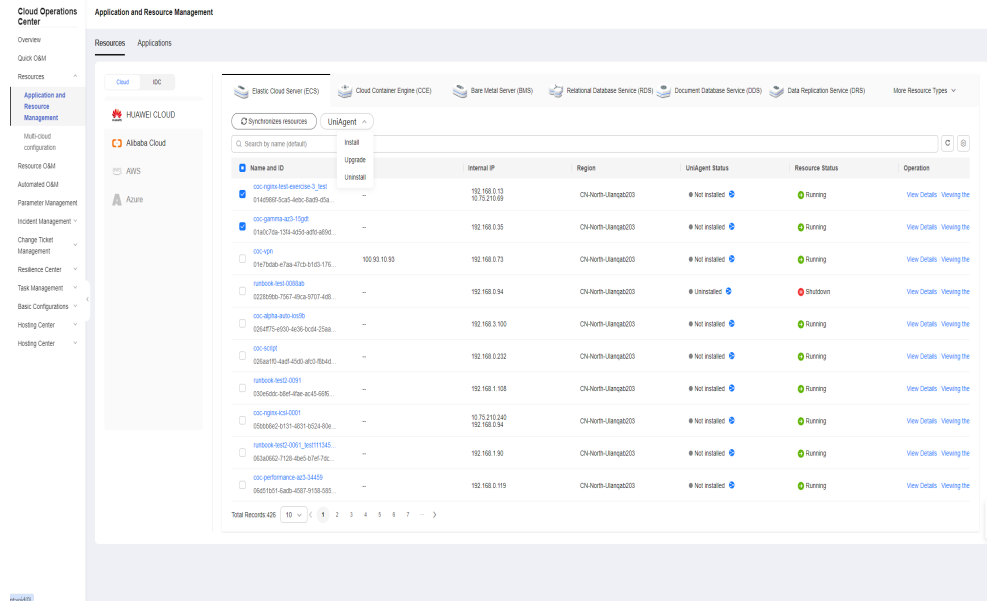
Step 3 On the displayed **Install UniAgent** page, specify required information by referring to **Table 3-1** and click **Submit** to trigger the automated installation process. Wait until the installation is complete.

Figure 3-5 Setting parameters



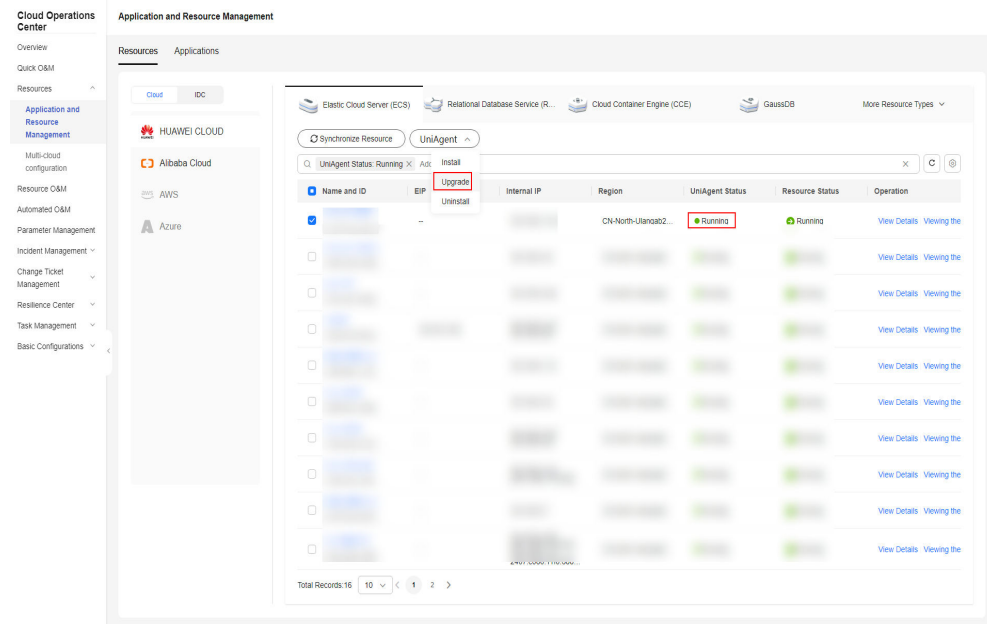
Step 4 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the **Resources** tab page, select ECSs for which you have installed a UniAgent and click **UniAgent** and choose **Upgrade**.

Figure 3-6 Upgrading a UniAgent



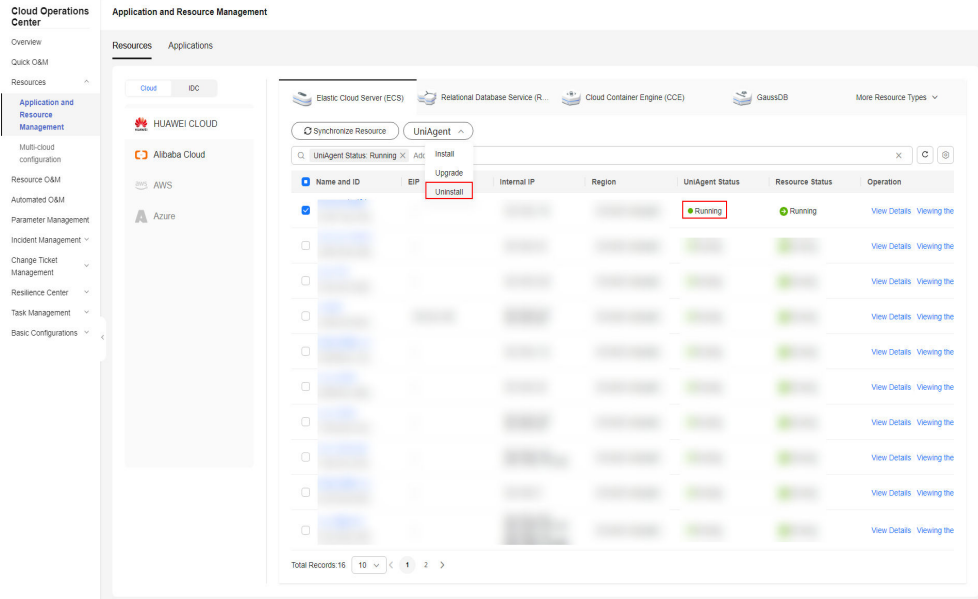
Step 5 In the drawer that is displayed on the right, select the UniAgent to be upgraded and click **OK** to trigger the automatic process. Wait until the operation is complete.

Figure 3-7 Parameters for upgrading a UniAgent



Step 6 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the **Resources** tab page, select ECSs for which you have installed a UniAgent and click **UniAgent** and choose **Uninstall**.

Figure 3-8 Uninstalling a UniAgent



Step 7 In the drawer that is displayed, click **OK** to trigger the automatic process. Wait until the operation is complete.

Table 3-1 Parameters for installing a UniAgent

| Parameter | Description | Example Value |
|------------------|--|--------------------------|
| UniAgent Version | (Mandatory) Version of a UniAgent. Currently, version 1.0.9 is supported. | 1.0.9 |
| Host Access Mode | There are three access modes: Direct access (private network) , Direct access (public network) , and Proxy access . <ul style="list-style-type: none"> • 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 a UniAgent on a host through the proxy. | Direct access (intranet) |
| 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. | - |

| Parameter | Description | Example Value |
|-------------------------------------|--|---------------|
| Installation Host | <p>An installation host is used to execute commands for remote installation. This parameter is mandatory.</p> <p>If no installation host has been configured, perform the following steps:</p> <ol style="list-style-type: none"> 1. Select Configure Installation Host from the drop-down list. 2. Access the AOM service to configure the installation host. | - |
| Hosts About to Accommodate UniAgent | <p>(Mandatory) Detailed information about the host where the UniAgent is to be installed.</p> <p>Specify the following information:</p> <ul style="list-style-type: none"> ● 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. ● Connection Test Result: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal. ● Operation: Test Connection <p>NOTE The hosts that run Windows do not support connectivity tests.</p> | - |

----End

3.1.3 Viewing Resource Details

You can view resource details.

Scenarios

View resource details on COC.

Precautions

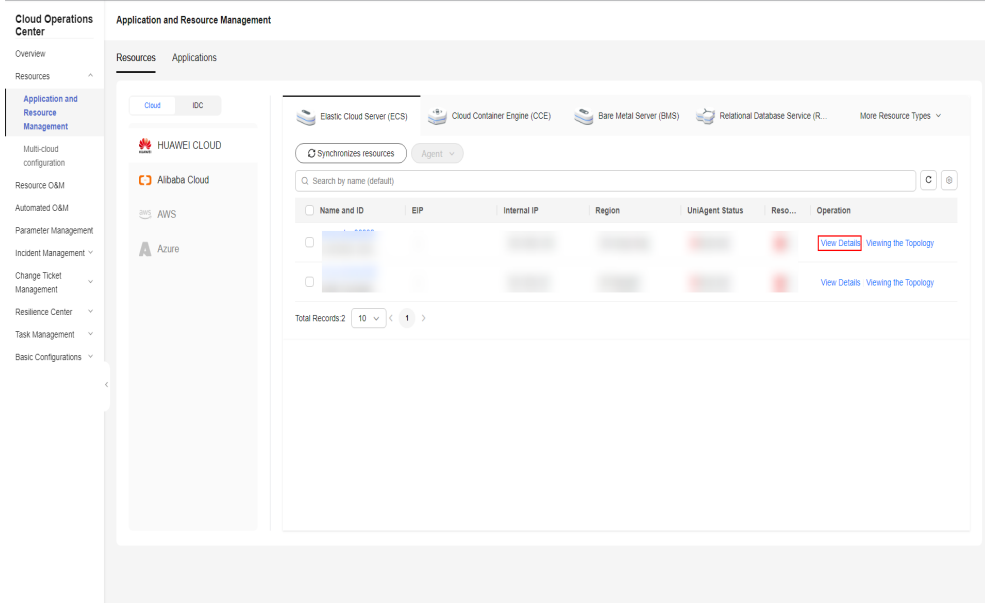
Currently, only resource details of ECS instances can be viewed.

Procedure

Step 1 Log in to [COC](#).

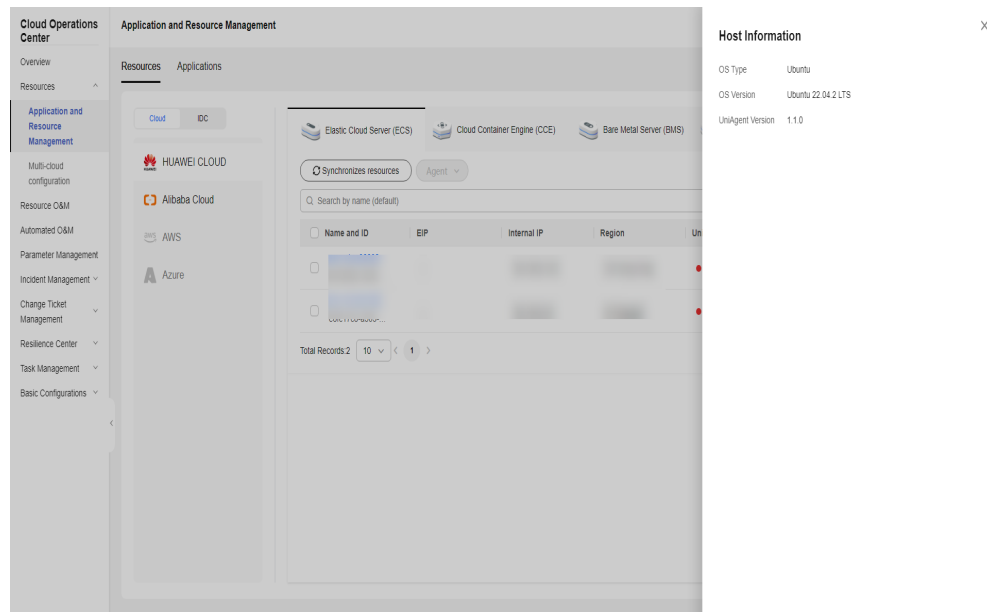
Step 2 In the navigation pane on the left, choose **Resources > Application Resource Management**. On the displayed **Resources > Elastic Cloud Server (ECS)** tab page, select an ECS whose details you want to view and click **View Details**.

Figure 3-9 Viewing details



Step 3 In the drawer that is displayed on the right, view the resource details.

Figure 3-10 Resource details



----End

3.1.4 Viewing Resource Topologies

You can view resource topologies.

Scenarios

View resource topologies on COC.

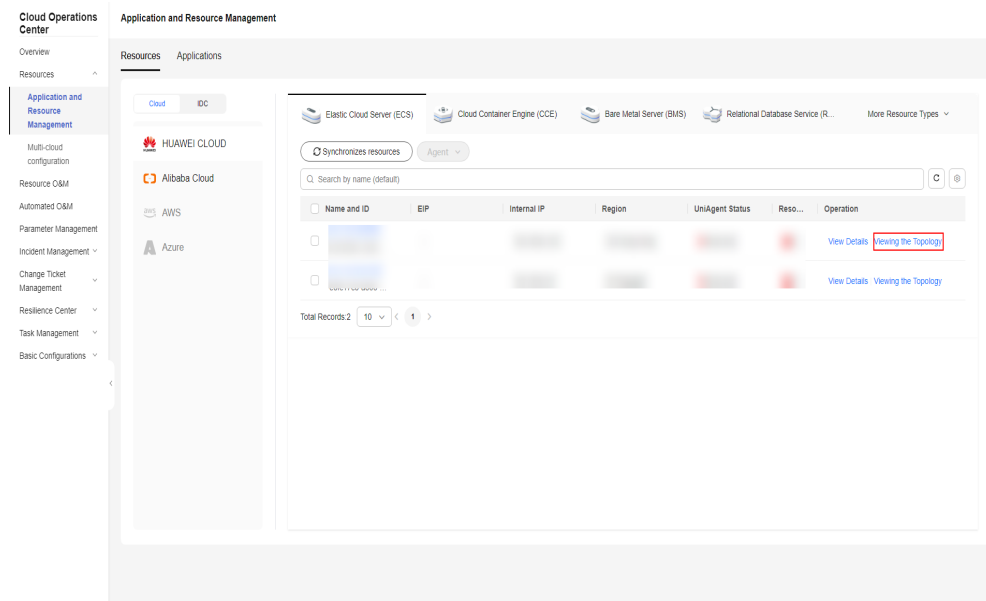
Precautions

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

Procedure

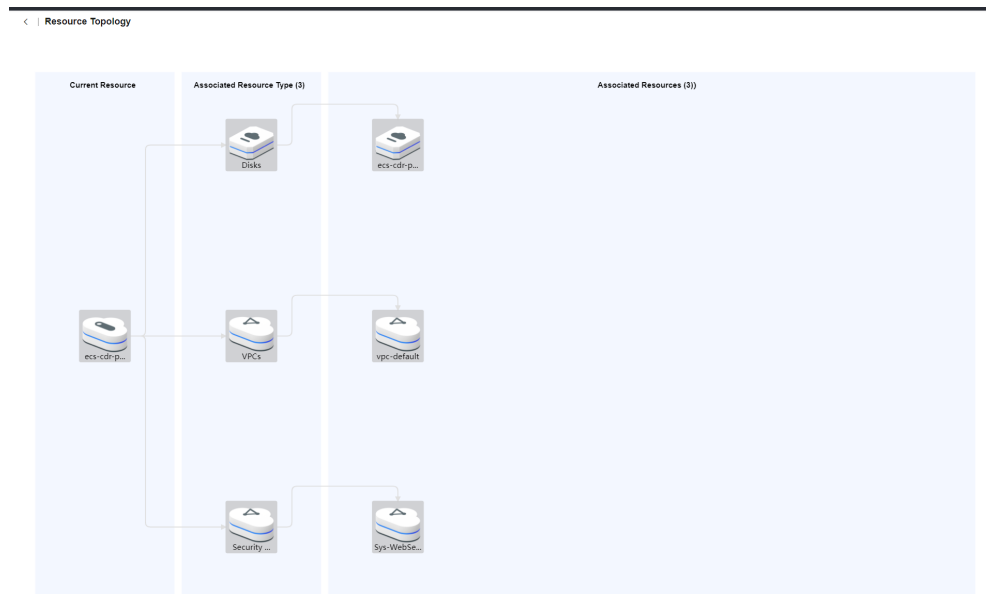
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resources > Application Resource Management**. On the displayed **Resources > Elastic Cloud Server (ECS)** tab page, select an ECS whose details you want to view and click **View Topology**.

Figure 3-11 Viewing resource topologies



Step 3 On the displayed resource topology page, view the topology relationships between the selected resource and other resources.

Figure 3-12 Topology relationship



----End

4 Resource O&M

4.1 Overview

Resource O&M allows users to manage patches and operate ECSs. Users can scan patches to manage patches on instances, and start, stop, and restart ECSs in batches, as well as switch and reinstall OSs.

4.2 Patch Management

Patch Management allows users to manage patches on (Elastic Cloud Server) ECS or Cloud Container Engine (CCE) instances by scanning and repairing patches.

 **NOTE**

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

[Table 4-1](#) lists the OSs and versions supported by the patch management feature.

[Table 4-2](#) lists the second-party package on which the patch management feature depends.

Table 4-1 OSs and versions supported by the patch management feature

| 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 4-2 Second-party packages on which the patch management feature depends

| Type | Dependency Item |
|----------------------|---|
| Second-party package | Python (Python2 or Python3) DNF (depended by Huawei Cloud EulerOS 2.0, CentOS 8.0 or later, and EulerOS 2.9 or later) YUM (depended by Huawei Cloud EulerOS 1.1, versions earlier than CentOS 8.0 and EulerOS 2.9) RPM |

4.2.1 Creating a Patch Baseline

Patch Baseline allows you to customize the rules for scanning and installing patches. Only patches that are compliant with the baseline can be scanned and repaired.

You can create patch baselines for ECS instances or CCE instances as required.

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

Scenarios

Create a patch baseline on Cloud Operations Center.

Procedure

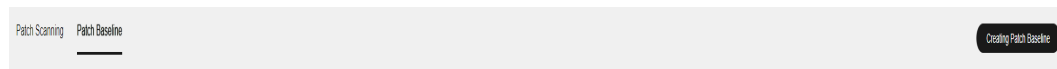
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Patch management**.
- Step 3** On the displayed page, click **Patch Baseline** to view the baseline list.

Figure 4-1 Patch baseline list

| ID/Name | Description | Scenario Type | OS | Patch Baseline Type | Default Baseline or Not | Common Baseline or Not | Created At | Operation |
|---|--------------------------------------|-----------------|----------------------|----------------------------|-------------------------|------------------------|---------------------------------|-------------------------------------|
| COC-EulerOSDefaultPatchBa... JK-D6982654738520522 | Default Patch Baseline for EulerO... | Virtualized ECS | EulerOS | Installation Rule Baseline | Yes | Yes | Jul 24, 2023 14:53:35 GMT+08:00 | Set Default Baseline Monthly Delete |
| COC-CentOSDefaultPatchBa... JK-83a7b205b49391643435e | Default Patch Baseline for CentO... | Virtualized ECS | CentOS | Installation Rule Baseline | Yes | Yes | May 26, 2023 20:42:19 GMT+08:00 | Set Default Baseline Monthly Delete |
| COC-HuaweiCloudEulerOSD... JK-92730194042a392973f | Default Patch Baseline for Huawe... | Virtualized ECS | Huawei Cloud EulerOS | Installation Rule Baseline | Yes | Yes | May 26, 2023 10:08:22 GMT+08:00 | Set Default Baseline Monthly Delete |

- Step 4** Click **Creating Patch Baseline**.

Figure 4-2 Creating a patch baseline



- Step 5** Set the patch baseline information as prompted.

Figure 4-3 Setting the patch baseline information

NOTE

Table 4-3 describes the parameters for creating an installation rule baseline.

Table 4-4 describes the parameters for creating a custom baseline.

Table 4-3 OS installation rule baseline

| Field | Options | Description |
|----------|---|---|
| Product | <ul style="list-style-type: none"> ● Huawei Cloud EulerOS <ul style="list-style-type: none"> - All - Huawei Cloud EulerOS 1.1 - Huawei Cloud EulerOS 2.0 ● CentOS <ul style="list-style-type: none"> - All - CentOS7.2 - CentOS7.3 - CentOS7.4 - CentOS7.5 - CentOS7.6 - CentOS7.7 - CentOS7.8 - CentOS7.9 - CentOS8.0 - CentOS8.1 - CentOS8.2 ● EulerOS <ul style="list-style-type: none"> - All - EulerOS 2.2 - EulerOS 2.5 - EulerOS 2.8 - EulerOS 2.9 - EulerOS 2.10 | OS of patches. Only the patches of the selected OS can be scanned and repaired. |
| Category | <ul style="list-style-type: none"> ● All ● Security ● Bugfix ● Enhancement ● Recommended ● Newpackage | Category of patches. The patches of the selected category are scanned and repaired. |

| Field | Options | Description |
|------------------------------|--|---|
| Severity | <ul style="list-style-type: none"> • All • Critical • Important • Moderate • Low • None | Severity level of patches. The patches of the selected severity level can be scanned and repaired. |
| Automatic Approval | <ul style="list-style-type: none"> • 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 to 365 | This parameter is mandatory when Approve the patch after a specified number of days. is selected. |
| Specified Date | None | This parameter is mandatory when Approve patches released before the specified date. is selected. |
| Compliance Reporting | <ul style="list-style-type: none"> • Unspecified • Critical • High • Medium • Low • Suggestion | Level of a patch that meets the patch baseline in the compliance report |
| Install Non-Security Patches | None | If you do not select this option, the patches with vulnerabilities will not be upgraded during patch repairing. |

| Field | Options | Description |
|---------------------|---------|---|
| Exceptional Patches | None | <p>The formats of the software packages of approved patches and rejected patches are as follows:</p> <ol style="list-style-type: none"> 1. The format of a complete software package name: <i>example-1.0.0-1.r1.hce2.x86_64.</i> 2. The format of the software package name that contains a single wildcard: <i>example-1.0.0*.x86_64.</i> |

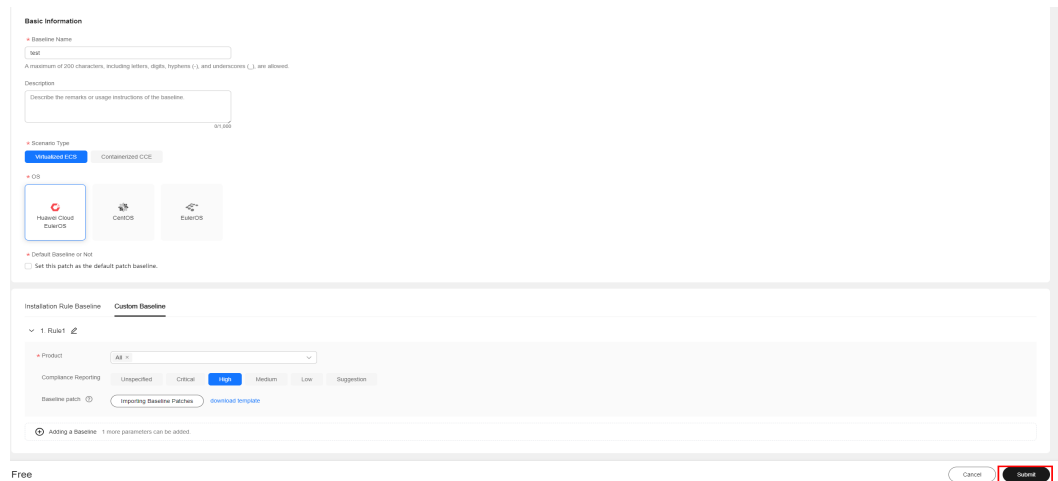
Table 4-4 Customized installation rule

| Field | Options | Description |
|----------------------|--|--|
| Product | <ul style="list-style-type: none"> ● Huawei Cloud EulerOS <ul style="list-style-type: none"> - All - Huawei Cloud EulerOS 1.1 - Huawei Cloud EulerOS 2.0 ● CentOS <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - All - EulerOS 2.2 - EulerOS 2.5 - EulerOS 2.8 - EulerOS 2.9 - EulerOS 2.10 | Product attribute of the patch. Only the patches of the selected OS can be scanned and repaired. |
| Compliance Reporting | Unspecified Critical High Medium Low Suggestion | Level of a patch that meets the patch baseline in the compliance report |

| Field | Options | Description |
|----------------|---------|--|
| Baseline patch | None | <p>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.</p> <ol style="list-style-type: none"> 1. A maximum of 1,000 baseline patches can be uploaded for a baseline. 2. The patch name can contain a maximum of 200 characters, including letters, digits, underscores (_), hyphens (-), dots (.), asterisks (*), and plus signs (+). 3. 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 **Submit**.

Figure 4-4 Creating a customized patching baseline



----End

4.2.2 Scanning a Patch

Patch Scanning allows you to scan patches on the target ECS or CCE instance. The scan is executed based on the selected default baseline, instance, and batch execution policy.

Scenarios

Scan patches on the ECS or CCE instances to generate patch compliance reports for analysis using Cloud Operations Center.

Precautions

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

- Whether the UniAgent status of the instance is normal.
- Whether the OS is supported by the Cloud Operations Center patch management feature.
- Whether the instance is stopped.

Procedure

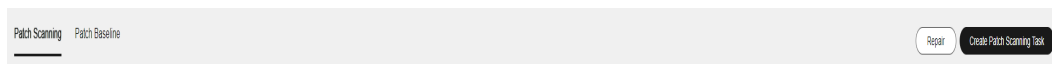
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Patch management**.
- Step 3** On the displayed page, click **Patch Scanning** to view the compliance report list.

Figure 4-5 Compliance report list

| NameID | IP Address | OS | Patch Baseline Type | Patch Baseline | Region | Enterprise Project | Application Group | Compliance Status | Non-ComplianceCom... | Reported At | Ticket ID | Operation |
|--------------------------------------|------------|----------------------|--------------------------|--|---------------------|--------------------|-------------------|-------------------|----------------------|--------------------|---------------------|----------------|
| ccc-patch-4c9156-78644801-4c9156... | | CentOS | Installation Rule Bas... | CDC-CentOS3x... JK-0307705046... | CN-North-Ulangeb203 | CDC | - | Non-compliant | 18 / 445 | Dec 14, 2023 14:53 | 0872023121414351... | Repair Summary |
| ccc-patch-4c9156-53393624-4c9156... | | Huawei Cloud EulerOS | Installation Rule Bas... | CDC-HuaweiEulerOS... JK-0307705046... | CN-North-Ulangeb203 | - | - | Compliant | 0 / 437 | Dec 14, 2023 11:15 | 0872023121017191... | Repair Summary |
| ccc-patch-4c9156-29495929-4c9156... | | EulerOS | Installation Rule Bas... | CDC-EulerOSD... JK-0308522564... | CN-North-Ulangeb203 | - | - | Compliant | 0 / 457 | Dec 14, 2023 11:15 | 0872023121017191... | Repair Summary |
| ccc-patch-euler25-47181623-4c9156... | | EulerOS | Installation Rule Bas... | CDC-EulerOSD... JK-0308522564... | CN-North-Ulangeb203 | - | - | Non-compliant | 1 / 347 | Dec 14, 2023 11:15 | 0872023121017191... | Repair Summary |
| ccc-patch-euler29-47293646-4c9156... | | EulerOS | Installation Rule Bas... | CDC-EulerOSD... JK-0308522564... | CN-North-Ulangeb203 | - | - | Compliant | 0 / 466 | Dec 14, 2023 11:15 | 0872023121017191... | Repair Summary |
| ccc-patch-4c9156-84434242-4c9156... | | EulerOS | Installation Rule Bas... | CDC-EulerOSD... JK-0308522564... | CN-North-Ulangeb203 | - | - | Compliant | 0 / 463 | Dec 14, 2023 11:15 | 0872023121017191... | Repair Summary |
| ccc-patch-cento-80641211-01042-4... | | CentOS | Installation Rule Bas... | CDC-CentOS3x... JK-0307705046... | CN-North-Ulangeb203 | CDC | - | Non-compliant | 37 / 491 | Nov 22, 2023 11:55 | 0872023122110143... | Repair Summary |
| ccc-beta-0001-71816326-39355... | | Huawei Cloud EulerOS | Installation Rule Bas... | CDC-HuaweiEulerOS... JK-0307705046... | CN-North-Ulangeb203 | default | - | Compliant | 0 / 450 | Nov 22, 2023 10:16 | 0872023122101055... | Repair Summary |
| ccc-patch-a22-513c3e3b-46211-4... | | EulerOS | Installation Rule Bas... | CDC-EulerOSD... JK-0308522564... | CN-North-Ulangeb203 | default | - | Compliant | 0 / 463 | Nov 22, 2023 10:16 | 0872023121010155... | Repair Summary |
| ccc-beta-0009-26271a3c-39355... | | Huawei Cloud EulerOS | Installation Rule Bas... | CDC-HuaweiEulerOS... JK-0307705046... | CN-North-Ulangeb203 | default | - | Non-compliant | 08 / 308 | Nov 22, 2023 10:16 | 0872023122101055... | Repair Summary |

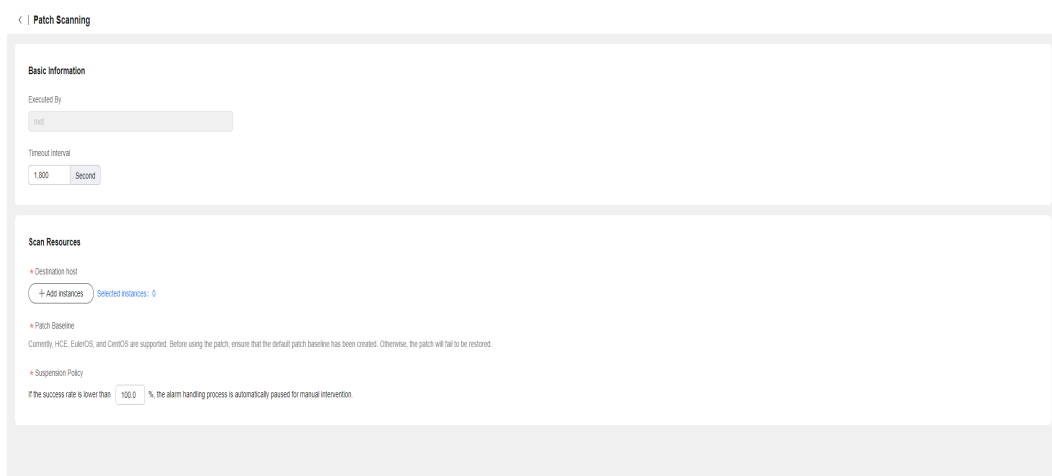
Step 4 Click Create Patch Scanning Task.

Figure 4-6 Creating a patch scanning task



Step 5 Click Add Instances.

Figure 4-7 Selecting instances



Step 6 Select the ECS or CCE instances whose patches need to be scanned.

Figure 4-8 Selecting the target ECS instances

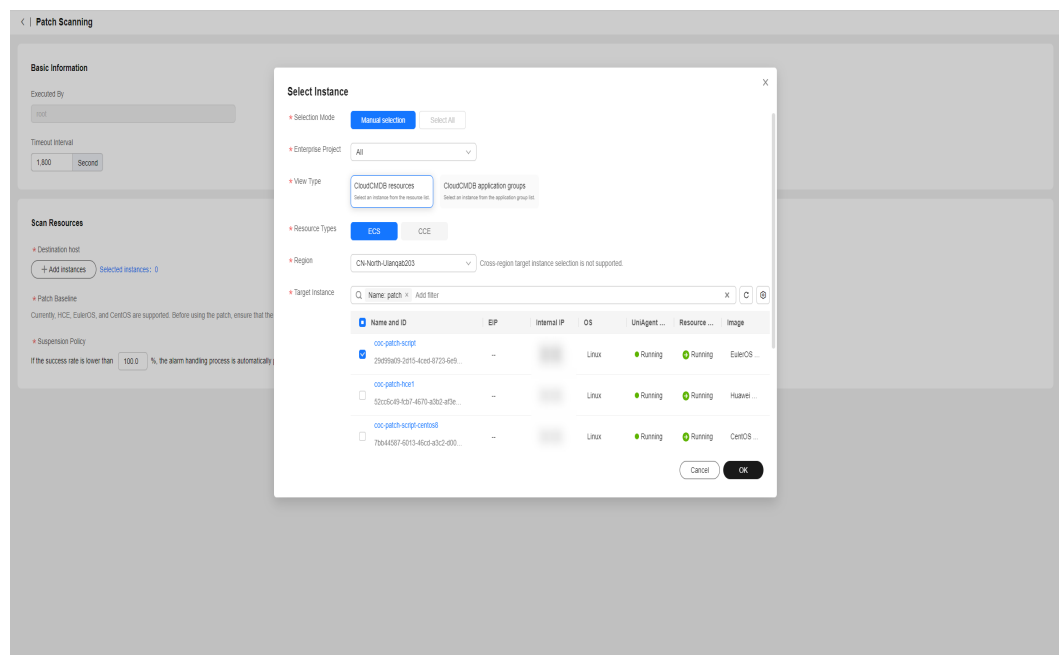
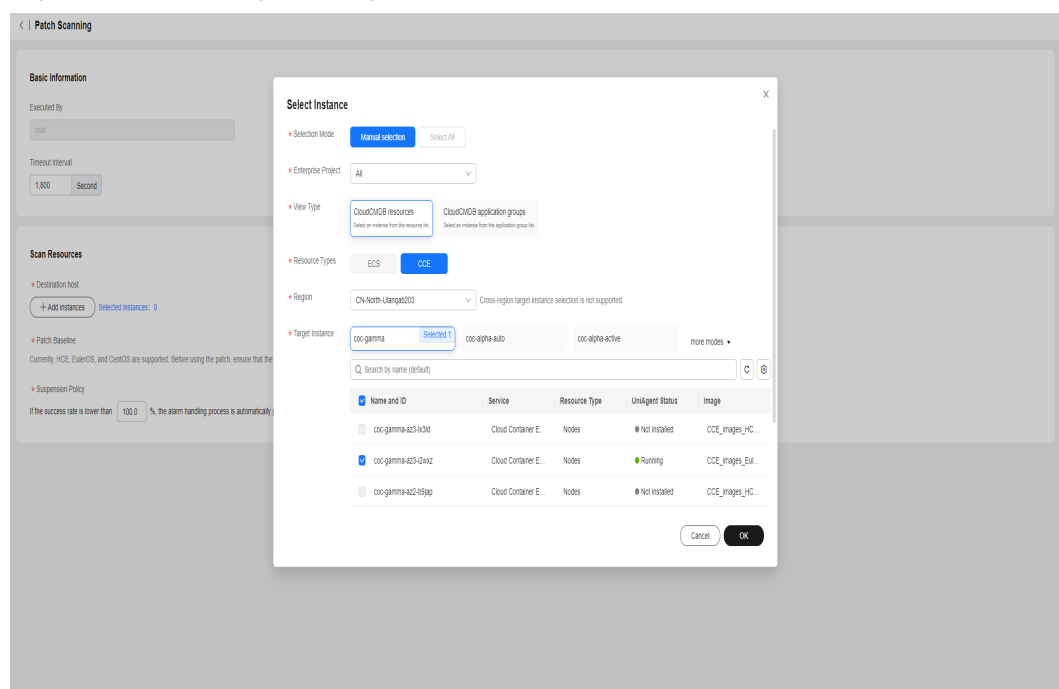


Figure 4-9 Selecting the target CCE instances

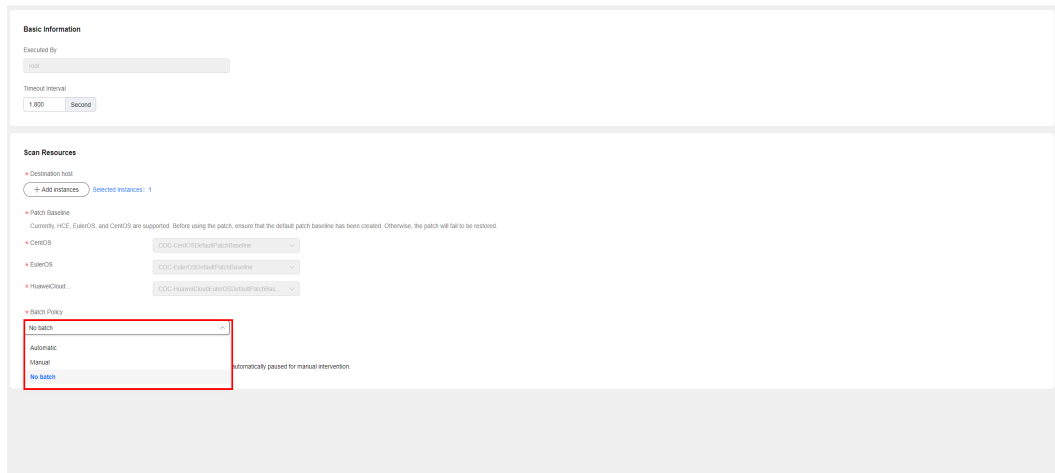


Step 7 Set the batch policy.

Batch policy

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

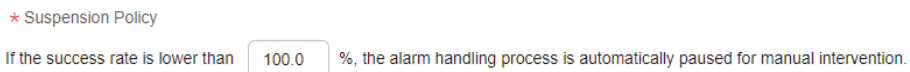
Figure 4-10 Selecting batch policies



Step 8 Configure a suspension policy.

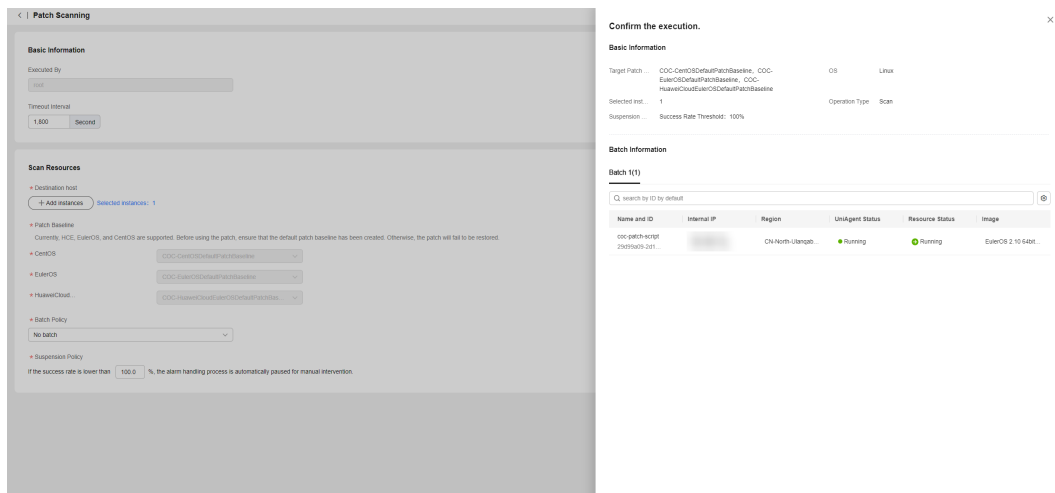
Suspension threshold: You can set the execution success rate. When the number of failed hosts reach the pre-defined suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

Figure 4-11 Suspension policy



Step 9 Click **Submit**.

Figure 4-12 Execution page after clicking **Submit**



Step 10 Confirm the execution information. If the information is correct, click **OK**.

Step 11 After the service ticket is executed, click **Compliance Reporting** to go to the **Compliance Reporting List** to view the compliance status of the ECS instance.

Figure 4-13 Service ticket details

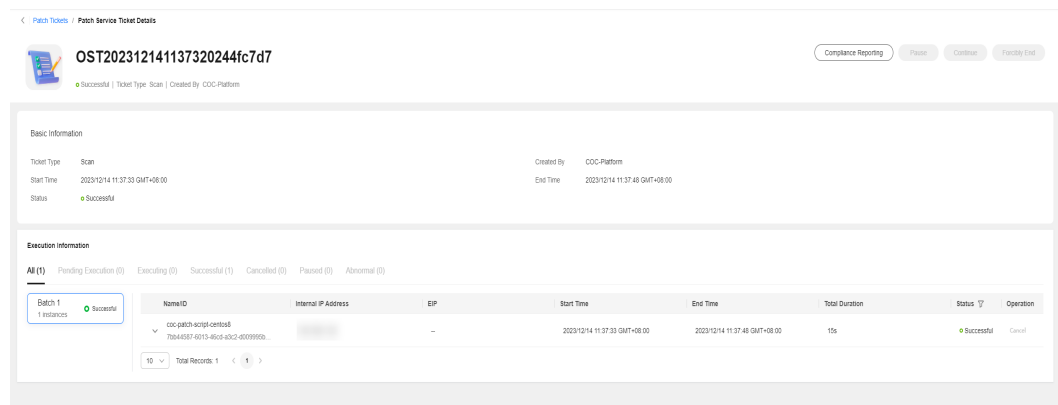
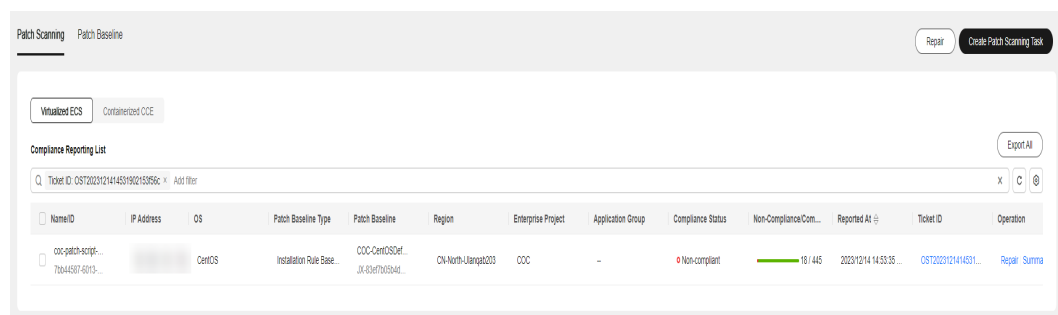


Figure 4-14 Compliance report list



----End

4.2.3 Repairing Patches

The patch repair feature allows users to repair non-compliant ECS or CCE instances scanned by patches. The patch repair feature upgrades or installs non-compliant patches on ECS or CCE instances.

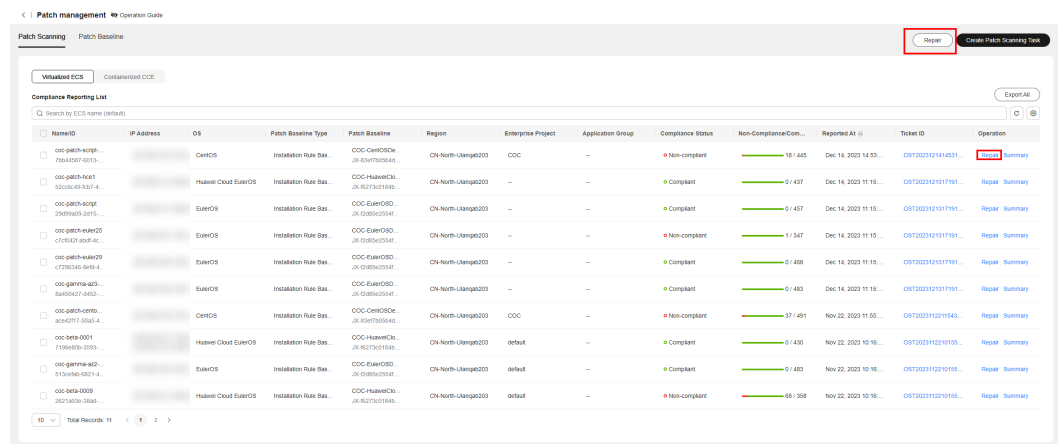
Scenarios

Repair patches on Cloud Operations Center.

Procedure

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Patch management**.
- Step 3** Select the instance whose patch needs to be repaired and click **Repair**.

Figure 4-15 Select the target instances

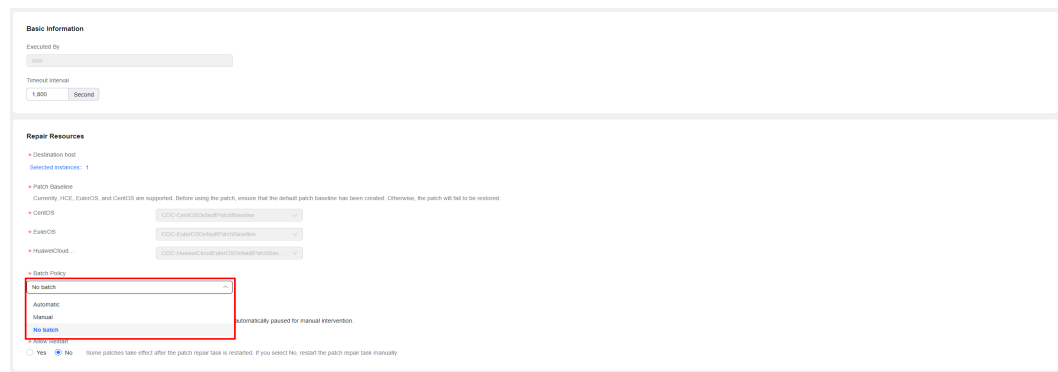


Step 4 Set the batch policy.

Batch policy

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

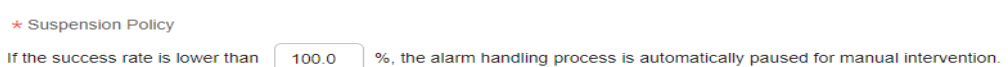
Figure 4-16 Selecting the batch policy



Step 5 Set a suspension policy.

Suspension threshold: You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

Figure 4-17 Suspension policy



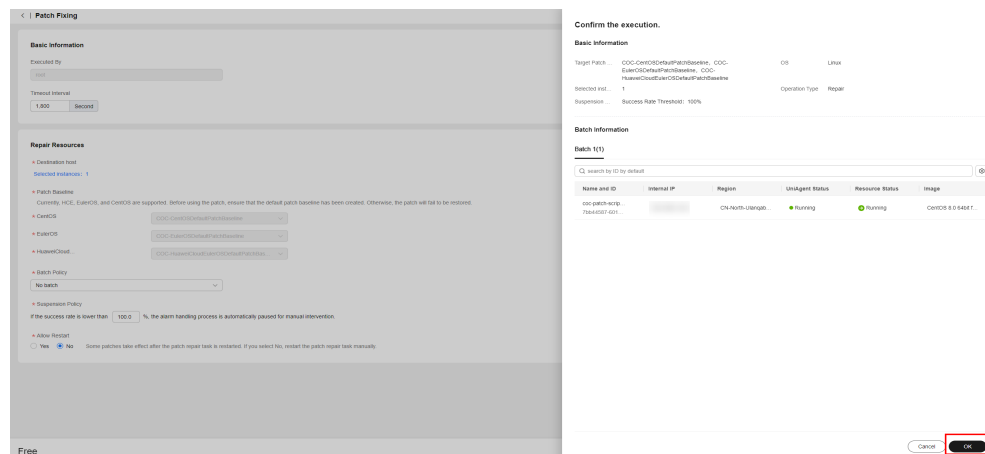
Step 6 Set whether to allow restart.

 **NOTE**

Some patches take effect only after the system is restarted. If you select No, you need to restart the system at another time.

Step 7 Confirm the execution information. If the information is correct, click **OK**.

Figure 4-18 Execution information page



----End

4.2.4 Viewing the Patch Compliance Report Details

After the patch compliance scan or repair, you can click Compliance Report Details Summary to view the details of the patch on the instance.

Scenarios

View the patch compliance scanning and patch repairing results on Cloud Operations Center.

Precautions

The patch compliance report retains only the scan or repair record at the latest time.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Patch management**.

Figure 4-19 Patch management

| NameID | IP Address | OS | Patch Baseline Type | Patch Baseline | Region | Enterprise Project | Application Group | Compliance Status | Non-ComplianceCom. | Reported At | Ticket ID | Operation |
|----------------------------------|------------|-----------------------|------------------------|--------------------------------------|--------------------|--------------------|-------------------|-------------------|--------------------|--------------------|-----------------|-----------|
| 000-0407-0426-75640000-0000-0000 | | CentOS | Installation Rule Bas. | CCC-CentOSDefaultPatchBaseline | CN-North-Harbin003 | CCC | | Non-compliant | 19 / 445 | Dec 14, 2023 14:55 | 00T202301414001 | Repair |
| 000-0407-0426-75640000-0000-0000 | | Harvest Cloud EulerOS | Installation Rule Bas. | CCC-HarvestCloudDefaultPatchBaseline | CN-North-Harbin003 | | | Compliant | 0 / 437 | Dec 14, 2023 11:18 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | EulerOS | Installation Rule Bas. | CCC-EulerOSDefaultPatchBaseline | CN-North-Harbin003 | | | Compliant | 0 / 437 | Dec 14, 2023 11:18 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | EulerOS | Installation Rule Bas. | CCC-EulerOSDefaultPatchBaseline | CN-North-Harbin003 | | | Non-compliant | 1 / 247 | Dec 14, 2023 11:15 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | EulerOS | Installation Rule Bas. | CCC-EulerOSDefaultPatchBaseline | CN-North-Harbin003 | | | Compliant | 0 / 450 | Dec 14, 2023 11:15 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | CentOS | Installation Rule Bas. | CCC-CentOSDefaultPatchBaseline | CN-North-Harbin003 | CCC | | Non-compliant | 27 / 493 | Nov 22, 2023 13:04 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | Harvest Cloud EulerOS | Installation Rule Bas. | CCC-HarvestCloudDefaultPatchBaseline | CN-North-Harbin003 | default | | Compliant | 0 / 430 | Nov 22, 2023 10:16 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | EulerOS | Installation Rule Bas. | CCC-EulerOSDefaultPatchBaseline | CN-North-Harbin003 | default | | Compliant | 0 / 430 | Nov 22, 2023 10:16 | 00T202301307191 | Repair |
| 000-0407-0426-75640000-0000-0000 | | Harvest Cloud EulerOS | Installation Rule Bas. | CCC-HarvestCloudDefaultPatchBaseline | CN-North-Harbin003 | default | | Non-compliant | 58 / 505 | Nov 22, 2023 10:16 | 00T202301307191 | Repair |

Step 3 Select the patch compliance report to be viewed and click **Summary** in the **Operation** column.

Status description:

- **Installed:** The patch complies with the patch baseline, has been installed on an ECS instance, and no update is available.
- **Non-baseline patches have been installed:** The patch is not compliant with the patch baseline but has been installed on an ECS instance.
- **Installed-to be restarted:** The patch has been repaired, and can take effect only after the ECS instance is restarted.
- **InstalledRejected:** The rejected patch defined in the exceptional patches of a patch baseline. This patch will not be repaired even if it is compliant with the patch baseline.
- **To be repaired:** The patch complies with the baseline, but the patch version is earlier than the baseline version.
- **Repair failed:** The patch is failed to be repaired.

Figure 4-20 Patch compliance report summary

| Patch Name | Category | Severity Level | Compliance Level | Patch Baseline | Installed At | Status |
|--|----------|----------------|------------------|--------------------------------|---------------------------------|-------------------------|
| curl.7.61.1-14.el8_3.1.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:37:38 GMT+08:00 | Non-compliant (Missing) |
| dbus-daemon.1.12.8-11.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:38:24 GMT+08:00 | Non-compliant (Missing) |
| dbus-libs.1.12.8-11.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:36:42 GMT+08:00 | Non-compliant (Missing) |
| NetworkManager-team.1.26.0-12.el8_3.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:38:44 GMT+08:00 | Non-compliant (Missing) |
| glibc-headers.2.28-127.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:37:24 GMT+08:00 | Non-compliant (Missing) |
| glibc.2.28-127.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:36:34 GMT+08:00 | Non-compliant (Missing) |
| NetworkManager.1.26.0-12.el8_3.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:38:25 GMT+08:00 | Non-compliant (Missing) |
| NetworkManager-ibm.1.26.0-12.el8_3.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:38:03 GMT+08:00 | Non-compliant (Missing) |
| dbus.1.12.8-11.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:38:24 GMT+08:00 | Non-compliant (Missing) |
| dbus-common.1.12.8-11.el8.el8_54 | - | - | Unspecified | CCC-CentOSDefaultPatchBaseline | Feb 26, 2021 11:37:26 GMT+08:00 | Non-compliant (Missing) |

----End

4.3 Batch ECS operations

ECS operations allow you to manage ECS instances, including starting, stopping, restarting, switching, and reinstalling ECSs in batches.

4.3.1 Starting ECSs

Scenarios

Start ECS instances in batches on Cloud Operations Center.

Precautions

Instances that have been started cannot be selected.

Procedure

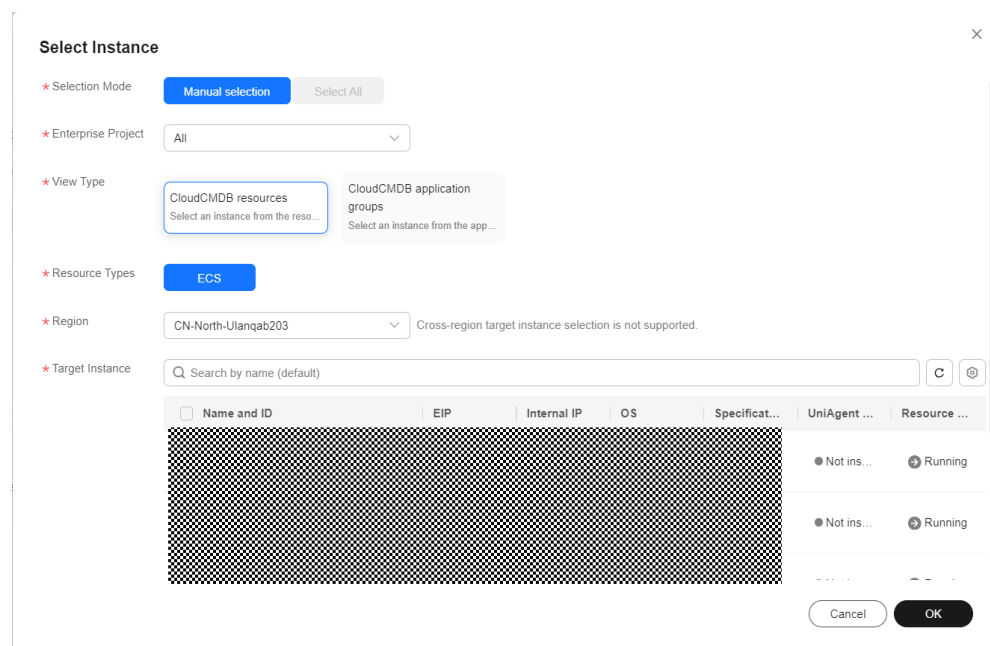
Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Batch ECS Operations**.

Step 3 Click **Start ECSs**.

Step 4 On the **Start ECSs** page, click **Add Instances**.

Figure 4-21 Selecting instances



Step 5 Select a batch policy.

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

Step 6 Set a suspension policy.

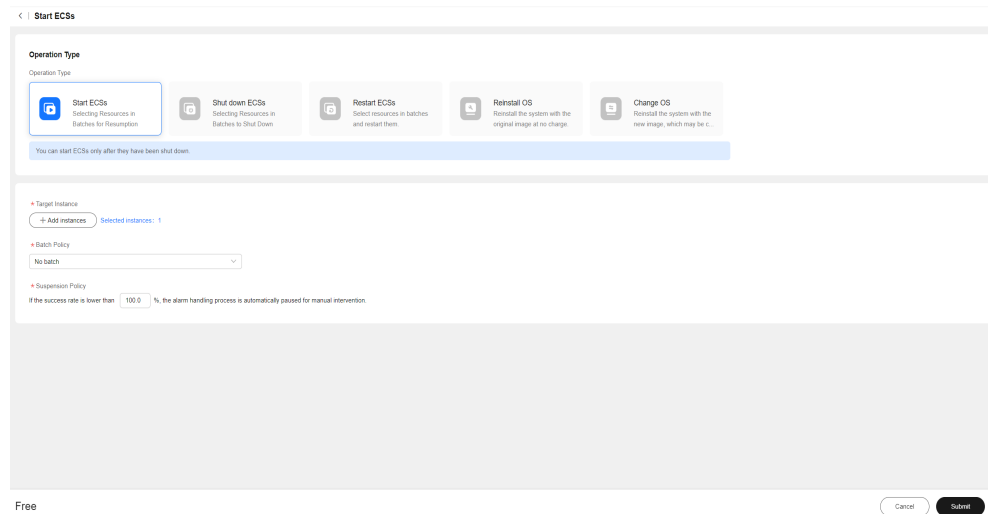
NOTE

You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

The value from 0 to 100 and can be accurate to one decimal place.

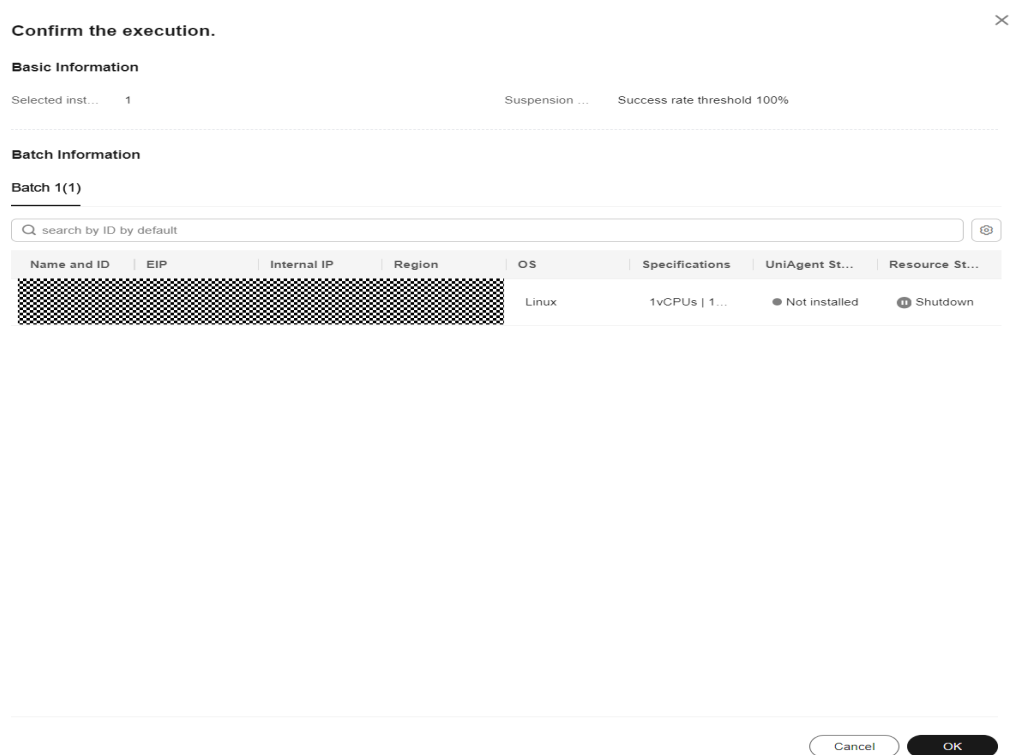
Step 7 Click **OK**.

Figure 4-22 Starting instances



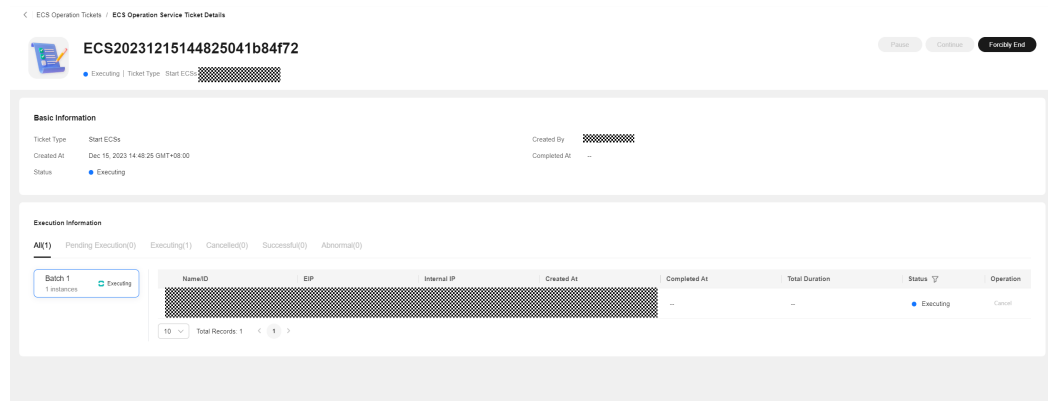
Step 8 Click **OK**.

Figure 4-23 Confirming the execution



Step 9 View the execution result.

Figure 4-24 Viewing the result



----End

4.3.2 Stopping ECSs

Scenarios

Stop ECS instances in batches on Cloud Operations Center.

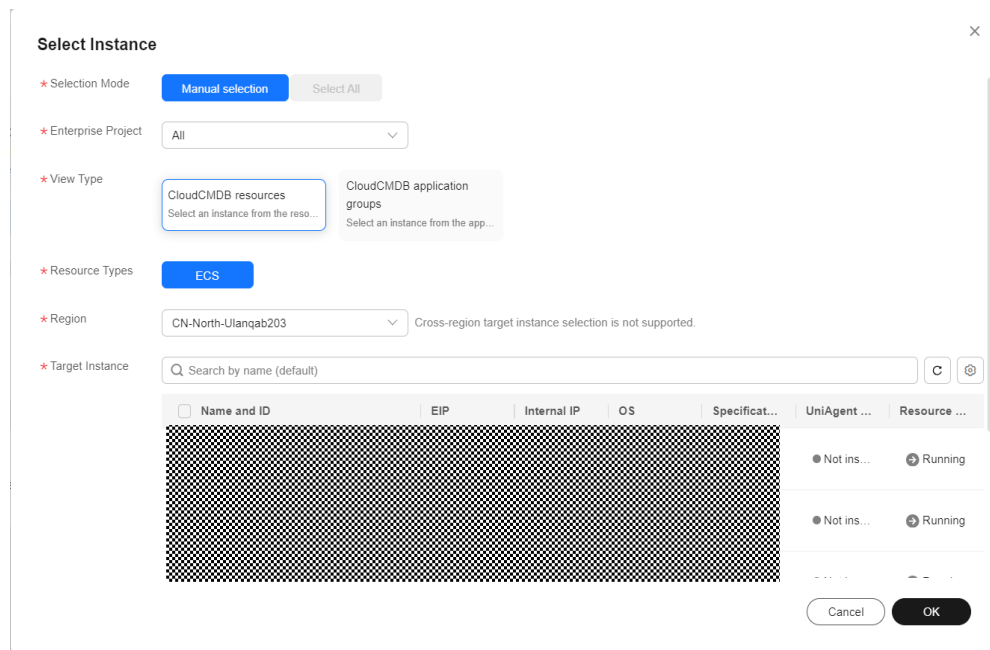
Precautions

Stopped instances cannot be selected.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Batch ECS Operations**.
- Step 3** Click **Shut down ECSs**.
- Step 4** On the **Shut down ECSs** page, click **Add Instances**.

Figure 4-25 Selecting instances



Step 5 Select a batch policy.

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

Step 6 Set a suspension policy.

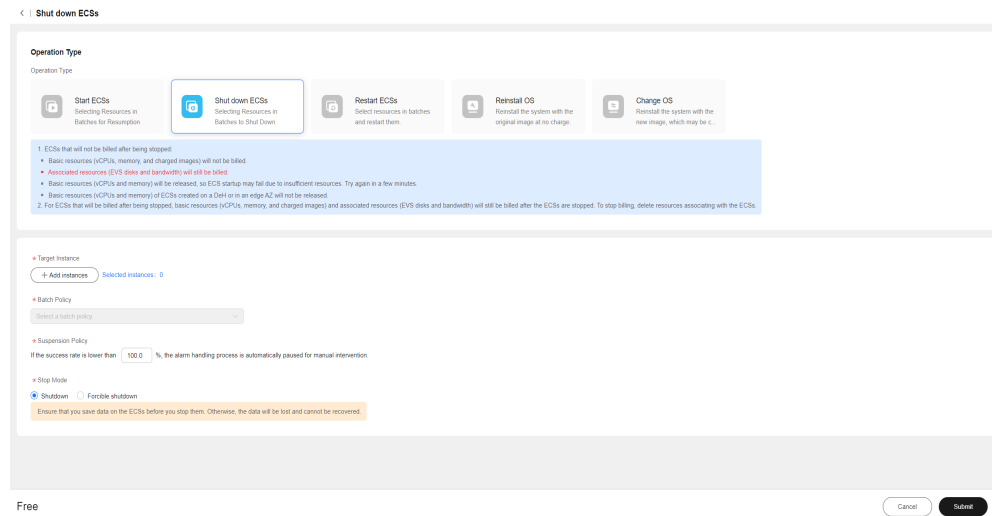
NOTE

You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

The value from 0 to 100 and can be accurate to one decimal place.

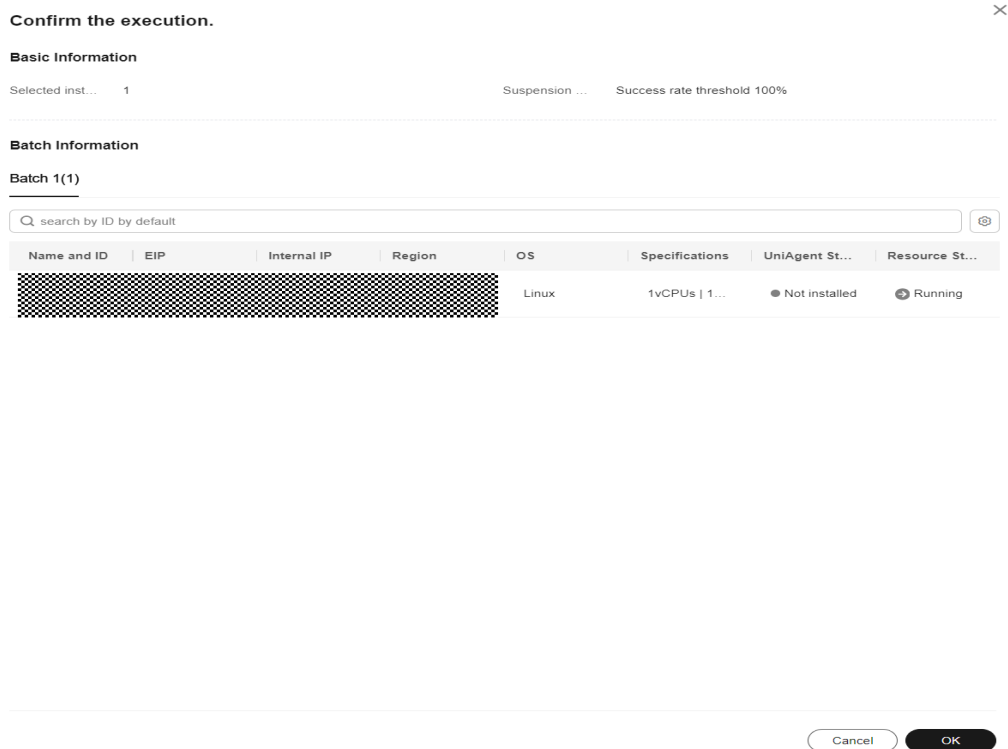
Step 7 Click **OK**.

Figure 4-26 Stopping instances



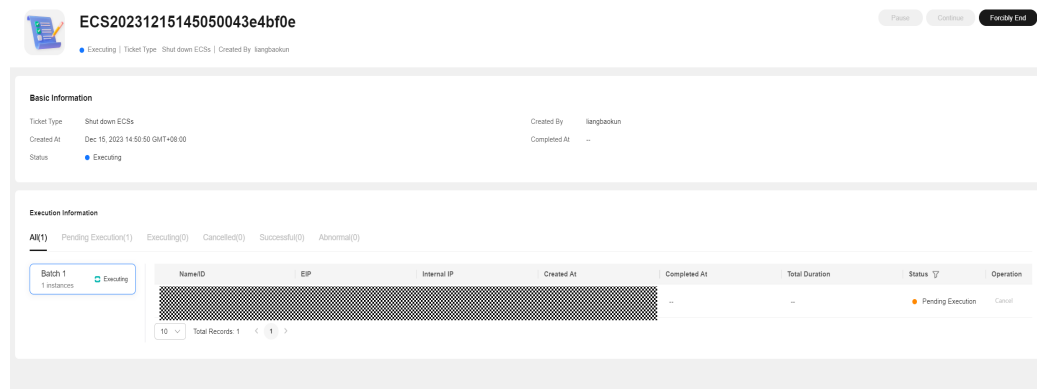
Step 8 Click OK.

Figure 4-27 Confirming the execution



Step 9 View the execution result.

Figure 4-28 Viewing the result



----End

4.3.3 Restarting ECSs

Scenarios

Restart ECS instances in batches on Cloud Operations Center.

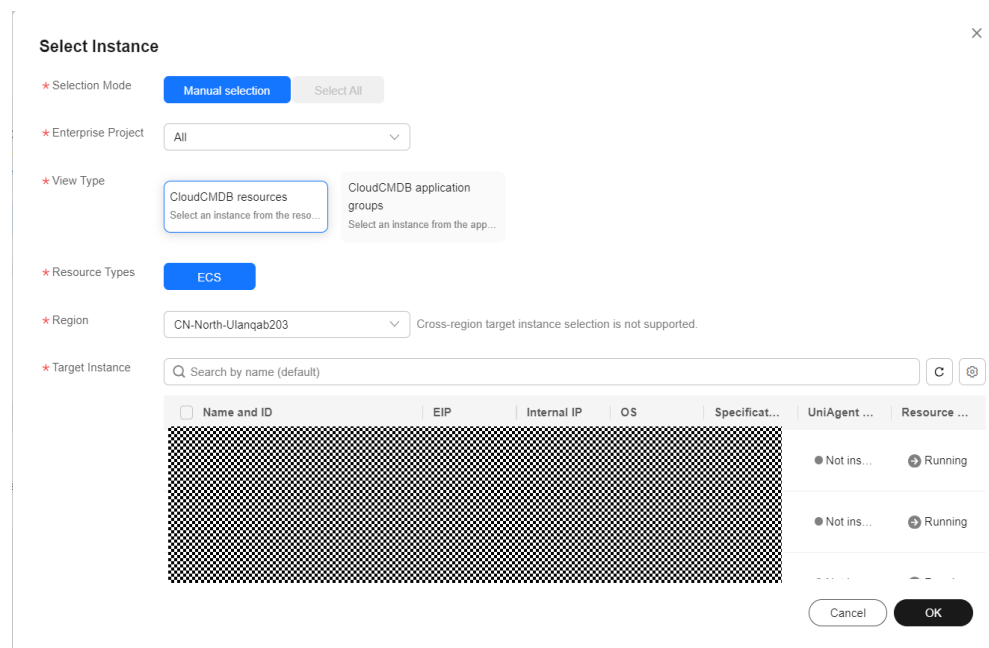
Precautions

Stopped instances cannot be selected.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Batch ECS Operations**.
- Step 3** Click **Restart ECSs**.
- Step 4** On the **Restart ECSs** page, click **Add Instances**.

Figure 4-29 Selecting instances



Step 5 Select a batch policy.

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

Step 6 Set the suspension policy.

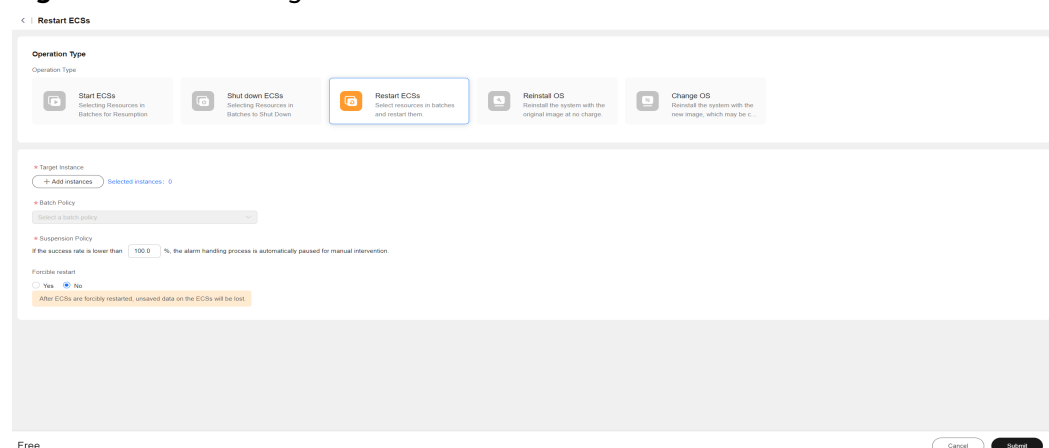
NOTE

You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

The value from 0 to 100 and can be accurate to one decimal place.

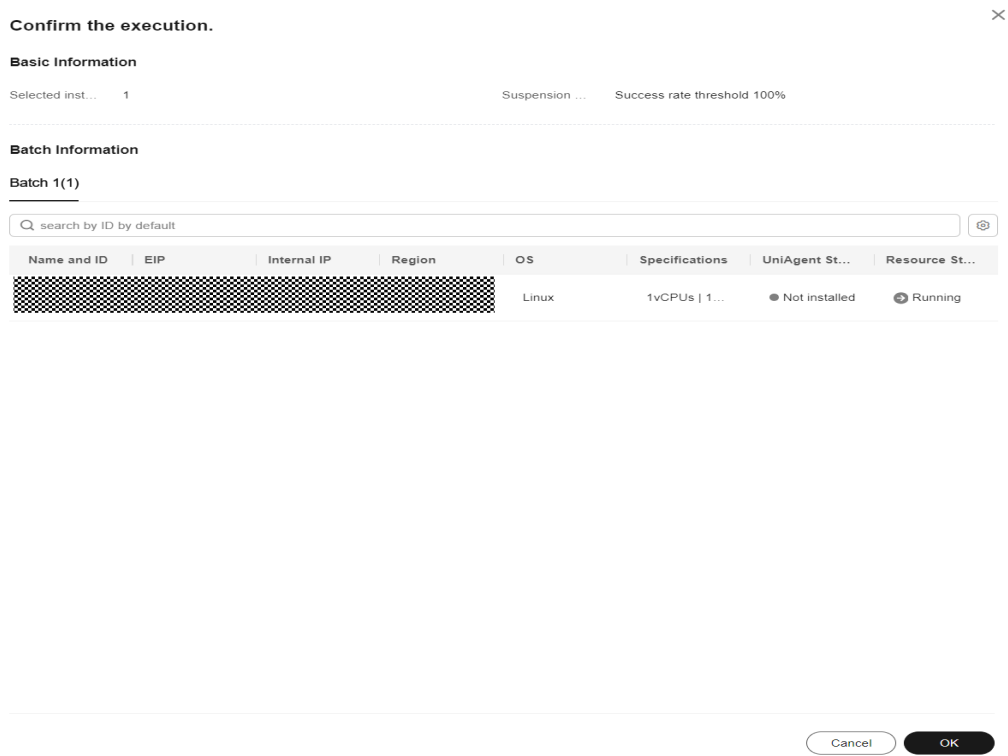
Step 7 Click **OK**.

Figure 4-30 Restarting instances



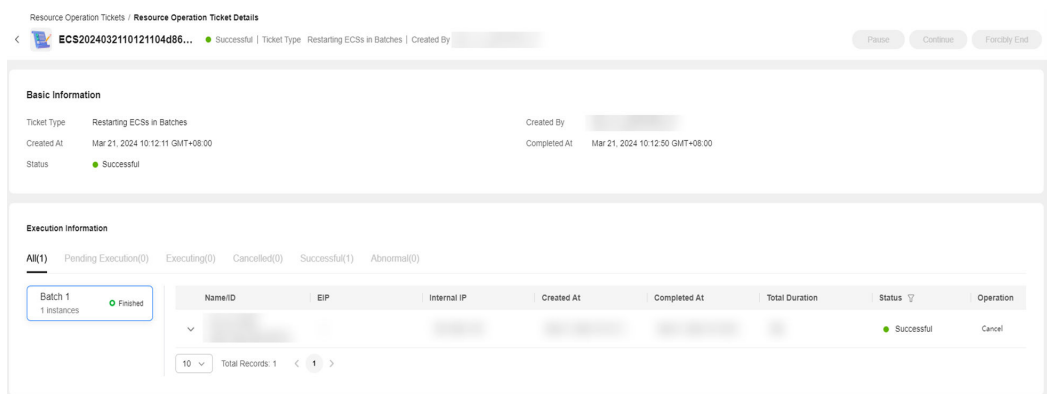
Step 8 Click **OK**.

Figure 4-31 Confirming the execution



Step 9 View the execution result.

Figure 4-32 Viewing the result



----End

4.3.4 Reinstalling OSs

Scenarios

Re-install OSs of ECS instances in batches on Cloud Operations Center.

Precautions

If the ECS is started, select **Stop now**.

If the ECS is stopped, submit the request directly.

Procedure

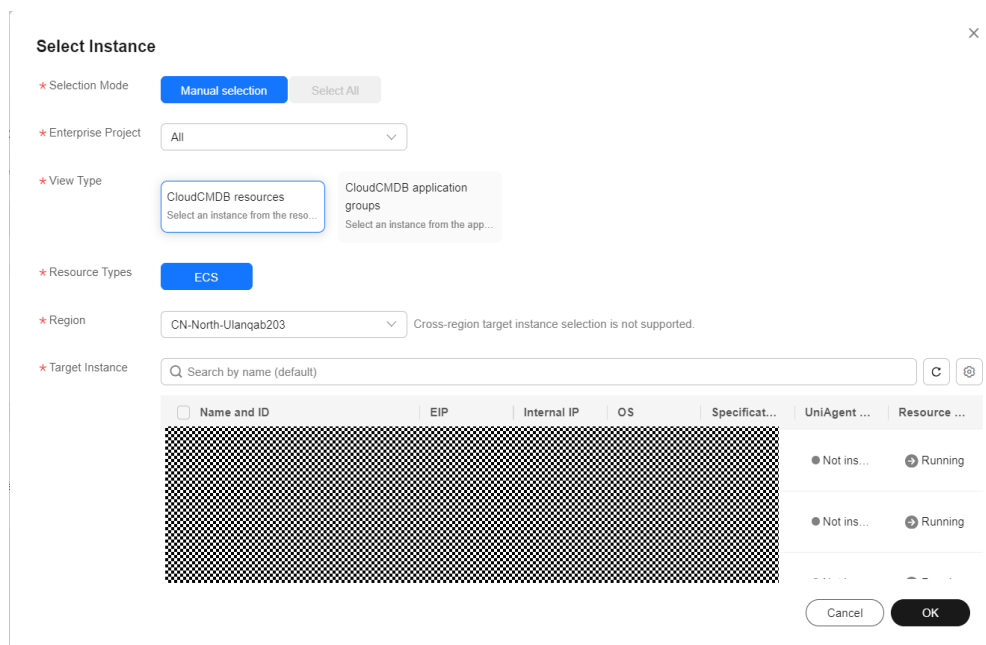
Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Batch ECS Operations**.

Step 3 Click **Reinstall OS**.

Step 4 On the **Reinstall OS** page, click **Add Instances**.

Figure 4-33 Adding instances



Step 5 Select a batch policy.

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

Step 6 Set a suspension policy.

NOTE

You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

The value from 0 to 100 and can be accurate to one decimal place.

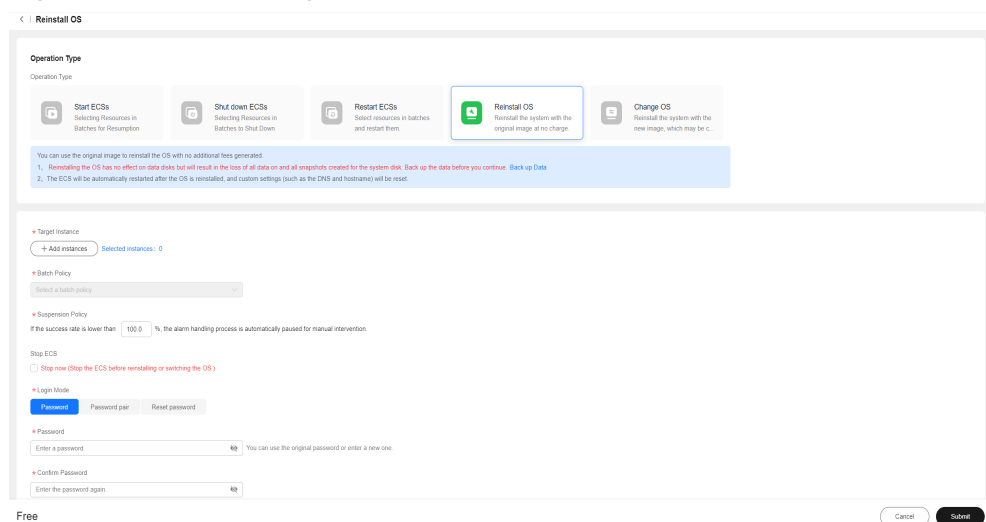
Step 7 Set the login mode.

Login mode:

- Password: You can use the original ECS password or enter the new one.
- Password pair: You can select the corresponding key pair in Key Pair Service.
- Configuration after creation: Before logging in to the ECS, reset the password.

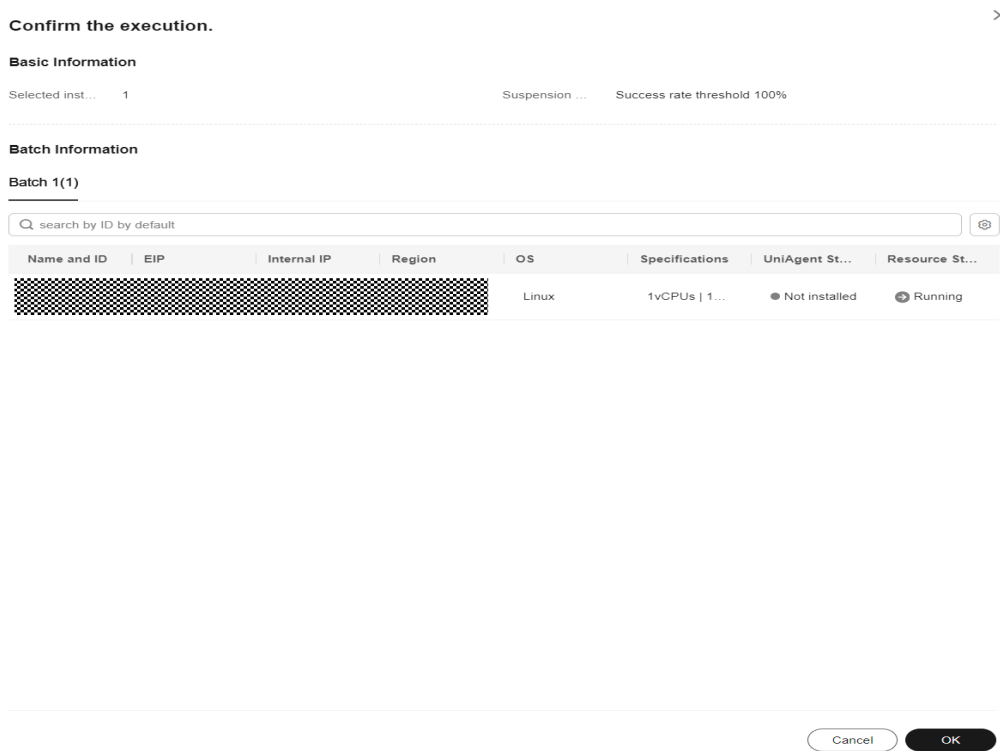
Step 8 Click **OK**.

Figure 4-34 Reinstalling OSs



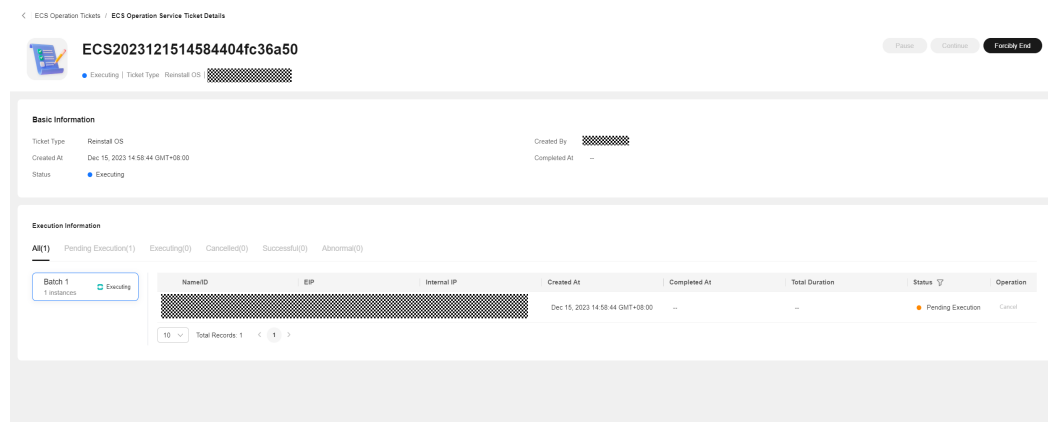
Step 9 Click **OK**.

Figure 4-35 Confirming the execution



Step 10 View the execution result.

Figure 4-36 Viewing the execution result



----End

4.3.5 Changing OSs

Scenarios

Change OSs of ECSs on Cloud Operations Center.

Precautions

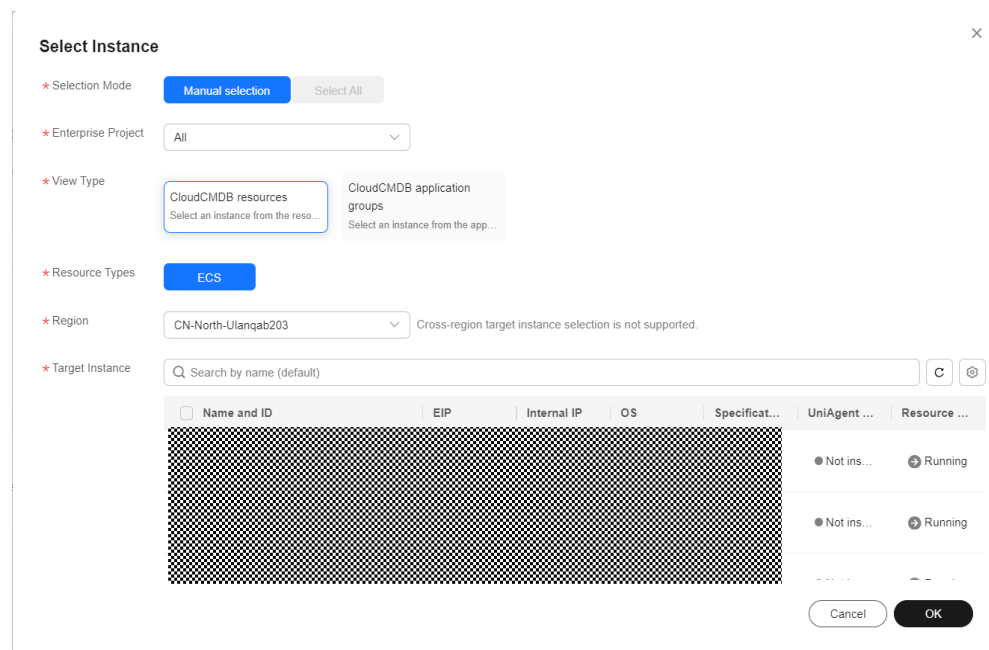
If the ECS is started, select **Stop now**.

If the ECS is stopped, submit the request directly.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resource O&M**. On the displayed page, click **Batch ECS Operations**.
- Step 3** Click **Change OS**.
- Step 4** On the **Change OS** page, click **Add Instances**.

Figure 4-37 Changing OSs



Step 5 Select a batch policy.

- **Automatic:** The selected hosts 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 hosts to be executed are in the same batch.

Step 6 Set a suspension policy.

NOTE

You can set the execution success rate. When the number of failed hosts meet the number calculated based on the suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

The value from 0 to 100 and can be accurate to one decimal place.

Step 7 Enter the image ID.

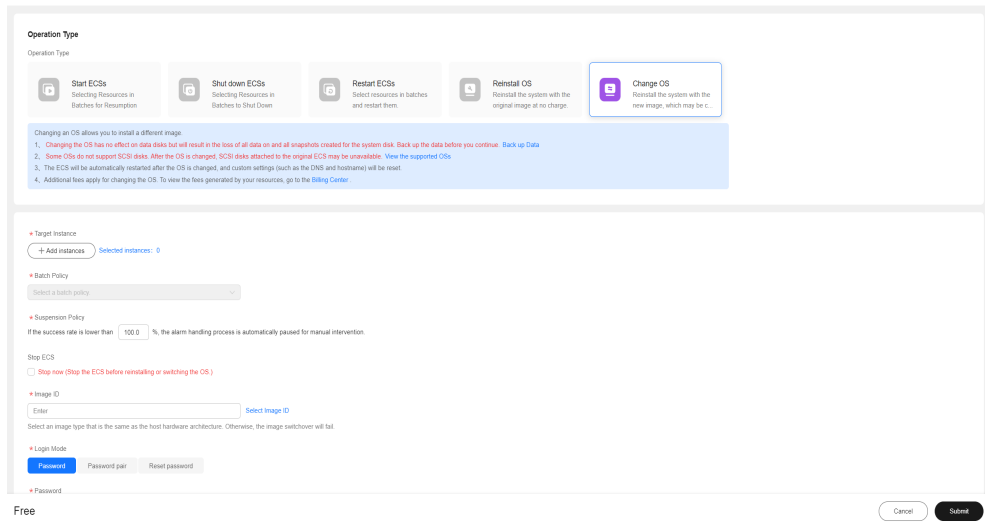
Step 8 Set the login mode.

Login mode:

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

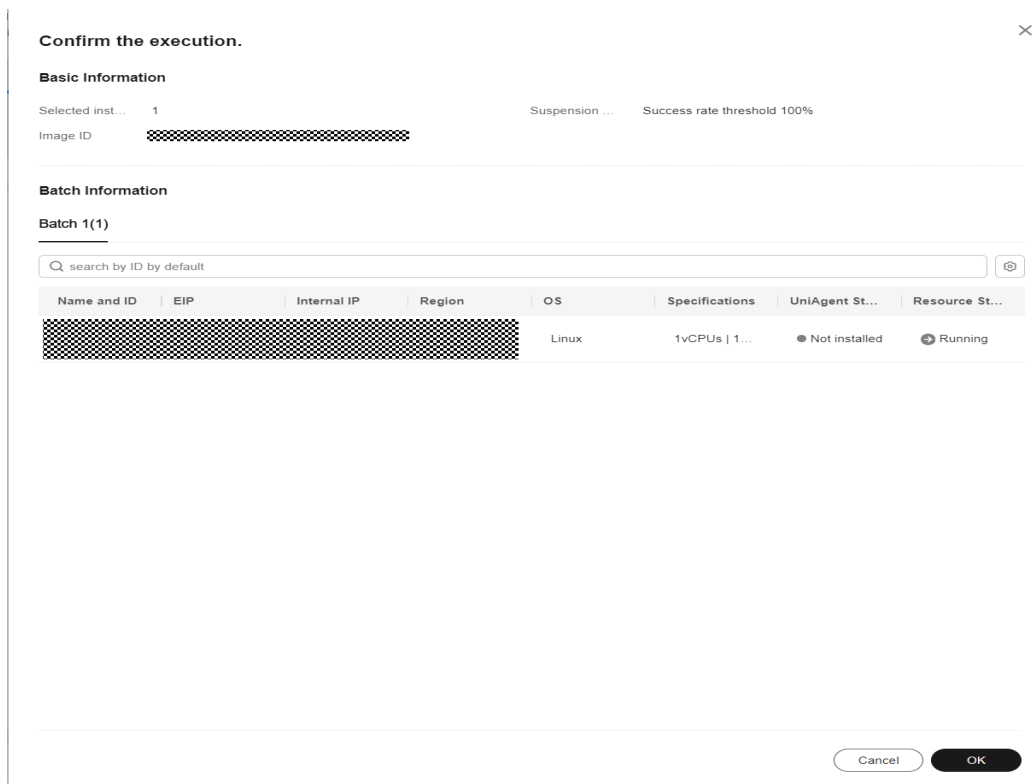
Step 9 Click **OK**.

Figure 4-38 Changing OSs



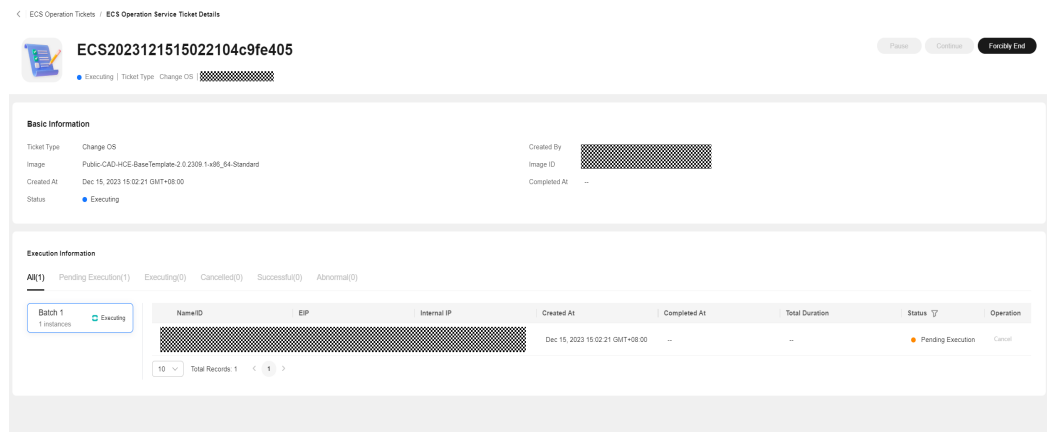
Step 10 Click OK.

Figure 4-39 Confirming the execution



Step 11 View the execution result.

Figure 4-40 Execution result



----End

4.4 Batch Operations on RDS Instances

5 Automated O&M

5.1 Script Management

The **Scripts** module allows you to create, modify, and delete scripts, and execute customized scripts and public scripts on target VMs (Only ECSs are supported currently).

5.1.1 Creating a Custom Script

The custom script creation capability is provided. Shell, Python, and BAT scripts can be created.

Scenarios

Create a custom script on Cloud Operations Center.

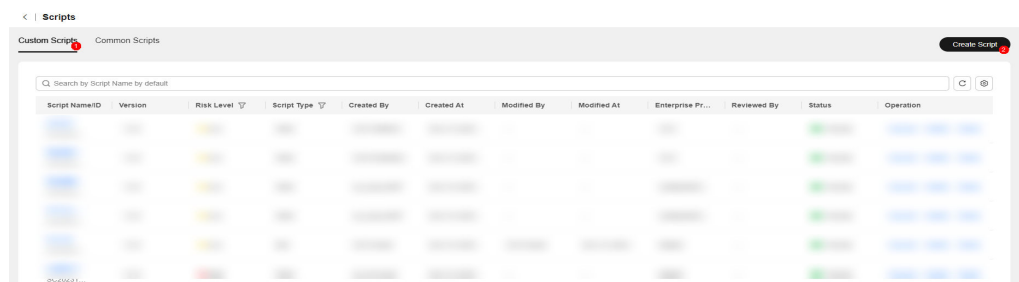
Precautions

Confirm and complete the risk level of the script content.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Automated O&M**. Click **Scripts**, click the **Custom Scripts** tab, and click **Create Script**.

Figure 5-1 Clicking **Create Script**



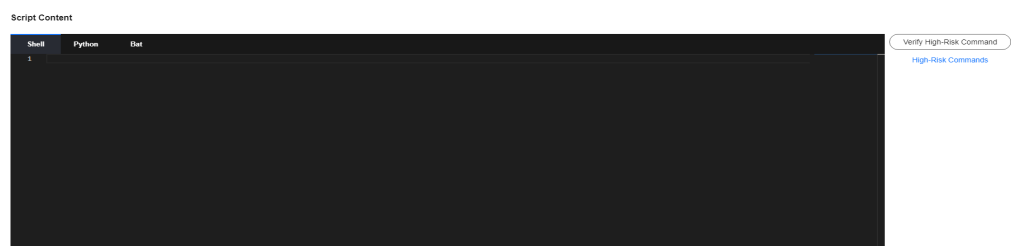
Step 3 Enter the basic script information.

Figure 5-2 Setting parameters



Step 4 Enter the script content. The script type can be Shell, Python, or Bat. And verify high-risk commands in the script.

Figure 5-3 Entering the script content



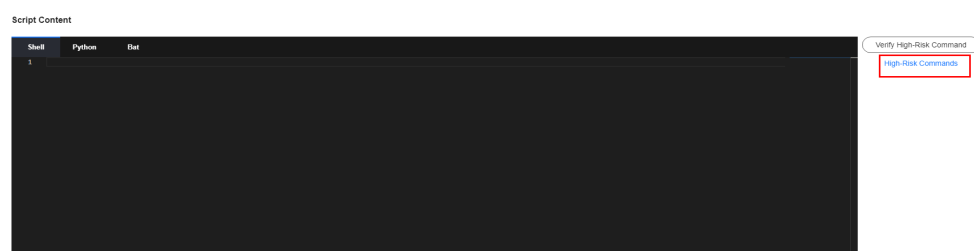
Step 5 Click **Verify High-Risk Command**.

- **Verification scope:** the high-risk commands involved in the detection. 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 check whether the script content is high-risk, that is, low-risk or high-risk.

NOTE

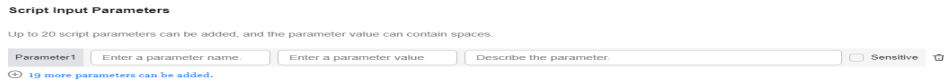
The result of high-risk command verification is used only as a reference for grading the script risk level. The system does not forcibly require the consistency between script risk level and the verification result. Evaluate the risk level based on the actual service impact.

Figure 5-4 Verifying high-risk commands



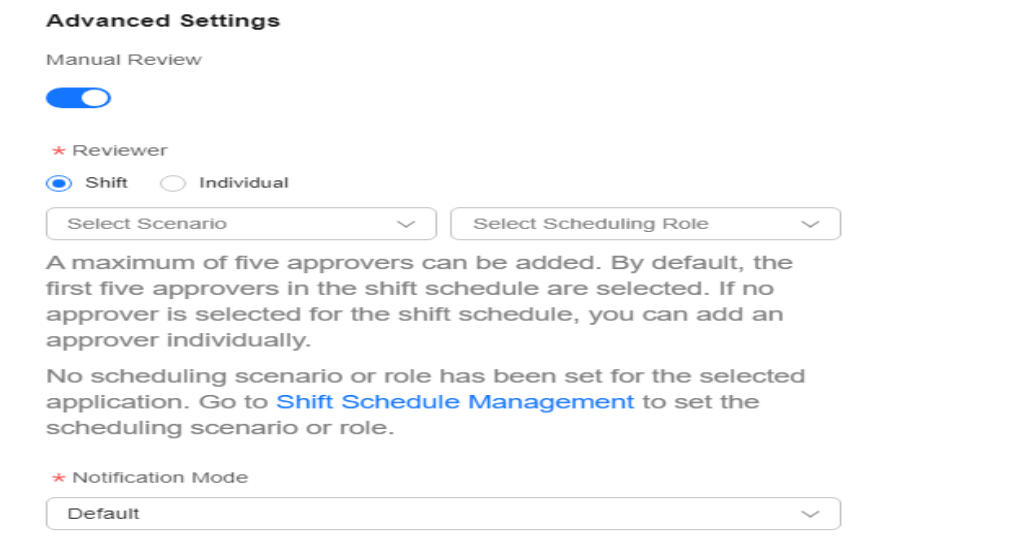
Step 6 Enter the script input parameters. You can select the **Sensitive** check box to encrypt the parameters.

Figure 5-5 Entering script input parameters



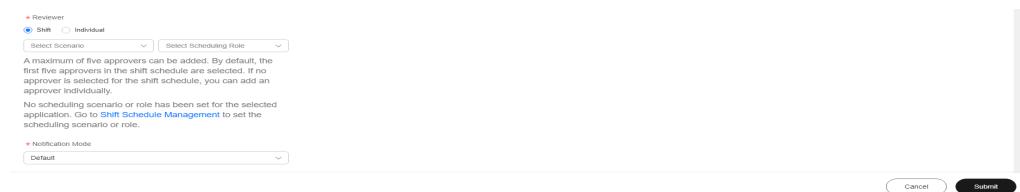
Step 7 Enable **Manual Review**. This switch is enabled automatically for high-risk scripts.

Figure 5-6 Selecting the reviewer and the notification mode



Step 8 Click **Submit**.

Figure 5-7 Submitting the request



----End

5.1.2 Managing Custom Scripts

The custom script modification and deletion capabilities are provided.

Scenarios

Modify and delete a custom script to be executed on Cloud Operations Center.

Precautions

Confirm and complete the risk level of the script content when modifying a script.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Automated O&M**. Click **Scripts**, click the **Custom Scripts** tab.

Figure 5-8 Script management

| Script Name | Version | Risk Level | Script Type | Created By | Created At | Modified By | Modified At | Enterprise Pr... | Reviewed By | Status | Operation |
|-------------|---------|------------|-------------|------------|-----------------|-------------|-----------------|------------------|-------------|--------|-----------------------|
| ... | 1.0.0 | Low | Shell | ... | Dec 19, 2023... | -- | -- | -- | -- | Normal | Execute Modify Delete |
| ... | 1.0.0 | Low | Shell | ... | Dec 19, 2023... | -- | -- | -- | -- | Normal | Execute Modify Delete |
| ... | 1.0.0 | Low | Shell | ... | Dec 18, 2023... | -- | -- | -- | -- | Normal | Execute Modify Delete |
| ... | 1.0.0 | Low | Shell | ... | Dec 18, 2023... | -- | -- | -- | -- | Normal | Execute Modify Delete |
| ... | 1.0.0 | Low | Bat | ... | Dec 18, 2023... | COC-Script | Dec 19, 2023... | -- | -- | Normal | Execute Modify Delete |

Step 3 Perform operations on the script.

- To modify a script, click **Modify** in the **Operation** column. You can modify the script based on instructions in [Creating a Custom Script](#). To cancel the modification, click **Cancel**.
- To delete a script, click **Delete** in the **Operation** column.
- To review a script, click Review.

Figure 5-9 Modifying and deleting a script

| | | | | | | | | | | | |
|-----|-------|------|-------|-----|--------------------|----|----|---------|----|--------|-------------------------------------|
| ... | 1.0.0 | High | Shell | ... | Dec 27, 2023 17... | -- | -- | default | -- | Normal | Execute Modify Delete |
|-----|-------|------|-------|-----|--------------------|----|----|---------|----|--------|-------------------------------------|

----End

5.1.3 Executing Custom Scripts

The custom script execution capability is provided.

Scenarios

Execute a custom script on Cloud Operations Center.

Precautions

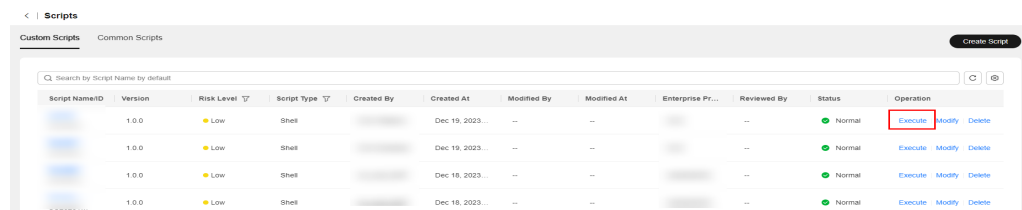
Ensure that you have the permission on the component to which the target VM belongs when executing a script.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Automated O&M** and click **Scripts**. On the displayed page, locate the target script to be executed, click **Execute** in the **Operation** column.

Figure 5-10 Selecting the customized script to be executed



Step 3 Enter the script input parameters. The parameter names and default values have been preset when a custom script is entered. During script execution, you can manually enter the script input parameter values or use the parameter warehouse. You need to select the region where the parameter is located, parameter name, and parameter association mode from **Parameter Warehouse**.

Figure 5-11 Manually entering script parameters

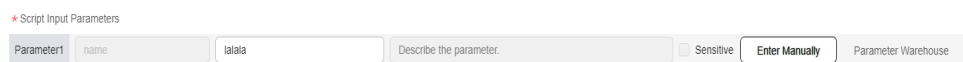


Figure 5-12 Selecting script parameters from the parameter warehouse

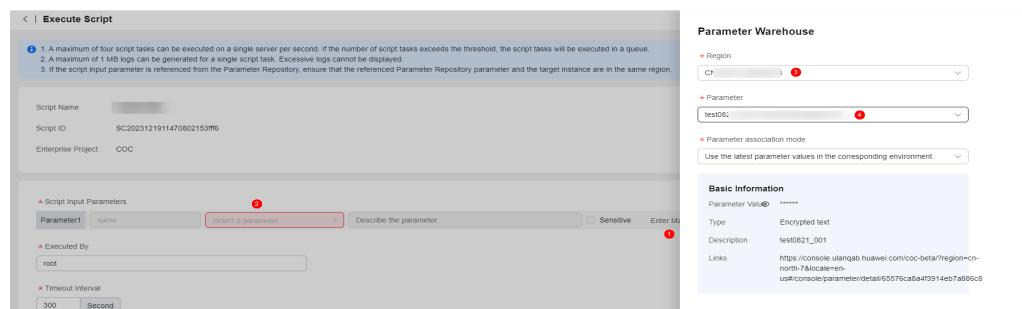


Table 5-1 Parameter association modes

| Parameter Association Mode | Description |
|---|---|
| Use the latest parameter value in the corresponding environment | This parameter is used during script execution. The parameter value is the latest parameter value obtained from the corresponding region in the parameter warehouse in real time. |

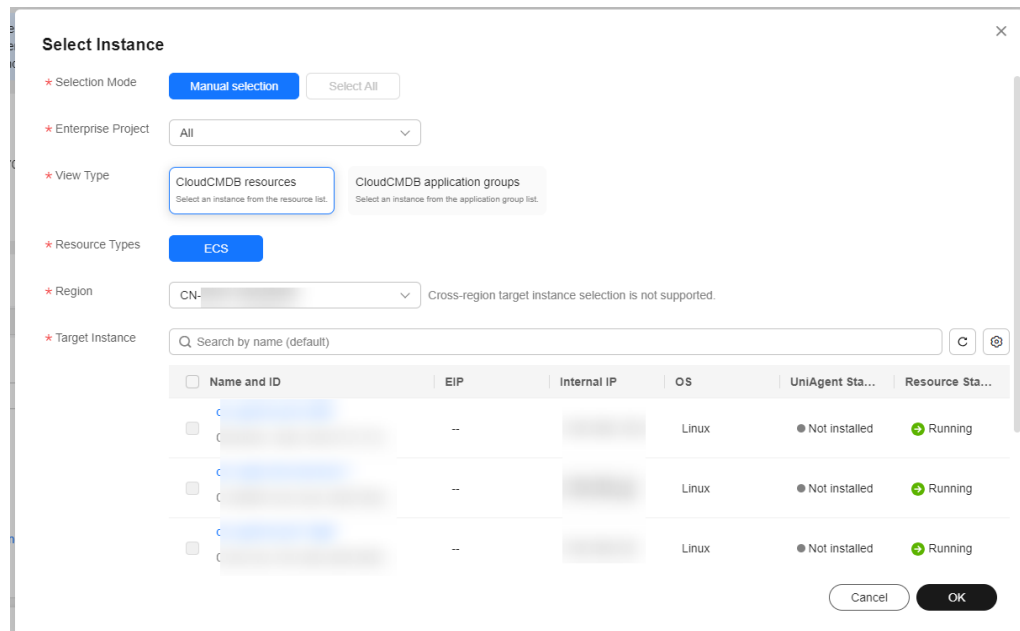
NOTE

If you select parameter warehouse, you need to create the parameters to be selected on the **Parameter Management > Parameter Center** page.

Step 4 Enter the execution user and execution timeout interval. **Executed by:** the user who executes the script on the target instance node. The default user is **root**. **Timeout Interval:** the timeout interval for executing the script on the current instance. The default value is **300**.

Step 5 Click **Add** to add the target instances for script execution. You can search for target instances by name, EIP, or resource status.

Figure 5-13 Selecting target instances



Step 6 Select a batch policy.

- **Automatic:** The selected instances are divided into multiple batches based on the default rule.
- **Manual:** You can manually divide instances into multiple batches as required.
- **No batch:** All instances to be executed are in the same batch.

Figure 5-14 Selecting a batch policy



Step 7 Set a suspension policy.

Suspension policy: You can set the execution success rate. When the number of failed instances meets the number calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.

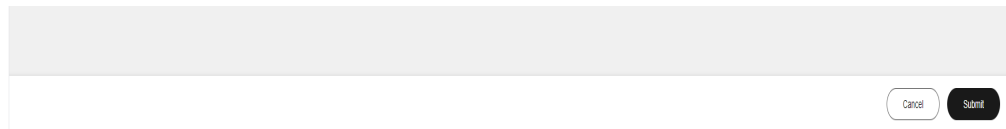
Figure 5-15 Setting a suspension policy

* Suspension Policy

If the success rate is lower than %, the alarm handling process is automatically paused for manual intervention.

Step 8 Click **Submit**.

Figure 5-16 Submitting the request



----End

5.1.4 Executing Common Scripts

The capability of executing the common scripts preset by the service is provided.

NOTE

Common scripts are available to all users. Users can read or execute the common scripts to perform common operations such as clearing disks.

Scenarios

Execute common scripts provided by the service on Cloud Operations Center.

Precautions

Ensure that you have the permission on the component to which the target VM belongs when executing a script.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Automated O&M**. Click **Scripts** and click the **Common Scripts** tab. On the displayed page, locate the target script to be executed, click **Execute** in the **Operation** column.

Figure 5-17 Selecting the target common script to be executed

| Script Name/ID | Version | Risk Level | Script Type | Created By | Created At | Modified By | Modified At | Operation |
|--|---------|------------|-------------|------------|----------------------------|-------------|---------------------------|------------|
| OS-DIAGNOSE SC20230608144846... | 1.0.2 | High | Shell | System | Dec 11, 2023 11:48:41 G... | -- | -- | Execute... |
| resettingWindowsAdm SC20230608144846... | 1.0.1 | High | Bat | System | Dec 11, 2023 11:48:41 G... | -- | -- | Execute... |
| resettingLinuxAdmin SC20230608144846... | 1.0.1 | High | Shell | System | Dec 11, 2023 11:48:41 G... | -- | -- | Execute... |
| modifyingVmIpsAddr SC20230608144846... | 1.0.2 | High | Shell | System | Dec 11, 2023 11:48:41 G... | -- | -- | Execute... |
| ClearingDisks SC20230608142637... | 1.0.4 | High | Shell | System | Jun 06, 2023 21:50:54 G... | System | Dec 15, 2023 14:46:34 ... | Execute... |
| ResettingNon-Admin SC20230608153515... | 1.0.8 | High | Shell | System | Jun 06, 2023 21:50:54 G... | System | Dec 15, 2023 14:46:34 ... | Execute... |

Step 3 Complete the script execution information. Input parameters are preset in common scripts and cannot be modified. Set **Executed By** and **Timeout Interval**. The default executor is user **root** and default timeout interval is 300 seconds.

Script parameters can be manually entered or stored in the parameter repository. (Disk clearing is not supported currently.) If you manually enter a parameter

value, you need to select the region where the parameter is located, parameter name, and parameter association mode from **Parameter Warehouse**.

Figure 5-18 Manually entering script parameters

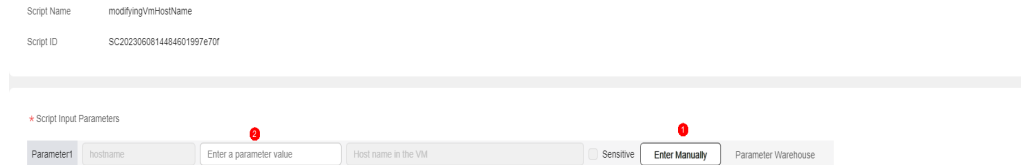


Figure 5-19 Selecting script parameters from repository

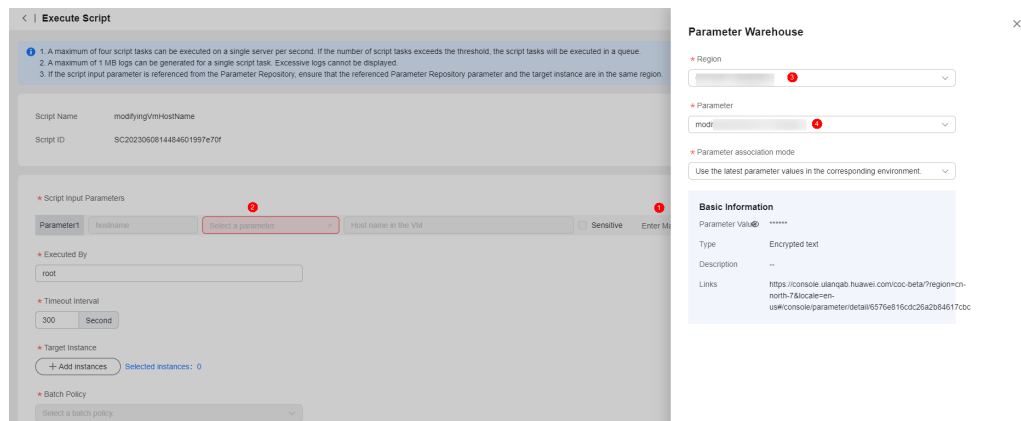
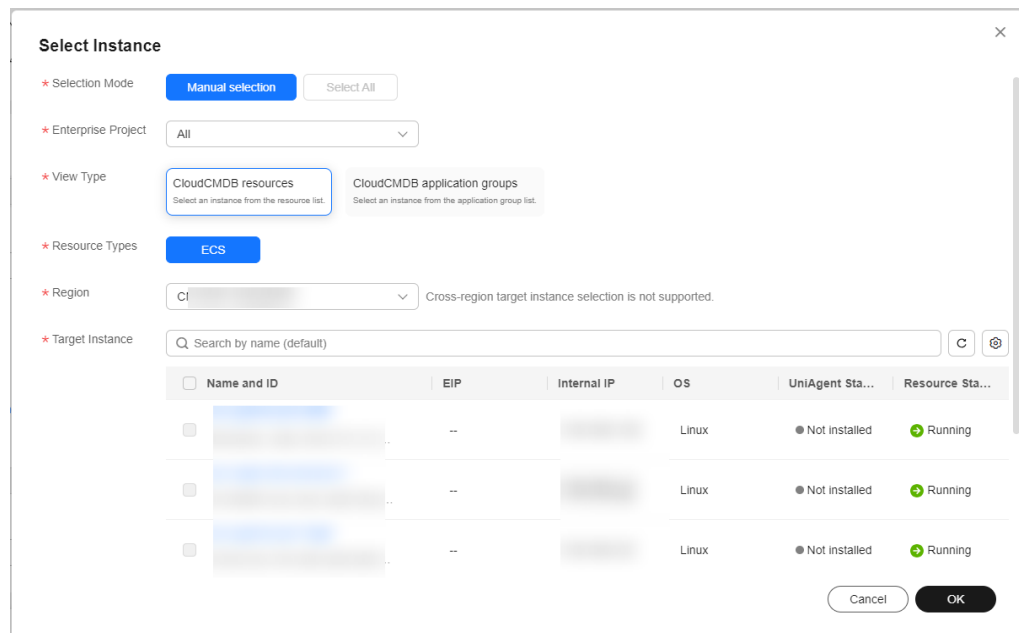


Table 5-2 Parameter association modes

| Parameter Association Mode | Description |
|---|---|
| Using the latest parameter value in the corresponding environment | This parameter is used during script execution. The parameter value is the latest parameter value obtained from the corresponding region in the parameter warehouse in real time. |

Step 4 Click **Add** to select the target instances. You can search for instances by name, EIP, or resource status.

Figure 5-20 Selecting target instances



Step 5 Select a batch policy.

- **Automatic:** The selected instances are divided into multiple batches based on the default rule.
- **Manual:** You can manually divide instances into multiple batches as required.
- **No batch:** All instances to be executed are in the same batch.

Figure 5-21 Selecting a batch policy



Step 6 Set a suspension policy.

Suspension policy: You can set the execution success rate. When the number of failed instances meets the number calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.

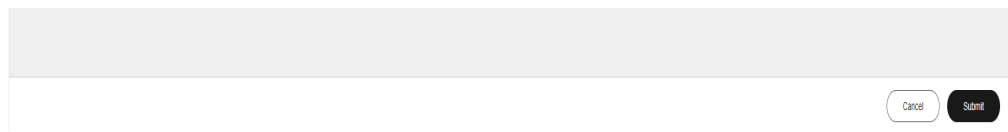
Figure 5-22 Setting a suspension policy

* Suspension Policy

If the success rate is lower than %, the alarm handling process is automatically paused for manual intervention.

Step 7 Click **Submit**.

Figure 5-23 Submitting the request



----End

5.2 Jobs

A job is a collection of operations. A job can contain one or more operations, such as restarting ECSs and executing scripts.

The **Jobs** module allows you to create, modify, clone, and delete public jobs and customized jobs, and perform the procedure defined in a job on target instances (Only ECS instances are supported currently).

5.2.1 Executing a Common Job

A list of public jobs are provided for you to execute common jobs on target instances.

Scenarios

Execute a common job on Cloud Operations Center.

Precautions

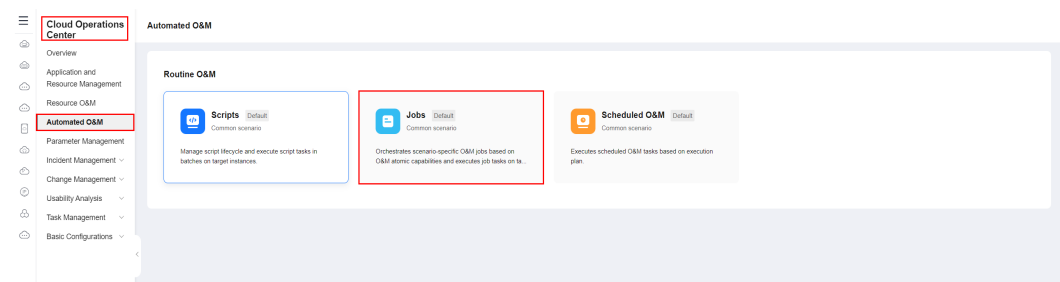
Before executing a common job, ensure that you have the resource permissions of target instances.

Procedure

Step 1 Log in to [COC](#).

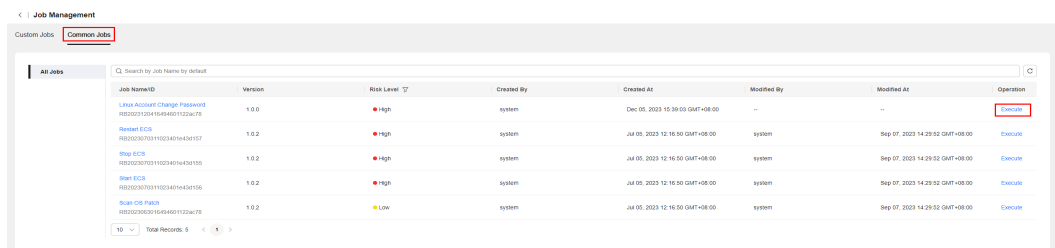
Step 2 In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-24 Clicking Jobs



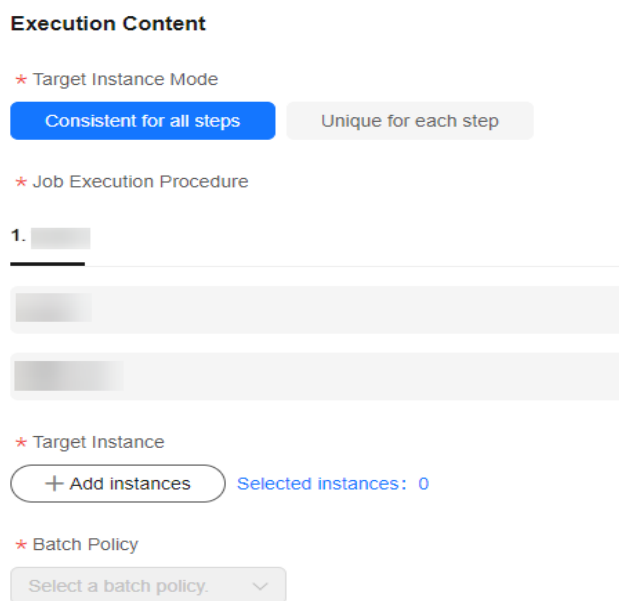
Step 3 Click the **Common Jobs** tab, click **All Jobs**, locate the public job to be executed, and click **Execute** in the **Operation** column.

Figure 5-25 Selecting and executing a common job



Step 4 Enter basic execution information, including the execution description and tag. You can create tags by following the instructions provided in [Tag Management](#).

Figure 5-26 Entering basic execution information



Step 5 Select **Target Instance Mode**. The options include **Consistent for all steps** and **Unique for each step**.

Table 5-3 Target instance mode description

| Mode | Description |
|--------------------------|--|
| Consistent for all steps | All steps are performed on the selected target instances. |
| Unique for each step | Custom configuration. A specified step is executed only on a specified instance. |

Figure 5-27 Consistent for all steps

Execution Content

* Target Instance Mode

Consistent for all steps Unique for each step

* Job Execution Procedure

1.

* Target Instance

Selected instances: 0

* Batch Policy

▾

Figure 5-28 Unique for each step

Execution Content

* Target Instance Mode

Consistent for all steps Unique for each step

* Job Execution Procedure

1.

^

* Target Instance

Selected instances: 0

* Batch Policy

▾

^

* Target Instance

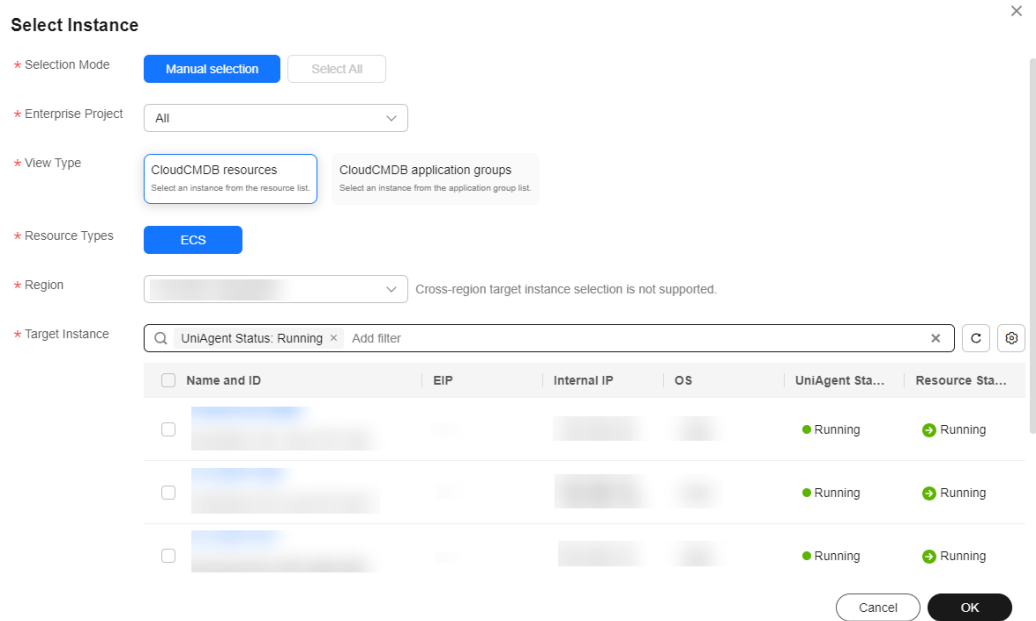
Selected instances: 0

* Batch Policy

▾

Step 6 Click **Add Instances**. In the displayed dialog box, select the target region, search for the target instances by name or UniAgent status and select them, click **OK**.

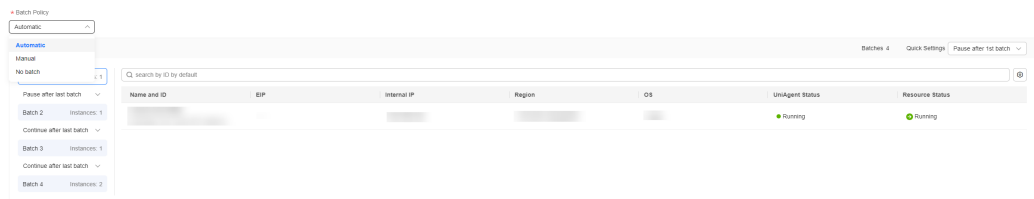
Figure 5-29 Selecting target instances



Step 7 Select a batch policy.

- **Automatic:** The selected instances are divided into multiple batches based on the default rule.
- **Manual:** You can manually divide instances into multiple batches as required.
- **No batch:** All instances to be executed are in the same batch.

Figure 5-30 Selecting a batch policy

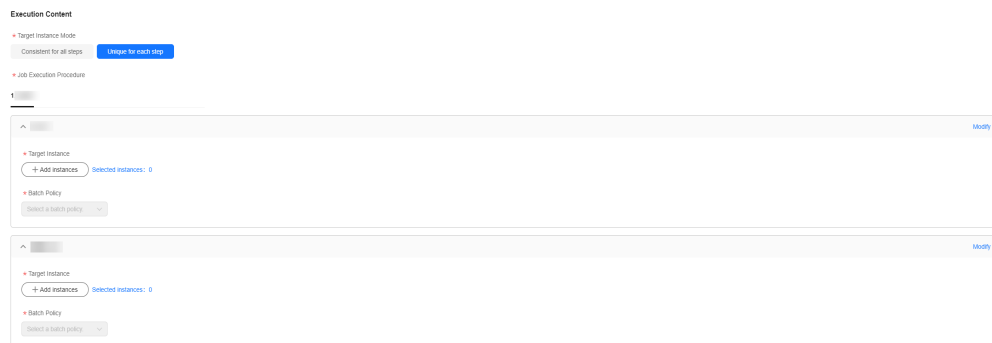


Step 8 Click **Submit** to execute the common job. The **Job Ticket Details** page is displayed. View the execution status of jobs and each batch on the details page.

Click **Forcibly End** to forcibly end all tasks of the current job.

Click **Terminate All** to end the execution tasks of all batches in the current step.

Figure 5-31 Job ticket details



----End

5.2.2 Creating a Custom Job

The custom job creation and step compilation capabilities are provided.

Scenarios

Create a custom job on Cloud Operations Center.

Precautions

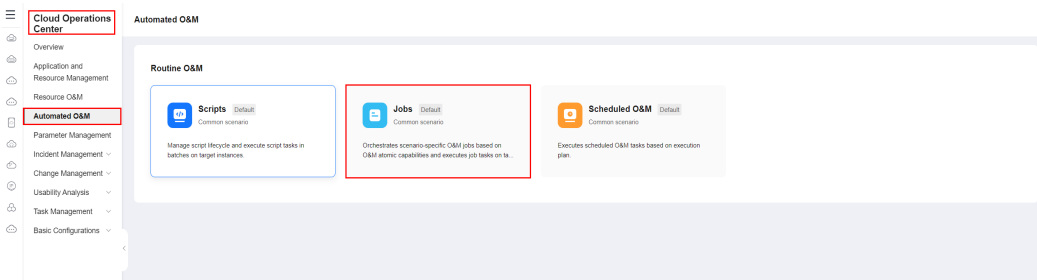
Confirm and fill in the risk level of the operation according to the operation procedure.

Procedure

Step 1 Log in to [COC](#).

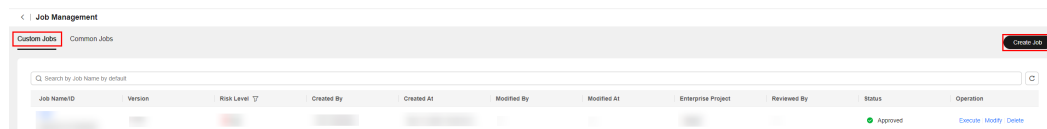
Step 2 In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-32 Job Management page



Step 3 Click **Custom Jobs** and click **Create Job**.

Figure 5-33 Clicking Create Job



Step 4 Enter the basic job information, including the job name, enterprise project, description, and tag. You can create tags by following the instructions provided in [Tag Management](#).

Figure 5-34 Entering basic job information

Basic Information

* Job

You are advised to name the job based on the application scenario provide

The task name can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).

* Enterprise Project

Select an enterprise project. ▾

* Version

1.0.0

Description

Describe the job application scenario or function.

0/500

Step 5 Select a job template. If no proper template is available, select **Custom**.

Figure 5-35 Selecting a job template

Template Select

Enter [Search] [Clear]

Custom
If no template is available, you can choose to customize

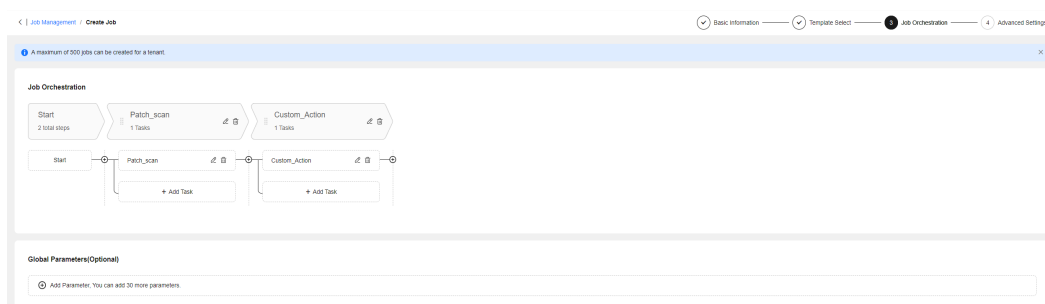
Reboot_and_Verify_ECS
1 Start — 2 Custom_Action — 3 Reboot_OS_of_ECS — 4 Sleep — 5 Custom_Action — 6 End

Routine_Scan
1 Start — 2 Patch_scan — 3 Custom_Action — 4 End

Custom_Action
1 Start — 2 Custom_Action — 3 End

Step 6 Orchestrate the job. Job orchestration includes global parameters and job steps.

Figure 5-36 Orchestrating a job



Step 7 Click **+Add Parameter** to add global parameters. After setting the parameters, click **OK**.

You can manually set the global parameters or obtain them from the parameter warehouse. If you select **Custom**, you need to enter the parameter name, preset value, and parameter description. If you select **Parameter Warehouse**, you need to select the region where the parameter is located, parameter name, and parameter association mode.

Figure 5-37 Selecting **Custom** and adding global parameters

Parameter1

Custom Parameter Warehouse

* Type

String Numeric Array

* Parameter

Enter

The parameter name consists of letters, digits, and underscores (_) with spaces excluded.

Preset Value

Enter

Description

Enter Description

0/200

OK Cancel

Figure 5-38 Obtaining and adding Global parameters from the parameter warehouse

Parameter1

Custom Parameter Warehouse

* Region

* Parameter

* Parameter association mode

Use the current parameter value in all environments

Parameter Value

Type

Description

Links

OK Cancel

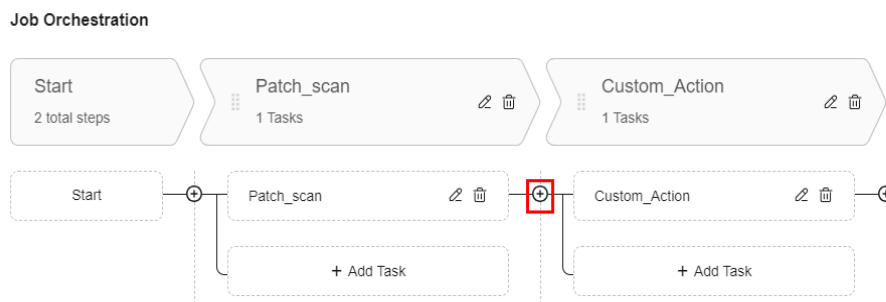
Table 5-4 Parameter association modes

| 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. |

| Parameter Association Mode | Description |
|---|--|
| 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 warehouse in real time. |

Step 8 Click  to add a new step.

Figure 5-39 Adding a step




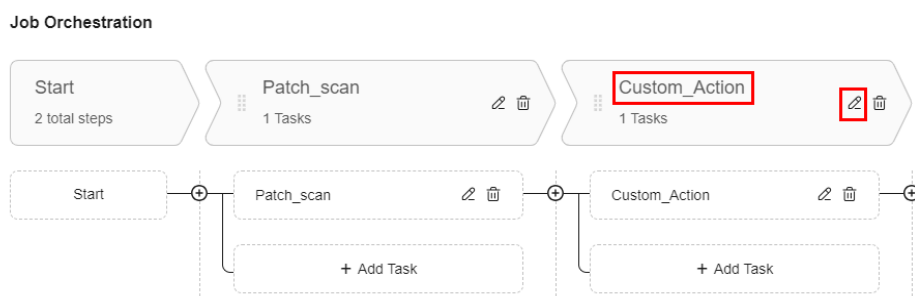
Step 9 Click the step name or  to change the step name.

Figure 5-40 Changing the step name




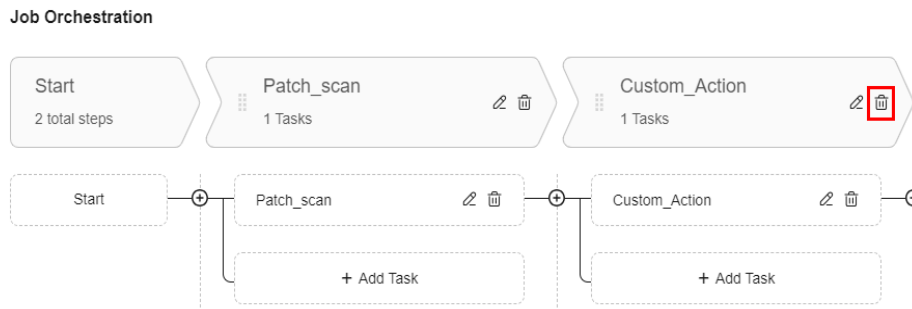
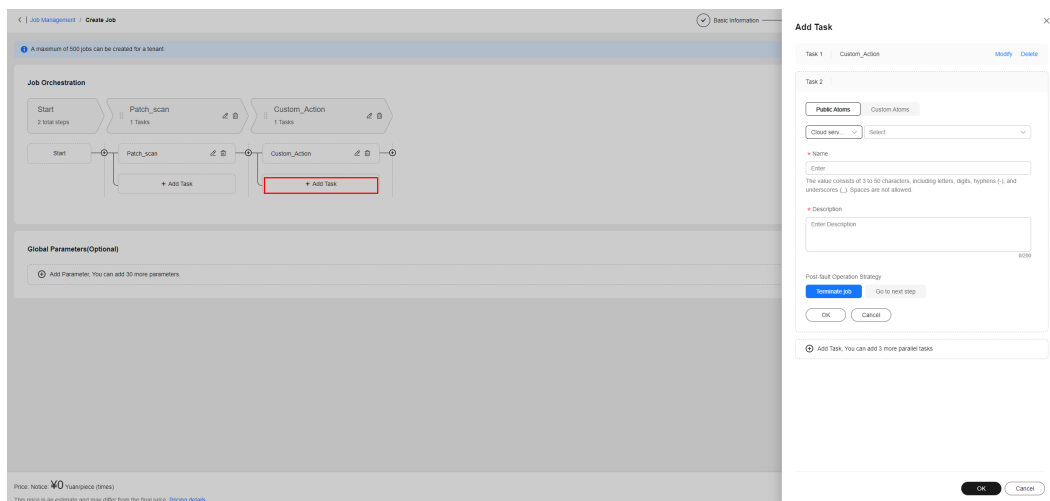
Step 10 If there are unnecessary steps, click  to delete them.

Figure 5-41 Deleting steps



Step 11 Click **+Add Task** to add a task for the step. After the task is added, click **OK**. After all tasks are added, click **OK**.

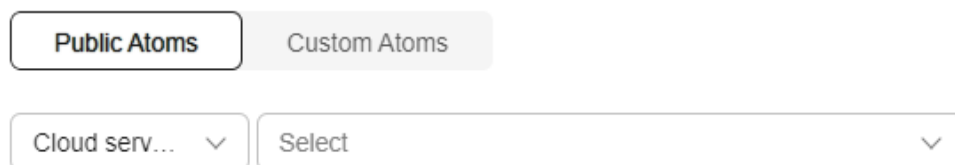
Figure 5-42 Adding tasks



Step 12 Set the operation type of the current task. The operation types are classified into public atoms and customized atoms.

- **Public atoms:** include control atoms and cloud service API atoms. Cloud service APIs support ECS operation atoms. For details, see ECS Operations.
- **Custom atoms:** You can select a custom script type. After a custom script is created, a custom atom record is automatically registered.

Figure 5-43 Selecting an operation type



Step 13 Based on the selected operation type, enter basic information such as the name and operation description, parameter information, and exception handling policy, and click **OK**.

Figure 5-44 Setting task information

The screenshot shows a form for setting task information. At the top, there are two tabs: "Public Atoms" (active) and "Custom Atoms". Below the tabs are two dropdown menus: "Cloud serv..." and "Select". A red asterisk indicates a required field for "Name", with a text input field containing "Enter". Below the "Name" field is a note: "The value consists of 3 to 50 characters, including letters, digits, hyphens (-), and underscores (_). Spaces are not allowed." Another red asterisk indicates a required field for "Description", with a text area containing "Enter Description" and a character count of "0/200". Below the description field is the "Post-fault Operation Strategy" section, which includes two buttons: "Terminate job" (blue) and "Go to next step" (grey). At the bottom of the form are two buttons: "OK" and "Cancel".

Step 14 After the job orchestration is complete, determine the risk level of the job based on the operation risks.

Set the manual review policy for job. Manual review is enabled by default for a job whose risk level is high.

If you select **Shift** for **Reviewer**, the users in the current schedule are reviewers. If you select **Individual**, some users are specified as reviewers.

If **Notification Mode** is set, the review request will be sent to the reviewer through the specified channel.

Figure 5-45 Advanced settings

Advanced Settings

* Risk Level

High Medium Low

Manual Review

* Reviewer

Shift Individual

Select Scenario Select Scheduling Role

A maximum of five approvers can be added. By default, the first five approvers in the shift schedule are selected. If no approver is selected for the shift schedule, you can add an approver individually.

* Notification Mode

Default

----End

5.2.3 Managing Custom Jobs

You can modify, clone, and delete recorded custom jobs.

Scenarios

Modify, clone, or delete a custom job on Cloud Operations Center.

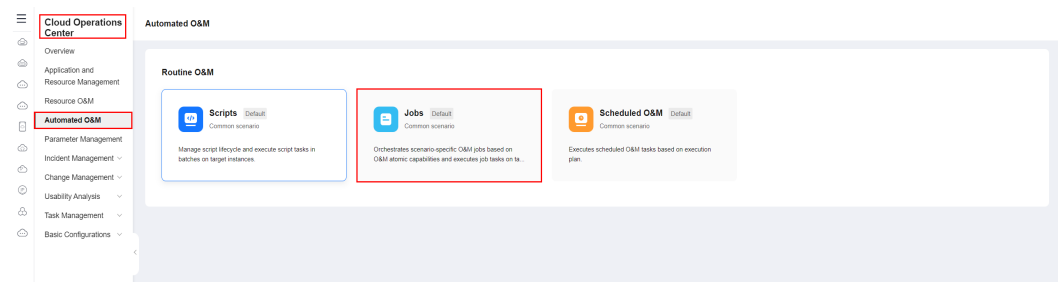
Precautions

When modifying or cloning a job, determine and fill out the risk level of the job.

Procedure

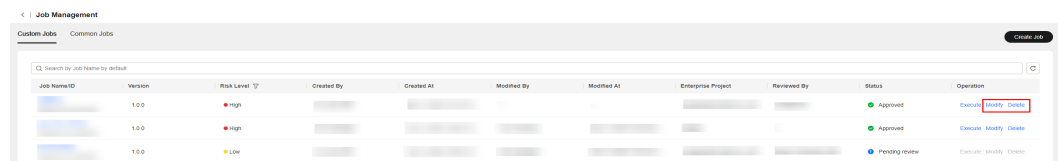
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-46 Job Management page



- Step 3** Select a job and click **Execute** in the **Operation** column.
- Modifying a job: Click **Modify** in the **Operation** column. For details, see section [Creating a Custom Job](#). Click **Cancel** to cancel the modification, click **Submit** to updating the job information and the job version number.
 - Cloning a job: Choose **More > Clone** in the **Operation** column. You can modify the cloned job based on the operations described in [Creating a Custom Job](#). You can click **Cancel** to cancel the modification. You can click **Submit** to create a job.
 - Deleting a job: Choose **More > Delete** in the **Operation** column
 - Modifying a tag: You can modify job tags by following the instructions provided in [Tag Management](#).

Figure 5-47 Performing operations on a job



----End

5.2.4 Executing a Custom Job

Execute recorded custom jobs.

Scenarios

Execute a custom job on Cloud Operations Center.

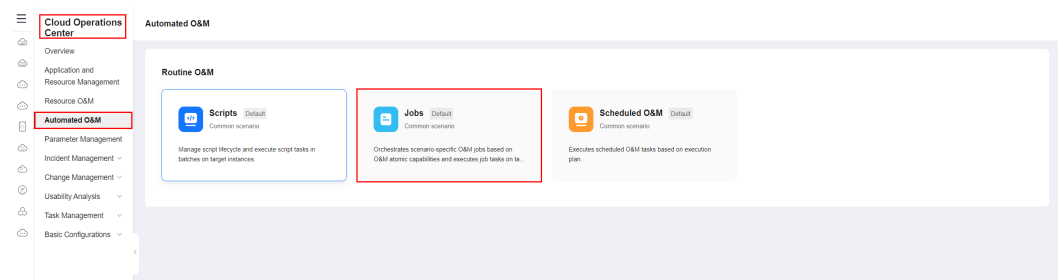
Precautions

Before executing a job, ensure that you have the resource permissions of target instances.

Procedure

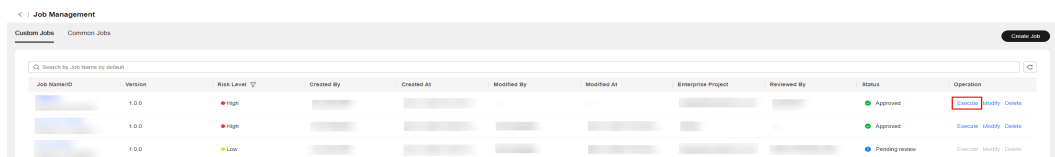
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-48 Job Management page



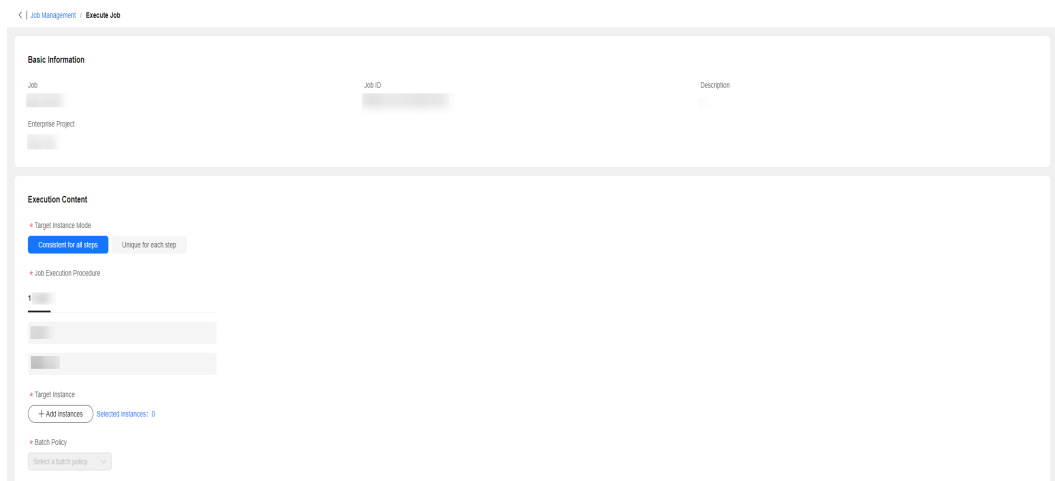
- Step 3** Select **Custom Jobs**, select the job to be executed, and click **Execute**.

Figure 5-49 Selecting the job to be executed



Step 4 Select a job version number and check whether the job steps meet the expectation.

Figure 5-50 Checking the job steps



Step 5 Enter basic execution information, including the execution description and tag. You can create tags by following the instructions provided in [Tag Management](#).

Figure 5-51 Entering basic execution information

Execution Description

Enter the execution description of the job.

0/500

Tag ?

[Refresh Label Data](#) ↻

[+ Add](#)

You can add 20 more tags.

Step 6 Select the execution mode of the job on the target instance. The options are **Consistent for all steps** and **Unique for each step**.

Table 5-5 Target instance mode description

| Target Instance Mode | Description |
|--------------------------|--|
| Consistent for all steps | All steps in this job are performed on the target instance in sequence. |
| Unique for each step | Customized configuration. You can configure that the specified step is executed only on the specified target instance. |

Figure 5-52 Selecting **Consistent for all steps**

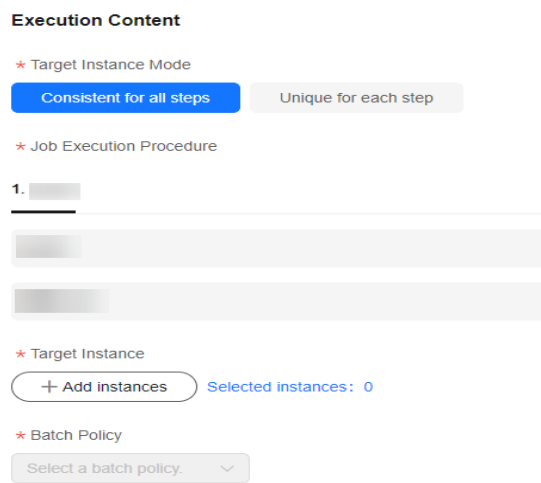
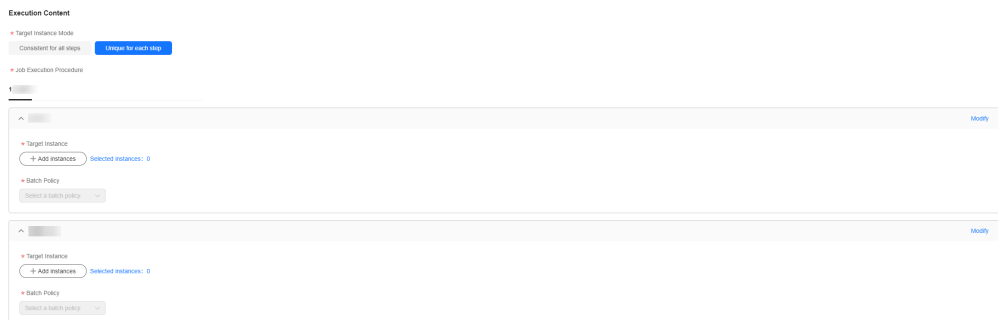
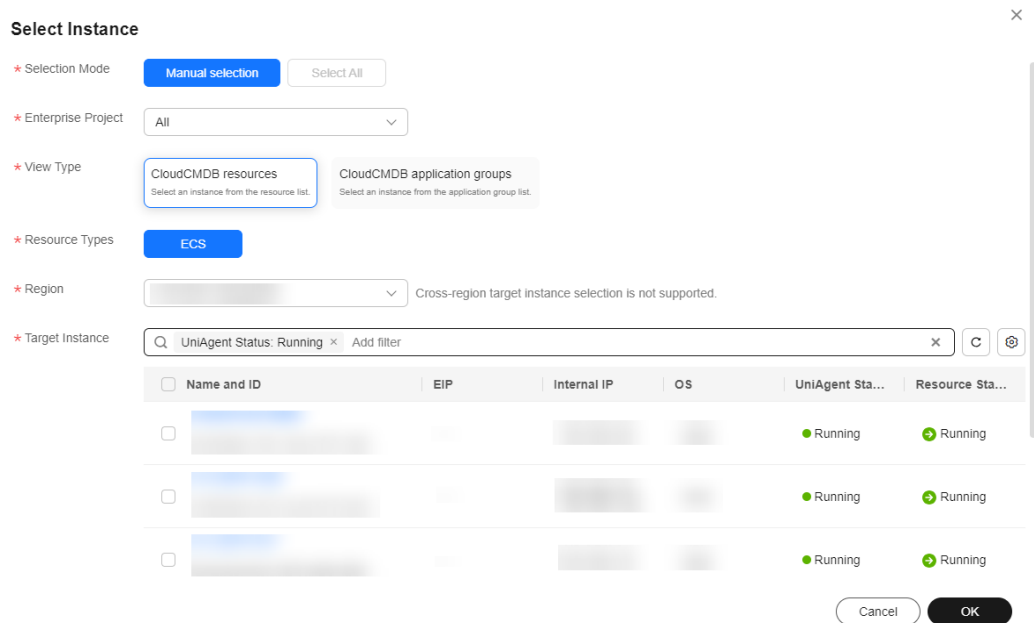


Figure 5-53 Selecting **Unique for each step**



Step 7 Click **Add Instances**. In the displayed dialog box, select the target region, search for the target instances by name or UniAgent status and select them, click **OK**.

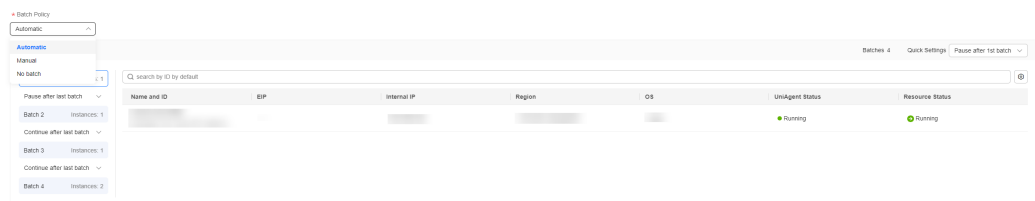
Figure 5-54 Selecting the target instance



Step 8 Select a batch policy.

- **Automatic:** The selected instances are divided into multiple batches based on the default rule.
- **Manual:** You can manually divide instances into multiple batches as needed.
- **No batch:** All target instances are in the same batch.

Figure 5-55 Selecting a batch policy

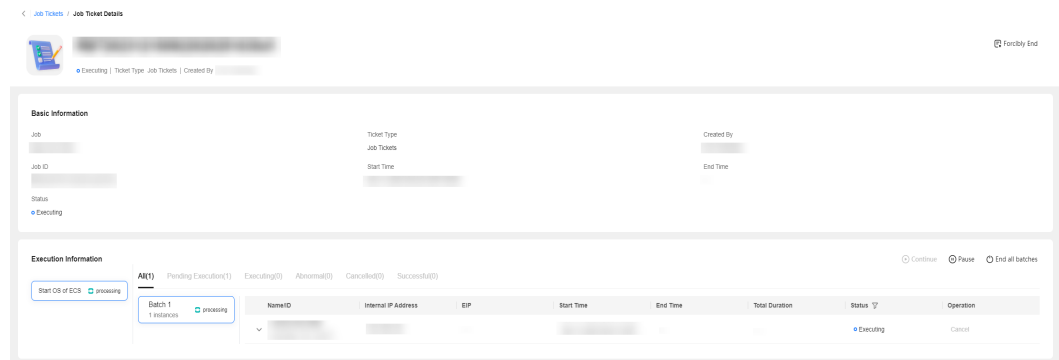


Step 9 Click **Submit** to execute the custom job. The **Job Ticket Details** page is displayed. View the execution status of jobs and each batch on the details page.

Click **Forcibly End** to forcibly end all tasks of the current job.

Click **Terminate All** to end the execution tasks of all batches in the current step.

Figure 5-56 Job ticket details



----End

5.2.5 Managing Tags

You can add tags to user-defined jobs and service tickets.

Scenarios

Add tags to a user-defined job or job ticket on COC.

Adding a Tag



- Step 1** Click **Add Tag** and enter the tag key and tag value.
- Step 2** Click **Delete** on the right of an added tag to delete the tag.
- Step 3** Click  to refresh predefined tag data.

Figure 5-57 Adding a tag

Tag

If you want to use the same tag to identify multiple cloud resources, that is, you can select the same tag for all services, you are advised to create a predefined tag in TMS. [View Predefined Tags](#) 

You can add 19 more tags.

----End

Editing a Tag


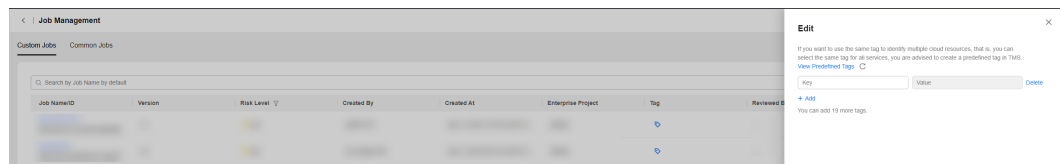
- Step 1** In the job list, click  of a job to edit the tag of the job.
- Step 2** Follow the procedure for [creating a tag](#) and click **OK**.

Figure 5-58 Editing a tag



----End

5.3 Scheduled O&M

Scheduled O&M allows users to execute specific scripts or jobs on certain instances as scheduled or periodically.

5.3.1 Scheduled Task Management

Creating a Scheduled Task

Step 1 Log in to **COC**.

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

Figure 5-59 Scheduled O&M

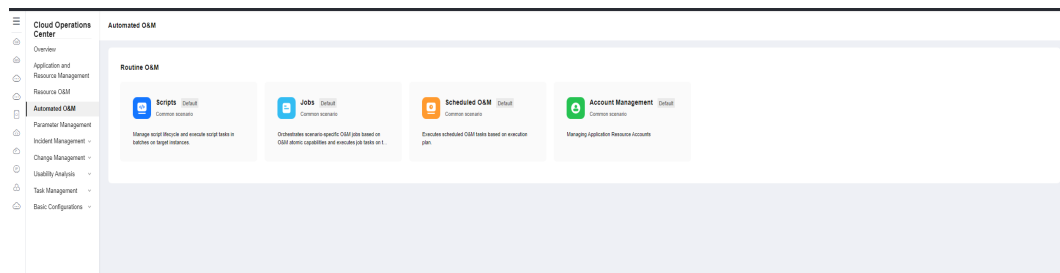
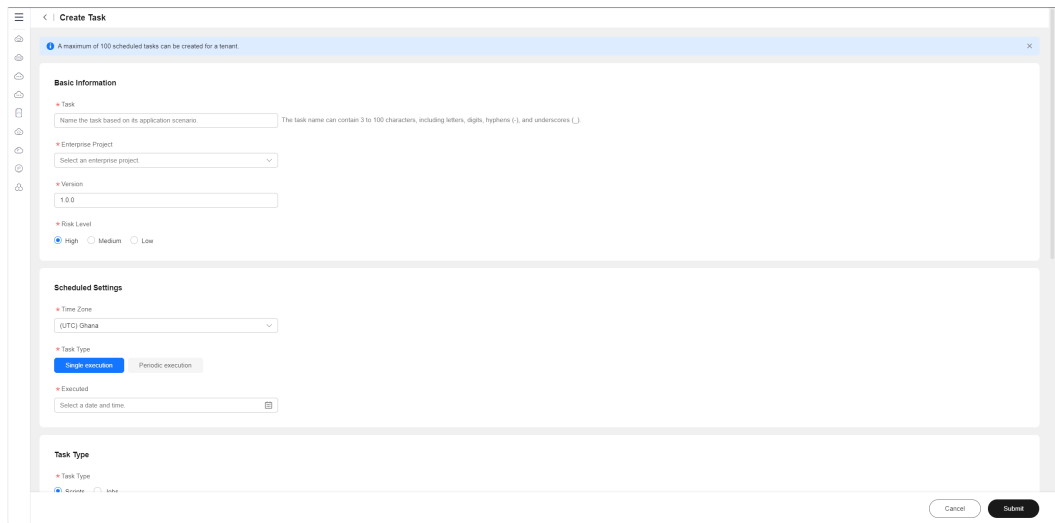


Figure 5-60 Scheduled task list

| Task ID | Task Type | Enterprise Project | Referenced Task | Risk Level | Execution Times | Created By | Reviewed By | Status | Last Executed | Last Execution S... | Enabled Status | Operation |
|---------|---------------------|--------------------|-----------------|------------|-----------------|------------|-------------|----------------|--------------------|---------------------|----------------|---------------------|
| | One-time execut... | default | Jobs | Low | 1 | | | Normal | Jan 02, 2024 09... | Successful | Unenabled | Enable Modify More |
| | One-time execut... | COC | Scripts | Low | 1 | | | Normal | Dec 26, 2023 16... | Successful | Enabled | Disable Modify More |
| | One-time execut... | default | Jobs | Low | 4 | | | Normal | Dec 26, 2023 21... | Successful | Enabled | Disable Modify More |
| | Periodic executi... | -- | Jobs | High | 8 | | | Normal | Jan 03, 2024 03... | Abnormal | Enabled | Disable Modify More |
| | One-time execut... | default | Jobs | Low | 3 | | | Normal | Dec 26, 2023 19... | Abnormal | Unenabled | Enable Modify More |
| | Periodic executi... | -- | Jobs | High | 8 | | | Normal | Jan 03, 2024 03... | Abnormal | Enabled | Disable Modify More |
| | One-time execut... | default | Scripts | High | 0 | | | Normal | -- | -- | Unenabled | Enable Modify More |
| | One-time execut... | -- | Jobs | High | 0 | | | Pending review | -- | -- | Unenabled | Enable Modify More |
| | One-time execut... | default | Jobs | High | 0 | | | Normal | -- | -- | Unenabled | Enable Modify More |
| | One-time execut... | default | Jobs | High | 1 | | | Normal | -- | -- | Enabled | Disable Modify More |

Step 3 Click **Create Task**.

Figure 5-61 Creating a scheduled task



Step 4 Enter the basic information about the scheduled task. [Table 5-6](#) describes the required parameters.

Figure 5-62 Entering basic information



Table 5-6 Parameters

| Parameter | Description |
|--------------------|---|
| Task | Mandatory. The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_). |
| Enterprise Project | Mandatory. The drop-down data source is maintained by Enterprise Project Management. |
| Version | Mandatory. Version number of version management. |

| Parameter | Description |
|------------|---|
| Risk Level | <p>Mandatory.</p> <p>There are three risk levels:</p> <ul style="list-style-type: none"> • High • Medium • Low <p>NOTE If high risk is selected, manual review is enabled by default.</p> |

Step 5 Set the time zone. If you select **Single execution**, select the task execution time. If you select **Periodic execution**, the **Simple Cycle** and **Cron** options are displayed, allowing you to customize the execution period. The scheduled task is executed periodically based on the customized execution period, until the rule expires. [Table 5-7](#) describes the required parameters.

Figure 5-63 Scheduled Settings

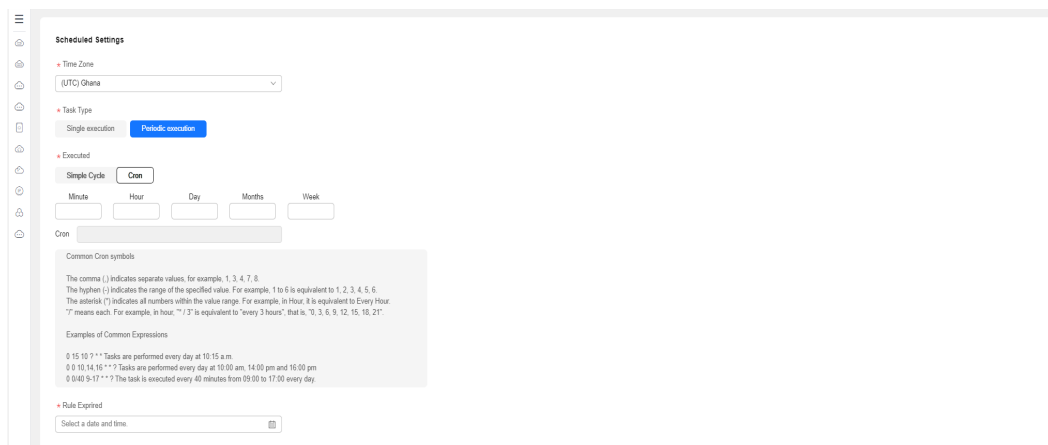


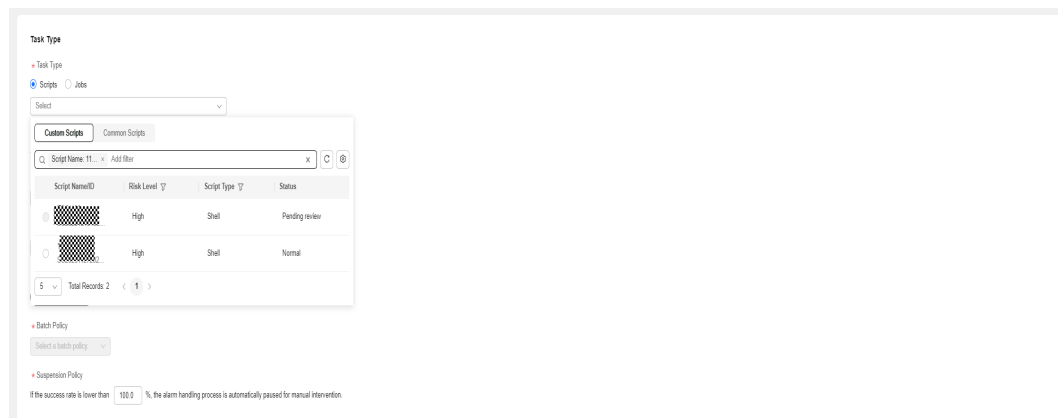
Table 5-7 Parameters

| Parameter | Sub-parameter Name | Description |
|-----------|--------------------|---|
| Time Zone | - | <p>Mandatory.</p> <p>The scheduled task is executed based on the time zone.</p> |
| Task Type | Single execution | Execute the scheduled task at the specified time. |
| | Periodic execution | Execute the task based on the specified rule until the rule expires. |

| Parameter | Sub-parameter Name | Description |
|--------------|--------------------|--|
| Executed | - | <p>This parameter is used together with the task type.</p> <ul style="list-style-type: none"> For a single execution, set this parameter to the execution time. For periodic execution, the following two modes are available: <ul style="list-style-type: none"> Simple Cycle Cron |
| Rule Expired | - | <p>If you select Periodic execution, you need to configure the rule expiration time.</p> |

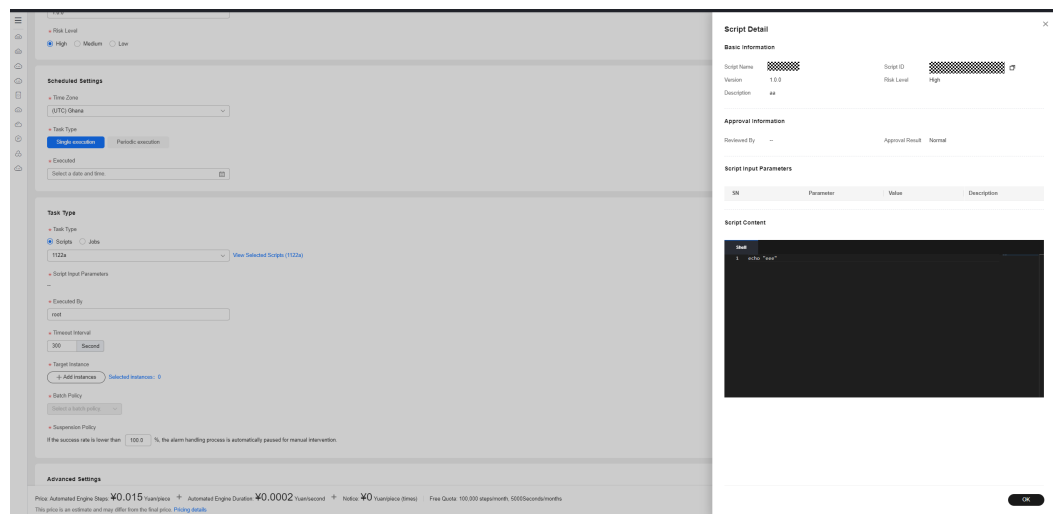
Step 6 a. Enter the task type. If you select **Scripts**, search for a desired script by keyword from the drop-down script lists. Select the desired script.

Figure 5-64 Task Type



b. Click **View Selected Scripts**. The script details are displayed on the right.

Figure 5-65 Script Details



c. Default script parameters are displayed in **Script Input Parameters**. You can select **Sensitive** to determine whether to display the parameters in plaintext. You can click the text box to edit the parameter values.

d. Enter the execution user and the timeout interval.

e. Select instances: **Manual selection**: manually select instances. **Select All**: Select all instances associated with a single region or application.

Manual selection: Click add instance. The select Instance dialog box is displayed. If you select **Manual selection**, search for the target instance list based on the enterprise project, view type, resource type, region, and target instance search boxes. Select the check box before the instance list and click **OK**. Only instances whose UniAgent status is running can be selected.

Figure 5-66 Manually selecting instances (CloudCmdb Resource)

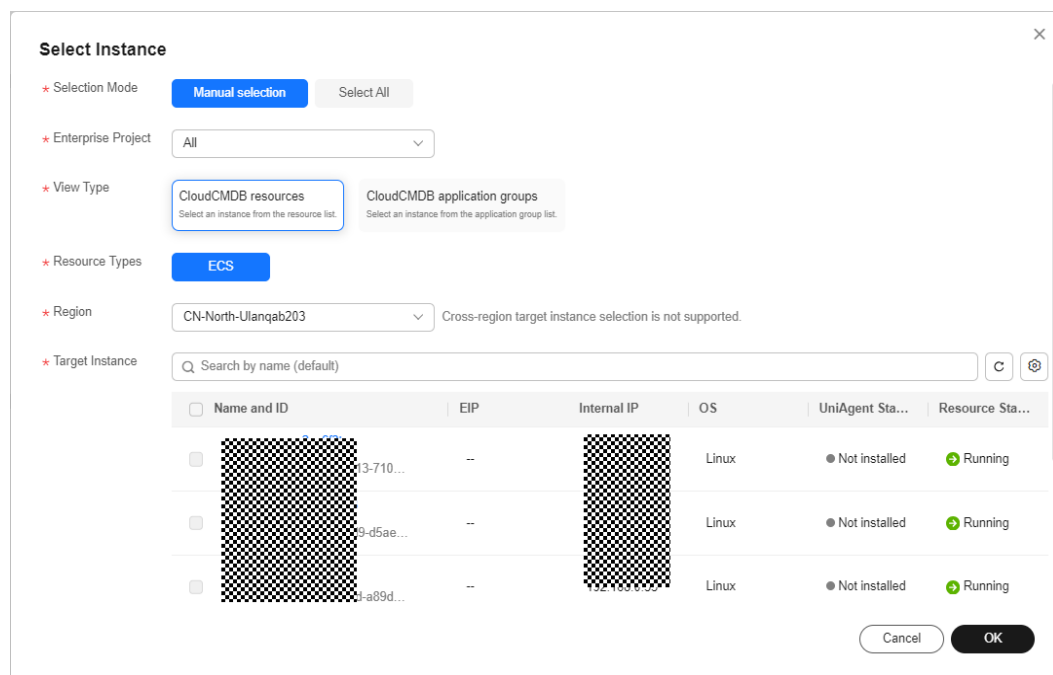
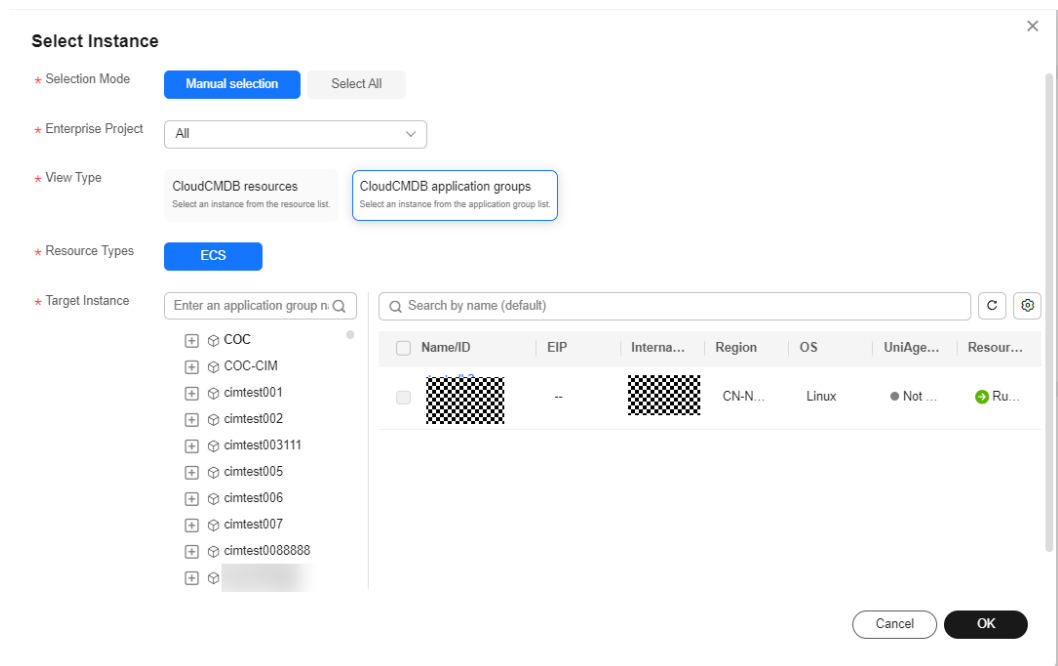


Figure 5-67 Manually selecting instances (CloudCmdb application groups)



Select All: Determine the target instance based on the search criteria such as Enterprise Project, View Type, Resource Type, Region, and Target Instance. The list displays the instances that meet the current filter criteria. When a scheduled task is executed, the system queries the target instances in real time based on the selected filter criteria and executes the scheduled task. By default, UniAgent status is running.

Figure 5-68 Selecting All (CloudCmdb resources)

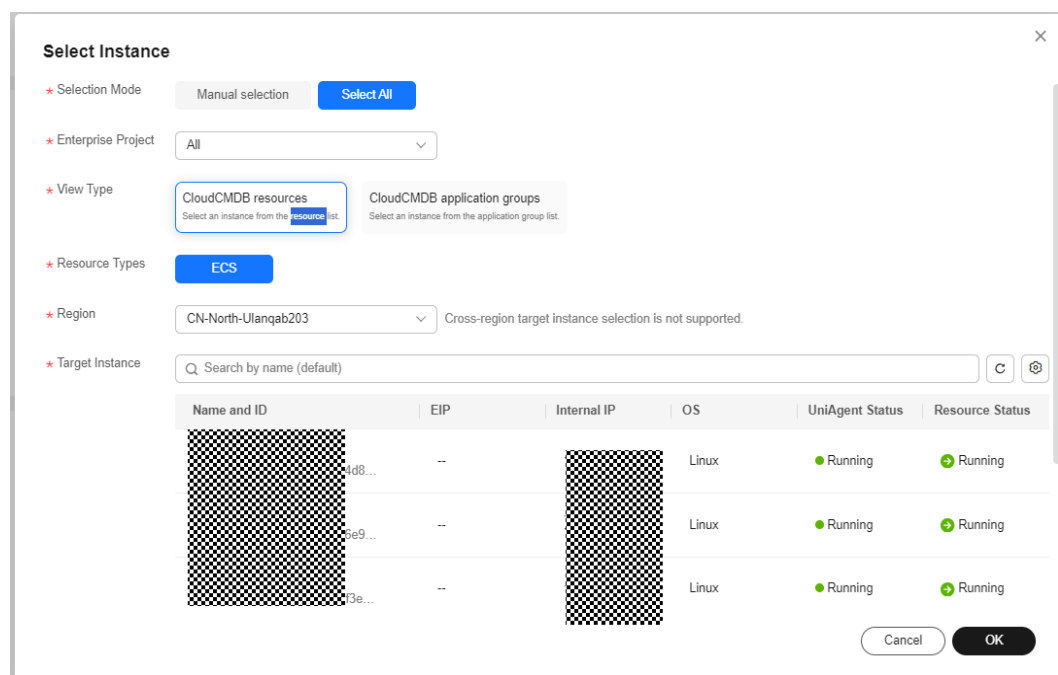
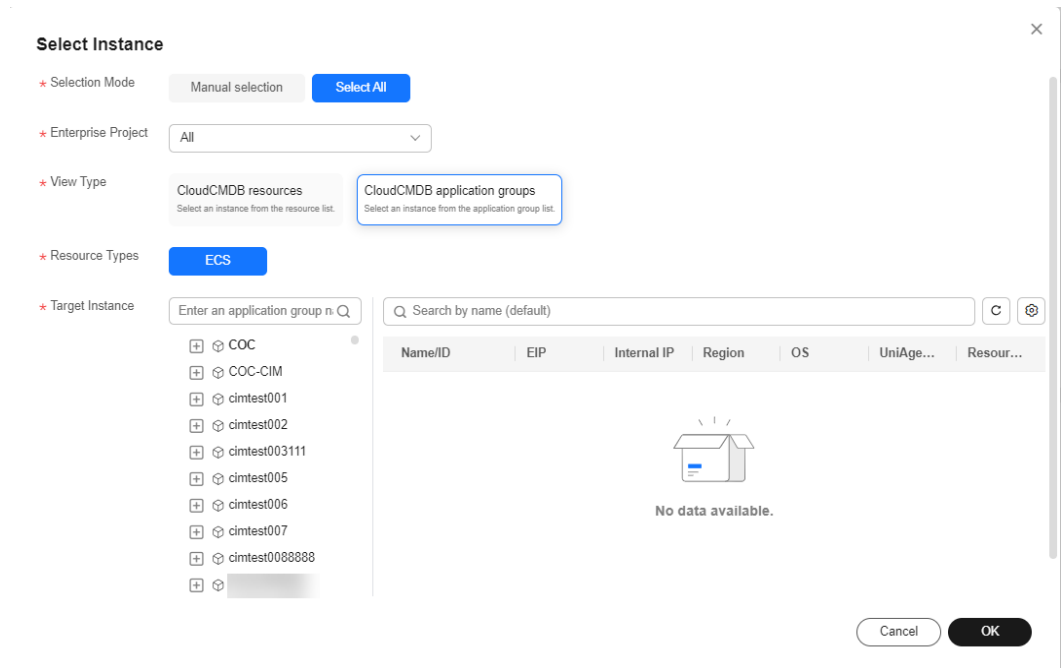


Figure 5-69 Selecting All (CloudCmdb Application groups)



f. Select the batch policy and suspension policy. If **Select All** is selected, the batch processing is automatically performed by default.

Figure 5-70 No batch

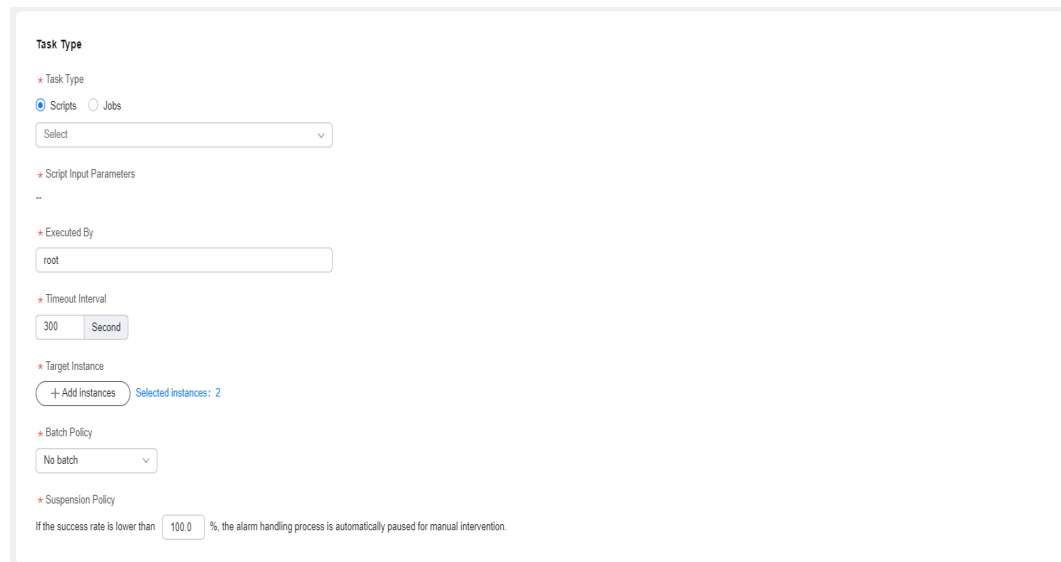
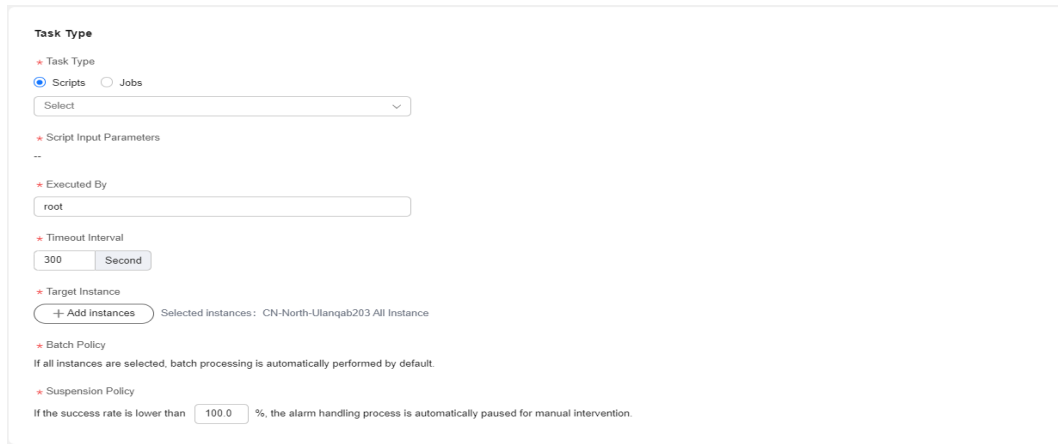
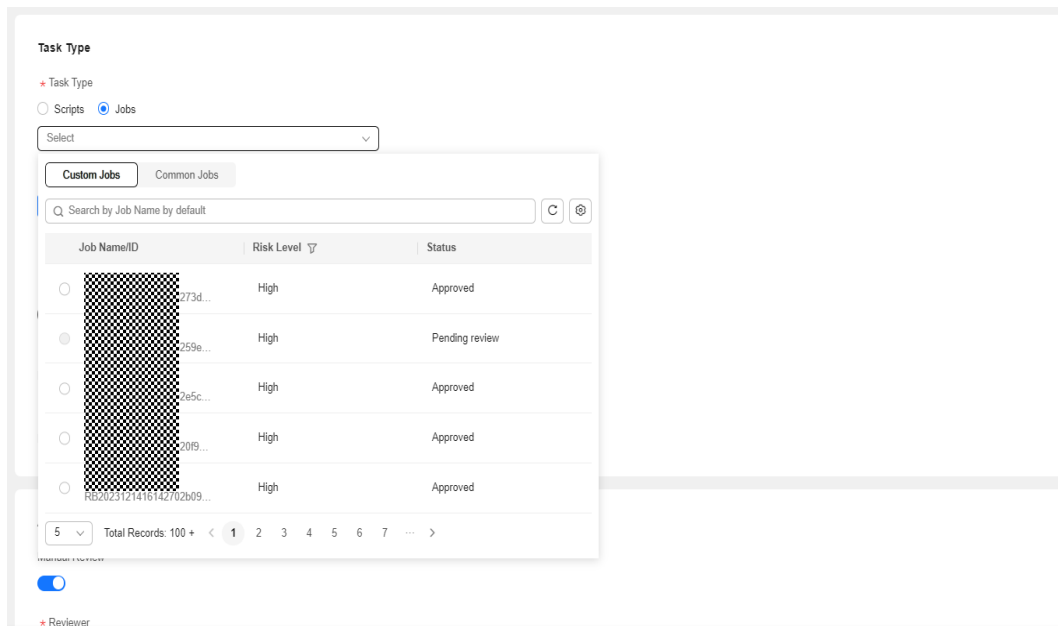


Figure 5-71 Automatic batch



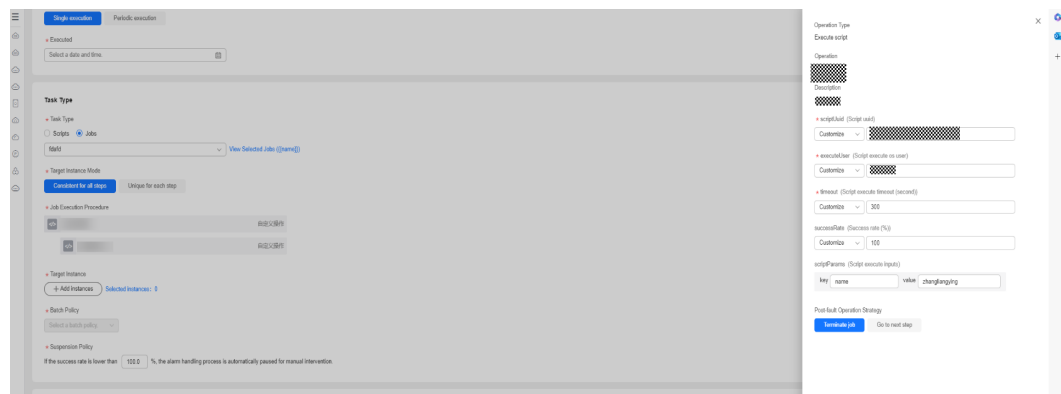
Step 7 a. Enter the task type. If you select **Jobs**, click the text box, and select custom jobs or common jobs by searching for the desired job name. Select the desired job.

Figure 5-72 Selecting Jobs



b. Click **View Selected Jobs**. The job details dialog box is displayed on the right.

Figure 5-73 Viewing job details



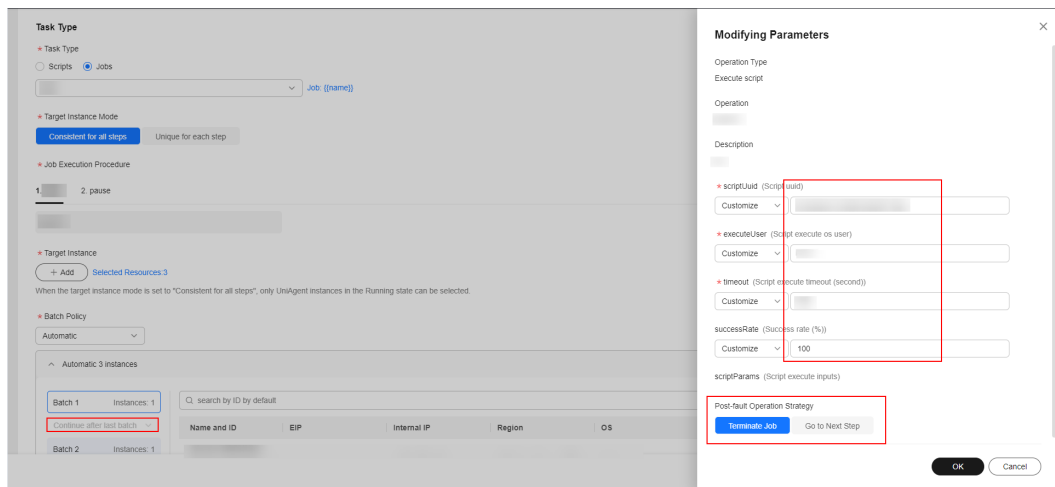
c. Select the target instance mode. If you select **Unique for each step**, you can set the target instance and batch policy for each job step.

Figure 5-74 Selecting **Unique for each step**



d. Modify job execution parameters. Click a job step name. The job step details are displayed on the right. Enter the success rate threshold, select the batch execution policy, select the post-fault operation strategy, and click **OK**.

Figure 5-75 Modifying job execution parameters

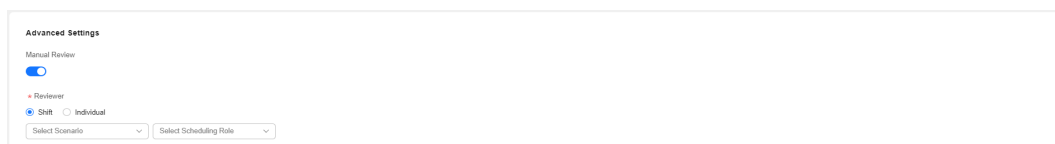


e. Select an instance. **Manual selection:** Manually select instances. **Select All:** Select all instances associated with a single region or application.

f. Select the batch policy and suspension policy.

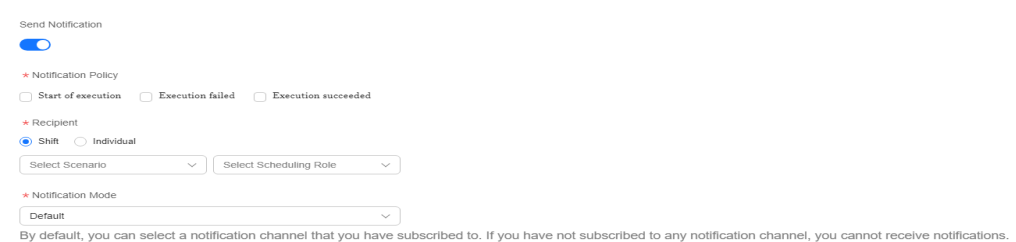
Step 8 You can select whether to manually review task.

Figure 5-76 Enabling manual review



Step 9 Determine whether to enable notification. If you enable notification, select the notification policy, notification object, and channel.

Figure 5-77 Setting notifications



Step 10 Click **Submit**.

NOTE

You can set the jobs and scripts to be executed on the **Automated O&M > Scripts** page or **Automated O&M > Jobs** page.

----End

Viewing a Scheduled Task

Step 1 Log in to [COC](#).

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

Figure 5-78 Scheduled tasks

| TaskID | Task Type | Enterprise Project | Referenced Task Type | Risk Level | Execution Times | Created By | Reviewed By | Status | Last Executed | Last Execution Status | Enabled Status | Operation |
|--------------------------|--------------------------|--------------------|----------------------|------------|-----------------|------------|-------------|----------------|----------------------|-----------------------|----------------|---------------------|
| Periodic-execution(CR... | Periodic-execution(CR... | - | Jobs | High | 1 | | | Normal | - | - | Enabled | Disable Modify More |
| Periodic-execution(CR... | Periodic-execution(CR... | - | Jobs | High | 0 | | | Normal | - | - | Unenabled | Enable Modify More |
| Periodic-execution(CR... | Periodic-execution(CR... | - | Jobs | High | 1 | | | Normal | - | - | Enabled | Disable Modify More |
| Periodic-execution(CR... | Periodic-execution(CR... | - | Jobs | High | 1 | | | Normal | - | - | Enabled | Disable Modify More |
| Periodic-execution(CR... | Periodic-execution(CR... | - | Jobs | High | 1 | | | Normal | - | - | Enabled | Disable Modify More |
| One-time-execution | One-time-execution | default | Jobs | High | 1 | | | Normal | Dec 14, 2023 9:16:49 | Successful | Enabled | Disable Modify More |
| One-time-execution | One-time-execution | default | Scripts | High | 0 | | | Pending review | - | - | Unenabled | Enable Modify More |
| One-time-execution | One-time-execution | COC-TLB | Scripts | High | 0 | | | Pending review | - | - | Unenabled | Enable Modify More |

Step 3 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Step 4 Click a task name to view the scheduled task details.

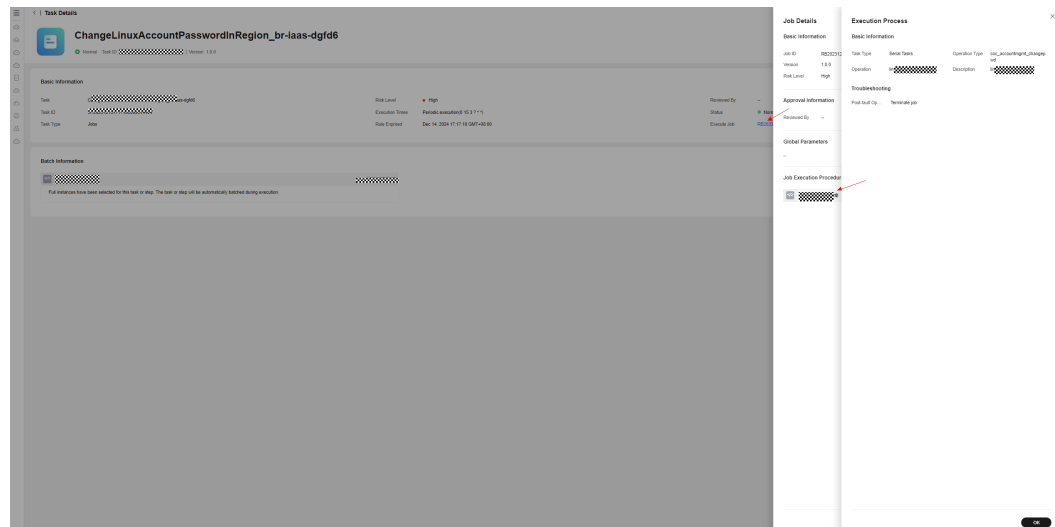
Figure 5-79 Viewing task details

| Basic information | | | |
|-------------------|--|-----------------|---------------------------------|
| Task | ChangeLinuxAccountPasswordInRegion_br-iaas-dgfd6 | Risk Level | High |
| Task ID | XXXXXXXXXXXXXXXXXXXX | Execution Times | Periodic-execution(15.311*) |
| Task Type | Jobs | Rule Expired | Dec 14, 2024 17:17:16 GMT+08:00 |
| Reviewed By | XXXXXXXXXX | Status | Normal |
| Executed Job | XXXXXXXXXX | | |

| Batch information | |
|---|------------|
| Batch ID | XXXXXXXXXX |
| Full instances have been selected for this task or step. The task or step will be automatically batched during execution. | |

Step 5 On the scheduled task details page, click the script or job ID. The script or job details are displayed on the right.

Figure 5-80 Script or job details



NOTE

System tenants are isolated. Only scheduled tasks created by tenant accounts or sub-accounts can be viewed.

----End

Enabling and Disabling a Scheduled Task

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Automated O&M > Scheduled O&M**.
- Step 3** Locate a target task, and click **Enable** or **Disable** in the **Operation** column to enable or disable a scheduled task.

Figure 5-81 Viewing task list

| TaskID | Task Type | Enterprise Project | Referenced Task | Risk Level | Execution Times | Created By | Reviewed By | Status | Last Executed | Last Execution S... | Enabled Status | Operation |
|--------|--------------------|--------------------|-----------------|------------|-----------------|------------|-------------|----------------|--------------------|---------------------|----------------|---------------------|
| | One-time execut... | | Scripts | High | 0 | | | Normal | | | Unenabled | Enable Modify More |
| | One-time execut... | | Scripts | High | 0 | | | Pending review | | | Unenabled | Enable Modify More |
| | Periodic execut... | | Jobs | High | 1 | | | Normal | | | Enabled | Disable Modify More |
| | Periodic execut... | | Jobs | High | 0 | | | Normal | | | Unenabled | Enable Modify More |
| | Periodic execut... | | Jobs | High | 1 | | | Normal | | | Enabled | Disable Modify More |
| | Periodic execut... | | Jobs | High | 1 | | | Normal | | | Enabled | Disable Modify More |
| | Periodic execut... | | Jobs | High | 1 | | | Normal | | | Enabled | Disable Modify More |
| | One-time execut... | | Jobs | High | 1 | | | Normal | Dec 14, 2023 09... | Successful | Enabled | Disable Modify More |
| | One-time execut... | | Scripts | High | 0 | | | Pending review | | | Unenabled | Enable Modify More |
| | One-time execut... | | Scripts | High | 0 | | | Pending review | | | Unenabled | Enable Modify More |

NOTE

1. Users can enable or disable only the scheduled tasks created by themselves. You can view scheduled tasks created by other users under the current tenant account.
2. 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 is deleted from the background and will not be executed.

----End

Editing a Scheduled Task

Step 1 Log in to [COC](#).

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

Step 3 Click **Modify** in the **Operation** column of a scheduled task. On the displayed page, modify the scheduled task information. Click **Submit**.

Figure 5-82 Modifying a scheduled task

The screenshot shows the 'Modify Task' page with the following details:

- Basic Information:**
 - Task: [Input field]
 - Enterprise Project: [Dropdown menu]
 - Version: [Input field]
 - Risk Level: High Medium Low
- Scheduled Settings:**
 - Time Zone: [Dropdown menu]
 - Task Type: Single execution Periodic execution
 - Executed: [Input field]
- Task Type:**
 - Task Type: Scripts Jobs
 - View Selected Scripts: [Button]
- Pricing Summary:**
 - Price: Automated Engine Step: ¥0.015 Yuan/step + Automated Engine Duration: ¥0.0002 Yuan/second + Notice: ¥0 Yuan/step (times) + Free Quota: 100,000 steps/month, 5000Seconds/month
 - Buttons: Cancel, Submit

NOTE

1. Only scheduled tasks in the pending review or disabled state can be modified.
2. After a scheduled task is modified and enabled again, it will be executed at the new execution time.

----End

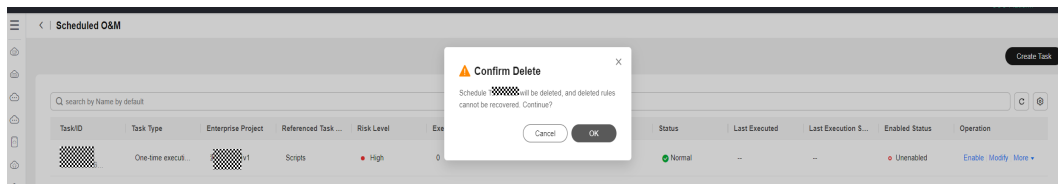
Deleting a Scheduled Task

Step 1 Log in to [COC](#).

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

Step 3 Locate the target task, click **More** in the **Operation** column, and click **Delete**. In the displayed confirmation dialog box, click **OK** to delete the scheduled task.

Figure 5-83 Deleting a scheduled task



NOTE

Only disabled scheduled tasks can be deleted.

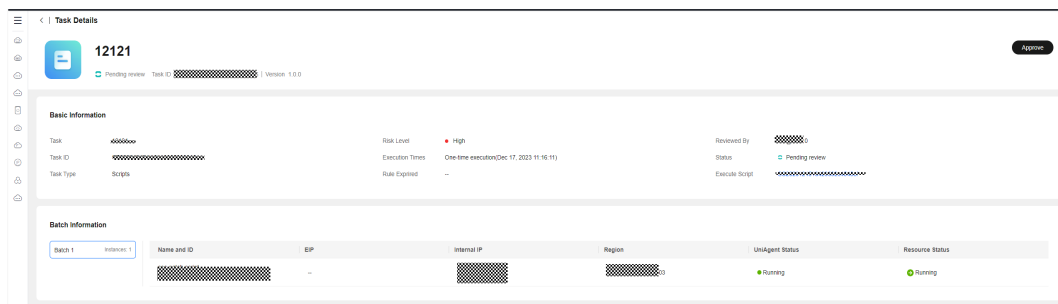
----End

Reviewing Scheduled O&M Tasks

Step 1 Log in to **COC**.

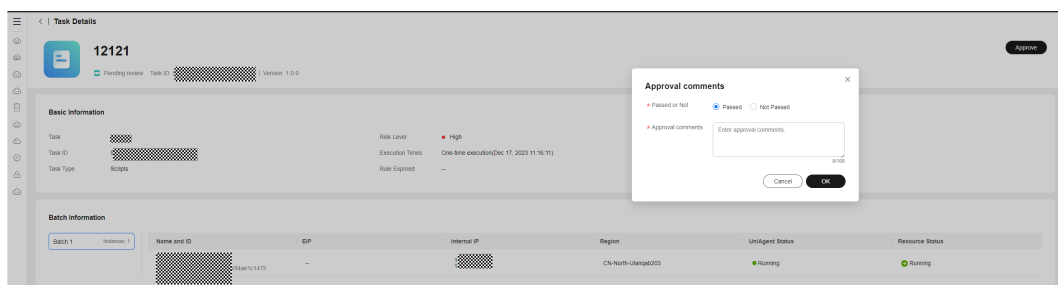
Step 2 In the navigation pane on the left, choose **Automated O&M > Scheduled O&M**. Select a record whose status is **Pending review** and click the task name.

Figure 5-84 Reviewing a scheduled task



Step 3 Click **Review** in the upper right corner. In the displayed dialog box, select the review result and enter review comments. Click **OK**.

Figure 5-85 Reviewing a scheduled task



NOTE

Only the task whose reviewer is the current login account can be reviewed. Only approved scheduled tasks can be enabled.

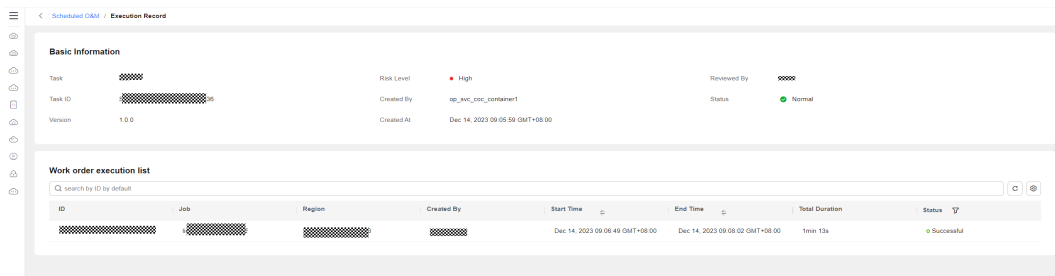
----End

5.3.2 Scheduled Task Execution Records

View the execution records of a scheduled task.

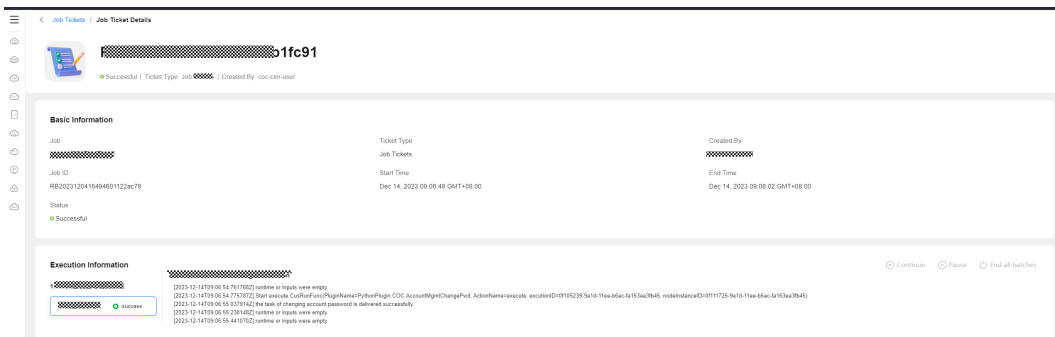
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Automated O&M > Scheduled O&M**.
- Step 3** Locate the target task, and click **More** in the **Operation** column, and then click **Execution Record** in the displayed dialog box.

Figure 5-86 Viewing task execution information



- Step 4** Click the ID in the service ticket execution list to go to the corresponding script or job service ticket details page. For details about how to perform operations on the script service ticket page, see Job Tickets or Script Tickets.

Figure 5-87 Job execution details



----End

6 Parameter Management

6.1 Parameter Center

6.1.1 Creating a Parameter

Scenarios

You can manage real-time parameters and manage the full lifecycle of text parameters and encrypted data.

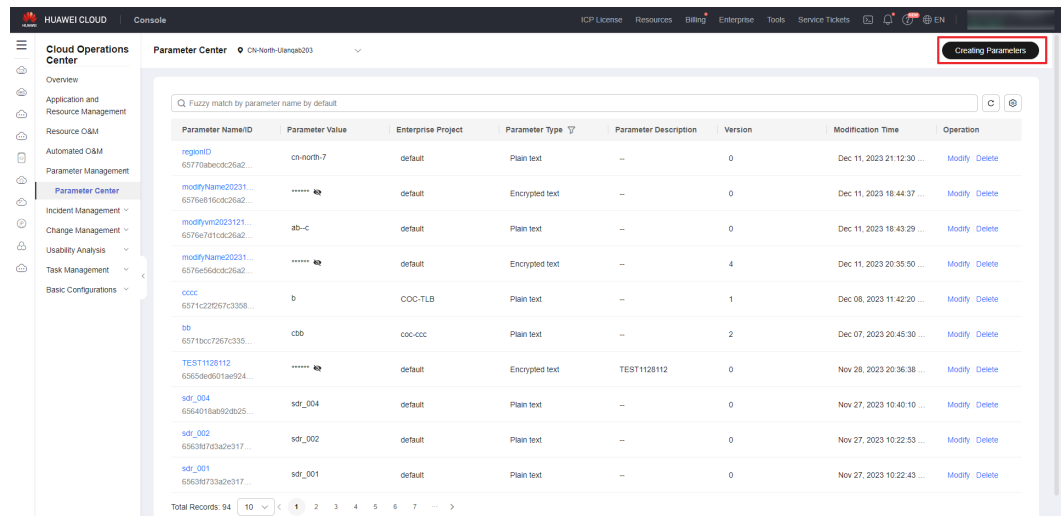
Precautions

Parameter policies may delete parameters. Exercise caution when configuring parameter policies.

Procedure

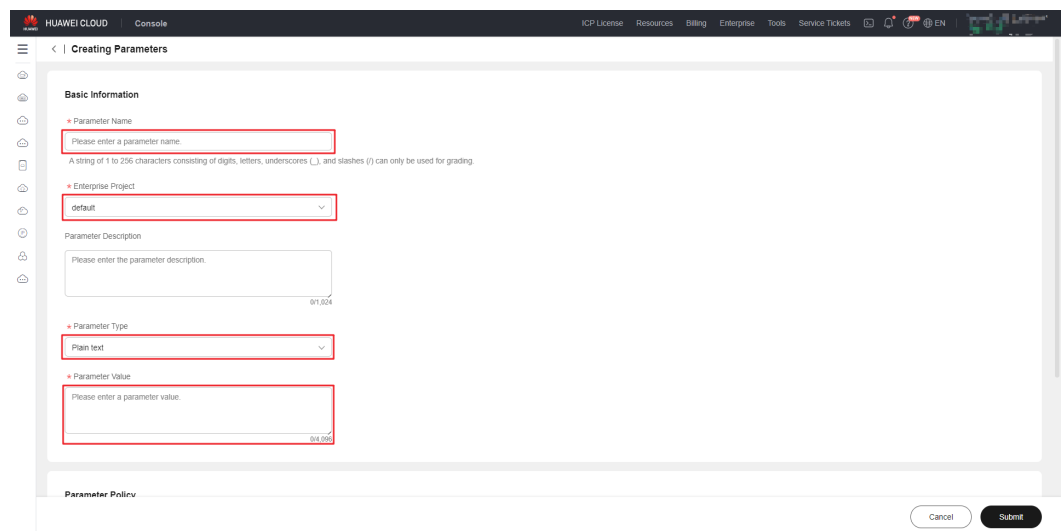
- Step 1** Log in to [COC](#).
- Step 2** In the left navigation pane, choose **Parameter Management > Parameter Center**. In the right pane, click **Creating Parameters**.

Figure 6-1 Creating a parameter



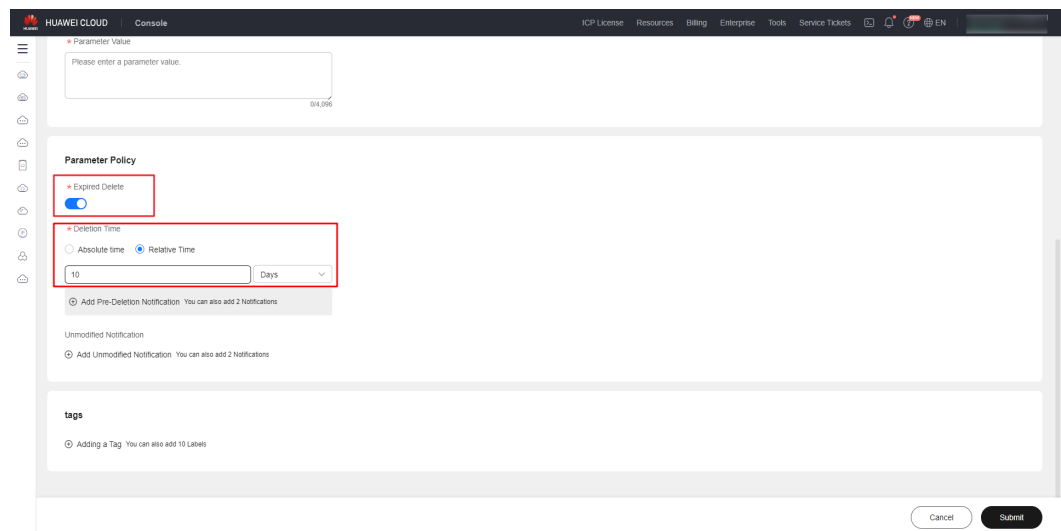
Step 3 Set the basic information, including **Parameter Name**, **Enterprise Project**, and **Parameter Type** (Parameter Name, Enterprise Project, and Parameter Type cannot be changed after the parameter is created.)

Figure 6-2 Basic information



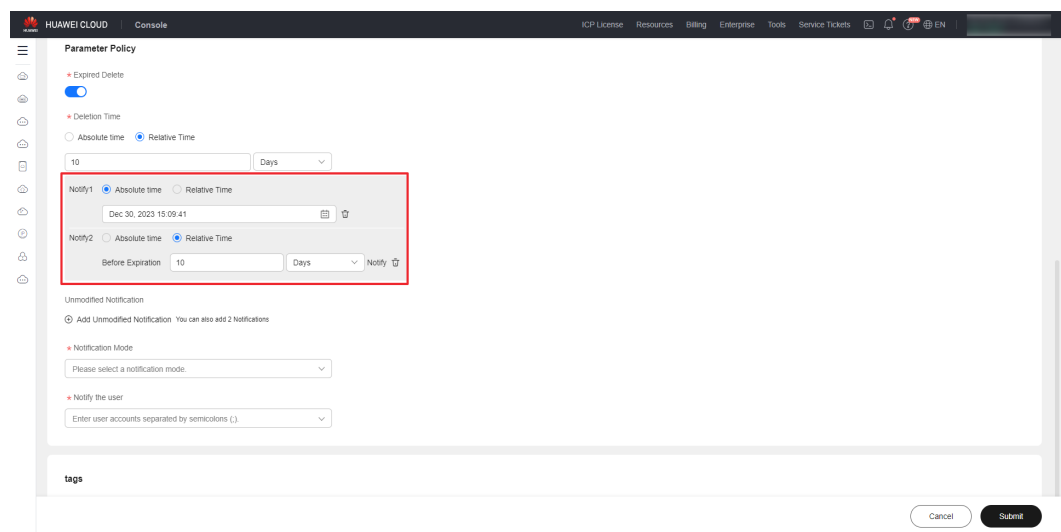
Step 4 Determine whether to set a policy for deleting the parameter upon expiration. If you do not want to set such a policy, skip steps 5 and 6.

Figure 6-3 Policy for deleting the parameter upon expiration



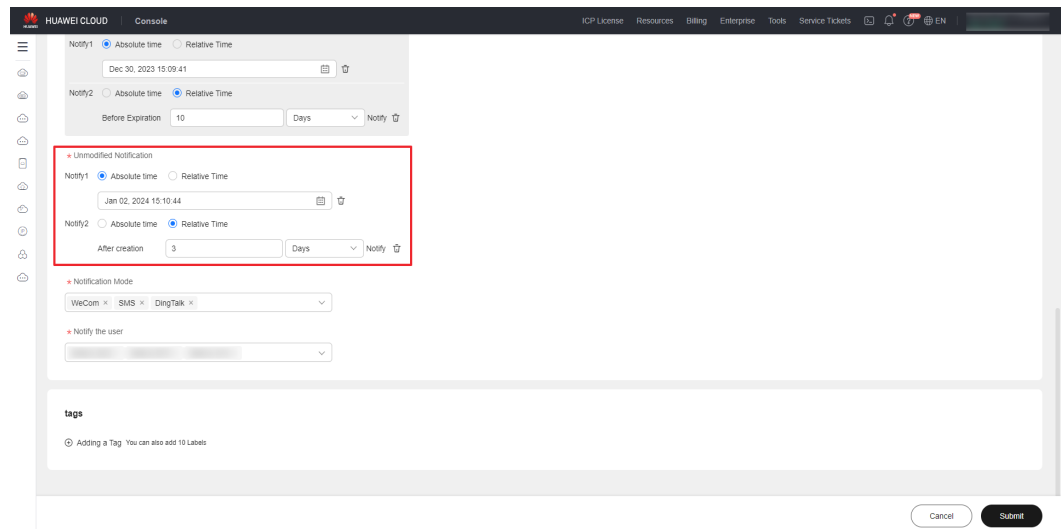
Step 5 Determine whether to set pre-deletion notifications. If you do not want to set such notifications, skip this step. If you want to set such notifications, click **Add Pre-Deletion Notification** and set the notification time.

Figure 6-4 Adding pre-deletion notifications



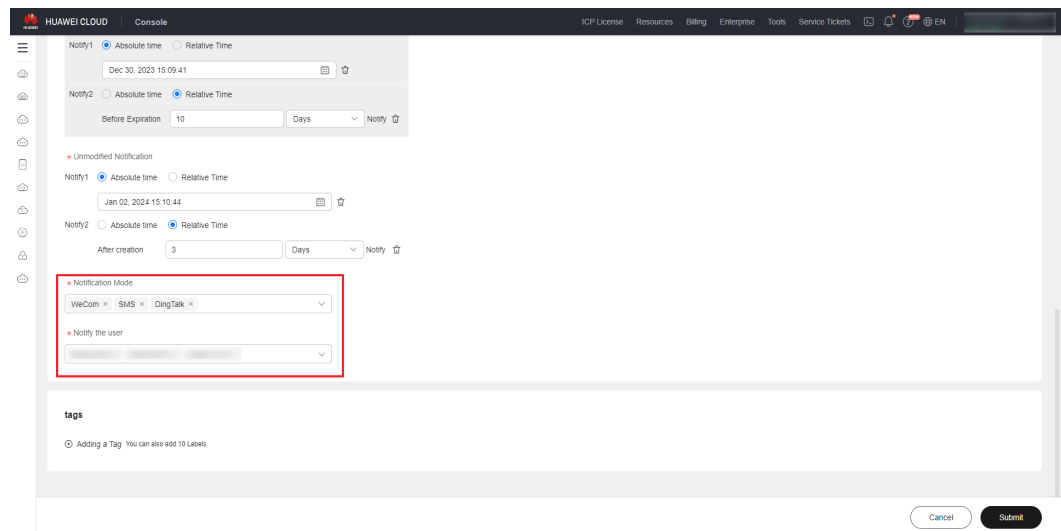
Step 6 Determine whether to set unmodified notifications. If you do not want to set such notifications, skip this step. If you want to set such notifications, click **Add Unmodified Notification** and set the notification time.

Figure 6-5 Adding unmodified notifications



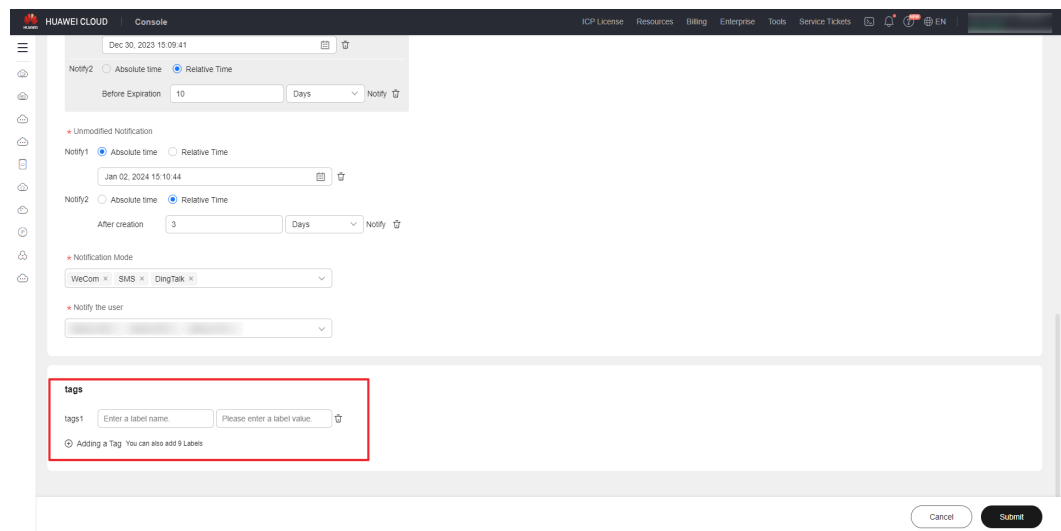
Step 7 If there are pre-deletion or unmodified notification policies, set **Notification Mode** and **Notify the user**.

Figure 6-6 Setting Notification Mode and Notify the user



Step 8 Click **Adding a Tag** to add tags to the parameter. If you do not want to add tags, skip this step.

Figure 6-7 Adding parameter tags



Step 9 Click **Submit**. After the creation request is submitted, the parameter list is displayed.

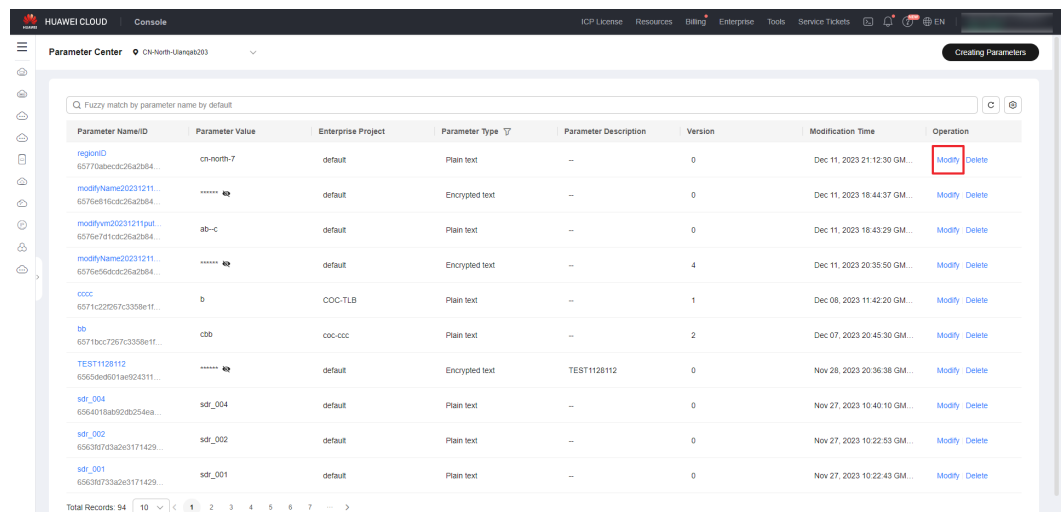
----End

6.1.2 Modifying a Parameter

Step 1 Log in to **COC**.

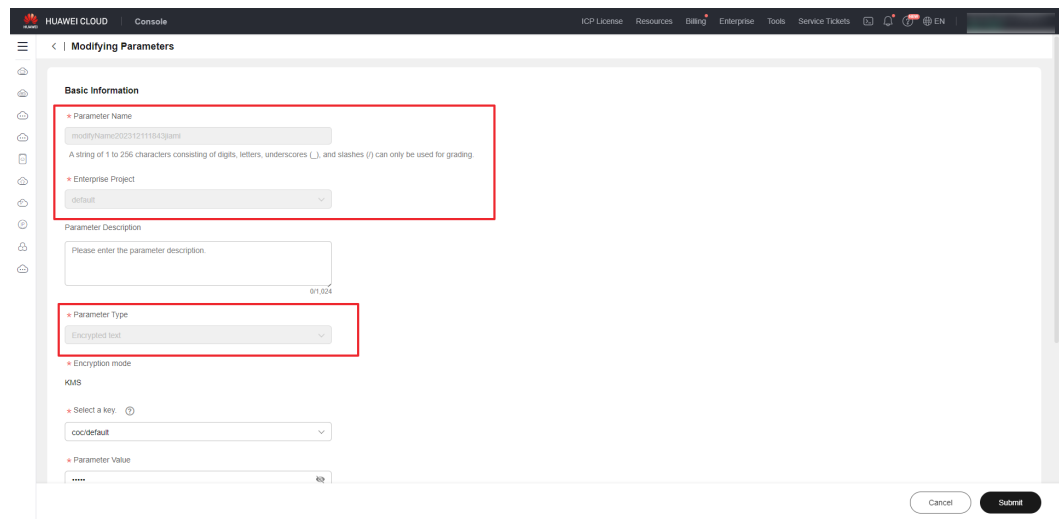
Step 2 In the left navigation pane, choose **Parameter Center**. Locate the target parameter and click **Modify** in the **Operation** column.

Figure 6-8 Parameter list



Step 3 On the displayed **Modifying Parameters** page, **Parameter Name**, **Enterprise Project**, and **Parameter Type** cannot be changed.

Figure 6-9 Parameter details



Step 4 Modify the parameter as needed. 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. For pre-deletion notifications: If you change the deletion time, the pre-deletion notification time will also change.

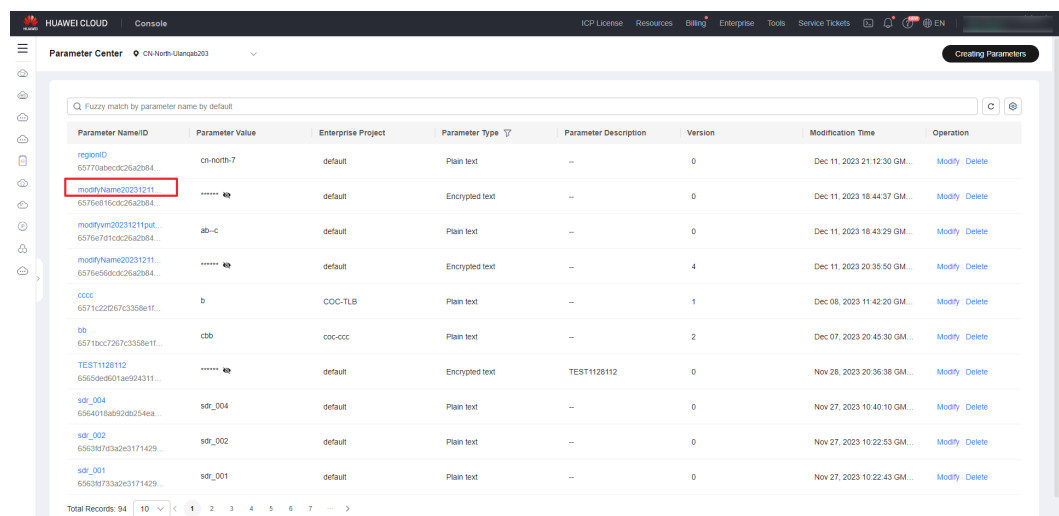
----End

6.1.3 Viewing Parameter Details

Step 1 Log in to [COC](#).

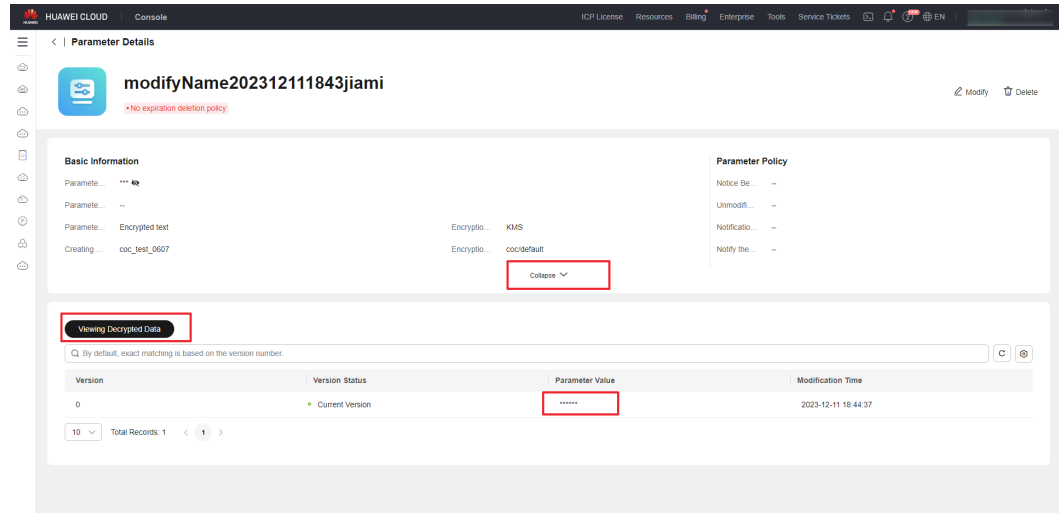
Step 2 In the navigation pane on the left, choose **Parameter Center**. Click the name of a parameter to go to the details page and view the parameter details and historical versions.

Figure 6-10 Parameter list



- Step 3** Click the icon next to the parameter value to view the sensitive value, click **Collapse** to expand the tag list, and click **Viewing Decrypted Data** to view the values of all parameter versions.

Figure 6-11 Parameter details



-----End

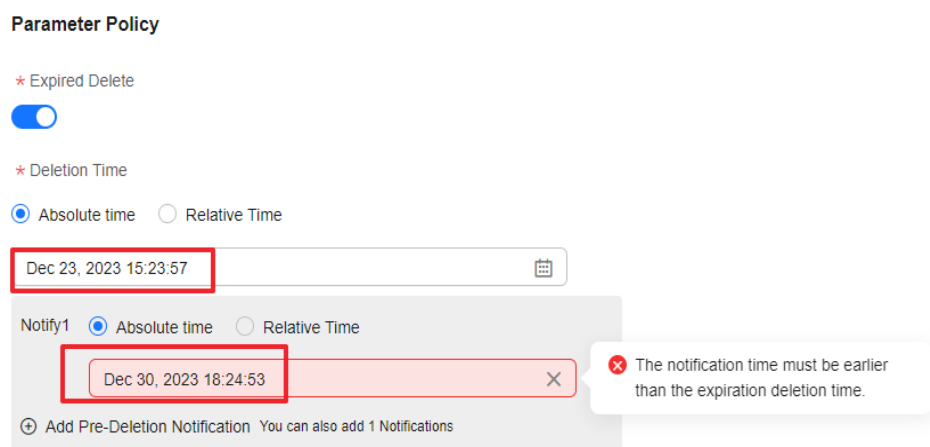
6.2 Notification Rules

Parameter notifications are affected by the deletion time and modification operation. When modifying a parameter, pay attention to the notification rule.

6.2.1 Expiration Notification

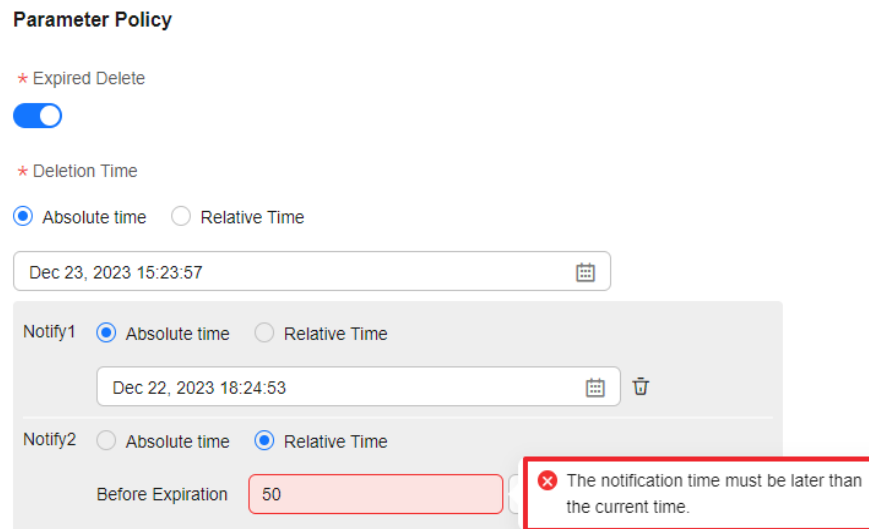
- The expiration notification time must be earlier than the time of deletion upon expiration.

Figure 6-12 Expiration notification time later than the time of deletion upon expiration



- The expiration notification time must be later than the parameter creation or modification time.

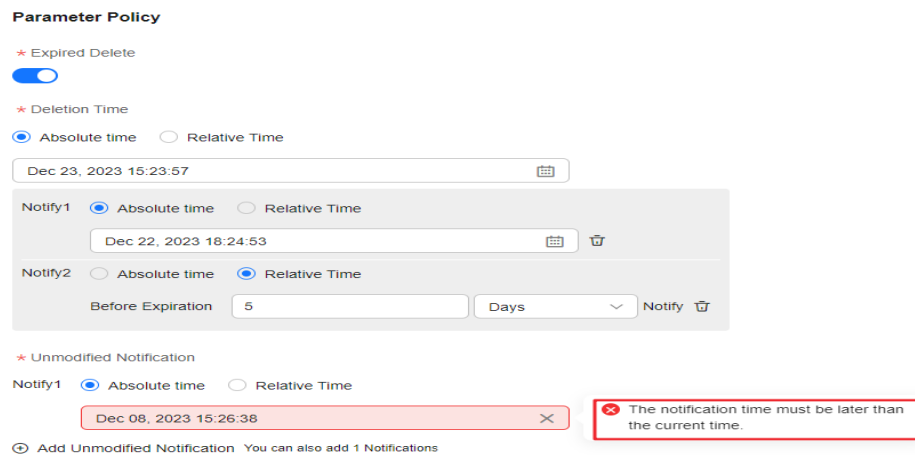
Figure 6-13 Expiration notification time earlier than the system time



6.2.2 Unmodified Notifications

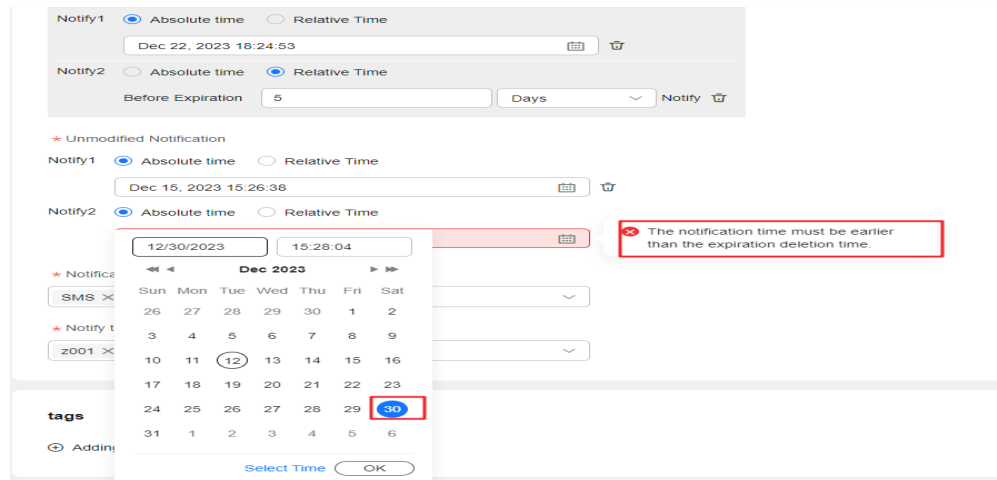
- The unmodified notification time cannot be earlier than the parameter creation or modification time.

Figure 6-14 Notification time earlier than the system time



- 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.

Figure 6-15 Unmodified notification time later than the time of deletion upon expiration



7 Incident Management

7.1 Incident Center

Incident Center manages all incidents of applications, including incident acceptance and rejection, ticket transfer, processing, and close management. Incidents can be generated based on transfer rules, or created by users or based on alarms.

7.1.1 Incidents

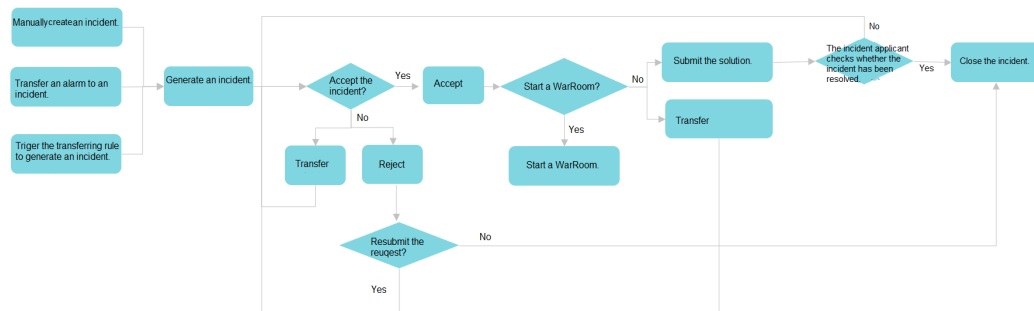
After an incident is created, it is in the unaccepted state. You can forward, reject, or accept the incident.

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, upgrade and downgrade, add remarks, and WarRoom start.

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.

Figure 7-1 Incident flowchart



7.1.2 Creating an Incident

Scenarios

Create an incident ticket using Cloud Operations Center.

Prerequisites

You have created an application by referring to Application Management.

Precautions

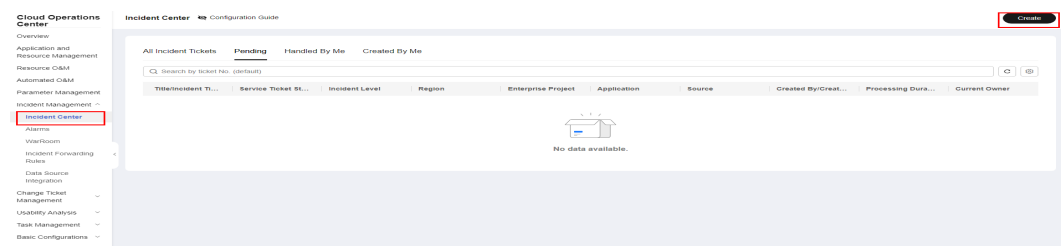
Create an incident service ticket.

Procedure

Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click **Create**.

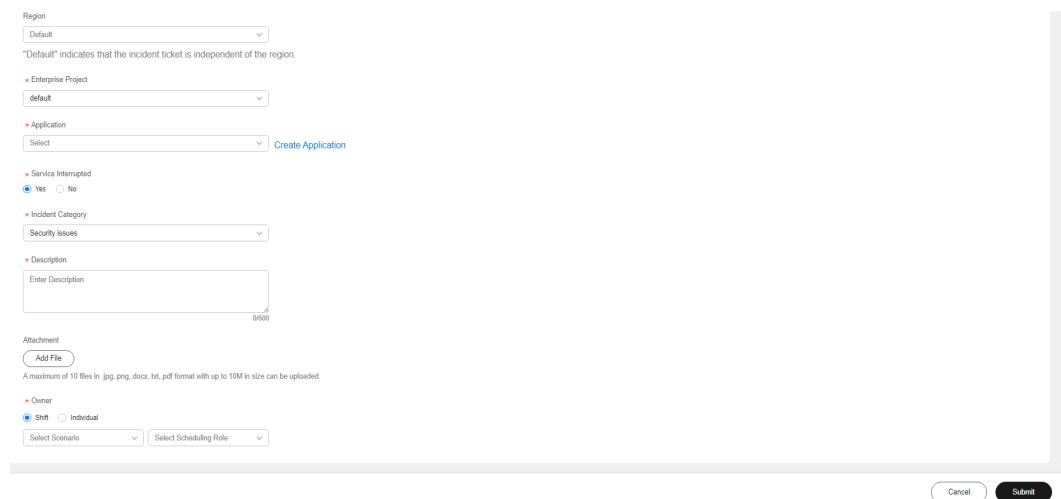
Figure 7-2 Incident ticket list



Step 3 Enter the basic information about the incident ticket and click **Submit**.

If no schedule is selected for the owner, create a schedule in Shift Schedule Management.

Figure 7-3 Creating an incident service ticket



 **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.

----End

7.1.3 Handling an Incident

7.1.3.1 Rejecting an Incident

Scenarios

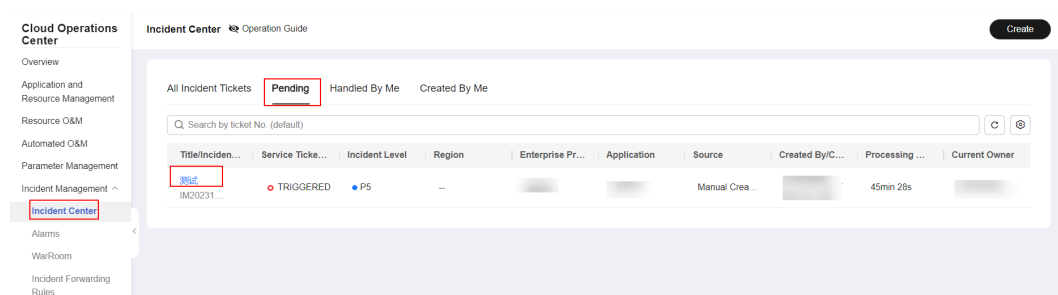
If an incident is unreasonable, the incident handler can reject the incident.

Procedure

Step 1 Log in to **COC**.

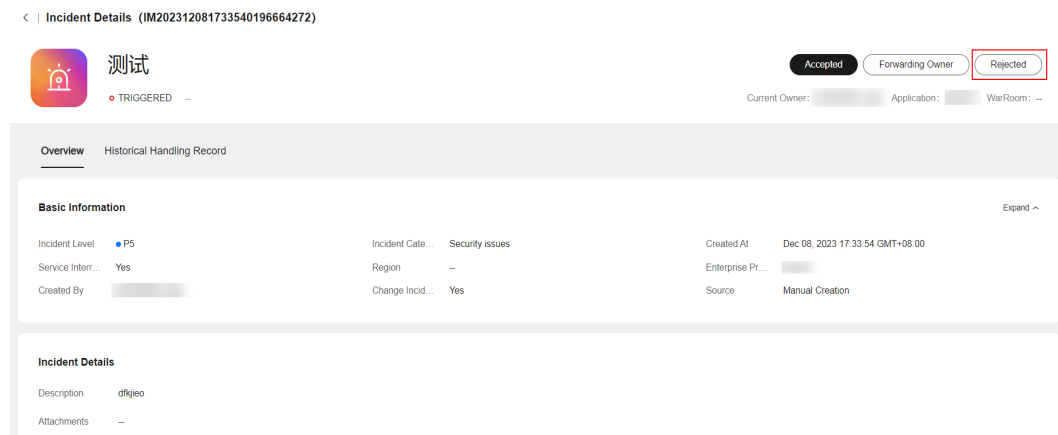
Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 7-4 List of incidents to be handled



Step 3 Click **Reject**.

Figure 7-5 Rejecting an incident



Step 4 Enter the rejection reason and click **OK**.

Figure 7-6 Entering a reason for rejection



----End

7.1.3.2 Resubmitting an Incident After Rejection

Scenarios

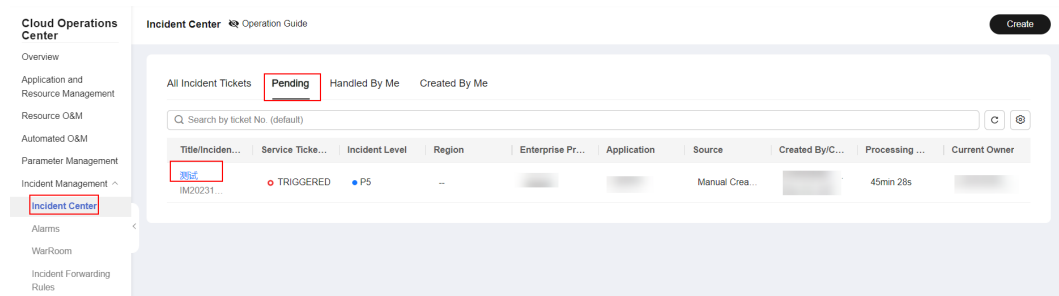
After an incident ticket is rejected, modify the incident ticket content.

Procedure

Step 1 Log in to **COC**.

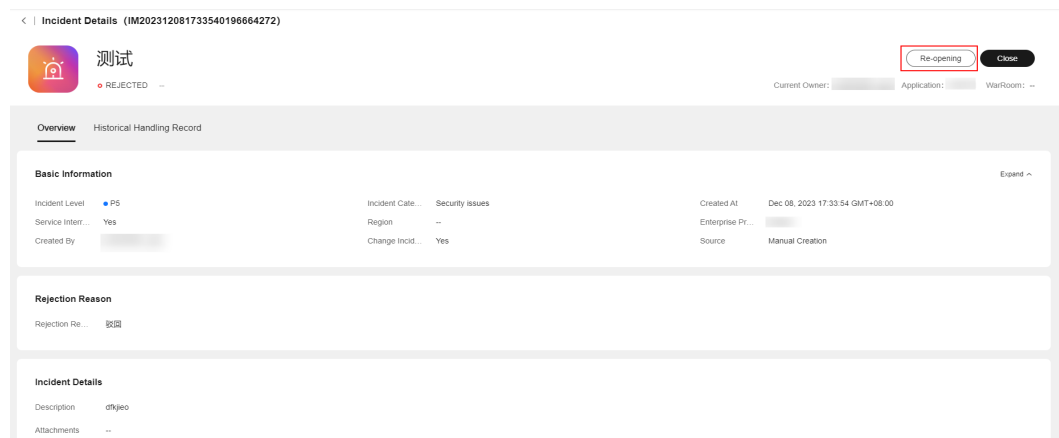
Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-7 Incident details



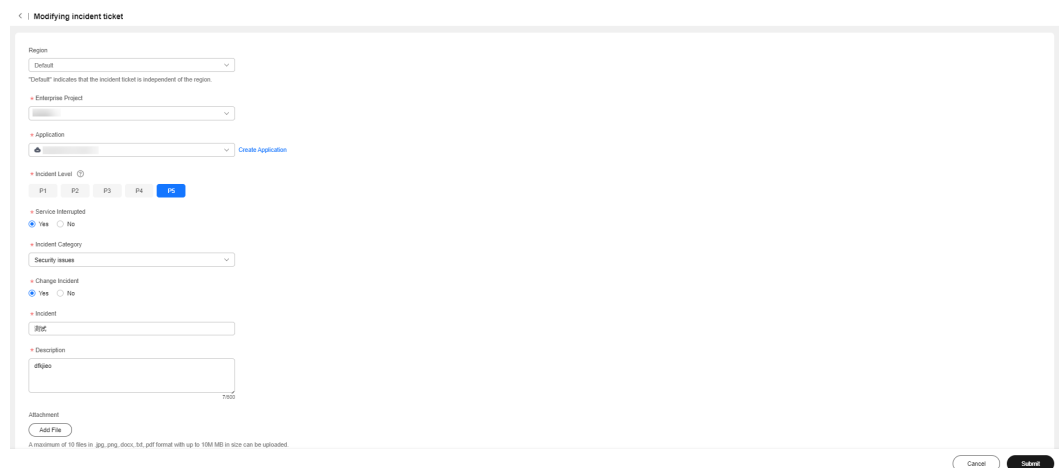
Step 3 Click **Restart**.

Figure 7-8 Restarting an incident



Step 4 After modifying the incident ticket content, click **Submit**.

Figure 7-9 Modifying the content of an incident ticket



----End

7.1.3.3 Forwarding Incidents

Scenarios

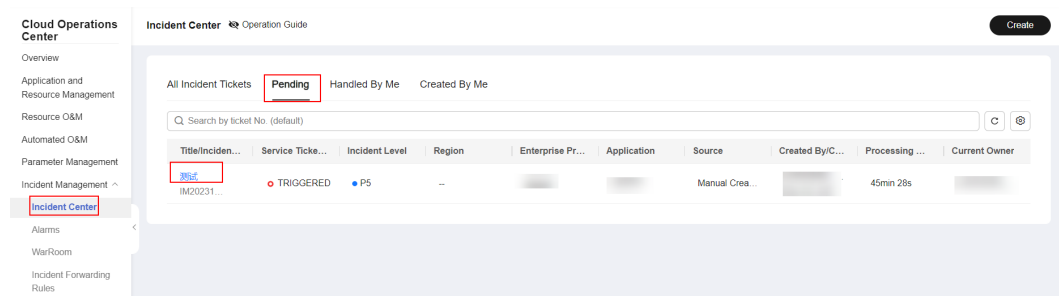
Forward the incident ticket to another person for processing.

Procedure

Step 1 Log in to **COC**.

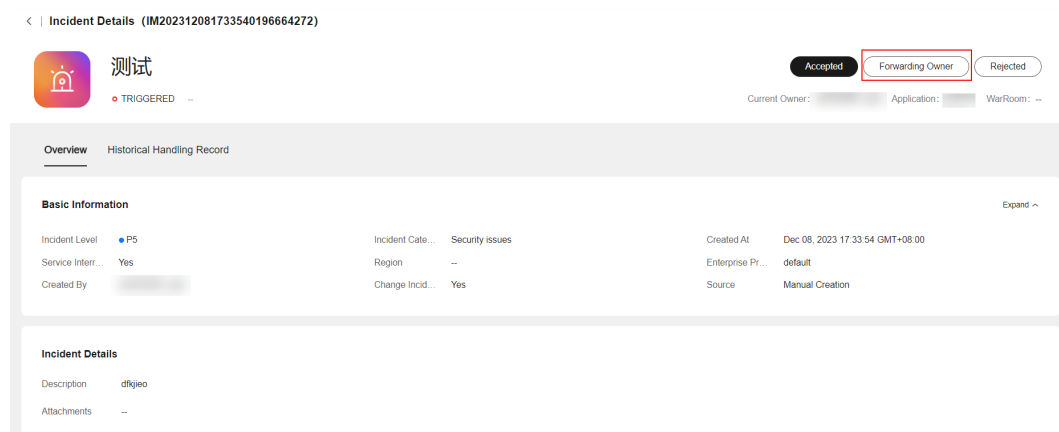
Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-10 Incident details



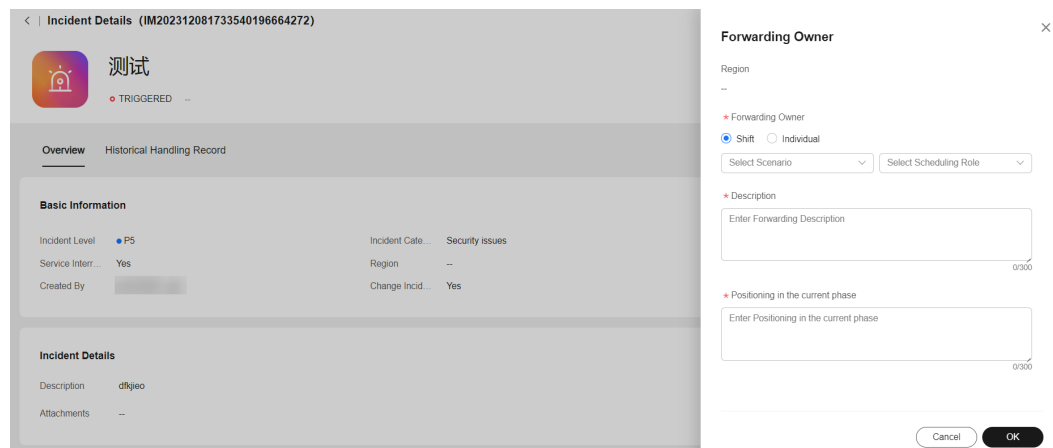
Step 3 Click forward owner.

Figure 7-11 Transferring the owner



Step 4 Enter the forwarding information and click **Submit**.

Figure 7-12 Entering forwarding information



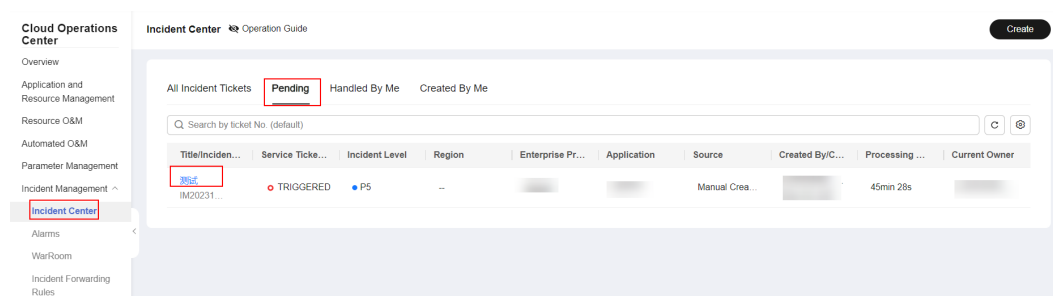
----End

7.1.3.4 Handling Incidents

Procedure

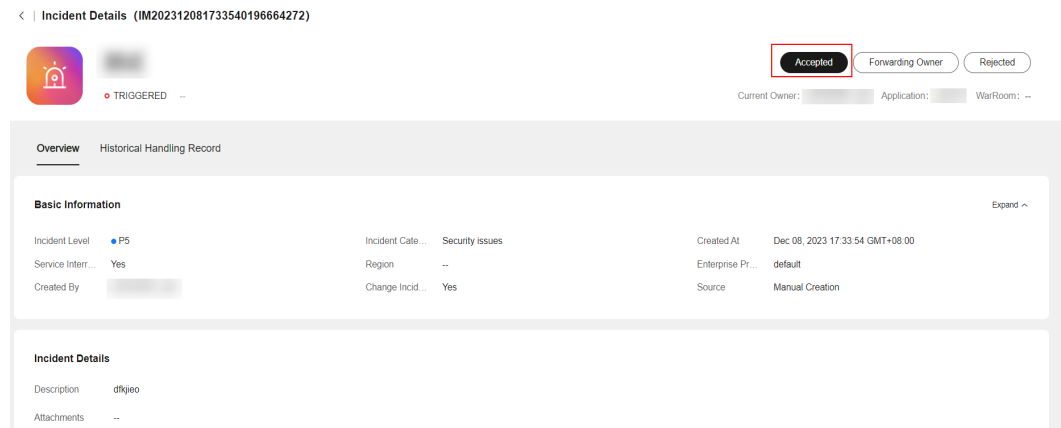
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-13 Incident details



- Step 3** Click **Accepted**.

Figure 7-14 Handling an incident



----End

7.1.3.5 Upgrading/Downgrading an Incident

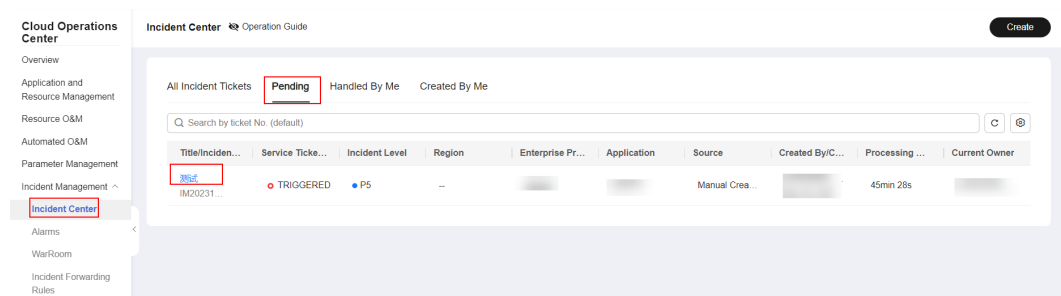
Scenarios

The incident ticket level is inconsistent with the actual situation. The incident level can be modified only after the incident is accepted.

Procedure

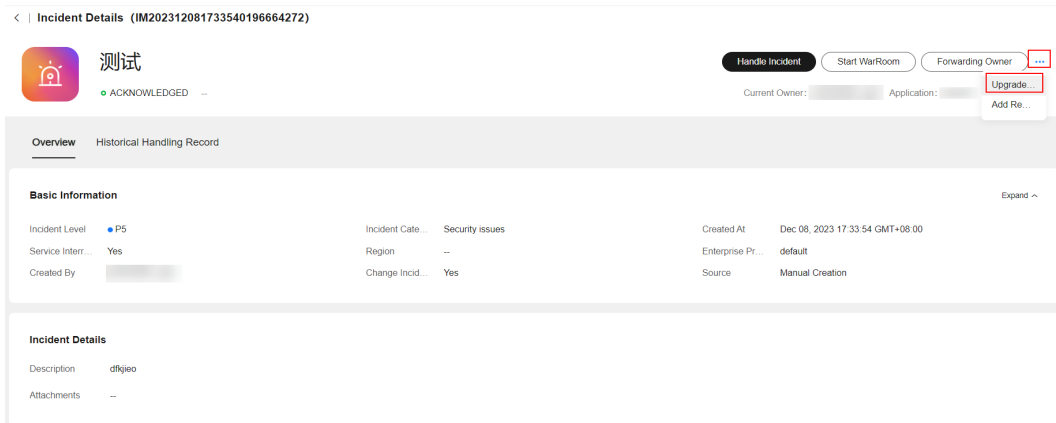
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-15 Incident details



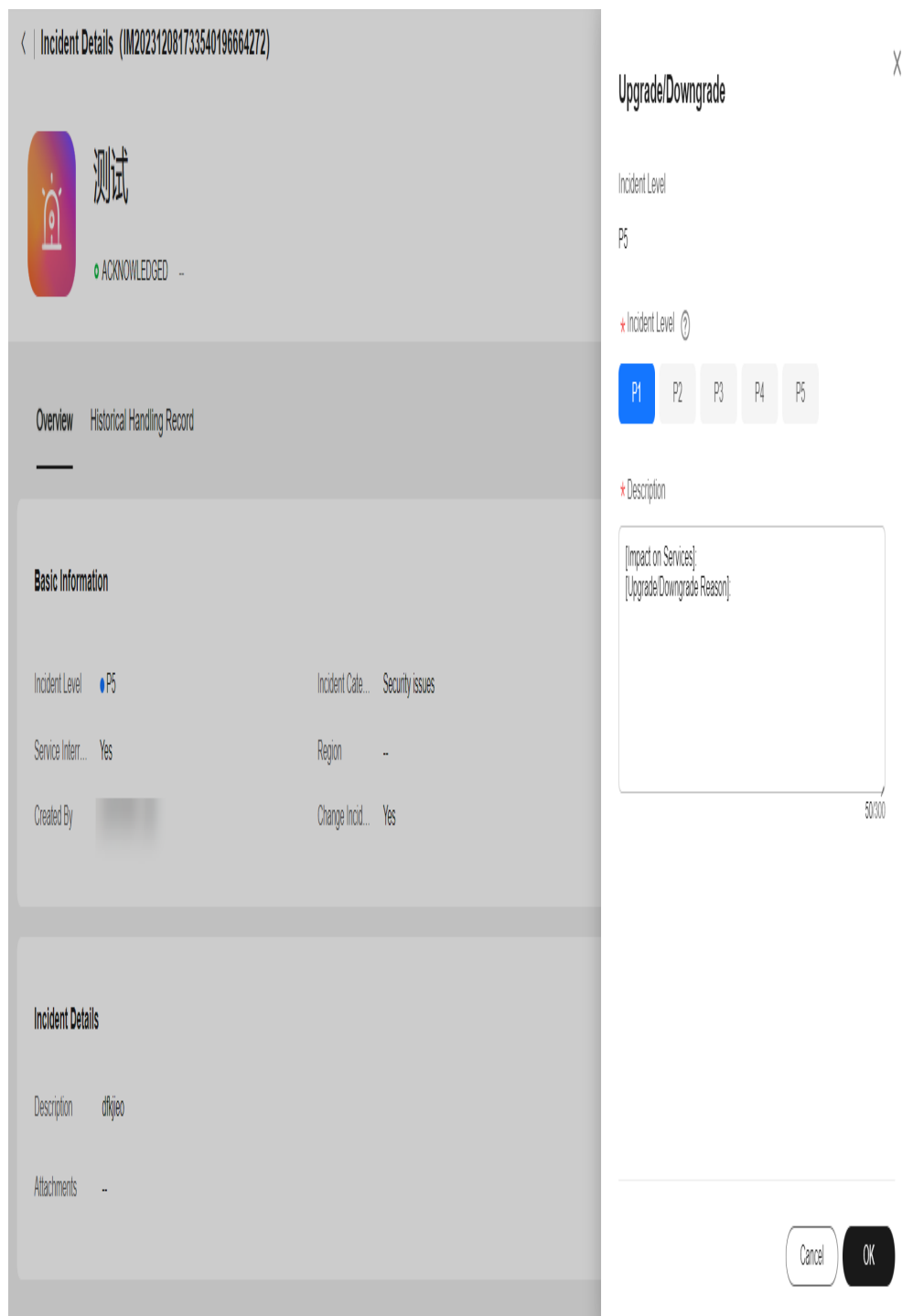
- Step 3** Click the ... icon and choose upgrade/degrade.

Figure 7-16 Upgrading/downgrading an incident



Step 4 Enter the upgrade or downgrade information and click **OK**.

Figure 7-17 Entering upgrade and downgrade information



----End

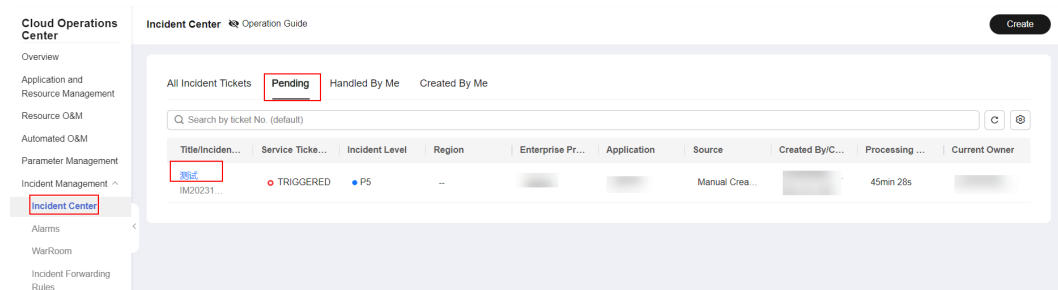
7.1.3.6 Adding Remarks

Procedure

Step 1 Log in to [COC](#).

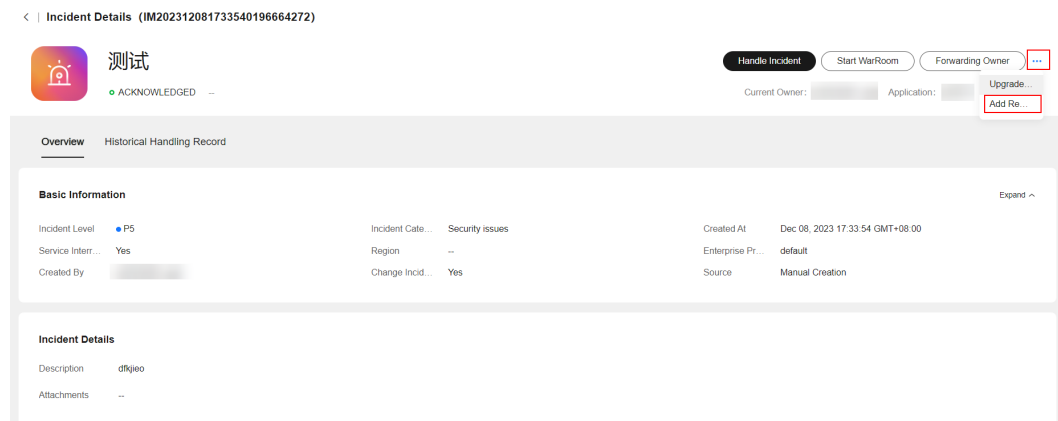
Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-18 Incident details



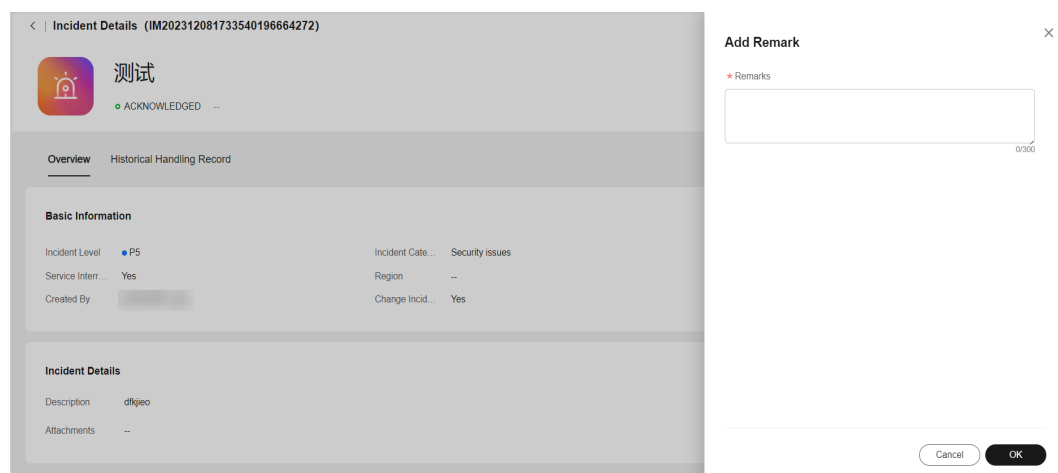
Step 3 Click the ... icon and choose add remarks.

Figure 7-19 Adding remarks



Step 4 Enter remarks and click **Submit**.

Figure 7-20 Entering remarks information



----End

7.1.3.7 Starting a WarRoom

Scenarios

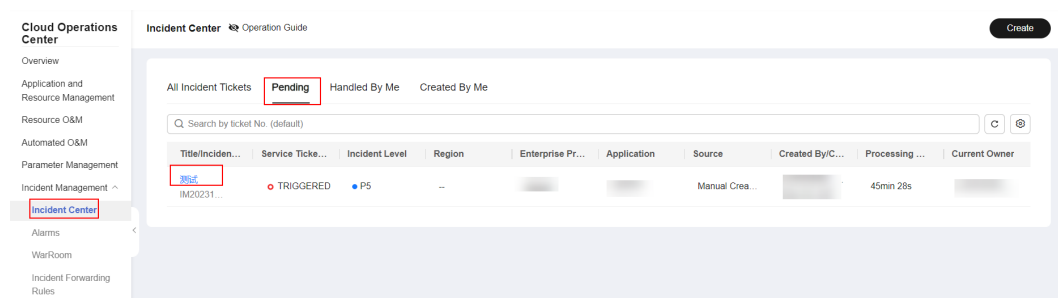
Start a WarRoom for critical incident to recovery the incident quickly.

Procedure

Step 1 Log in to **COC**.

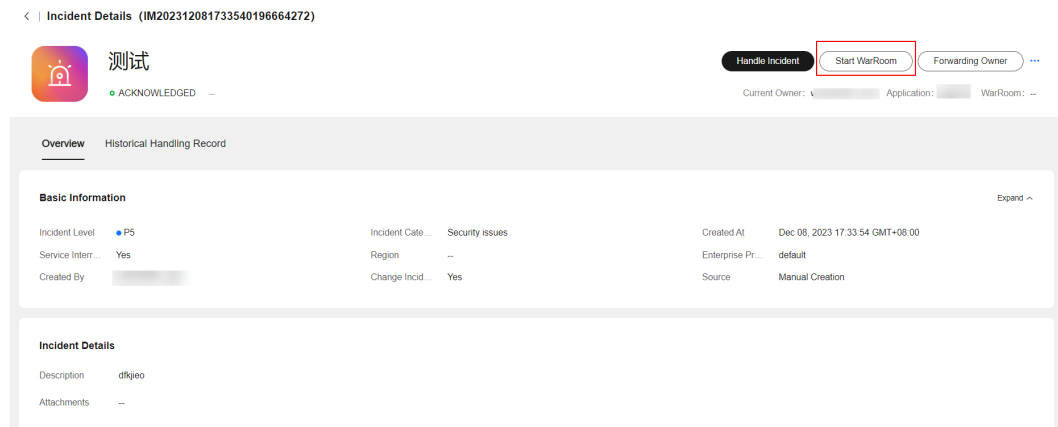
Step 2 In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 7-21 Incident ticket details



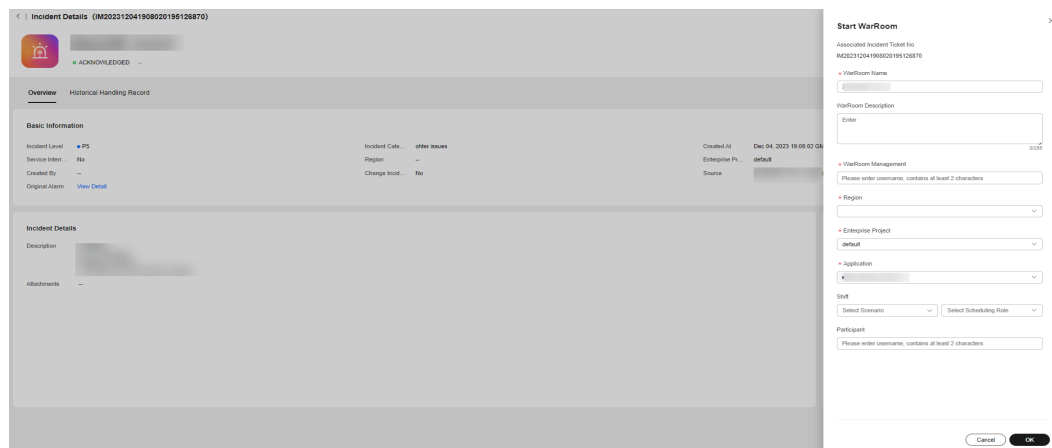
Step 3 Click start WarRoom.

Figure 7-22 Starting a WarRoom



Step 4 Enter WarRoom information and click **Submit**.

Figure 7-23 Entering WarRoom information



CAUTION

If a group (Only enterprise WeChat groups and DingTalk groups are supported) needs to be added when a WarRoom is started, configure the following information:

- (1) Configure applications in mobile application management.
- (2) Configure the enterprise WeChat email address on the personnel management page.
- (3) If shift is selected, you need to create a schedule and add personnel to the schedule. Then the enterprise WeChat accounts will be added when the WarRoom starting rule is met.

----End

7.1.3.8 Handling an Incident

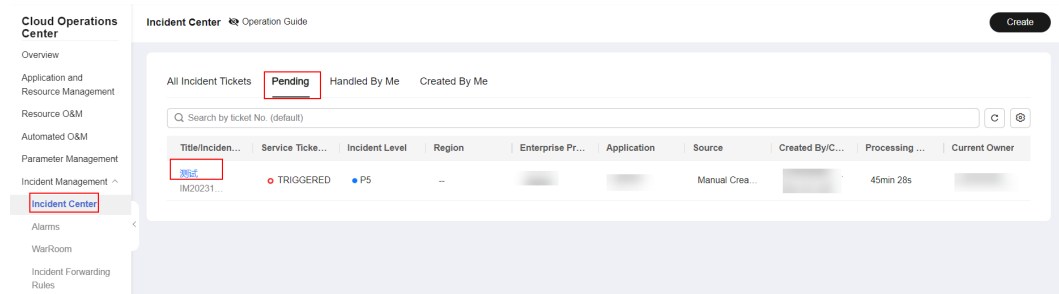
Scenarios

Handle the incident ticket after accepting the incident.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

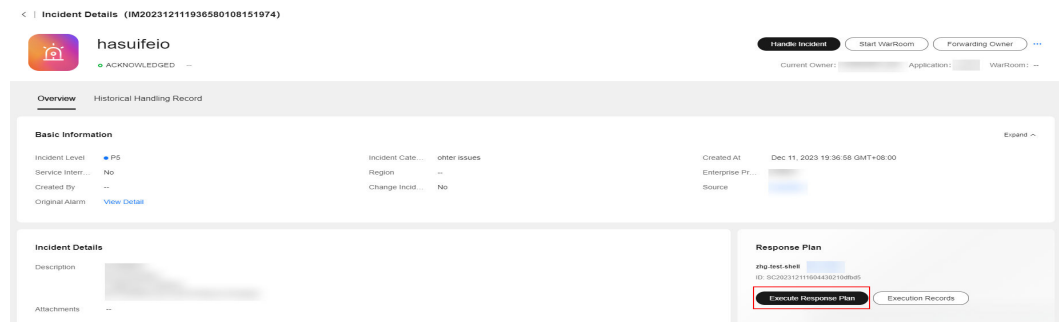
Figure 7-24 Incident details



Step 3 If an incident ticket created based on the transfer rule is associated with a contingency plan, the contingency plan can be executed during incident ticket processing. Click **Execute Response Plan**.

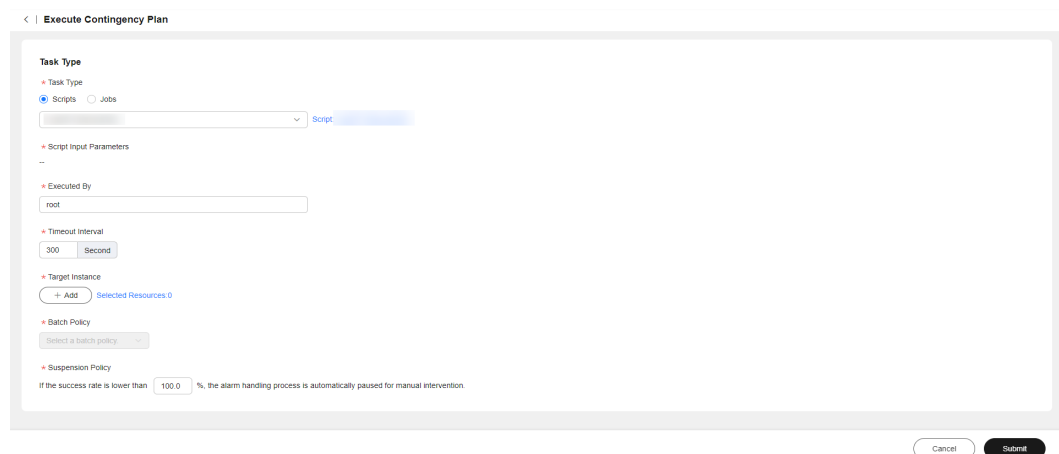
If the incident ticket that is generated through alarm transferring to incident, manual creation, and transferring rules does not associate with a response plan, you can create a contingency plan, script, or job.

Figure 7-25 Executing the response plan



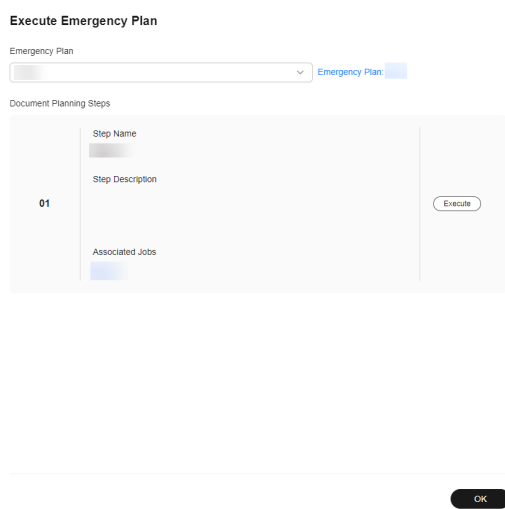
Step 4 If the response plan is a job and script, verify the job and script information and click **Submit**.

Figure 7-26 Page for executing a job or script



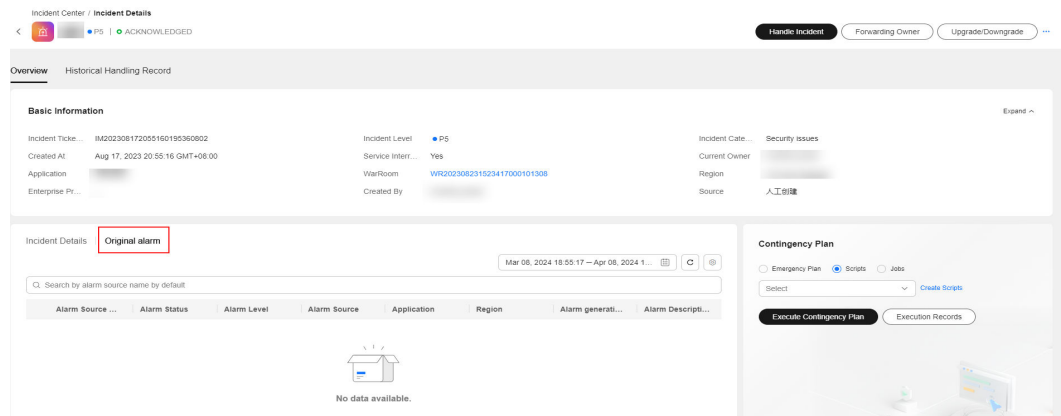
If Contingency Plan is selected for Response Plan, and the response plan is an automatic plan, click **Execute** to execute the script or job and then click **Submit**. If the contingency plan is a text plan, perform the corresponding steps and click **Submit**.

Figure 7-27 Executing a contingency plan



Step 5 View the original alarms associated with the incident.

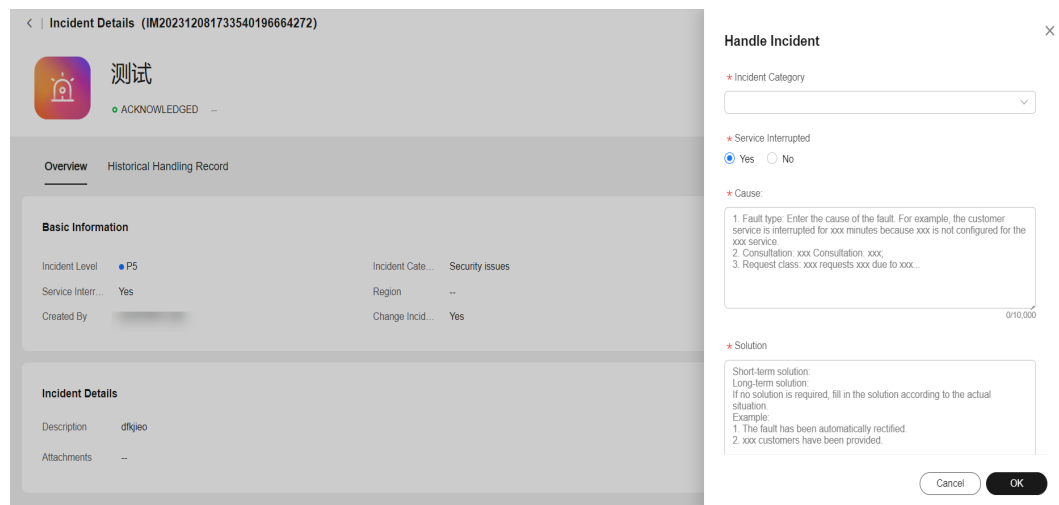
Figure 7-28 Viewing the alarm associated with an incident



Step 6 Click **Handle Incident** to specify the incident processing result.

Step 7 Enter the incident processing information and click **OK**.

Figure 7-29 Incident handling



----End

7.1.3.9 Verifying Incident

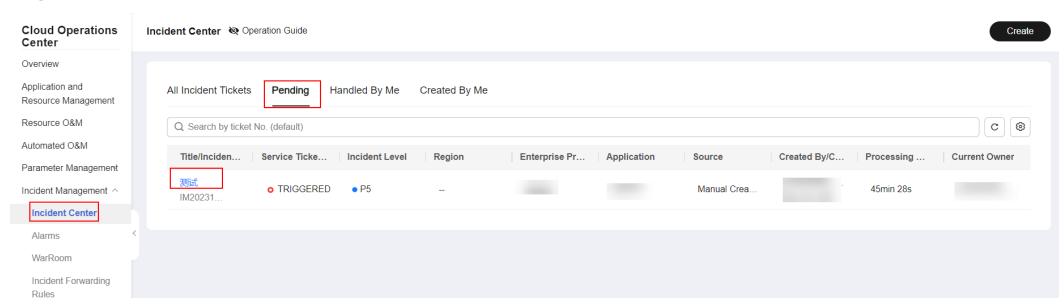
Scenarios

After the incident ticket is processed, verify whether the incident processing is completed.

Procedure

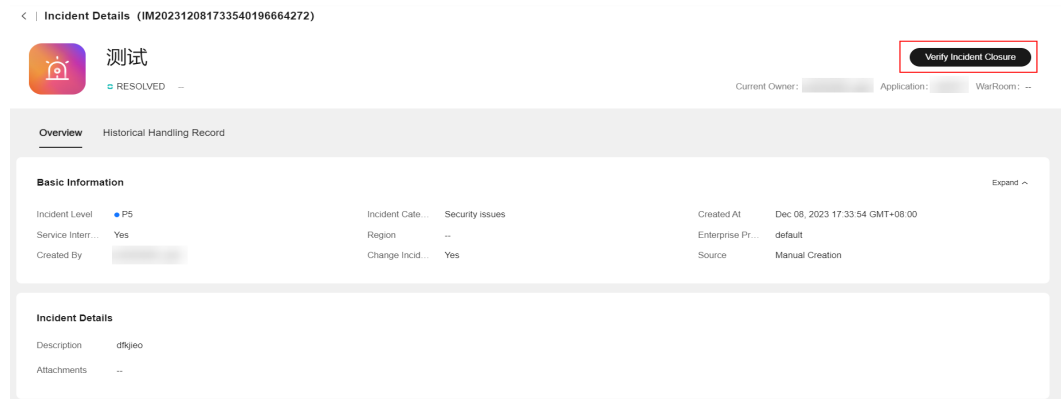
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 7-30 Incident details



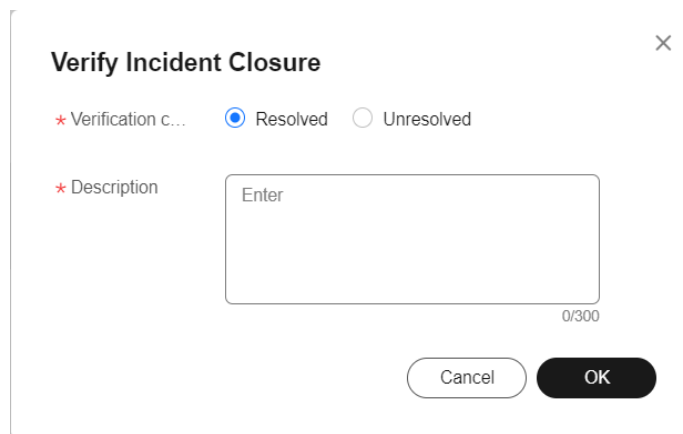
- Step 3** Click **Verify Incident Closure**.

Figure 7-31 Verifying whether the incident is closed



Step 4 Enter the verification information and click **OK**.

Figure 7-32 Verifying close page



-----End

7.1.4 Incident History

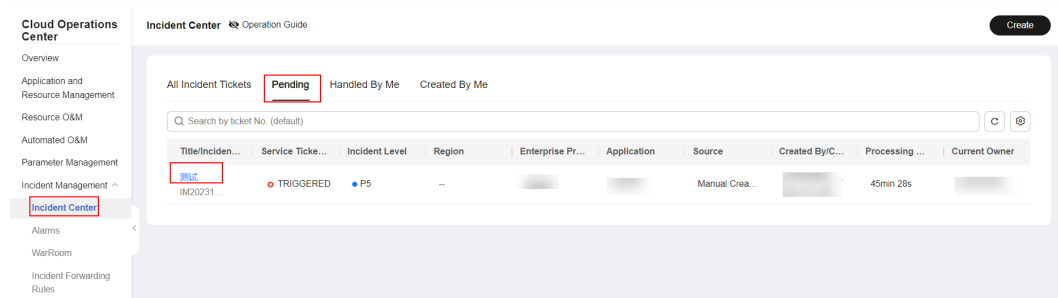
Scenarios

View the historical records of an incident, including the entire incident handling process.

Procedure

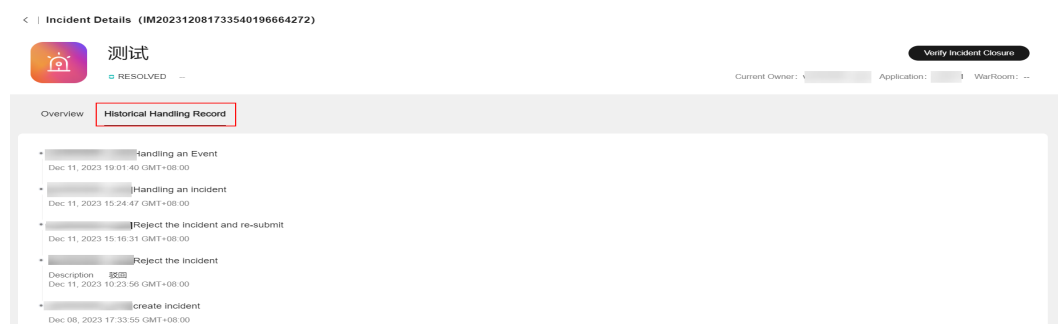
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 7-33 Incident details



Step 3 Click **Historical Handling Record**.

Figure 7-34 Viewing incident history



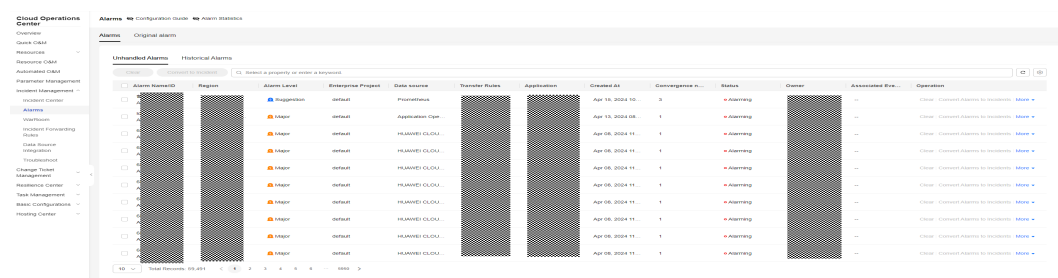
----End

7.2 Alarms

7.2.1 Viewing Alarms

- Step 1 Log in to **COC**.
- Step 2 In the navigation pane, choose **Incident Management > Alarms** to view the integrated alarm list.
- Step 3 In the upper part of the displayed page, search for the alarms by alarm ID or name.
- Step 4 Aggregated alarms include current alarms and historical alarms.

Figure 7-35 Alarm list



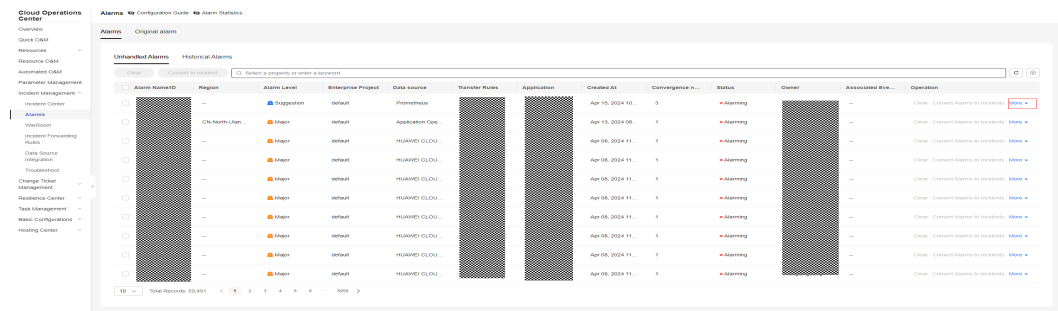
----End

7.2.1.1 Handling Alarms

Step 1 Log in to **COC**.

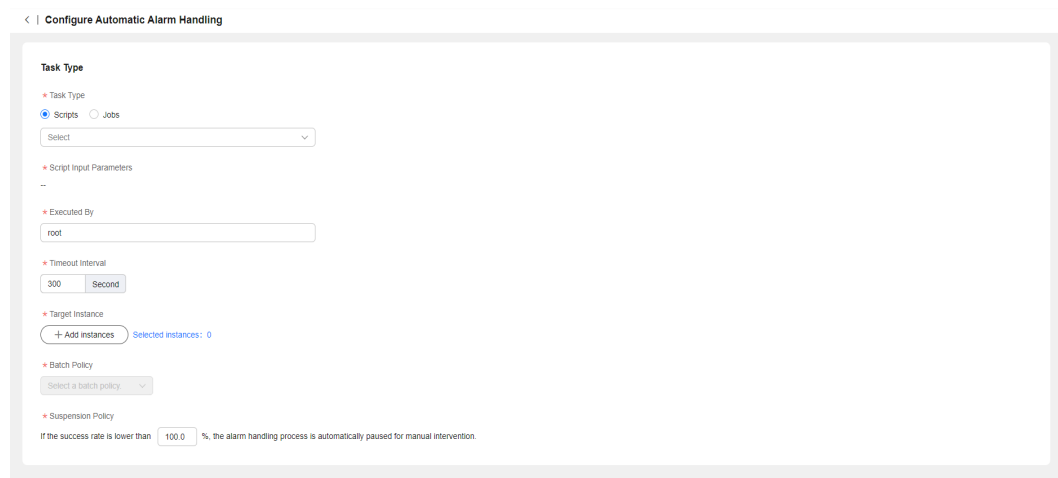
Step 2 In the navigation pane, choose **Incident Management > Alarms**. On the displayed **Alarms** tab page, click the **Unhandled Alarms** tab. In the displayed alarm list, locate the alarm you want to handle, click **More** in the **Operation** column and choose **Handle** to handle the alarms.

Figure 7-36 Handling alarms



Step 3 Configure the parameters and click **Submit**.

Figure 7-37 Handling an alarm



NOTE

If a script is selected, configure the parameters by referring to Executing Custom Scripts and Executing Public Scripts.

If a job is selected, configure the parameters by referring to Executing Custom Jobs and Executing Public Jobs.

----End

7.2.1.2 Converting an Alarm to an Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Incident Management > Alarms**. On the displayed **Alarms** tab page, click the **Unhandled Alarms** tab to view the existing alarms.

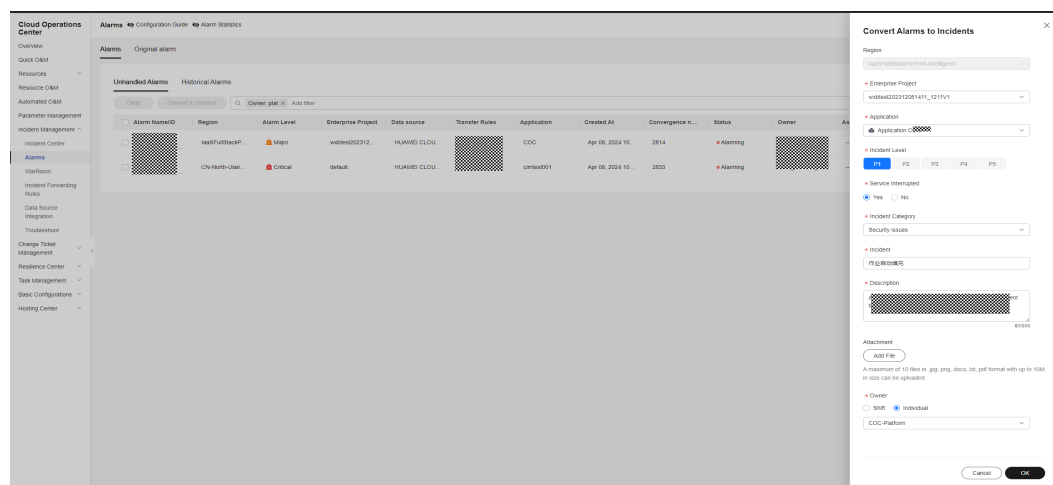
Step 3 Select the target alarms and click **Convert to Incident**.

NOTE

Only alarms in the same region can be converted to incidents in batches.

Step 4 Enter the incident information and click **OK**.

Figure 7-38 Converting an alarm to an incident



NOTE

For details about the incident parameters, see [Creating an Incident](#).

----End

7.2.1.3 Clearing Alarms

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Incident Management > Alarms**. On the displayed **Alarms** tab page, click the **Unhandled Alarms** tab to view the existing alarms.

Step 3 Select the alarms to be deleted and click **Clear**.

Step 4 Enter the remarks and click **OK** to clear the alarms. The remarks can contain at most 100 characters, including Chinese characters, letters, digits, and special characters.

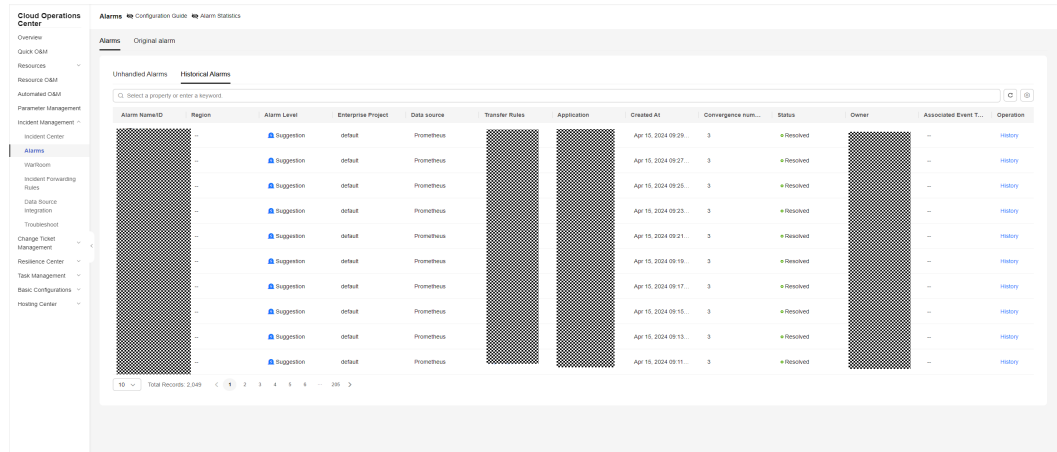
----End

7.2.1.4 Historical Alarms

Step 1 Log in to **COC**.

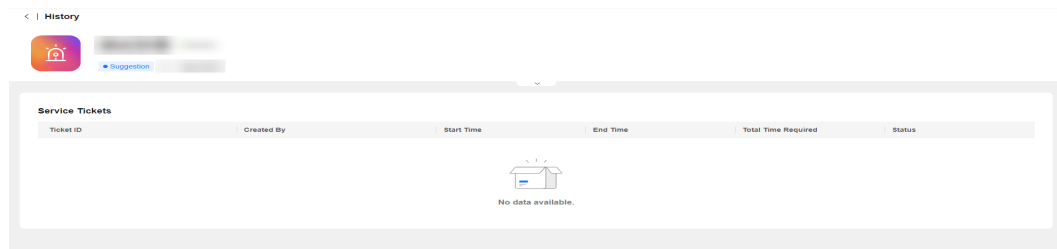
Step 2 In the navigation pane, choose **Incident Management > Alarms**. On the displayed **Alarms** tab page, click the **Historical Alarms** tab to view the historical alarms.

Figure 7-39 Historical alarm list



Step 3 Click **History** in the **Operation** column to view the historical records of the target alarm.

Figure 7-40 Historical records of an alarm



----End

7.2.2 Original Alarms

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Incident Management > Alarms**. Click the **Original Alarms** tab to view the original alarm list. By default, alarms generated in the last month are displayed.

Step 3 In the alarm list, click **∨** in front of the alarm whose information you want to view.

Figure 7-41 Original alarms

| Alarm Source NameID | Alarm Status | Alarm Level | Alarm Source | Application | Region | Alarm generation time | Alarm Description |
|---------------------|--------------|-------------|--------------|-------------|--------|---------------------------------|-------------------|
| [Redacted] | alarm | major | Prometheus | [Redacted] | Region | Apr 09, 2024 16:42:41 GMT+08:00 | [Redacted] |
| [Redacted] | Received | major | Prometheus | [Redacted] | Region | Apr 09, 2024 16:55:56 GMT+08:00 | [Redacted] |
| [Redacted] | Received | major | Prometheus | [Redacted] | Region | Apr 09, 2024 15:50:11 GMT+08:00 | [Redacted] |
| [Redacted] | alarm | major | Prometheus | [Redacted] | Region | Apr 09, 2024 15:20:11 GMT+08:00 | [Redacted] |
| [Redacted] | Received | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:57:41 GMT+08:00 | [Redacted] |
| [Redacted] | Received | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:51:26 GMT+08:00 | [Redacted] |
| [Redacted] | Received | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:44:56 GMT+08:00 | [Redacted] |
| [Redacted] | ... | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:36:41 GMT+08:00 | [Redacted] |
| [Redacted] | ... | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:32:56 GMT+08:00 | [Redacted] |
| [Redacted] | ... | major | Prometheus | [Redacted] | Region | Apr 09, 2024 14:20:11 GMT+08:00 | [Redacted] |

----End

7.3 WarRoom

A WarRoom is a meeting that facilitates rapid service recovery through the joint efforts of O&M, R&D, and operations personnel. On the WarRoom page, you can add participants, send fault progress, and add affected applications.

Prerequisites

There is an incident ticket being processed under this application and a WarRoom is started on the incident processing page.

7.3.1 WarRoom Status

Scenarios

After a WarRoom is started, you can view and update the WarRoom status.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Incident Management > WarRoom**.
- Step 3** Click a WarRoom ID. The WarRoom status is displayed in the upper part.
- Step 4** Click **Update Status** on the right to update the WarRoom status.

CAUTION

1. Before changing to the **Fault Rectified** status, ensure that the status of the affected application is **Recovered**.
2. Before changing to the **WarRoom Shut Down** status, ensure that the fault information of the WarRoom has been completed.

----End

7.3.2 Fault Information

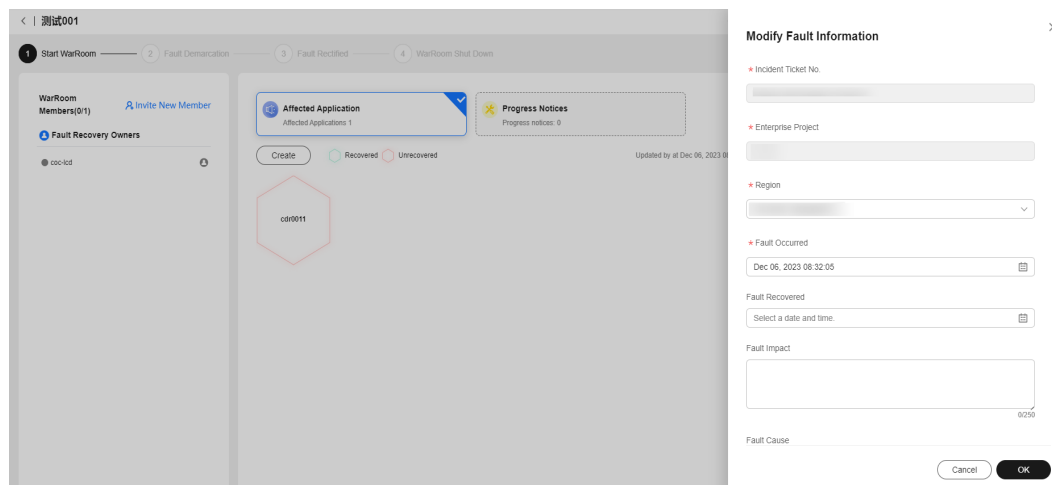
Scenarios

After the WarRoom is started, you can view and edit fault information.

Procedure

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > WarRoom**.
- Step 3** Click a WarRoom ID.
- Step 4** Click **Modify**, and modify fault information as prompted, and click **OK**.

Figure 7-42 Modifying fault information



----End

7.3.3 Affected Application Management

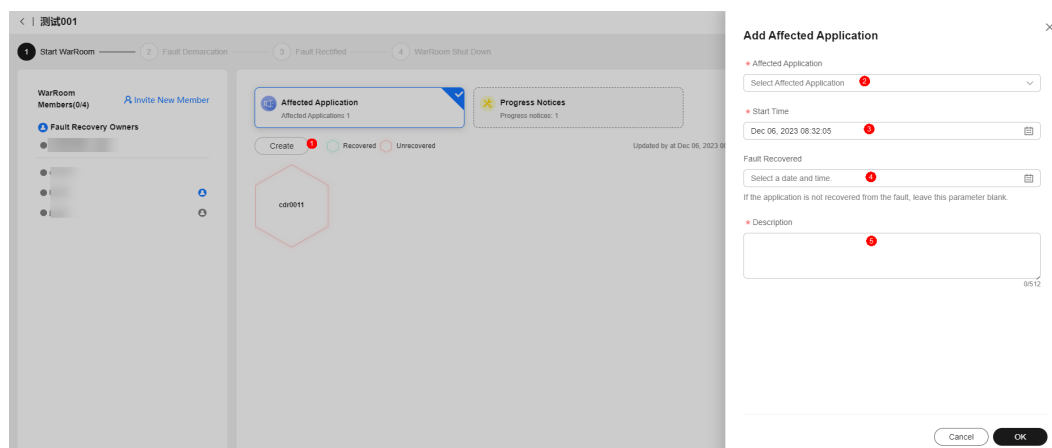
Scenarios

Add affected applications after a WarRoom is started.

Procedure

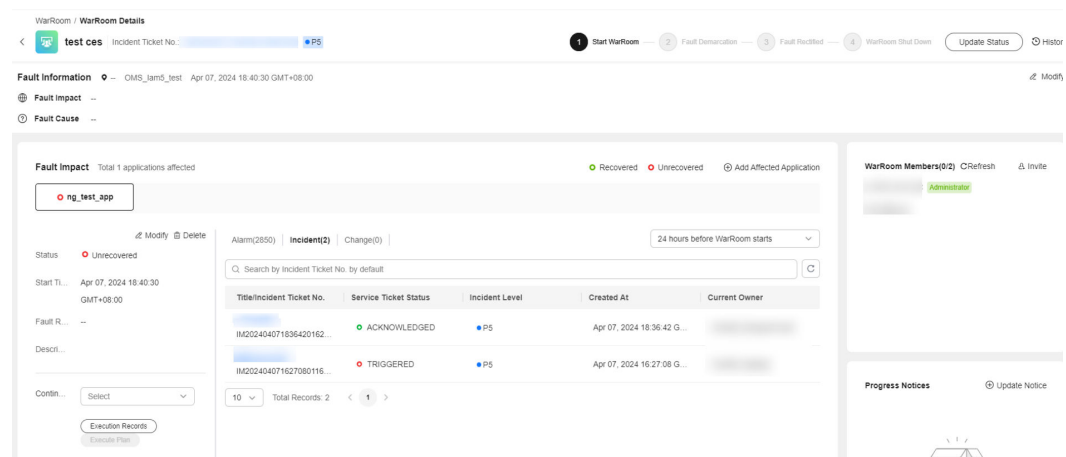
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Incident Management > WarRoom**.
- Step 3** On the **WarRoom** tab page, enter the associated incident ticket number or WarRoom name in the search text box and click the search icon to query the target WarRoom. Then click the queried WarRoom name.
- Step 4** Click **Create**.
The **Add Affected Application** page is displayed.
- Step 5** Set the information about the new affected application as prompted.
- Step 6** Click **OK**.

Figure 7-43 New affected applications



- Step 7** View the added applications on the **WarRoom Details** page. Enter the fault start time, recovery time, and fault description. Submit the modification and the application status becomes **Recovered**.
- Step 8** Select and execute an emergency plan to quickly rectify faults of the affected application as needed. You can also view alarms, incidents, and changes of the application.

Figure 7-44 Affected application page



----End

7.3.4 WarRoom Members

Scenarios

After a WarRoom is started, you can view members, invite members, set recovery owners and members, and remove members.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Incident Management > WarRoom**.
- Step 3** Click a WarRoom ID.
- Step 4** Click **Invite New Member**, select the joining mode and the members to be invited, and click **Add to WarRoom**.

----End

7.3.5 Progress Notification

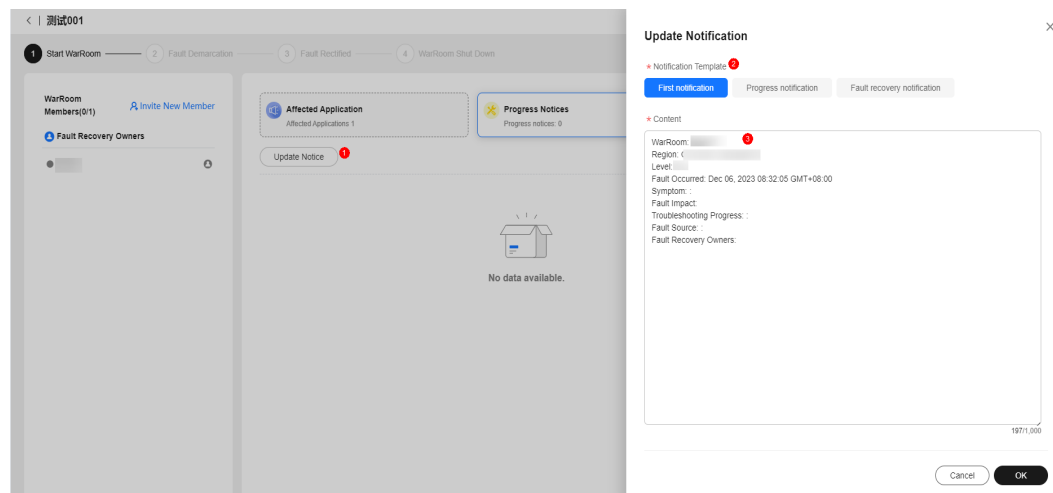
Scenarios

After a WarRoom is started, you can view, update, and send notifications.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Incident Management > WarRoom**.
- Step 3** Click a WarRoom ID.
- Step 4** Click **Progress Notices** to view the current progress notice.
- Step 5** Click **Update Notice**, enter the notice content as prompted, and click **OK** to update the notice.

Figure 7-45 Updating notification



Step 6 Click **Release**, enter the required information as prompted, and click **OK** to release the notification.

If the notification object is set to schedule, create the schedule in **Shift Scheduling Management**.

----End

7.3.6 Adding a WarRoom Initiation Rule

Scenarios

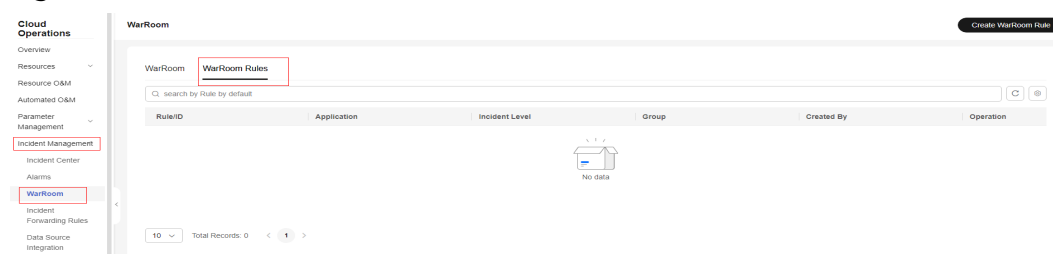
Create a WarRoom initiation rule.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Incident Management > WarRoom**. Click the **WarRoom Rules** tab.

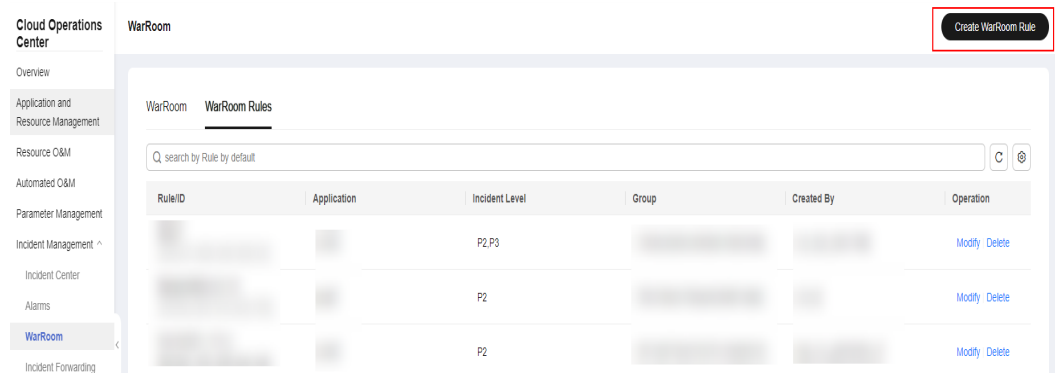
Figure 7-46 WarRoom rules



Step 3 Click **Create WarRoom Rule**. In the displayed dialog box, set the rule name, region, application, incident level, and group information, and click **OK**.

The WarRoom rule matching logic: The region, application, and level of an incident will match with those of a WarRoom rule, and the personnel in the group will be added to the WarRoom and the mobile app. For details about how to configure the mobile app, see **Mobile App Management**.

Figure 7-47 Adding a WarRoom rule



Step 4 After the rule is created, query the new rule in the rule list.

----End

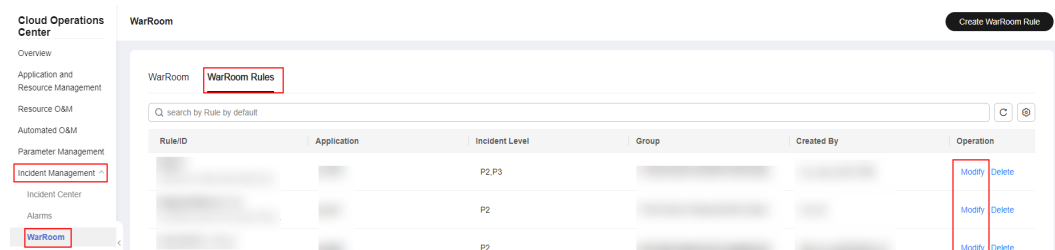
7.3.7 Modifying a WarRoom Rule

Procedure

Step 1 Log in to **COC**.

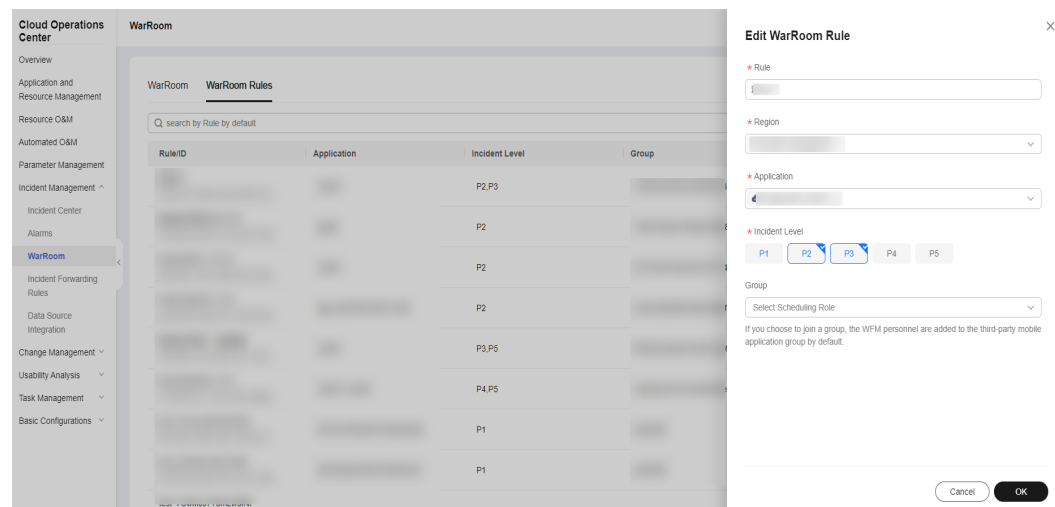
Step 2 In the navigation pane on the left, choose **Incident Management > WarRoom**. Click the **WarRoom Rules** tab.

Figure 7-48 WarRoom rules



Step 3 Locate the WarRoom rule to be modified and click **Modify** in the **Operation** column. Enter the rule name, select the region, application, incident level, and group information, and click **OK**.

Figure 7-49 Modifying a WarRoom rule



Step 4 After the modification is complete, you can query the modified rule in the rule list.

----End

7.4 Forwarding Rules

7.4.1 Overview

Incident forwarding rules deduplicate all received and integrated original alarms. When you configure incidents for an incident forwarding rule, notification objects and notification policies are assigned by default for accurate notification.

7.4.2 Forwarding rules

This topic describes how to configure a forwarding rule.

Prerequisites

Before configuring a forwarding rule, ensure that the monitoring source for which the forwarding rule is configured has been connected to Integration Management.

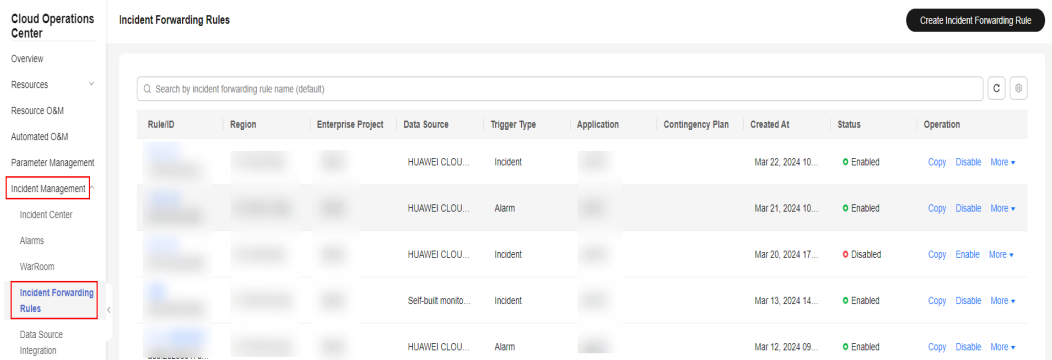
Scenarios

Manage forwarding rules. You can customize rules for incidents and alarms based on forwarding rules.

Procedure for Adding a Forwarding Rule

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Incident Management > Incident Forwarding Rules**. The configuration page is displayed.
- Step 3** In the upper part of the list, click **Create Incident Forwarding Rule**.

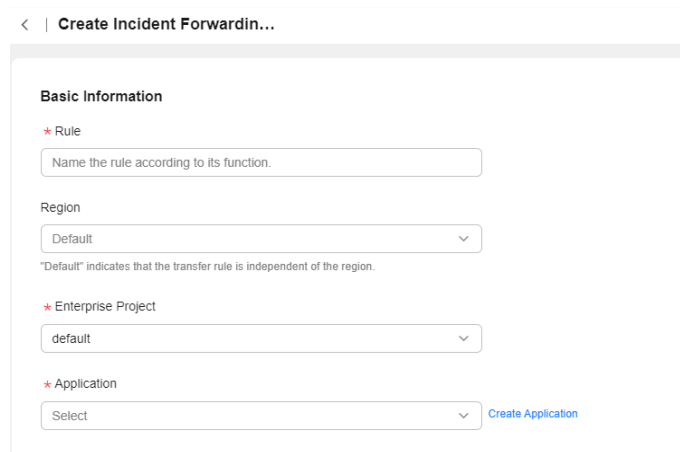
Figure 7-50 Creating an incident forwarding rule



If the information in the two forwarding rules is similar, click **Copy** in the **Operation** column to quickly create a forwarding rule.

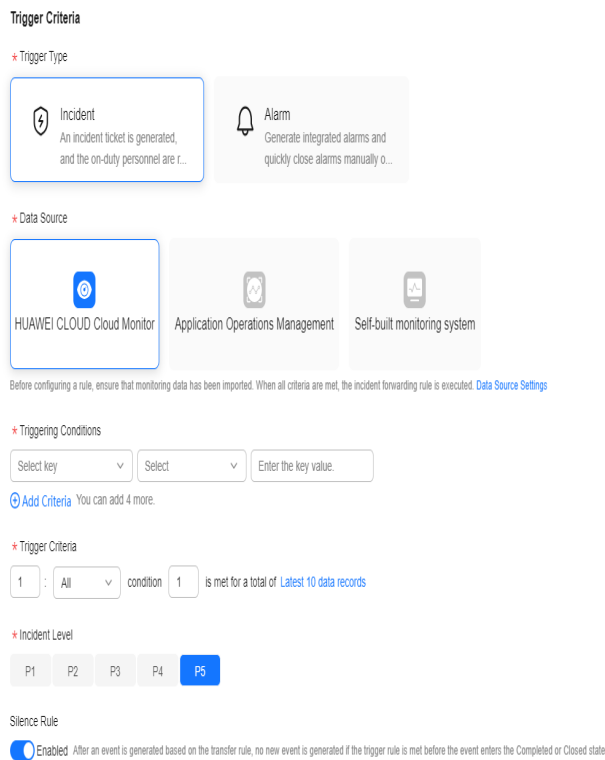
Step 4 Enter basic information such as the rule name and application name as prompted.

Figure 7-51 Entering basic information



Step 5 In the **Trigger Criteria** area, select the **Trigger Type**, select the **Data Source** for triggering the rule, configure the **Triggering Conditions**, and select the **Incident Level**.

Figure 7-52 Entering a trigger criteria



The key in the trigger conditions is described as follows:

| Parameter | Description | CES Alarm Field | AOM Alarm Field |
|-------------|---|-----------------------------|--|
| alarmId | Alarm ID | alarm_id | id |
| alarmName | Alarm name | alarm_name | event_name in metadata |
| alarmLevel | Specifies the alarm severity, which can be Critical, Major, Minor, or Suggestion . | AlarmLevel | event_severity |
| time | Time when an alarm is generated | time | starts_at |
| namespace | Specifies the service namespace. | namespace | namespace |
| region | Region | Region in template_variable | Regions can be distinguished by calling domain name. |
| application | Application name | / | / |

| | | | |
|---------------|---|--|--|
| resource Name | Resource name | ResourceName in template_variable | resource_id in metadata |
| resource Id | Resource ID | ResourceId in template_variable | / |
| alarmDesc | Alarm description | AlarmDesc in template_variable | / |
| URL | Original alarm URL | Link in template_variable | / |
| alarmStatus | Alarm status. The value can be alarm or ok. | alarm_status | / |
| alarmSource | Alarm source name. For example, if an alarm is reported from CES, the value of this field is CES. | / | / |
| additional | Additional alarm information. The format is additional.xxx. | Except the preceding parameters, other parameters are contained in this parameter and are represented by additional.xxx. For more information about CES fields, click here | Except the preceding parameters, other parameters are contained in this parameter and are represented by additional.xxx. For more information about AOM fields, click here . |

Step 6 In the **Contingency Plan** area, select the scripts or jobs associated with the forwarding rule. For details about how to add a script or job, see Automated O&M.

Figure 7-53 Entering the contingency plan.

Contingency Plan

Select Task

Emergency Plan Scripts Jobs

Select Create




Step 7 In the **Assignment Details** area, select the object and click **Submit**.

Figure 7-54 Filling the assignment rule



----End

Procedure for Editing, Enabling, Disabling, and Deleting a Forwarding Rule

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** Click , search for **Cloud Operations Center**, and click .
- Step 4** In the navigation pane on the left, choose **Incident Management > Incident Forwarding Rules**. The configuration page is displayed.
- Step 5** On the list page, click **More > Modify** or **Delete** in the **Operation** column to modify or delete a rule, click **Enable** or **Disable** in the **Operation** column to enable or disable a forwarding rule. After a forwarding rule is disabled, no incidents or alarms will be triggered.

----End

7.5 Integration Management

7.5.1 Overview

Integration configurations enable effortless and rapid integration with current or external monitoring systems for centralized alarm management. Each monitoring system employs distinct integration access keys for seamless interconnectivity.

Once a monitoring system is integrated, you can configure incident forwarding rules to convert alarms to incidents.

Currently, you can integrate CES, AOM, Prometheus, and other user-built monitoring systems into COC.

7.5.2 Integration Management

This document describes how to integrate monitoring sources.

Scenarios

Each monitoring source has a distinct integration process. For details, see the integration process description.

Integration Process

- Step 1** Log in to [COC](#).

- Step 2** In the navigation tree on the left, choose **Incident Management > Data Source Integration**.
 - Step 3** On the displayed page, select the data source to be accessed based on service requirements and click **Access integration**.
 - Step 4** On the integration page, you can view the integration introduction and integration procedure. After the integration is complete, click **Integrate** at the bottom.
 - Step 5** After the integration is confirmed, the status of the data source changes to **Enabled** in the **Integrated** area on the **Data Source Integration** page.
- End

Enabling and Disabling Integration

- Step 1** Log in to **COC**.
 - Step 2** In the navigation tree on the left, choose **Incident Management > Data Source Integration**.
 - Step 3** On the **Data Source Integration** page, click the **Enable** or **Disable** button to enable or disable a data source. You can also click a data source to go to the details page and click **Enable** or **Disable** at the bottom.
- End

Updating an Integration Sign


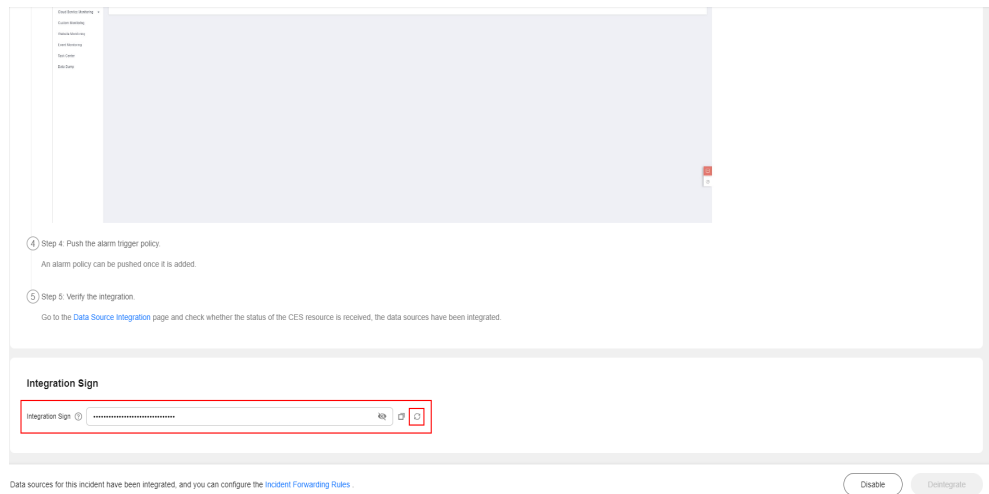
- Step 1** Log in to **COC**.
- Step 2** In the navigation tree on the left, choose **Incident Management > Data Source Integration**.
- Step 3** On the **Data Source Integration** page, click a data source. On the data source details page that is displayed, click  next to Integration sign to update the integration sign.

Figure 7-55 Updating an integration sign



----End

8 Change Management

8.1 Change Center

The change center provides a unified platform for engineers to manage change tasks. With the change center, engineers can submit tickets to manage change applications, approval, and execution.

Core capabilities: Currently, change management and configuration are supported.

8.1.1 Creating a Change Ticket

Scenarios

Create a change ticket in **Cloud Operations Center**.

Prerequisites

1. You have created an application by referring to Application Management page.
2. You have created an approver shift schedule by referring to Shift Schedule Management.

Precautions

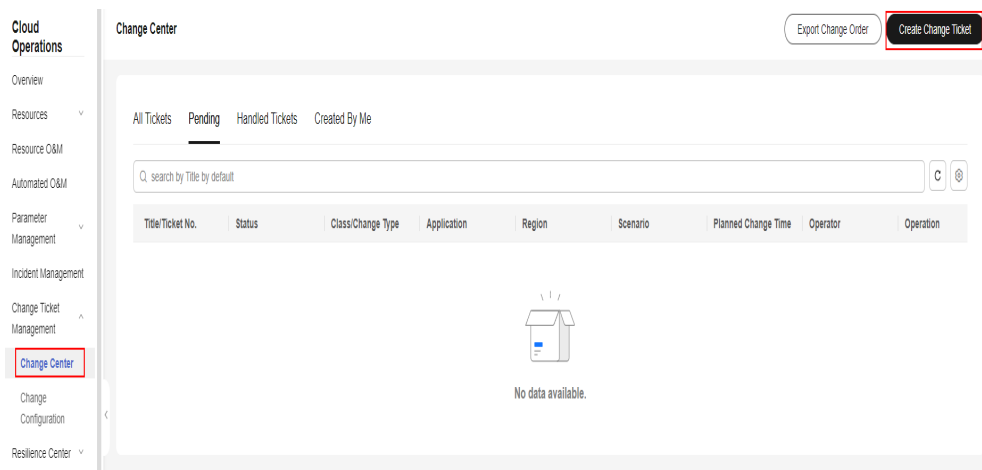
Confirm the content of change ticket and apply for the change based on the actual change requirement.

Procedure

Step 1 Log in to [COC](#).

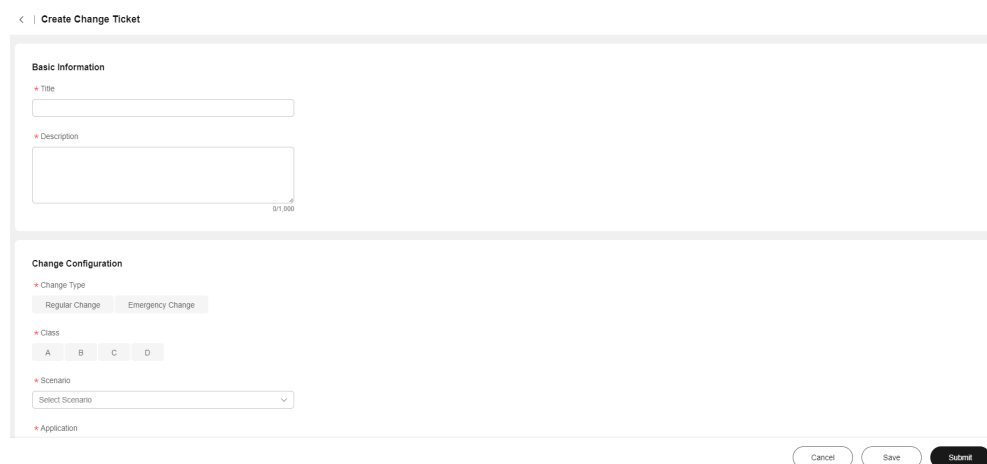
Step 2 In the navigation pane on the left, choose **Change Ticket Management > Change Center** and click **Create Change Ticket**.

Figure 8-1 Creating a change ticket



Step 3 Enter the basic information about the change ticket.

Figure 8-2 Configuring the basic change information



 **NOTE**

1. Change Type

Regular changes are non-emergency changes that can be requested, evaluated, approved, sorted, planned, tested, implemented, and reviewed using normal procedures.

Emergency 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.

2. Class: A > B > C > D

3. Scenario: Customize configurations based on service requirements.

4. Application: Select an application first and then the specific application resources.

5. Region: The change scope is defined by the change area and change application.

6. Change Plan: Generated by region.

The operator and coordinator need to be configured by region.

The planned change time window needs to be configured by region. (Note: The allowed change time window is restricted by the change level and change type.)

7. Change Plan: Change solution

After the configuration, click **Submit**.

8.2 Change Configuration

Overview

In the **Approval Configuration** page, engineers can specify the approval configurations.

Users can customize the change ticket approval process and approvers based on service requirements.

8.2.1 Configuring Approval Settings

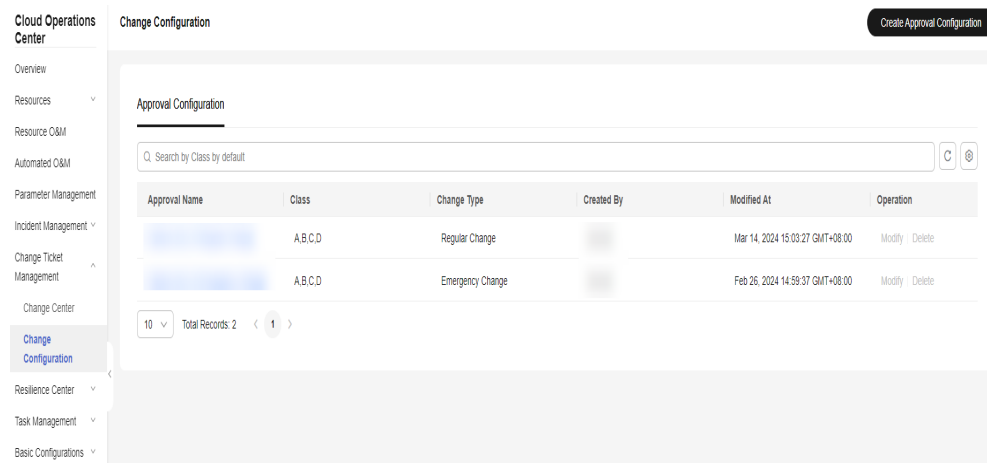
Overview

Users can configure the change type, change level, review process, and reviewer.

Creating an Approval Configuration

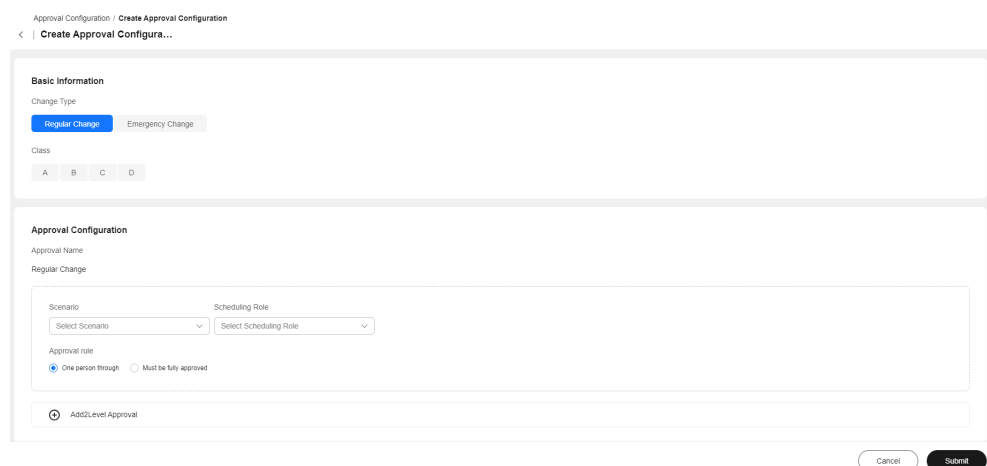
Step 1: In the navigation pane on the left, choose **Change Ticket Management > Change Configurations**. Click the **Review Configurations** tab and click **Create Review Configuration** in the upper right corner.

Figure 8-3 Creating a review configuration



Step 2: Configure the approval configuration.

Figure 8-4 Setting the review configurations



1. Basic Information

One change type and multiple change classes can be selected at a time.

2. Approval Configuration

The approval name is automatically generated.

The approver is determined by the scheduling scenario and scheduling role.

Approval rule: one person through or fully approved

3. Adding Multiple Approval Levels

Note: The scheduling role takes effect only after the approver is configured. If the approver is not specified, the change application cannot be submitted.

9 Resilience Center

9.1 Chaos Drills

9.1.1 Overview

COC allows users to perform automatic chaos drills covering from risk identification, emergency plan management, fault injection, and review and improvement, to mitigate risks and improve resilience of your applications.

9.1.2 Fault Type

Scenarios

You can analyze the possible faults of the system and establish the fault mode.

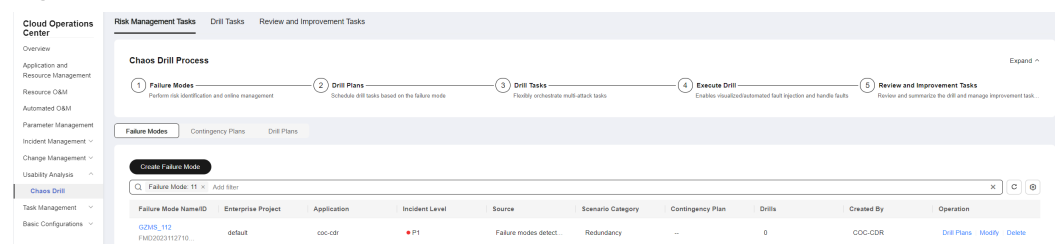
Precautions

Check whether the application of the target host or container and the incident level is correct.

Procedure

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill**, choose **Risk Management Tasks**, and switch to the **Failure Modes**.

Figure 9-1 Failure Modes



Step 3 Click **Create Failure Mode** and enter the failure mode information.

Figure 9-2 Creating a failure mode

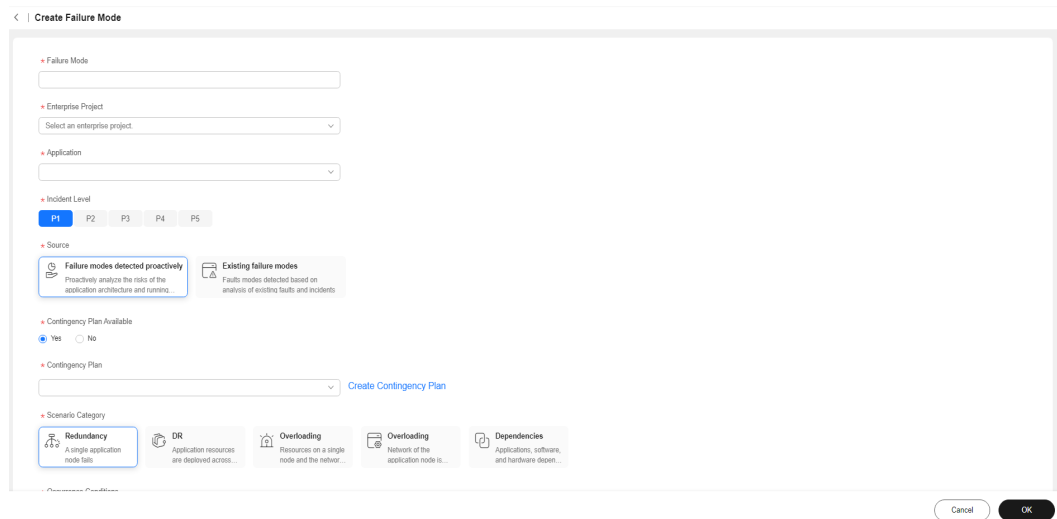


Table 9-1 Failure mode parameters

| Parameter | Description |
|----------------------------|---|
| Failure Mode | Custom failure mode name |
| Enterprise Project | Enterprise project to which the failure mode resource belongs. The default enterprise project is selected by default. |
| Application | Application to which the drill target belongs |
| Incident Level | For details about the incident level, see Incident Center . |
| Source | Including Failure modes detected proactively and Existing failure modes . |
| Contingency Plan Available | Yes or No . The default value is Yes . |
| Contingency Plan | Select a contingency plan from the drop-down list box. If no plan is available, create one. For details, see Emergency Plan . |
| Scenario Category | Failure scenario, including redundancy, disaster recovery, overload, configuration, and dependency |
| Occurrence Conditions | Possible conditions that cause the failure |

| Parameter | Description |
|--------------------|---|
| Fault Symptom | Service symptom when the failure occurs |
| Impact on Customer | Failure impact on customers |

Step 4 Select whether a contingency plan is provided. If you select **Yes**, select a contingency plan name from the text box. If no contingency plan is available, create a contingency plan and click **OK**.

----End

9.1.3 Drill Plan

Scenarios

When creating a drill plan, you can specify an executor. The executor creates a drill task by receiving a ticket. A drill task is associated with the fault mode and region.

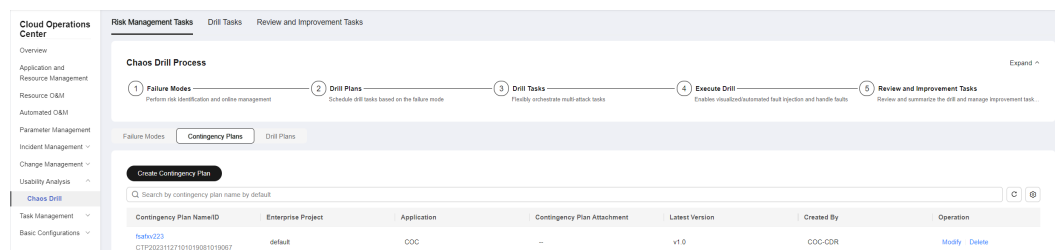
Precautions

You do not need to specify the enterprise project to which the drill plan belongs. The enterprise project must be the same as that associated with the fault mode.

Procedure

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill**, choose **Risk Management Tasks**, and switch to the **Drill Plans**.

Figure 9-3 Drill Plan page



Step 3 Click **Create Drill Plan**, select the failure mode, executor, region, and planned drill time, and click **OK**.

Figure 9-4 Creating a drill plan

Create Drill Plan ✕

* **Failure Mode**

* **Executed By**

* **Region**

* **Planned Drill Time** ⓘ

Step 4 The executor specified in the drill plan clicks Accept in the **Operation** column. The page for creating a drill task is displayed. The drill task is associated with the specified failure mode and region. In addition, the executor can track the progress of the drill task.

Figure 9-5 Creating a drill task

< | Create Task

Basic Information

Drill Task

Expected Recovery Duration (Minutes) ⓘ

Associated Failure Modes

| Failure Mode Name/ID | Enterprise Project | Application | Incident Level | Source | Scenario Category | Contingency Plan | Drills | Created By |
|----------------------|--------------------|-----------------|----------------|------------------------------|-------------------|------------------|--------|------------|
| bdskE2D14a29f68 | default | TestApplication | P1 | Failure modes detected pr... | Overloading | 0314 | 0 | perfest |

Attack Task Selection

Start Drill

1 Attack Task Group ⓘ Attack tasks in a task group are executed in parallel

Create Attack Task. 5 more Attack Tasks can be created

Create Task Group. 9 more Attack Task Groups can be created

End Drill

----End

9.1.4 Drill Tasks

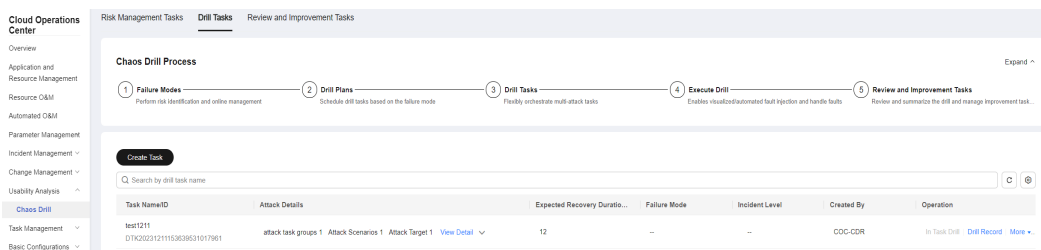
Creating a Drill Task

Create a drill task on COC.

Procedure - Creating a Drill Task

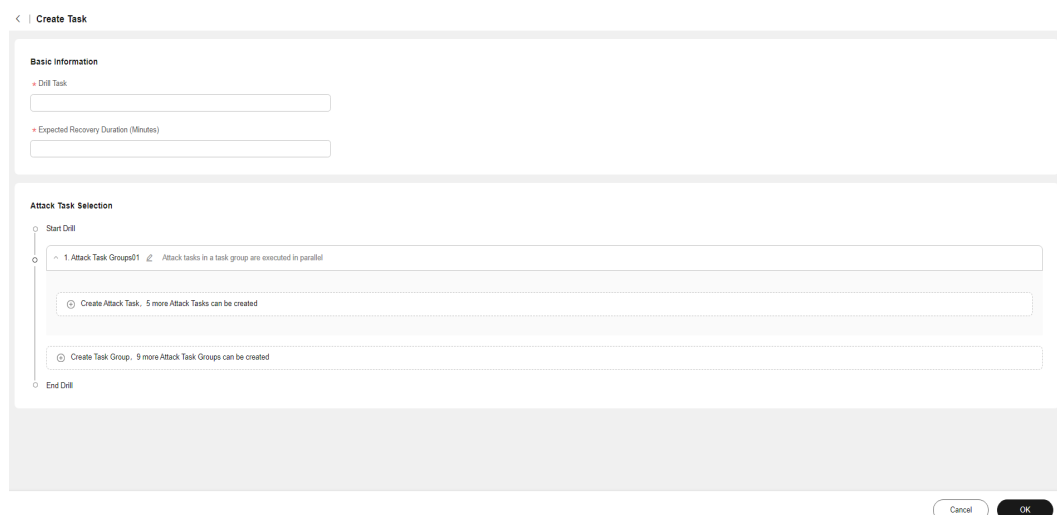
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.
- Step 3** Click **Create Task**. Or you can accept a drill plan to access the page for creating a drill task by following the instructions in [Drill Plan](#).

Figure 9-6 Creating a drill task

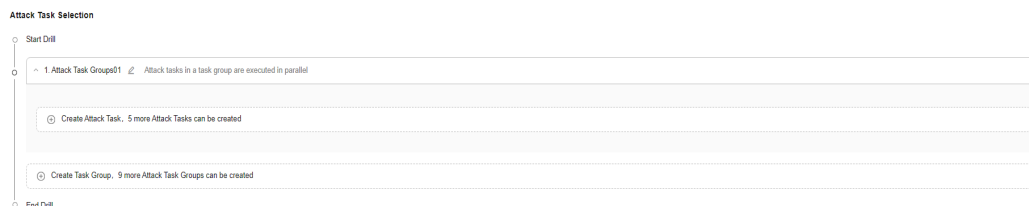


- Step 4** Enter the basic information about the drill task, including the drill task name and expected recovery duration (in minutes).

Figure 9-7 Basic information of a drill task

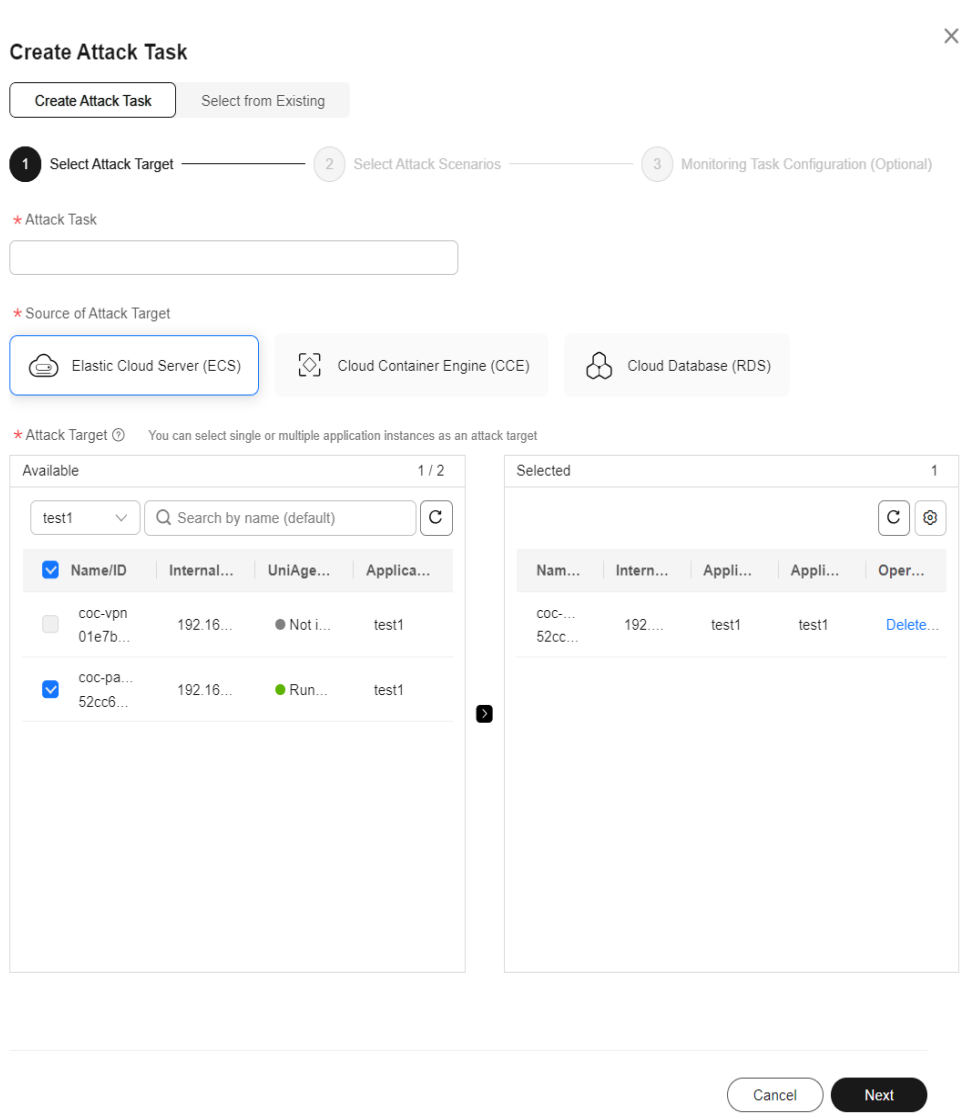


- Step 5** Select an attack task. By default, there is one attack task group. You can click **Create Task Group** to add a task group or click **Create Attack Task** to access the page for creating an attack task.

Figure 9-8 Selecting an attack task

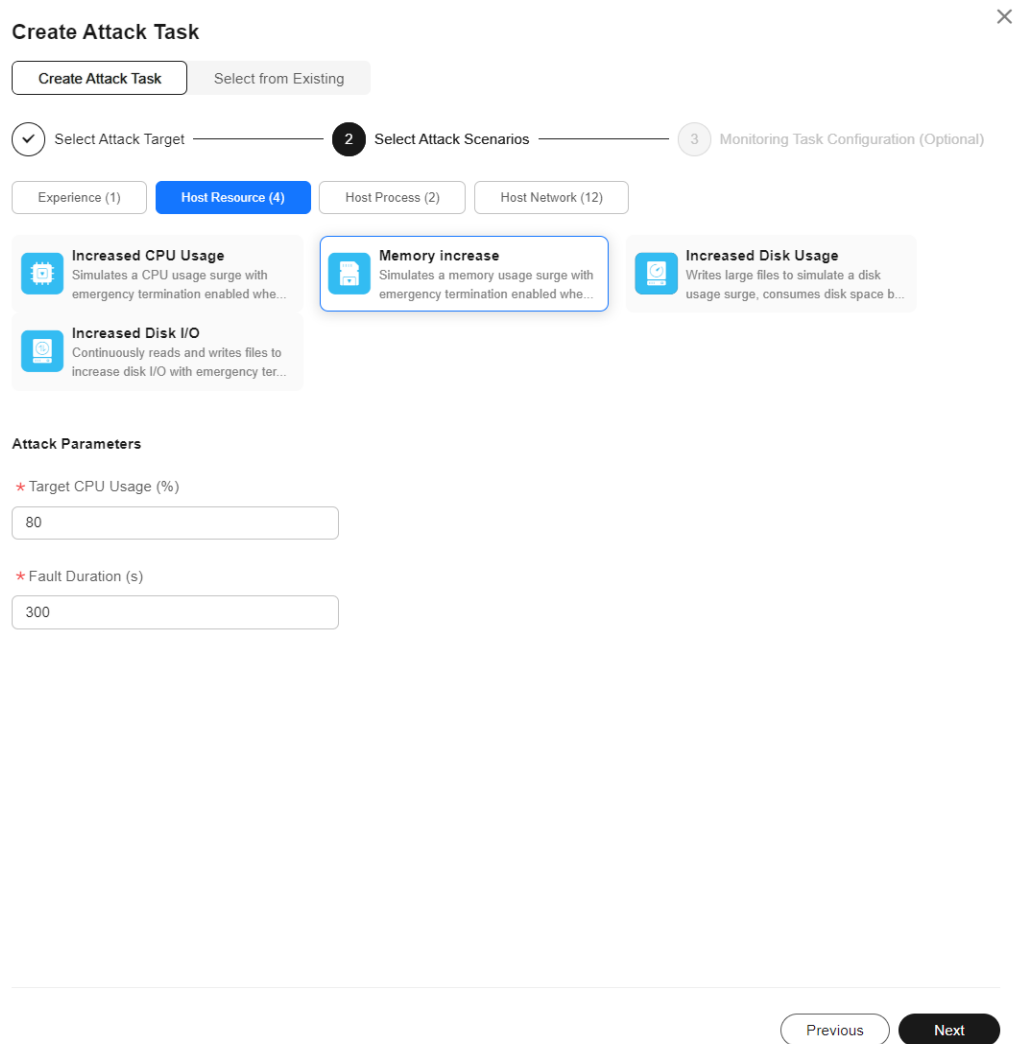
- Step 6** Add an attack task. You can create an attack task or select an existing attack task. If you have not created an attack task before, you need to click **Create Attack Task**. However, if you have created attack tasks previously, you can select **Select from Existing**.
- Step 7** Create an attack task. First, select an attack target, and then select an attack scenario. Different attack targets correspond to different attack scenarios. Enter the attack task name. The attack target sources include **Elastic Cloud Server (ECS)** or **Cloud Container Engine (CCE)**, **Cloud Database (RDS)**, and **Distributed Cache Service (DCS)**. If you select ECS, you will need to select the corresponding server from the list below and click **Next**.

Figure 9-9 Selecting ECS as the attack target source



Step 8 Select an attack scenario, set attack parameters, and click **OK**. The scenarios include **Host Resource**, **Host Process**, and **Host Network**.

Figure 9-10 ECS attack scenarios



Step 9 (Optional) Configure drill monitoring task metrics that include **Stable-Status Metrics** and **Monitoring Metrics**. You can specify the host in the attack target and the name of the metric to be monitored. During the drill, you can view the real-time drill line chart of the corresponding metric.

Figure 9-11 ECS attack scenario drill monitoring configuration

Create Attack Task ×

▼ Select Attack Target ————— ▼ Select Attack Scenarios ————— ● **3** Monitoring Task Configuration (Optional)

Steady-state Indicators ?

| | | | | |
|---------------------------|-------------------|---|----|----|
| Host name: coc-patch-h... | proc_zombie_count | 1 | 20 | 🗑️ |
|---------------------------|-------------------|---|----|----|

⊕ Add pursuant to 99

Monitoring Indicators ?

| | | | | |
|---------------------------|-------------------|---|----|----|
| Host name: coc-patch-h... | proc_zombie_count | 1 | 20 | 🗑️ |
|---------------------------|-------------------|---|----|----|

⊕ Add pursuant to 99

Step 10 If you select **Cloud Container Engine (CCE)** as the attack target source, you will need to select an application and pod (select a cluster, namespace, workload type, and workload in sequence). You can specify pods or the number of pods, and click **Next**.

Figure 9-12 Selecting CCE as the attack target source and specifying a pod

✕

Create Attack Task

1 Select Attack Target — 2 Select Attack Scenarios — 3 Monitoring Task Configuration (Optional)

* Attack Task

* Source of Attack Target

* Application

* POD ⓘ

Cluster: coc-alpha-auto | namespace: coc-chaos | Workload Type: Deploy... | Workload: coc-cdr

Selected PODs: 1

🔍 Search by POD name

| <input checked="" type="checkbox"/> POD | POD Status |
|---|--|
| <input checked="" type="checkbox"/> coc-cdr-7f9d84cfb-j5nzs | ● Running |

Total Records: 1 10 < 1 >

Figure 9-13 Selecting CCE as the attack target source and specifying the quantity

Create Attack Task ✕

1 Select Attack Target — 2 Select Attack Scenarios — 3 Monitoring Task Configuration (Optional)

* Attack Task

* Source of Attack Target

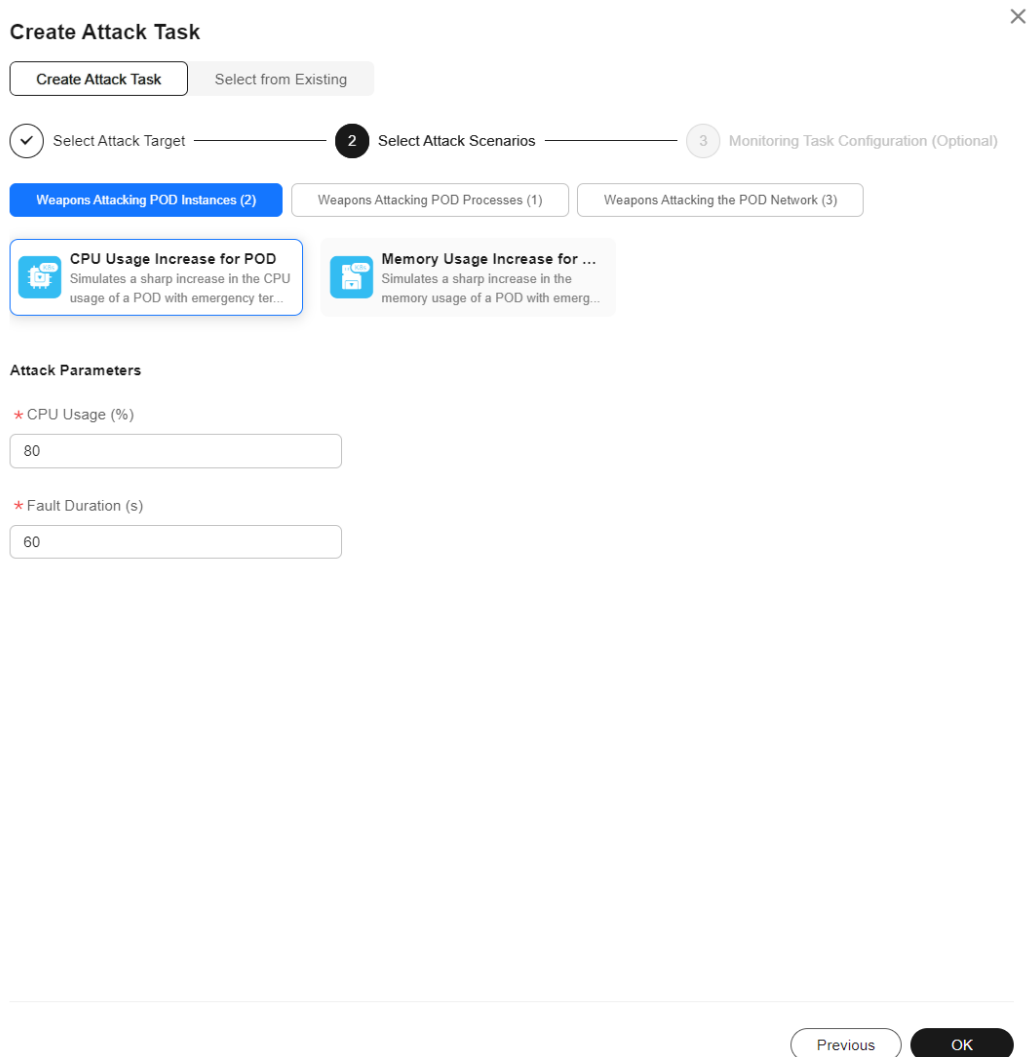
* Application

* POD ⓘ

* PODs

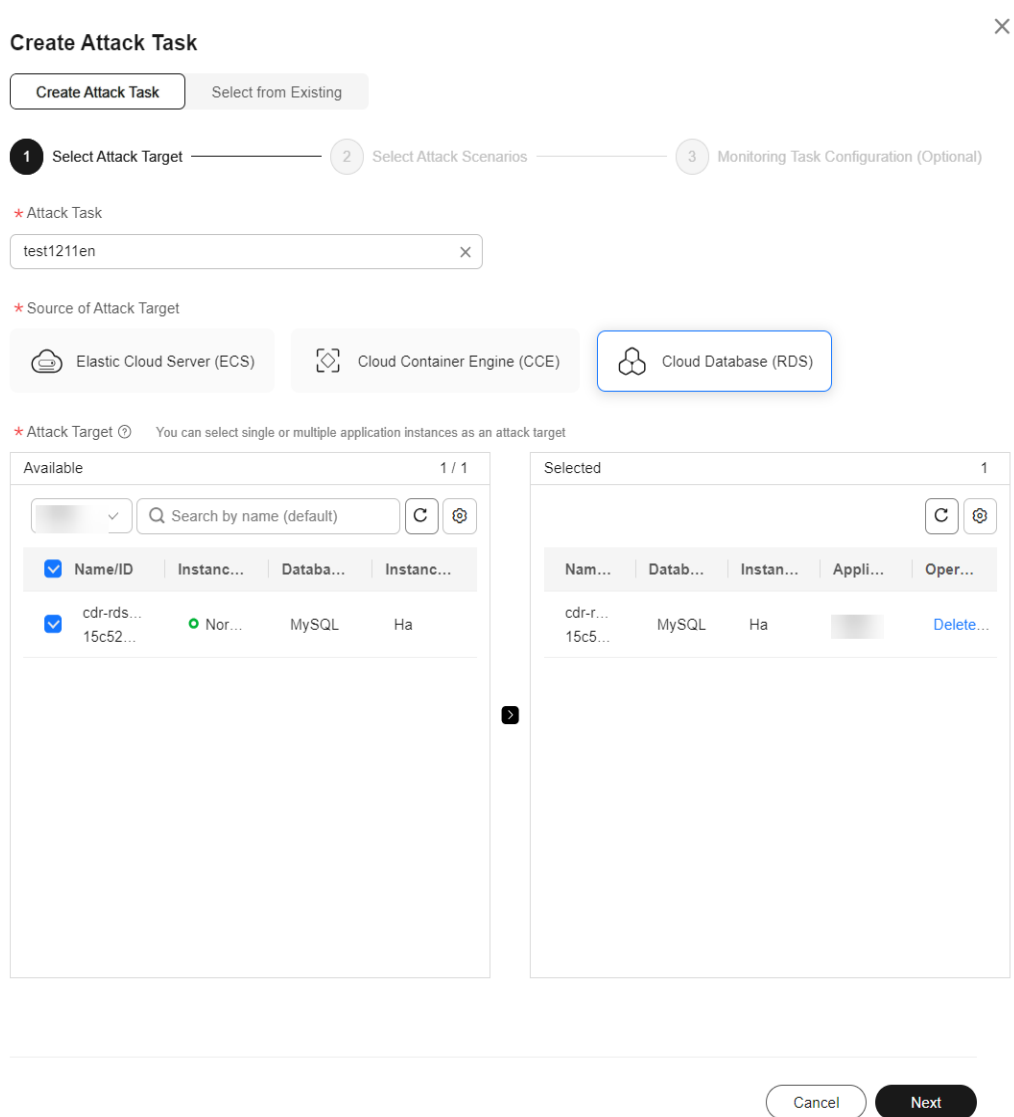
Step 11 Select a CCE attack scenario, set attack parameters, and click **OK**. The scenarios include **Weapons Attacking POD Instances**, **Weapons Attacking POD Processes**, and **Weapons Attacking the POD Network**.

Figure 9-14 CCE attack scenarios



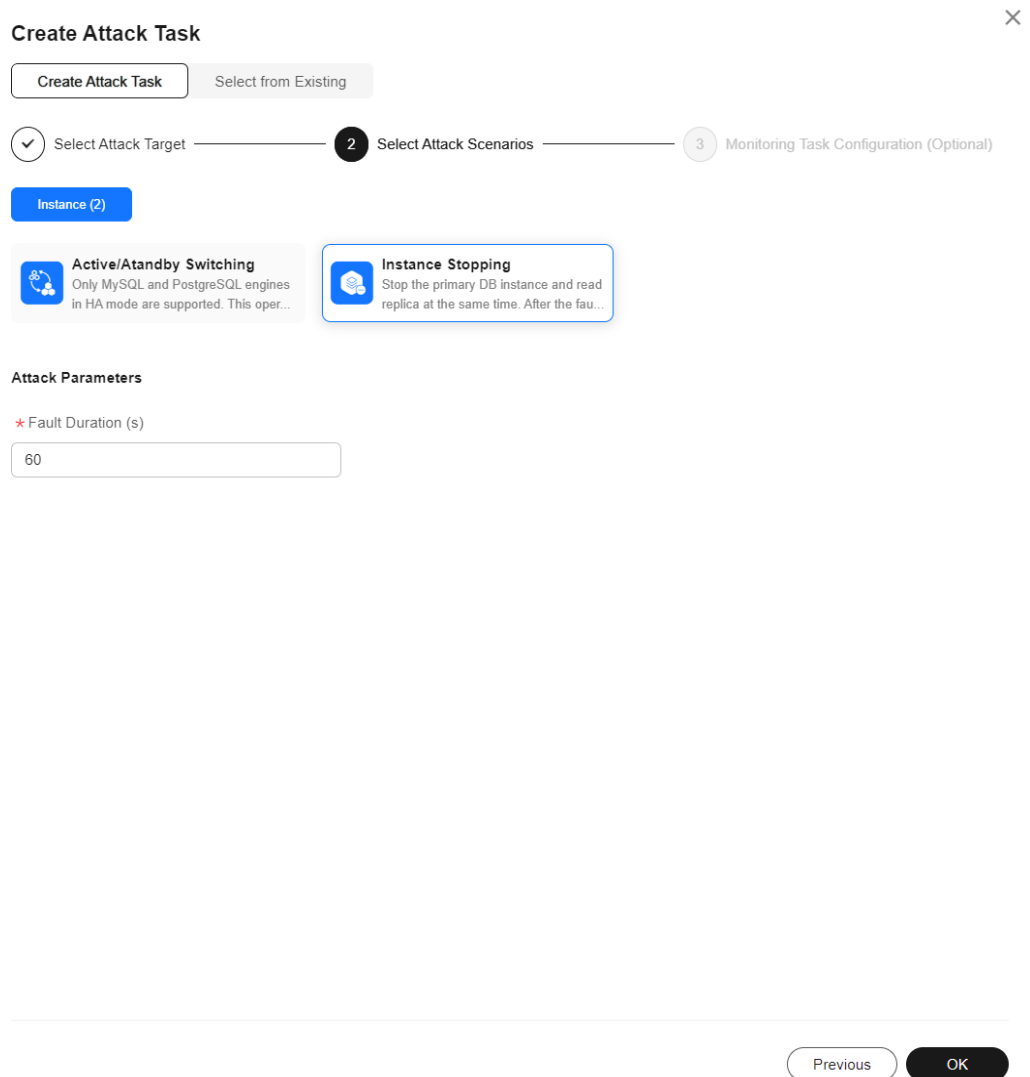
Step 12 If you select RDS as the attack source, select an RDS DB instance and click **Next**.

Figure 9-15 Selecting RDS as the attack target source



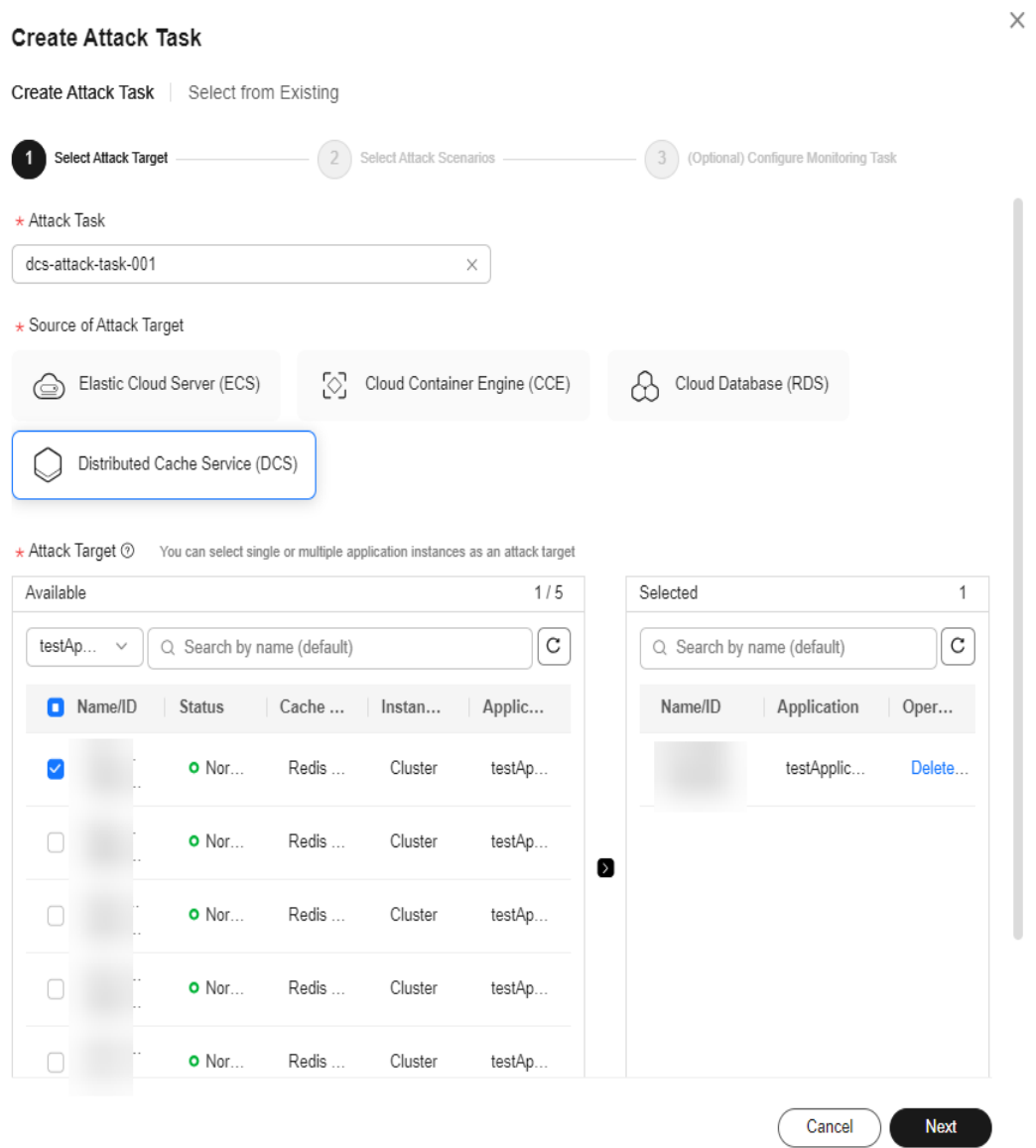
Step 13 Select an RDS attack scenario, set attack parameters, and click **OK**.

Figure 9-16 Cloud Database (RDS) attack scenarios



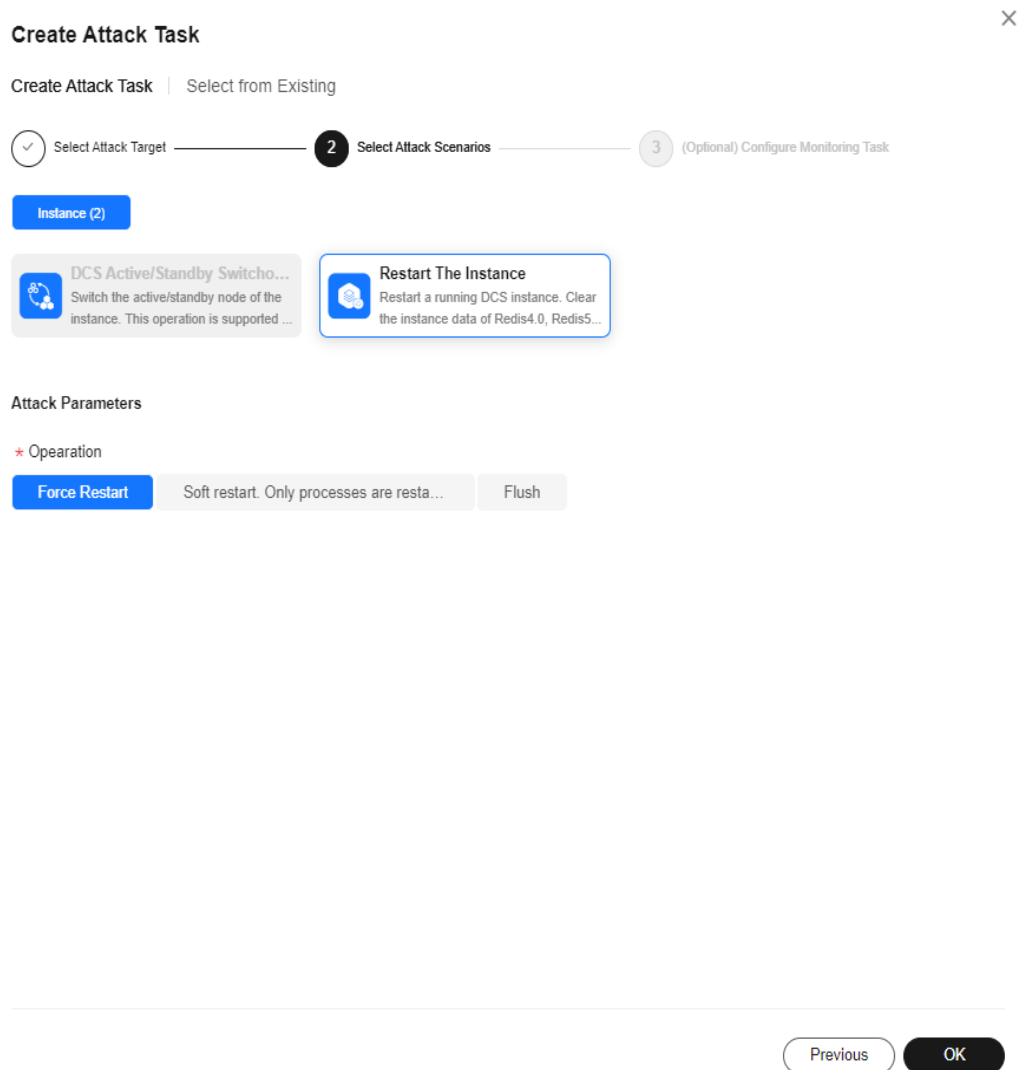
Step 14 If you select DCS as the attack source, select a DCS instance and click **Next**.

Figure 9-17 DCS attack scenarios



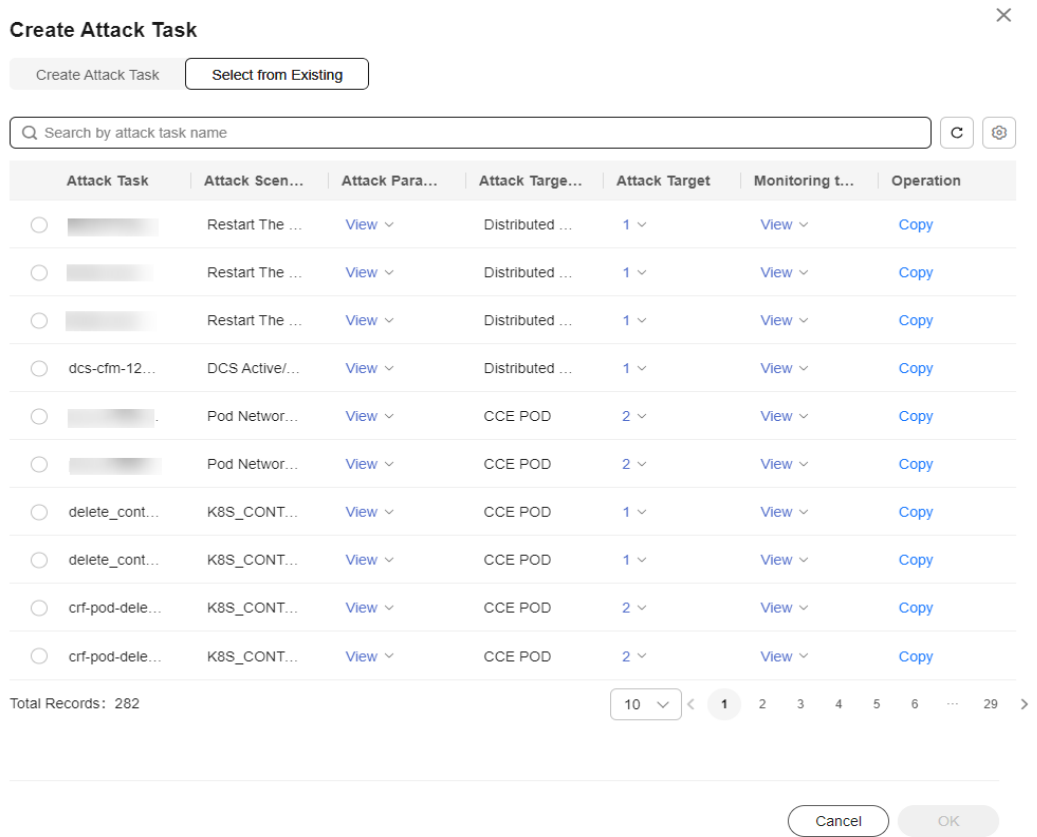
Step 15 Select the DCS attack scenario, set required parameters, and click **OK**.

Figure 9-18 DCS attack scenarios



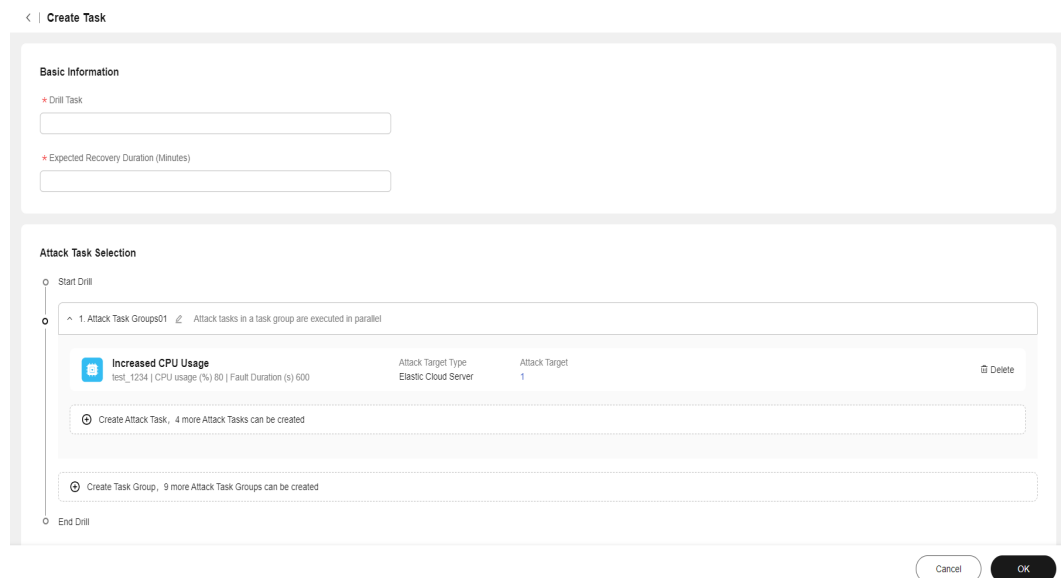
Step 16 If you select **Select from Existing**, select the created attack task from the task list below and click **OK**.

Figure 9-19 Selecting an existing attack task



Step 17 Click **OK**. The drill task is created.

Figure 9-20 Clicking OK



----End

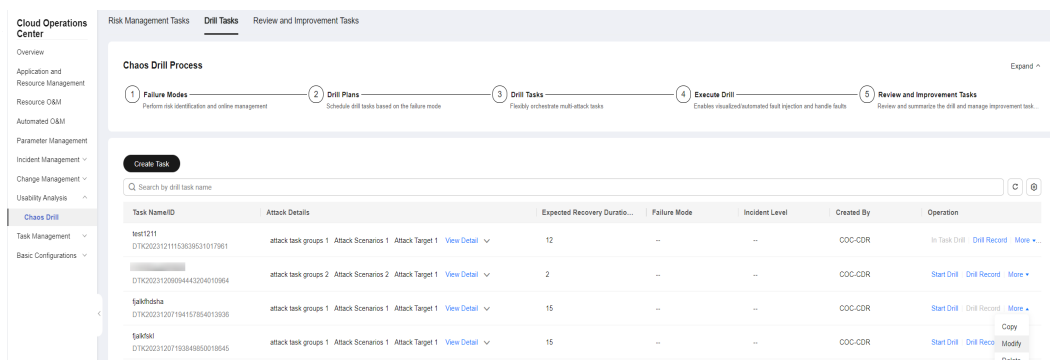
Editing a Drill Task

You can edit a drill task. However, if a drill record has been generated for the drill task, the task cannot be edited.

Procedure - Editing a Drill Task

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.
- Step 3** Choose **More > Edit** in the **Operation** column to modify the basic information about the drill task.

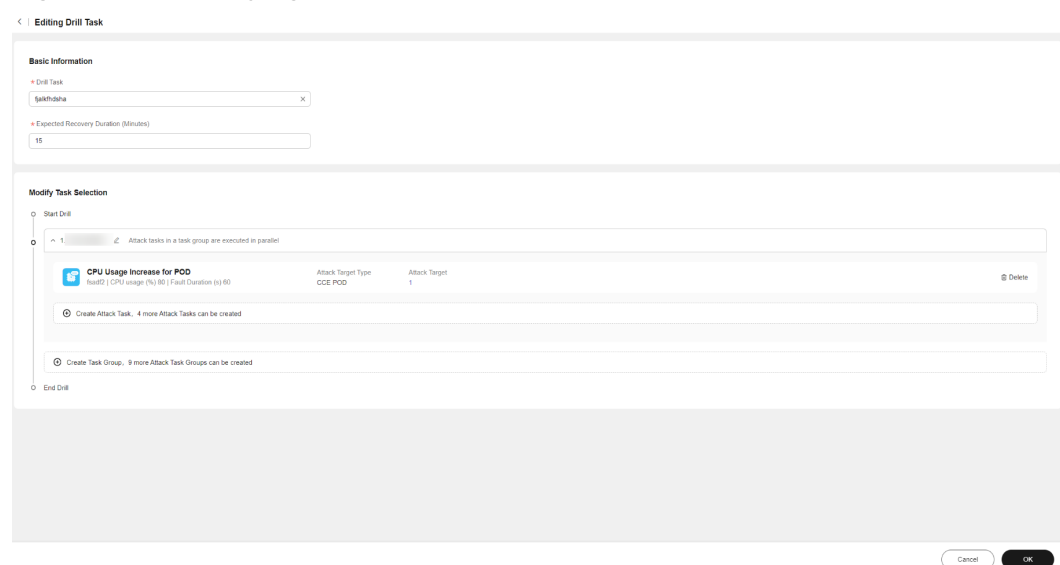
Figure 9-21 Locate the target task, click Modify in the **Operation** column.



- Step 4** You can add a task group, add an attack task, or delete an existing attack task. An existing attack task cannot be modified.

- Step 5** Click **OK**.

Figure 9-22 Modifying a drill task



----End

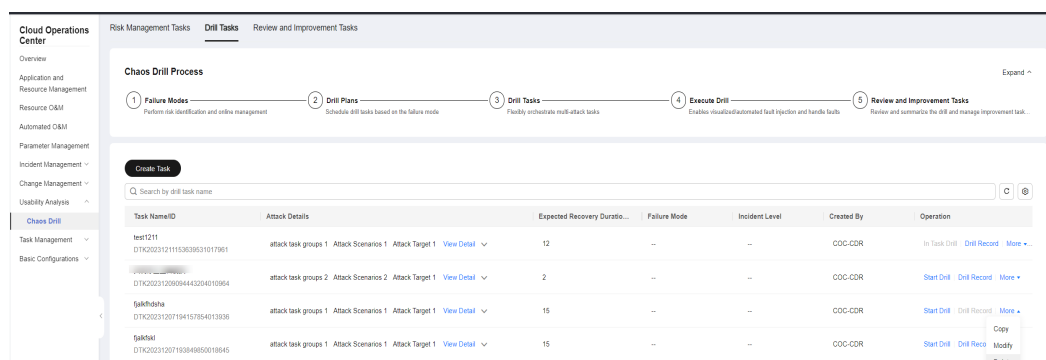
Deleting a Drill Task

Delete a created drill task. A task that has generated drill records or has associated with drill plans cannot be deleted.

Procedure - Deleting a Drill Task

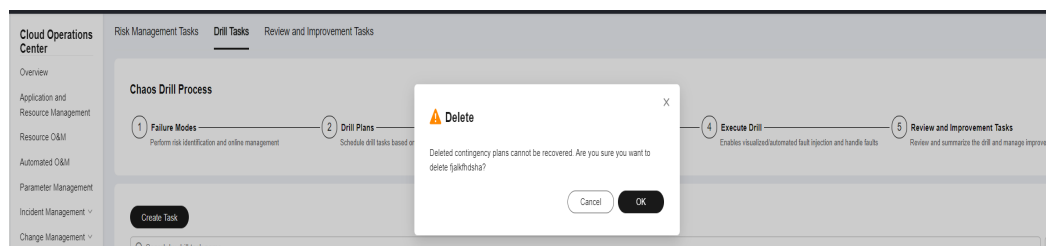
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.
- Step 3** Locate the target drill task, choose **More > Delete** in the **Operation** column.

Figure 9-23 Drill task list



- Step 4** In the displayed dialog box, click **OK**.

Figure 9-24 Deleting a drill task



----End

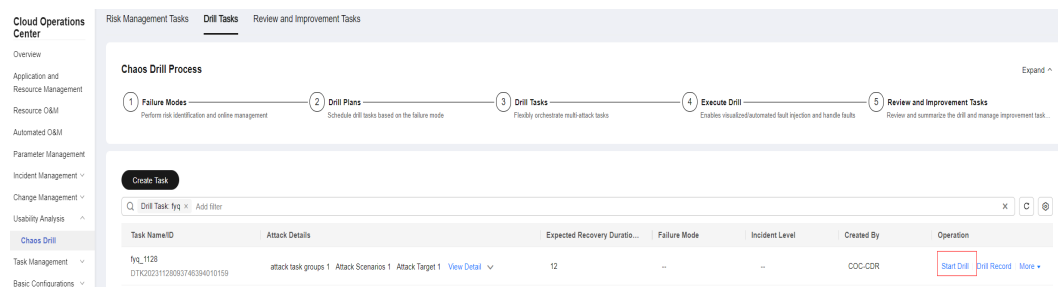
Starting a Drill Task

Start a drill task.

Procedure - Starting a Drill Task

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.
- Step 3** Locate the target drill task, click **Start Drill** in the **Operation** column.

Figure 9-25 Starting a drill task



Step 4 Click **Drill Record** in the **Operation** column to view the attack progress, including probe installation, drill execution, and environment clearance. The system automatically executes the drill task. The execution time depends on the attack time of the weapon.

Figure 9-26 Attack progress

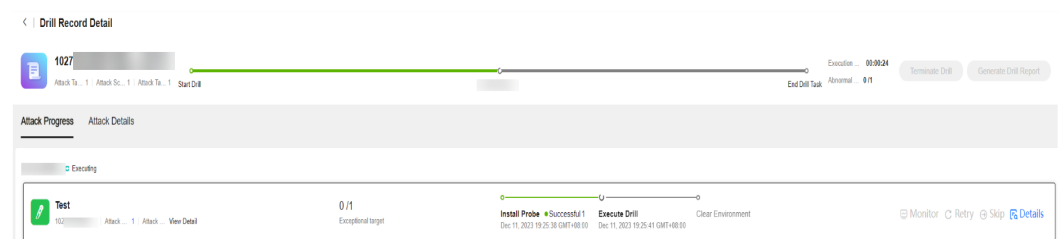
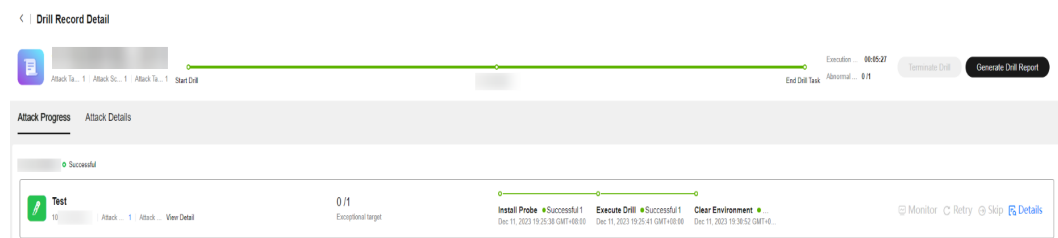
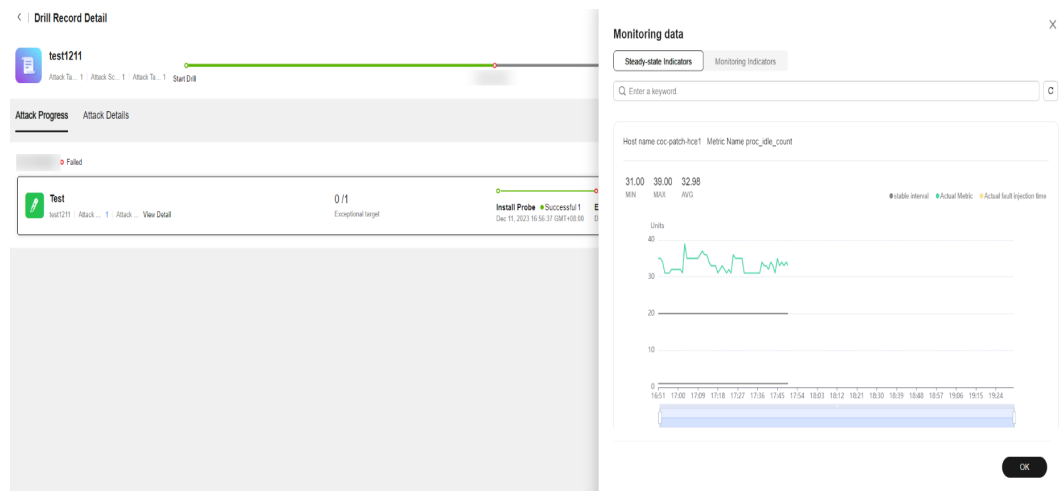


Figure 9-27 Attack completed



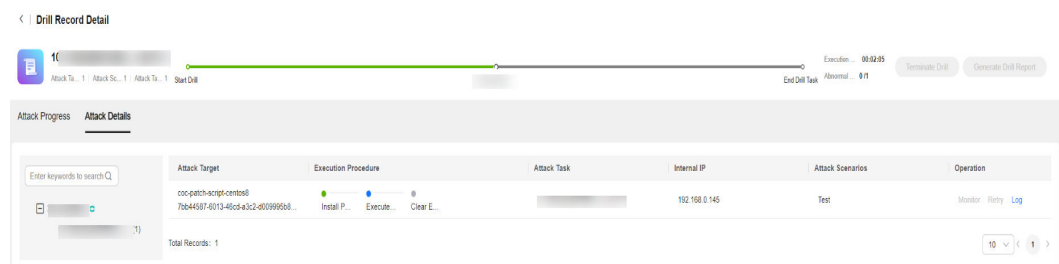
Step 5 During the drill task execution, you can click **Terminate Drill** to end the drill task, click **Retry** to retry the current step, or click **Skip** to skip the current step and go to the next step. If you have configured a drill monitoring task when creating the attack target, you can click **Monitor** to view the real-time monitoring data of the attack target.

Figure 9-28 Drill monitoring data



Step 6 Click **Details** to go to the **Attack Details** tab page.

Figure 9-29 Attack details



----End

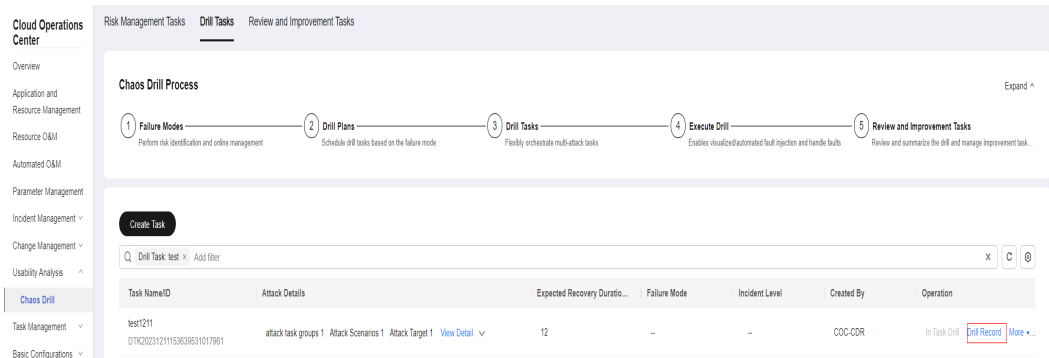
Viewing Drill Records

View the drill records of a drill task. A drill task that has not been drilled does not contain drill record.

Procedure - Viewing Drill Records

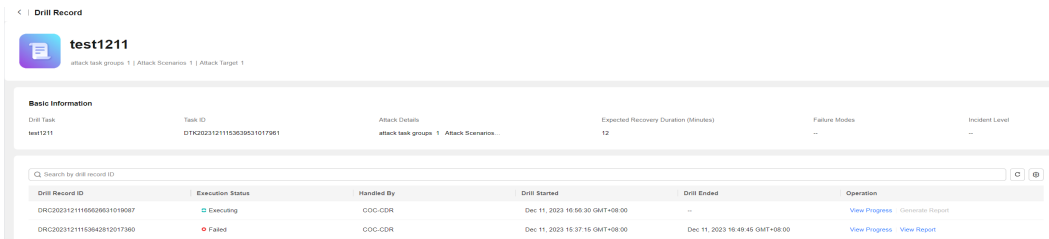
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.
- Step 3** Locate the target drill task, click **Drill Record** in the **Operation** column.

Figure 9-30 Drill task list



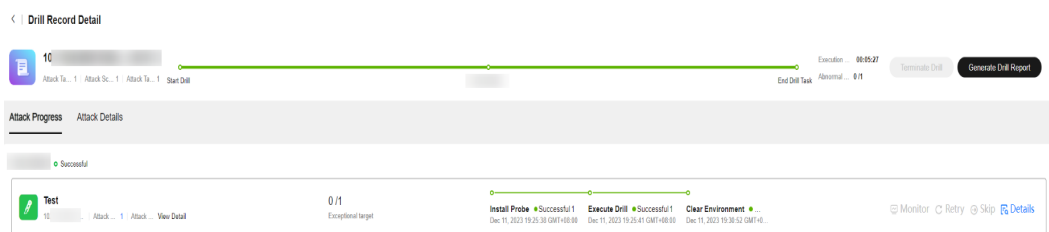
Step 4 The basic information about the drill task includes the drill task name, drill task ID, attack details, and failure mode. All drill records include the drill record ID, execution status, executor, drill start time, and drill end time.

Figure 9-31 Drill Records



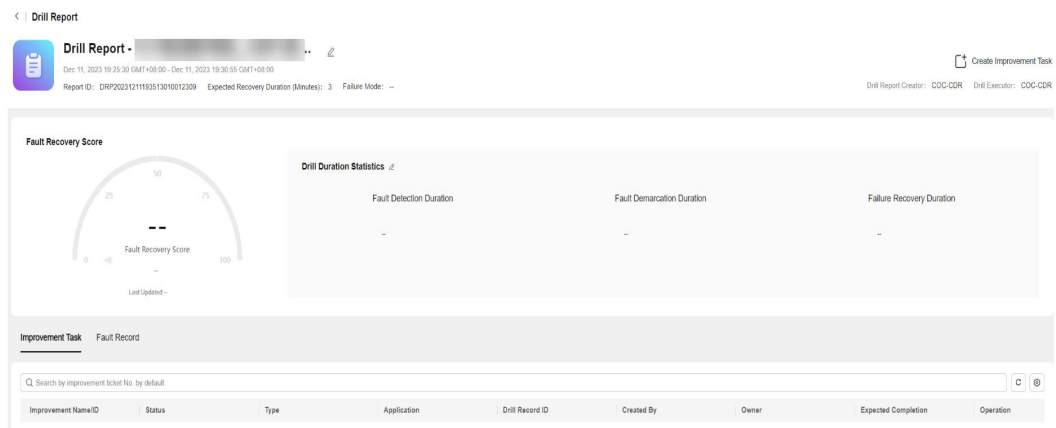
Step 5 Click **View Progress** to view the attack progress and attack details of the current drill task.

Figure 9-32 Attack progress



Step 6 Click **Generate Report** to create or view a drill report. For details, see [Drill Report](#).

Figure 9-33 Viewing a drill report



----End

9.1.5 Drill Report

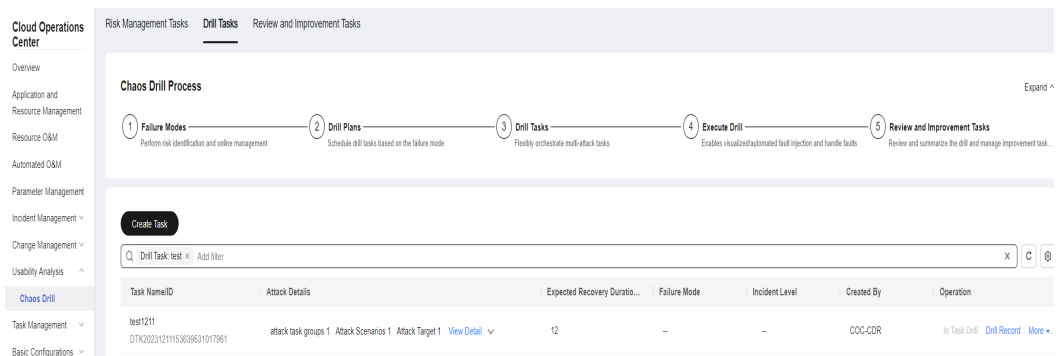
Creating a Drill Report

Once a drill is finished, you can create a drill report.

Procedure

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Chaos Drill** and click **Drill Tasks**.

Figure 9-34 Drill tasks



- Step 3** Locate the row containing the finished drill task and click **Drill Record** in the **Operation** column. In the displayed drill record list, locate a desired drill record, click **Create Report** or **View Progress** in the **Operation** column. On the displayed **Drill Record Detail** page, click **Create Drill Report** on the right.

Figure 9-35 Drill record list

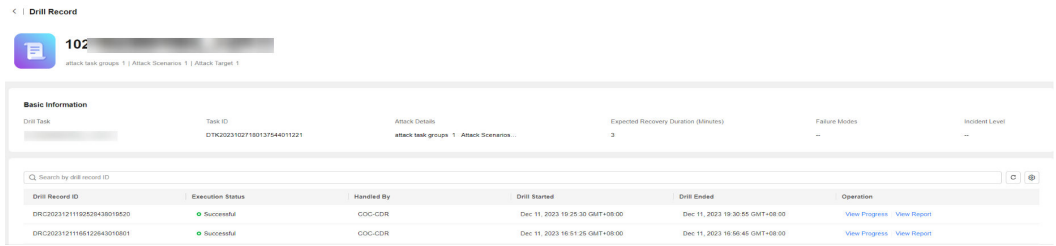
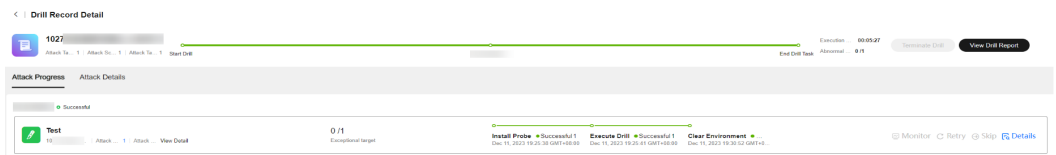
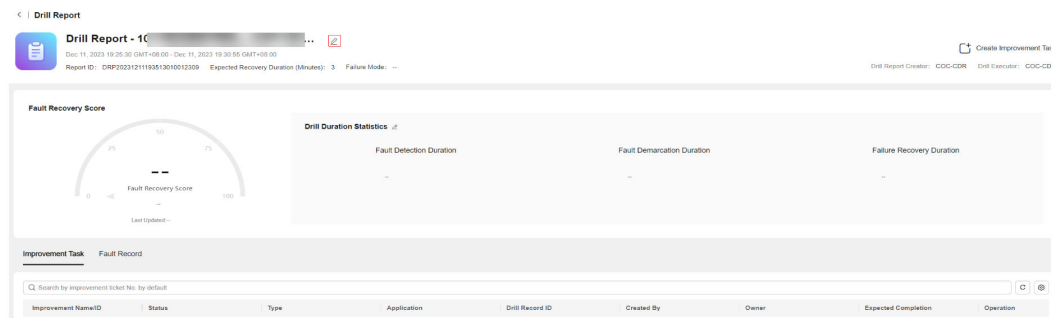


Figure 9-36 Drill Record Detail page



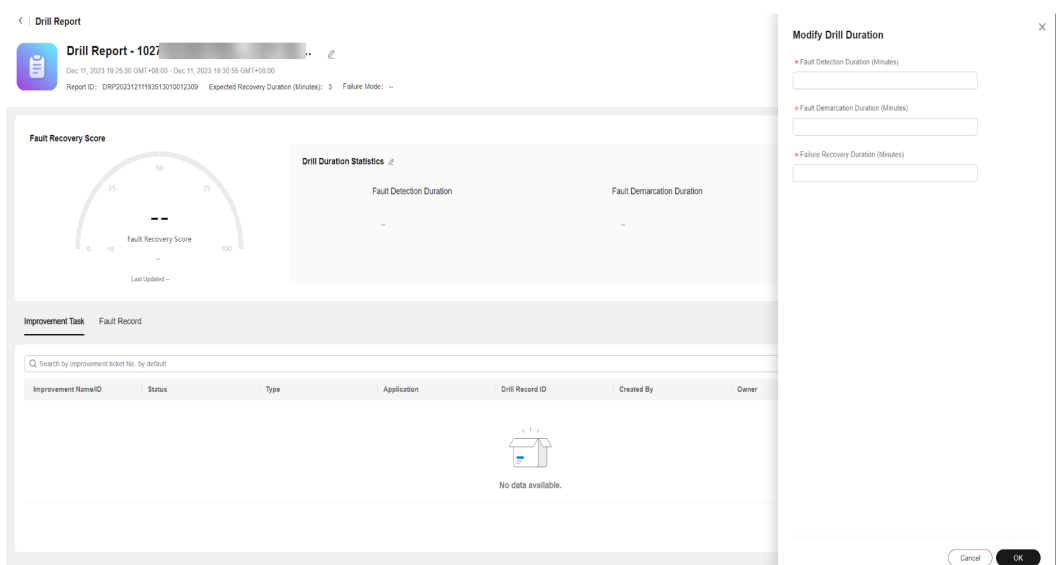
Step 4 Go to the drill report page and update the report name.

Figure 9-37 Drill report details



Step 5 On the drill report details page, enter the drill duration and click OK.

Figure 9-38 Modifying drill duration



Step 6 Go to the drill report page, click **Create Improvement Task**, enter information about the improvement item, and click **OK** to save the created improvement ticket.

Figure 9-39 Creating Improvement Item

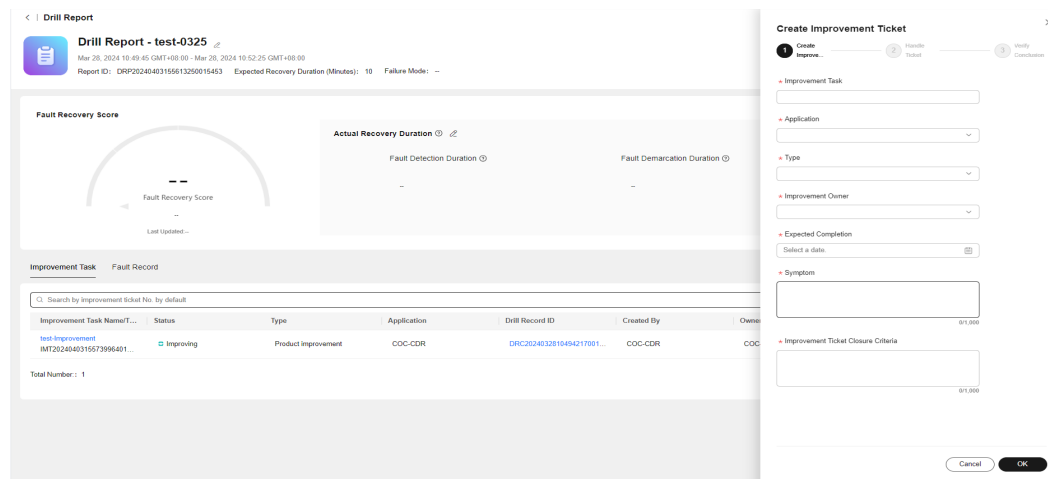
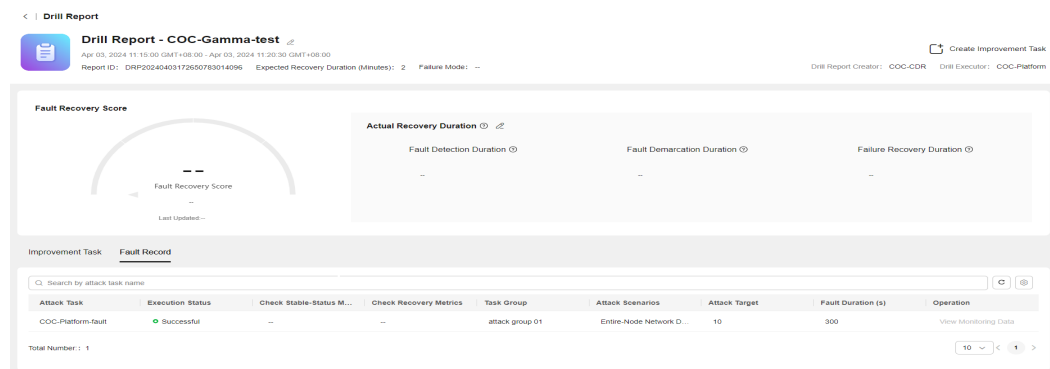


Table 9-2 Improvement ticket parameters

| Parameter | Description |
|-------------------------------------|--|
| Improvement Task | Improvement task name |
| Application | Application to which the improvement task belongs |
| Type | Type of the improvement task |
| Improvement Owner | Owner of the improvement task |
| Expected Completion | Expected completion time of the improvement task |
| Symptom | Symptom |
| Improvement Ticket Closure Criteria | Criteria for the closure of the improvement ticket |

Step 7 Go to the drill report page and click the **Fault Record** tab to view fault records.

Figure 9-40 Fault record



----End

9.2 Emergency Plan

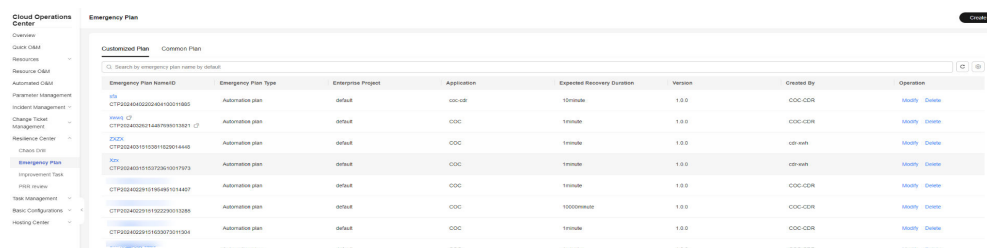
Overview

You can create an emergency plan for a system fault that may occur and use the plan if the fault occurs.

Creating an Emergency Plan

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Resilience Center > Emergency Plan**. Click the **Customized Plan** tab.

Figure 9-41 Customized Plan tab page



- Step 3** Click **Create**. On the displayed page, set the basic information about the emergency plan.

Figure 9-42 Creating an emergency plan

Table 9-3 Parameters for configuring basic information about an emergency plan

| Parameter | Description |
|---------------------|---|
| Emergency Plan Name | Customized emergency plan name |
| Enterprise Project | Enterprise project to which the emergency plan belongs. The default value is default . |
| Application | Application to which the emergency plan belongs |
| Recovery Duration | Fault recovery duration |
| Version | Version number |
| Summary | Description about the emergency plan |

Step 4 Set the troubleshooting information. The emergency plan type can be set to **Automation Plan** or **Document Plan**.

Step 5 If **Automation Plan** is selected, you can select **Scripts** or **Jobs** for **Handling Method**.

Figure 9-43 Troubleshooting

Step 6 If **Scripts** is selected as the handling method, you can select custom scripts or common scripts as the associated scripts.

Figure 9-44 Associating a custom script

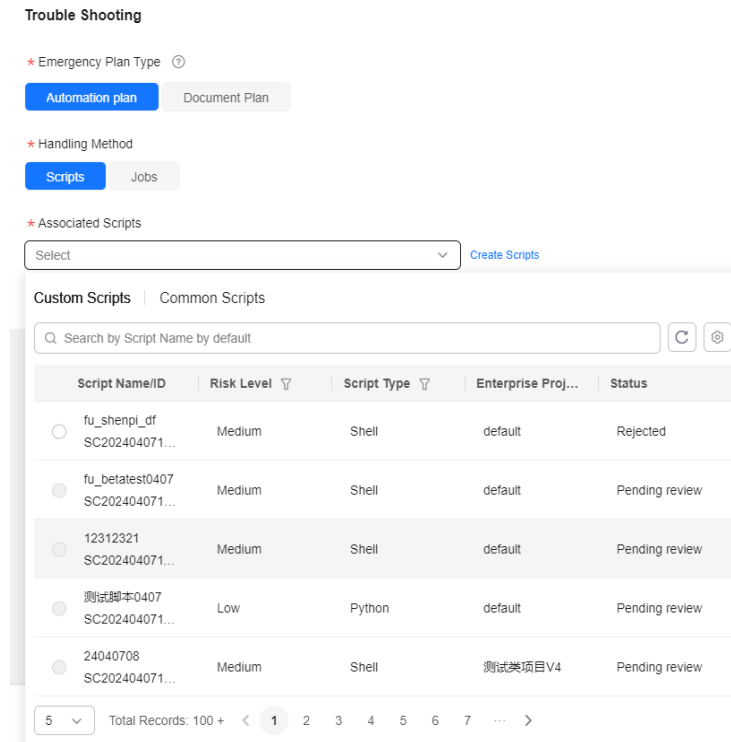
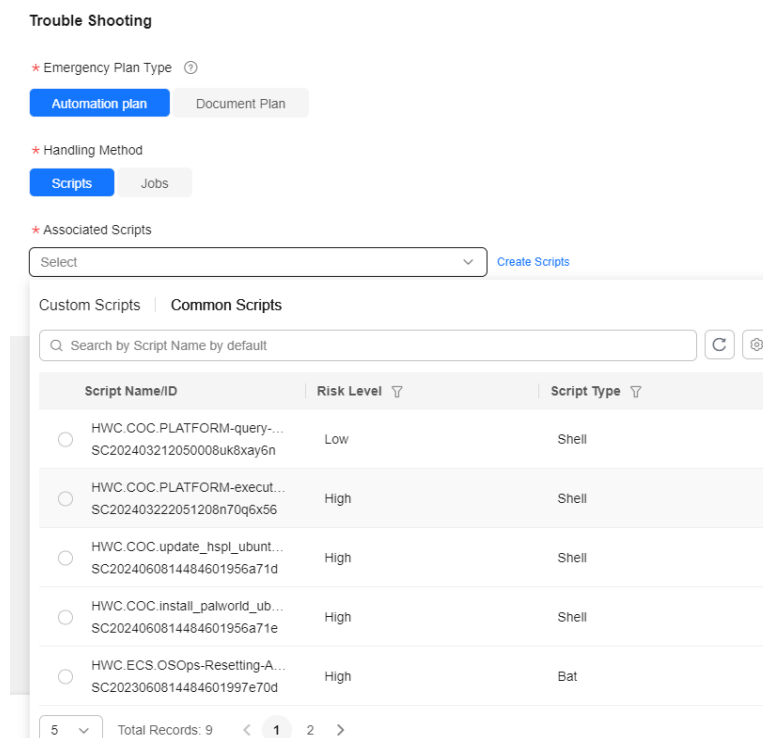


Figure 9-45 Associating a common script



Step 7 If **Jobs** is selected as the handling method, you can select custom jobs or common jobs as the associated job.

Figure 9-46 Associating a custom job

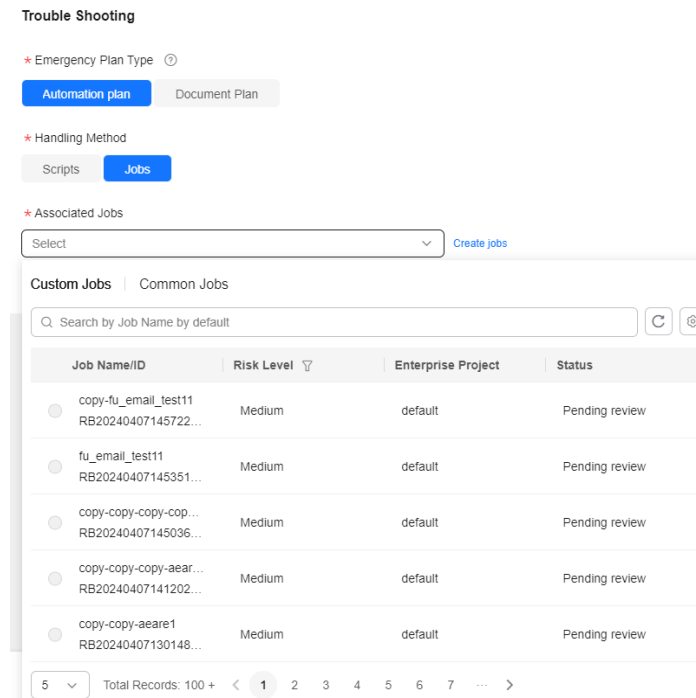
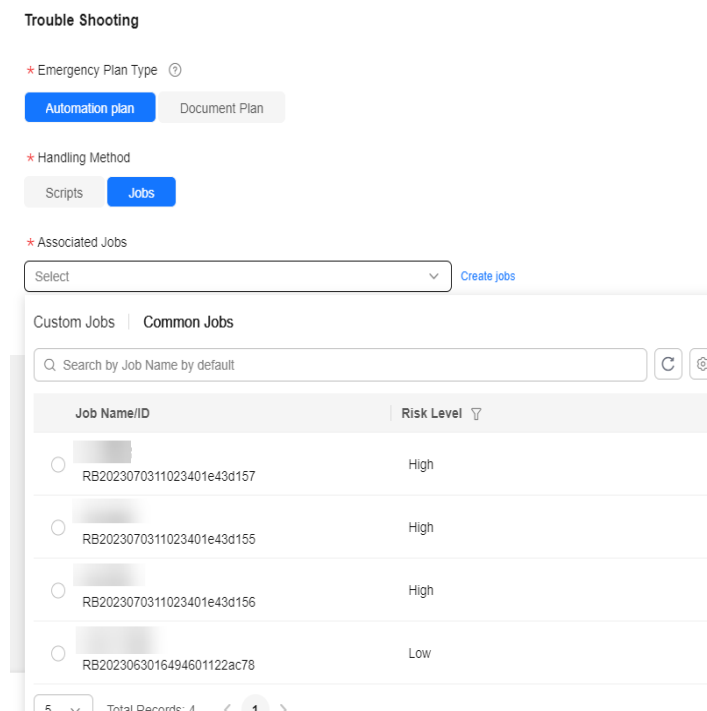
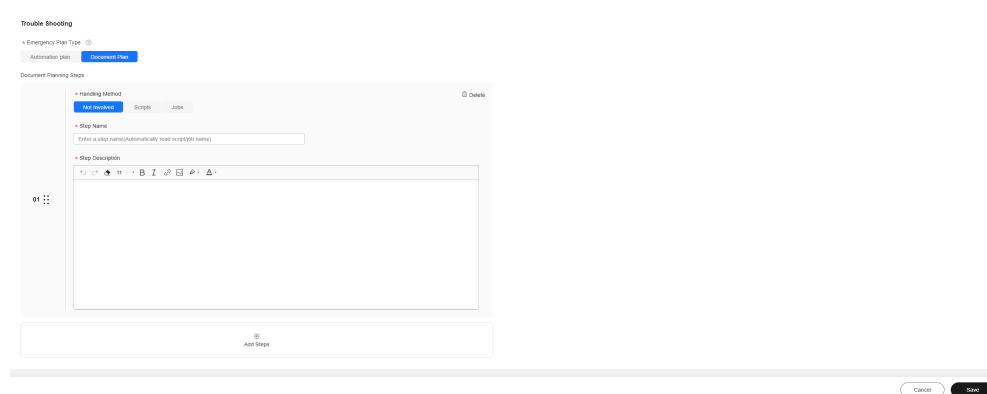


Figure 9-47 Associating a common job



Step 8 If **Document Plan** is selected as the emergency plan type, you can select **Not Involved**, **Scripts**, or **Jobs** for **Handling Method**, enter the step name and description, and click **Save**.

Figure 9-48 Document plan steps

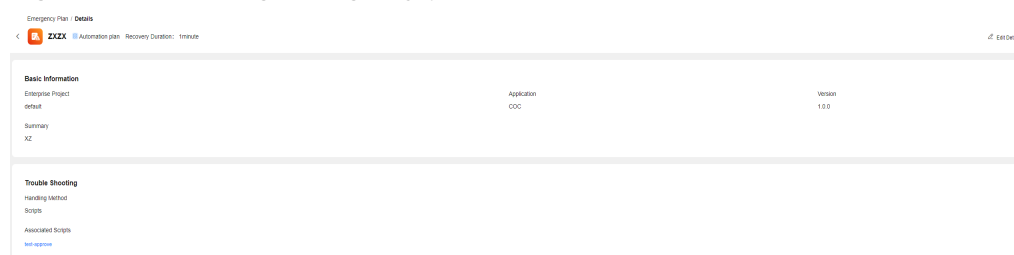


----End

Viewing Emergency Plan Details

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resilience Center > Emergency Plan**. Click the **Customized Plan** tab.
- Step 3** Click the name of an emergency plan.

Figure 9-49 Viewing emergency plan information

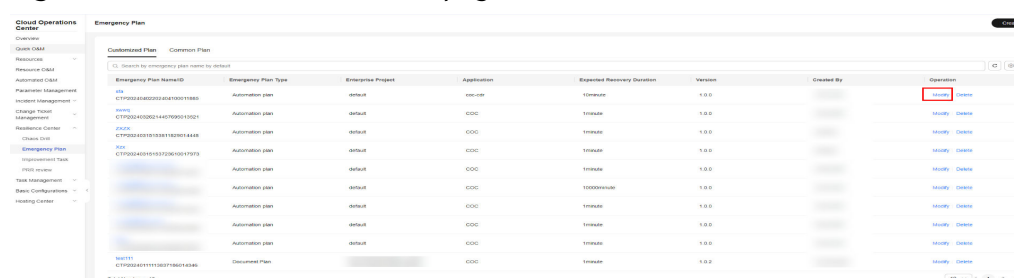


----End

Editing an Emergency Plan

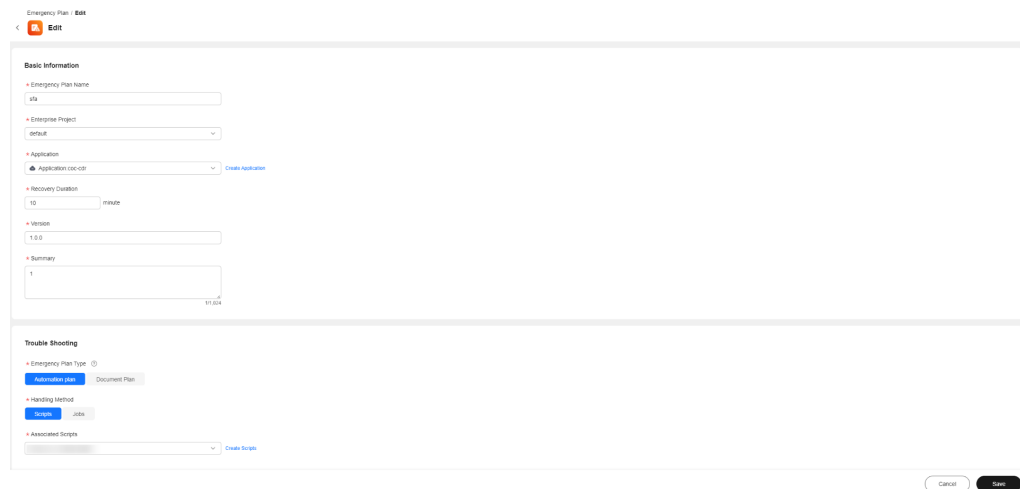
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Resilience Center > Emergency Plan**. Click the **Customized Plan** tab.

Figure 9-50 Customized Plan tab page



Step 3 Locate the target plan and click **Modify** in the **Operation** column.

Figure 9-51 Modifying an Emergency Plan



----End

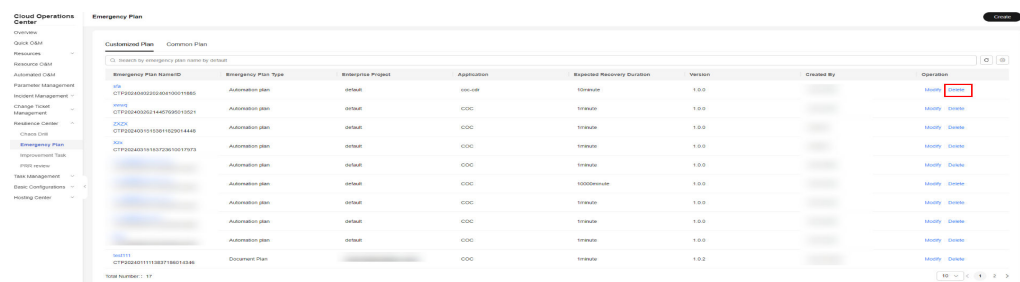
Deleting an Emergency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center > Emergency Plan**. The emergency plan list is displayed.

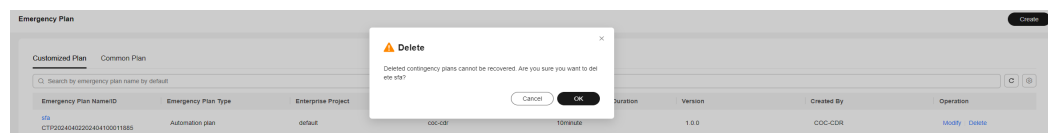
Step 3 Locate the target emergency plan and click **Delete** in the **Operation** column.

Figure 9-52 Emergency plans



Step 4 In the displayed dialog box, click **OK**.

Figure 9-53 Deleting an emergency plan



----End

9.3 Improvement Task

9.3.1 Overview

You can create an improvement task for an existing system fault or issue, and specify an owner to handle the task.

9.3.2 Improvement Task Management

Viewing Improvement Tasks

Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Resilience Center > Improvement Task**.

Figure 9-54 Improvement tasks

| Improvement Task No. | Status | Type | Application | Date Recored ID | PRR Review ID | Created By | Owner | Expected Completion | Scorecard of improvement | Operation |
|-------------------------|----------------------|------------------------|--------------|-------------------------|-------------------------|------------|-------|---------------------|--------------------------|-----------|
| IMT20240309527436018052 | Improving | Product improvement | COC-CIM | COC20240309527436018052 | PRR20240309527436018052 | | | Apr 06, 2024 | Check Data | Process |
| IMT20240309527436018052 | Pending verification | Product improvement | COC | | PRR20240309527436018052 | | | Mar 29, 2024 | PRR review | Verify |
| IMT20240309527436018052 | Improving | Product improvement | COC-COC-MEIV | | PRR20240309527436018052 | | | Mar 26, 2024 | PRR review | Process |
| IMT20240309527436018052 | Pending verification | Product improvement | COC-COC-MEIV | | PRR20240309527436018052 | | | Mar 23, 2024 | PRR review | Verify |
| IMT20240309527436018052 | Pending verification | Product improvement | COC-COC-MEIV | COC20240309527436018052 | | | | Mar 21, 2024 | Check Data | Verify |
| IMT20240309527436018052 | Improving | Product improvement | COC | | PRR20240309527436018052 | | | Mar 21, 2024 | PRR review | Process |
| IMT20240309527436018052 | Improving | Monitoring & alerting | COC | | PRR20240309527436018052 | | | Mar 21, 2024 | PRR review | Process |
| IMT20240309527436018052 | Improving | Monitoring & alerting | COC | | PRR20240309527436018052 | | | Mar 20, 2024 | PRR review | Process |
| IMT20240309527436018052 | Improving | Management improvement | COC | | PRR20240309527436018052 | | | Mar 20, 2024 | PRR review | Process |
| IMT20240309527436018052 | Improving | CBM improvement | COC | | PRR20240309527436018052 | | | Mar 21, 2024 | PRR review | Process |

Step 3 Click the name of an improvement task. The details of the improvement task will be displayed in the dialog box on the right.

Figure 9-55 Improvement task details

Improvement Ticket Details ✕

Basic Information

| | |
|------------------|-------------------------|
| Improvement Task | Improvement Ticket No |
| 0403改进事项 | IMT20240309527436018052 |

Ticket Creation

| | |
|--|-------------------------------------|
| Status | Owner |
| ▶ Improving | |
| Type | Expected Completion |
| Product improvement | Apr 06, 2024 |
| Application | Created At |
| COC-CIM | Apr 03, 2024 09:55:27 GMT+08:00 |
| Symptom | Improvement Ticket Closure Criteria |
| 11 | 11 |

----End

Viewing the Chaos Drill Record of an Improvement Task

Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Resilience Center > Improvement Task**.

Figure 9-56 Improvement tasks

| Improvement Task No. | Status | Type | Application | Drill Record ID | PRR Review ID | Created By | Owner | Expected Completion | Source of Improvement | Operation |
|-----------------------|----------------------|------------------------|-------------|---------------------|-----------------------|------------|-------|---------------------|-----------------------|-----------|
| IFT202403030227436 | Improving | Product improvement | COO-CRM | DRM202403030227436 | PRR202403030227436 | | | Apr 06, 2024 | China DR | Process |
| IFT2024030303046377 | Pending verification | Product improvement | COO | | PRR2024030303046377 | | | Mar 28, 2024 | PRR review | Verify |
| IFT2024030303042047 | Improving | Product improvement | COO-CRM-NEW | | PRR2024030303042047 | | | Mar 28, 2024 | PRR review | Process |
| IFT2024030303050604 | Pending verification | Product improvement | COO-CRM-NEW | | PRR2024030303050604 | | | Mar 22, 2024 | PRR review | Verify |
| IFT2024030303050218 | Pending verification | Product improvement | COO-CRM-NEW | DRM2024030303050218 | | | | Mar 21, 2024 | China DR | Verify |
| IFT2024030303051509 | Improving | Product improvement | COO | | PRR2024030303051509 | | | Mar 21, 2024 | PRR review | Process |
| IFT2024030303051790 | Improving | Monitoring & alerting | COO | | PRR2024030303051790 | | | Mar 21, 2024 | PRR review | Process |
| IFT2024030303051793 | Improving | Monitoring & alerting | COO | | PRR2024030303051793 | | | Mar 20, 2024 | PRR review | Process |
| IFT20240303030524743 | Improving | Management improvement | COO | | PRR20240303030524743 | | | Mar 20, 2024 | PRR review | Process |
| IFT202403030305222113 | Improving | CRM improvement | COO | | PRR202403030305222113 | | | Mar 21, 2024 | PRR review | Process |

Step 3 Click the drill record ID of an improvement task. The **Drill Record Detail** page is displayed.

Figure 9-57 Drill record detail

Drill Record Detail

Attack Progress: Successful

Attack Details:

- RDS Active@Sanby S... (0/1) - Abnormal Alarm - Verify
- Check Instance # Success#1 (Mar 21, 2024 03:01:00) - Success - 0000-00
- Execute Drill # (Mar 21, 2024 03:01:00) - Success - 0000-00

----End

Viewing the PRR Review of an Improvement Task

Step 1 Log in to **COC**.

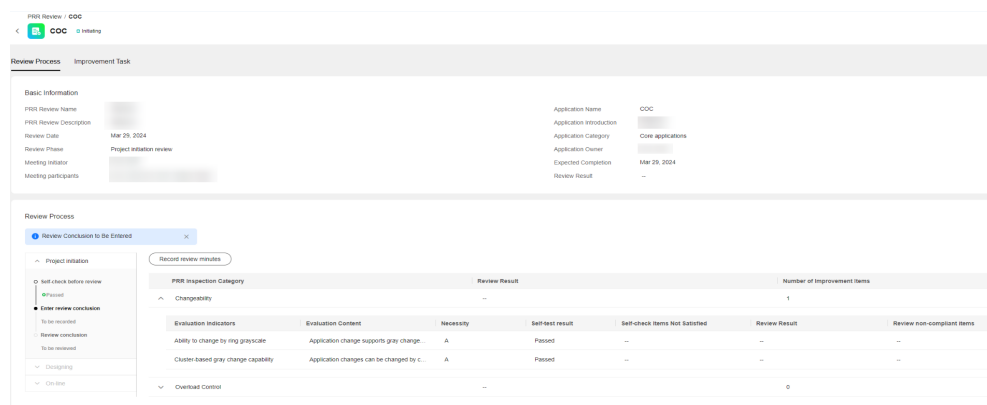
Step 2 In the navigation pane on the left, choose **Resilience Center > Improvement Task**.

Figure 9-58 Improvement tasks

| Improvement Task No. | Status | Type | Application | Drill Record ID | PRR Review ID | Created By | Owner | Expected Completion | Source of Improvement | Operation |
|-----------------------|----------------------|------------------------|-------------|---------------------|-----------------------|------------|-------|---------------------|-----------------------|-----------|
| IFT2024030303050604 | Improving | Product improvement | COO-CRM | DRM2024030303050604 | | | | Apr 06, 2024 | China DR | Process |
| IFT2024030303046377 | Pending verification | Product improvement | COO | | PRR2024030303046377 | | | Mar 28, 2024 | PRR review | Verify |
| IFT2024030303042047 | Improving | Product improvement | COO-CRM-NEW | | PRR2024030303042047 | | | Mar 28, 2024 | PRR review | Process |
| IFT2024030303050604 | Pending verification | Product improvement | COO-CRM-NEW | | PRR2024030303050604 | | | Mar 22, 2024 | PRR review | Verify |
| IFT2024030303050218 | Pending verification | Product improvement | COO-CRM-NEW | DRM2024030303050218 | | | | Mar 21, 2024 | China DR | Verify |
| IFT2024030303051509 | Improving | Product improvement | COO | | PRR2024030303051509 | | | Mar 21, 2024 | PRR review | Process |
| IFT2024030303051790 | Improving | Monitoring & alerting | COO | | PRR2024030303051790 | | | Mar 21, 2024 | PRR review | Process |
| IFT2024030303051793 | Improving | Monitoring & alerting | COO | | PRR2024030303051793 | | | Mar 20, 2024 | PRR review | Process |
| IFT20240303030524743 | Improving | Management improvement | COO | | PRR20240303030524743 | | | Mar 20, 2024 | PRR review | Process |
| IFT202403030305222113 | Improving | CRM improvement | COO | | PRR202403030305222113 | | | Mar 21, 2024 | PRR review | Process |

Step 3 Click the PRR review ID of an improvement task to view the PRR details.

Figure 9-59 PRR details



----End

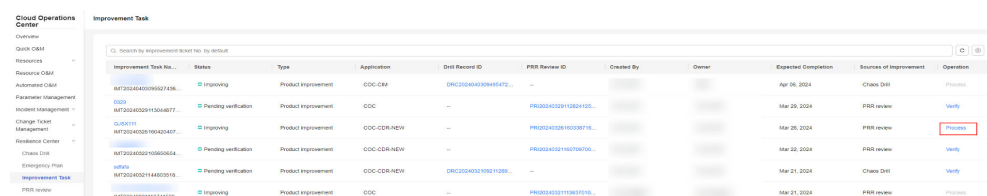
Handling an Improvement Task

An improvement task needs to be handled by a specified owner. And then the task creator needs to verify the handling result. Only the owner can handle the task.

Step 1 Log in to **COC**.

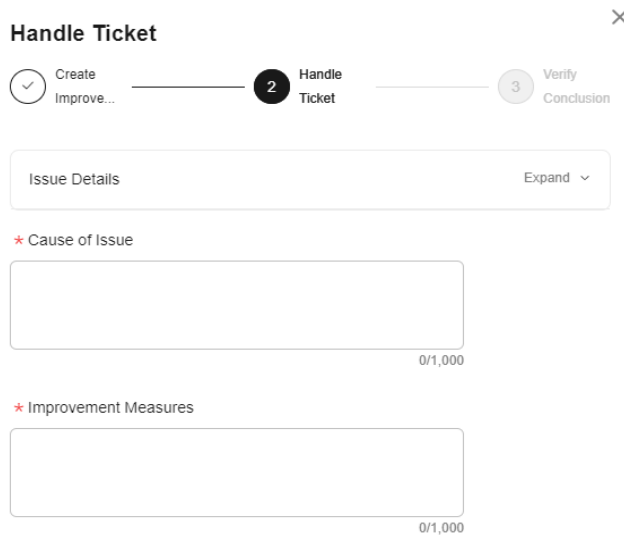
Step 2 In the navigation pane on the left, choose **Resilience Center > Improvement Task**. Locate the improvement to be handled, and click **Process** in the **Operation** column.

Figure 9-60 Improvement tasks



Step 3 In the displayed dialog box, enter the cause of the issue and improvement measures, and click **OK**.

Figure 9-61 Handling the improvement task



----End

Verifying an Improvement Task

After an improvement task is handled, the task creator needs to verify the handling result. Only the creator can verify the handling result. If the result is accepted, the improvement task is completed. If the result is rejected, the owner needs to handle the task again.

Step 1 Log in to [COC](#).

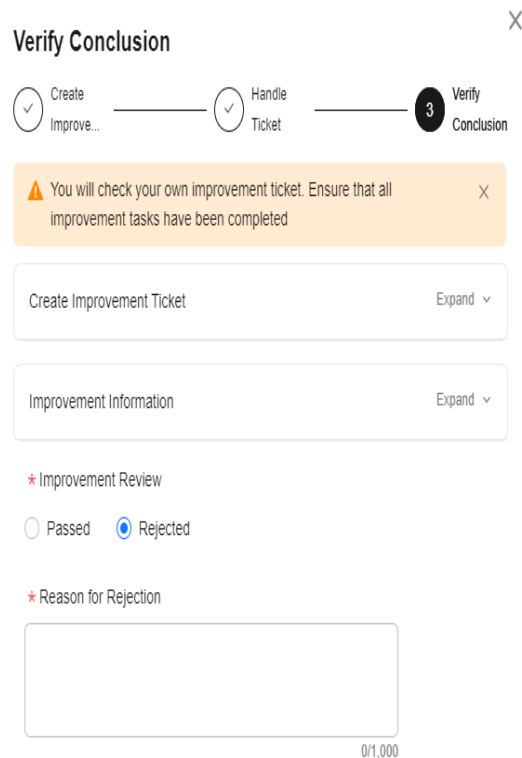
Step 2 In the navigation pane on the left, choose **Resilience Center > Improvement Task**. Locate the improvement to be verified, and click **Verify** in the **Operation** column.

Figure 9-62 Improvement tasks

| Improvement Task No. | Status | Type | Application | DRB Record ID | PRR Review ID | Created By | Owner | Expected Completion | Source of Improvement | Operation |
|----------------------|----------------------|---------------------|-------------|---------------------|---------------------|------------|-------|---------------------|-----------------------|-----------|
| MFT202402010040467 | Pending verification | Product improvement | COC-CDR-NEW | --- | PRR202402010040467 | | | Aug 07, 2024 | PRR review | Verify |
| MFT2024020110044877 | In progress | Product improvement | COC-CRM | DRB2024020110044877 | --- | | | Aug 08, 2024 | Check DRB | Process |
| MFT2024020110044877 | Pending verification | Product improvement | COC | --- | PRR2024020110044877 | | | Mar 29, 2024 | PRR review | Verify |
| MFT2024020110040664 | Pending verification | Product improvement | COC-CDR-NEW | --- | PRR2024020110040664 | | | Mar 22, 2024 | PRR review | Verify |
| MFT2024020114488318 | Pending verification | Product improvement | COC-CDR-NEW | DRB2024020114488318 | --- | | | Mar 21, 2024 | Check DRB | Verify |
| MFT2024020110040664 | In progress | Product improvement | COC | --- | PRR2024020110040664 | | | Mar 21, 2024 | PRR review | Process |

Step 3 Select **Passed** or **Rejected**. If you select **Rejected**, provide the rejection reason.

Figure 9-63 Verifying the improvement task



----End

9.4 PRR Review

9.4.1 Overview

Production Readiness Review (PRR).

PRR Review provides the baselines for service availability and O&M capabilities from dimensions such as SLI/SLO, redundancy, disaster recovery, overload control, fault management, change capability, O&M, 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.

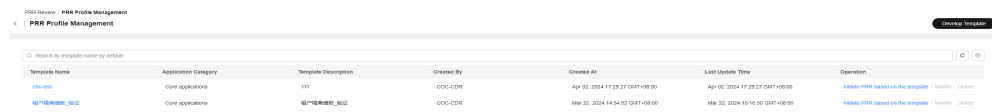
9.4.2 PRR Template Management

Creating a PRR Template

Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 9-64 PRR template management



Step 3 Click **Develop Template**. On the **Develop PRR template** page, specify the template information.

Figure 9-65 Creating a PRR template

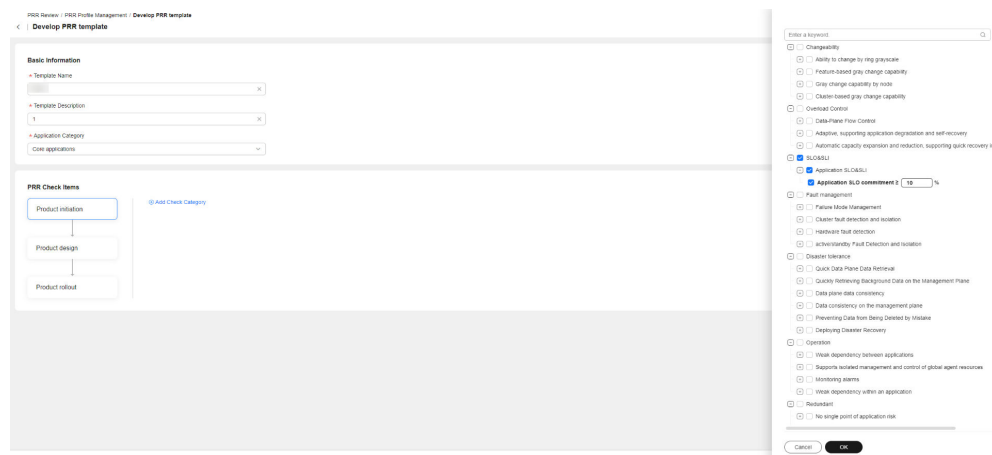
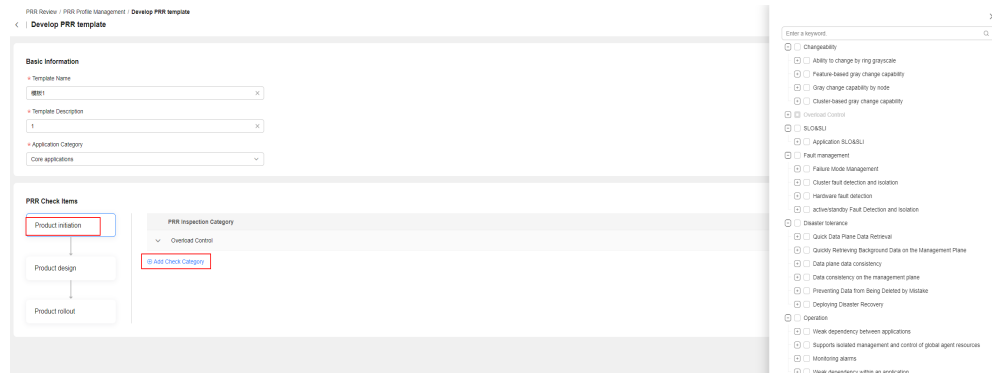


Table 9-4 Parameters for creating a PRR template

| Parameter | Description |
|----------------------|---|
| Template Name | Name of the PRR template |
| Template Description | Description of the PRR template |
| Application Category | Application category to which the PRR template belongs |
| PRR Check Items | Check items in the product initiation, product design, and product launch phases defined in the PRR template in advance |

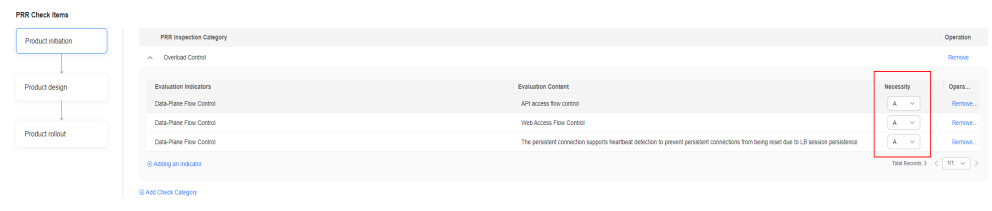
Step 4 Set check item information. Click **Product initiation**, **Product design**, or **Product rollout**, and click **Add Check Category**. The check items are displayed on the right. Select the check item as required.

Figure 9-66 Specifying check items



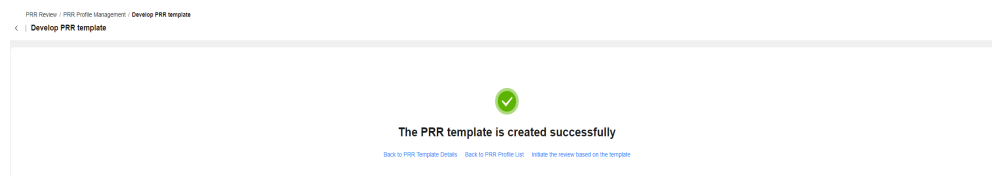
Step 5 Select the importance levels of check items. Note: If a check item whose importance level is A fails, the PRR review will fail.

Figure 9-67 Selecting the importance level of a check item



Step 6 Click OK.

Figure 9-68 PRR template created



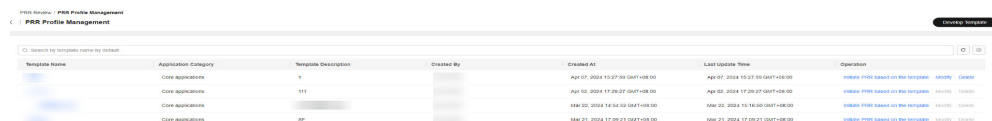
----End

Viewing PRR Template Details

Step 1 Log in to **COC**.

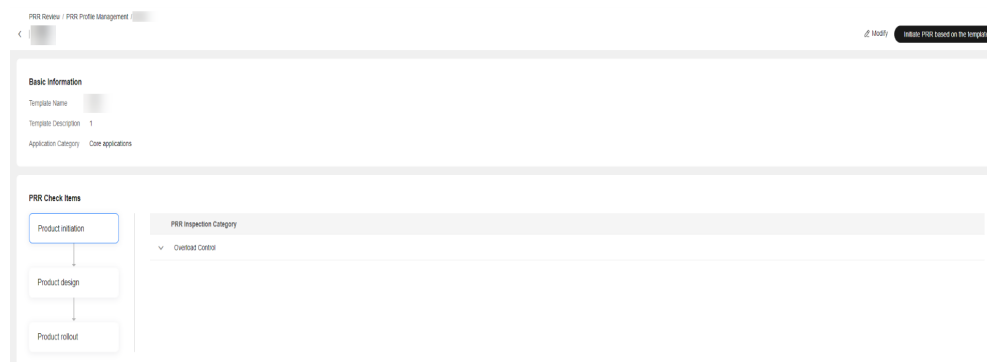
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 9-69 PRR template list



Step 3 Click the name of the target template.

Figure 9-70 PRR template details



----End

Modifying a PRR Template

Step 1 Log in to **COC**.

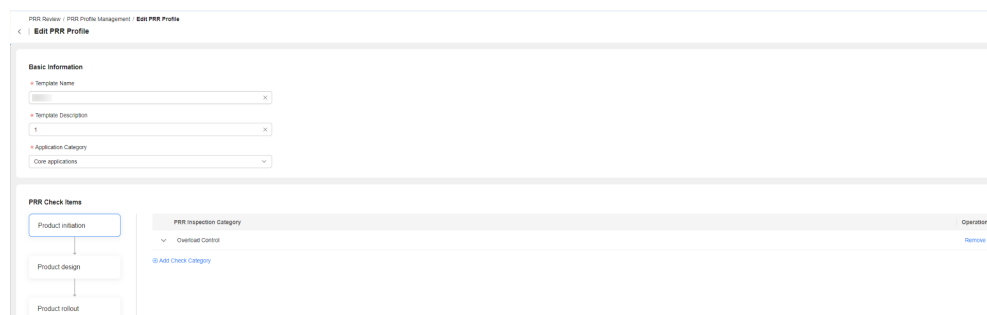
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 9-71 PRR template list

| Template Name | Application Category | Template Description | Created By | Created At | Last Update Time | Operation |
|---------------|----------------------|----------------------|------------|---------------------------------|---------------------------------|--|
| | Core applications | 1 | | Apr 07, 2024 10:27:59 GMT+08:00 | Apr 07, 2024 10:27:59 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | 111 | | Apr 02, 2024 17:28:27 GMT+08:00 | Apr 02, 2024 17:28:27 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | | | Mar 22, 2024 16:34:33 GMT+08:00 | Mar 22, 2024 16:34:33 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | SP | | Mar 21, 2024 17:59:21 GMT+08:00 | Mar 21, 2024 17:59:21 GMT+08:00 | Initiate PRR based on the template Initiate Delete |

Step 3 Locate the target template, and click **Modify** in the **Operation** column.

Figure 9-72 Modifying a PRR template



----End

Deleting a PRR Template

Step 1 Log in to **COC**.

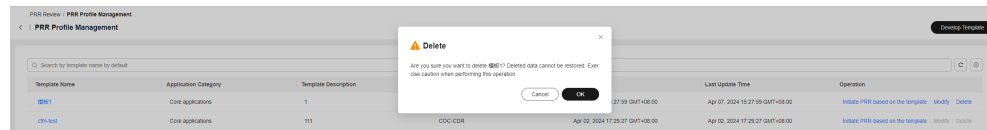
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 9-73 PRR template list

| Template Name | Application Category | Template Description | Created By | Created At | Last Update Time | Operation |
|---------------|----------------------|----------------------|------------|---------------------------------|---------------------------------|--|
| | Core applications | 1 | | Apr 07, 2024 10:27:59 GMT+08:00 | Apr 07, 2024 10:27:59 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | 111 | | Apr 02, 2024 17:28:27 GMT+08:00 | Apr 02, 2024 17:28:27 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | | | Mar 22, 2024 16:34:33 GMT+08:00 | Mar 22, 2024 16:34:33 GMT+08:00 | Initiate PRR based on the template Initiate Delete |
| | Core applications | SP | | Mar 21, 2024 17:59:21 GMT+08:00 | Mar 21, 2024 17:59:21 GMT+08:00 | Initiate PRR based on the template Initiate Delete |

Step 3 Locate the target template, and click **Delete** in the **Operation** column.

Figure 9-74 Deleting a PRR template



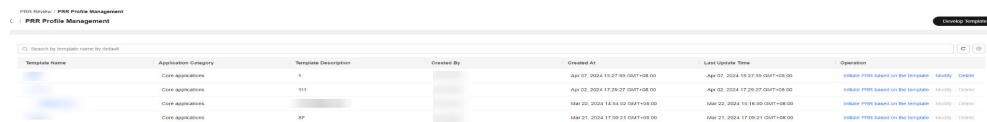
----End

Initiating PRR Based on a Template

Step 1 Log in to **COC**.

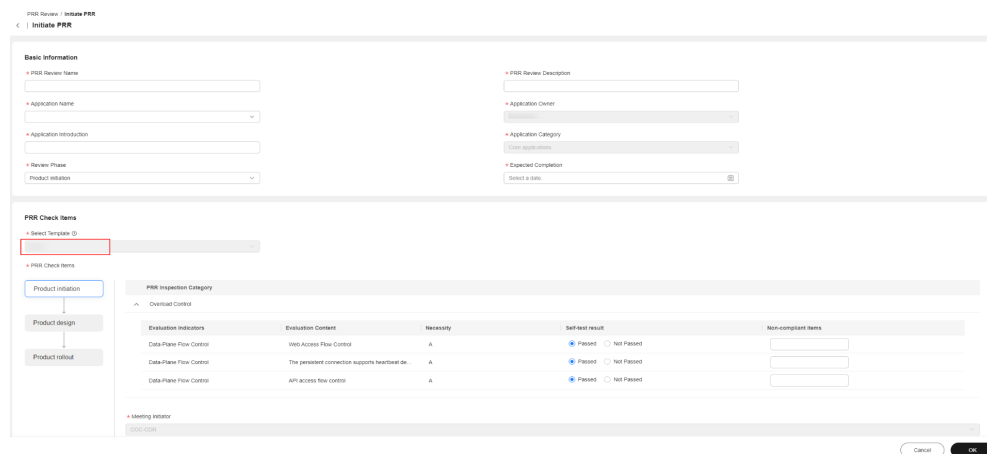
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 9-75 PRR template list



Step 3 Locate the target template, and click **Initiate PRR based on the template**. This template is selected to initiate PRR by default. For details about how to initiate PRR, see **PRR Management**.

Figure 9-76 Initiating PRR based on a template



----End

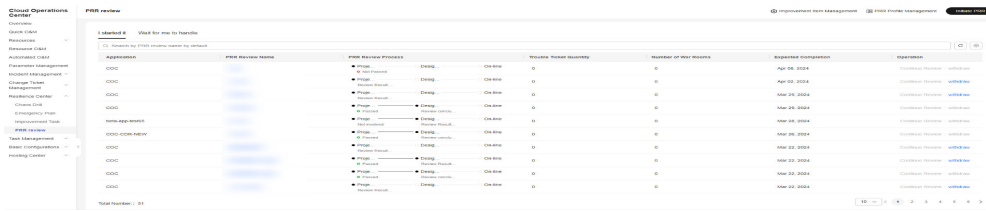
9.4.3 PRR Management

Initiating PRR

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**.

Figure 9-77 PRR list



Step 3 Click **Initiate PRR**. On the **Initiate PRR** page, enter basic PRR information.

Figure 9-78 Initiating PRR- Specifying PRR basic information

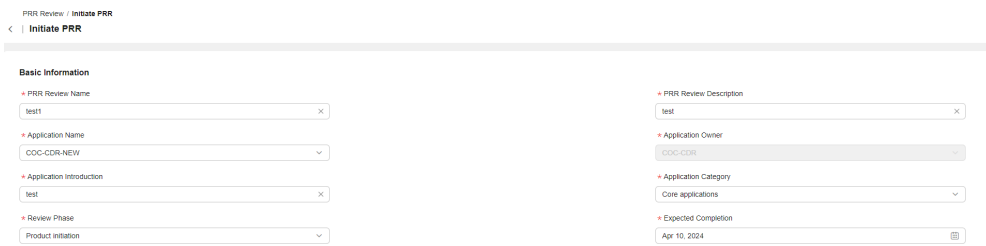


Table 9-5 Basic parameters for initiating PRR

| Parameter | Description |
|--------------------------|--|
| PRR Review Name | Name of the PRR |
| PRR Review Description | Description of the PRR |
| Application Name | Name of the application to which the PRR belongs |
| Application Owner | Owner of the application to which the PRR belongs |
| Application Introduction | Introduction to the application to which the PRR belongs |
| Application Category | Category of the application to which the PRR belongs |
| Review Phase | Review phase of the PRR meeting |
| Expected Completion | Expected time when the PRR completes |

Step 4 Select a PRR template. The check items required in the review phase of the template will be displayed. Specify the check items for the PRR.

Figure 9-79 Initiating PRR - Specifying PRR check items

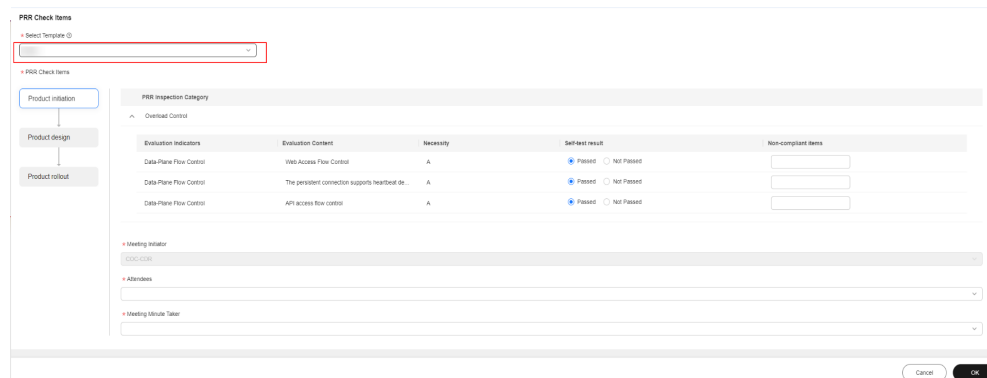
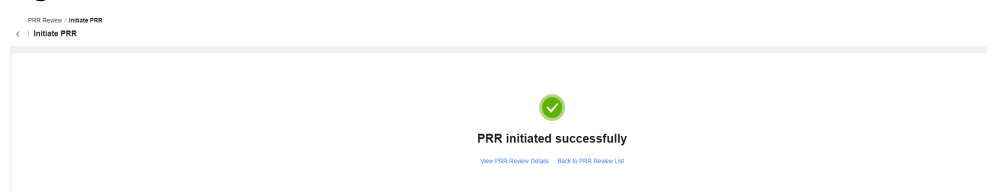


Table 9-6 Parameters of check items

| Parameter | Description |
|-----------------------|--|
| Self-test result | Self-check result of a check item (If a check item whose necessity is A fails, the PRR cannot be initiated.) |
| Non-compliant Items | Information about the item that fails to pass the check |
| Meeting Initiator | Initiator of the PRR review meeting |
| Attendees | Attendees of the PRR review meeting |
| Meeting Minutes Taker | Minutes maker of the PRR review meeting |

Step 5 Click **OK**.

Figure 9-80 PRR initiated



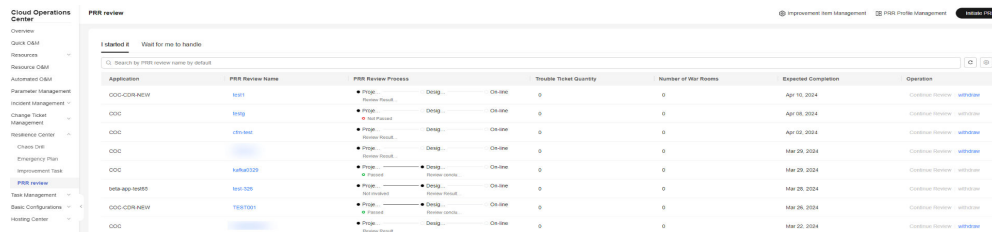
----End

Viewing PRR Details

Step 1 Log in to **COC**.

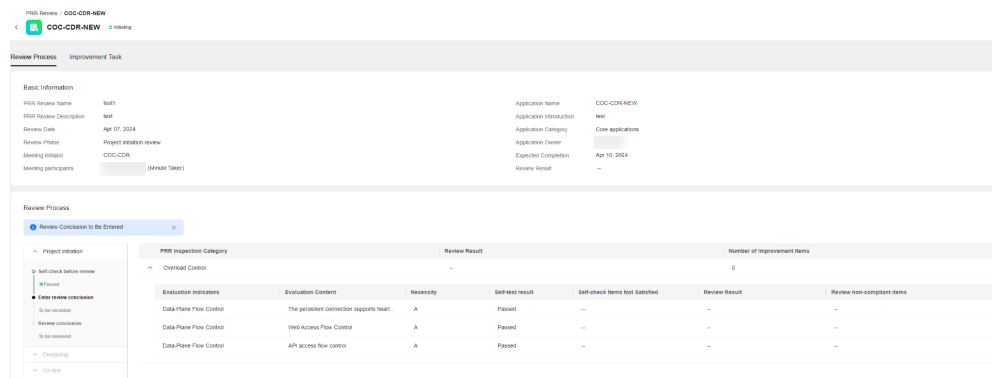
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**.

Figure 9-81 PRR list



Step 3 Click the name of the target PRR.

Figure 9-82 PRR details



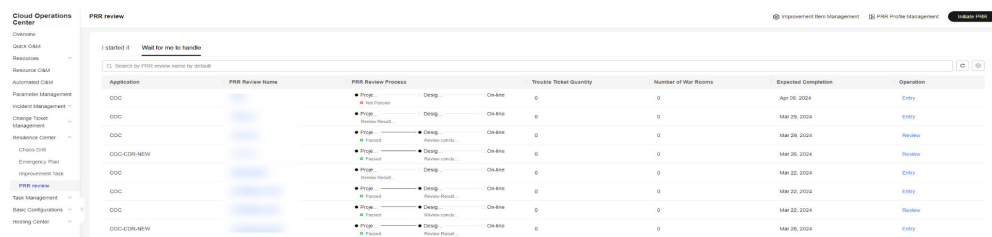
----End

Recording Review Minutes

Step 1 Log in to **COC**.

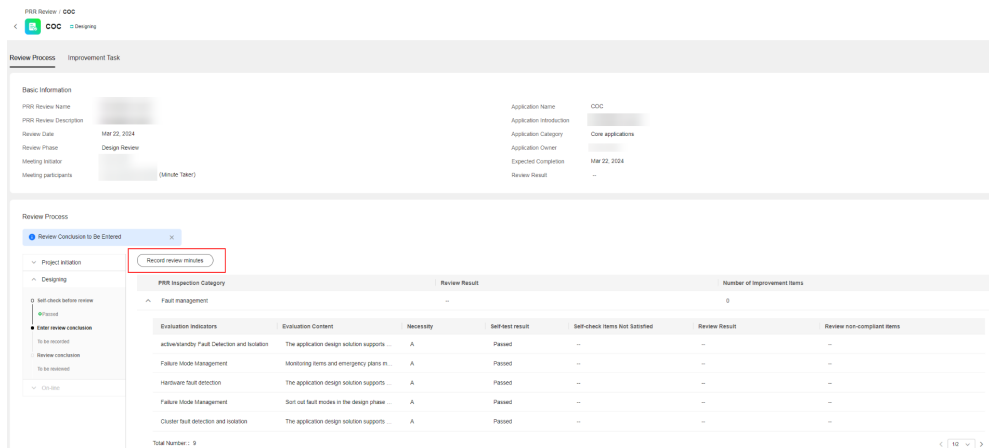
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. On the displayed page, click the **Wait for me to handle**.

Figure 9-83 PRR to be processed



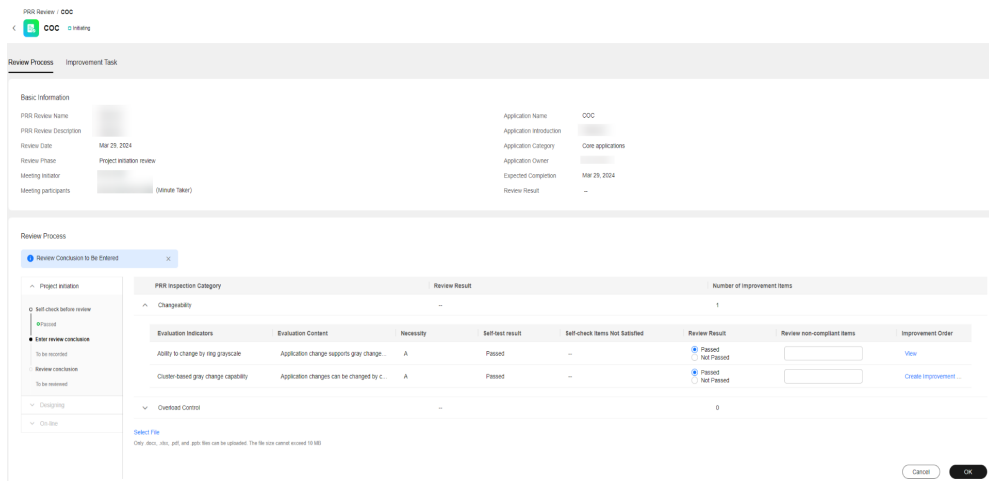
Step 3 Locate the target PRR record, and click **Entry**. On the displayed PRR details page, click **Record review minutes** to enter the review minutes.

Figure 9-84 PRR details - entering review minutes



Step 4 Enter review minutes.

Figure 9-85 Entering review minutes



Step 5 Locate the target check item that does not pass the check, and click **Create Improvement Ticket** in the **Improvement Order** column. On the displayed page, specify the information about the improvement ticket and click **OK**.

Figure 9-86 Entering review minutes - creating an improvement ticket

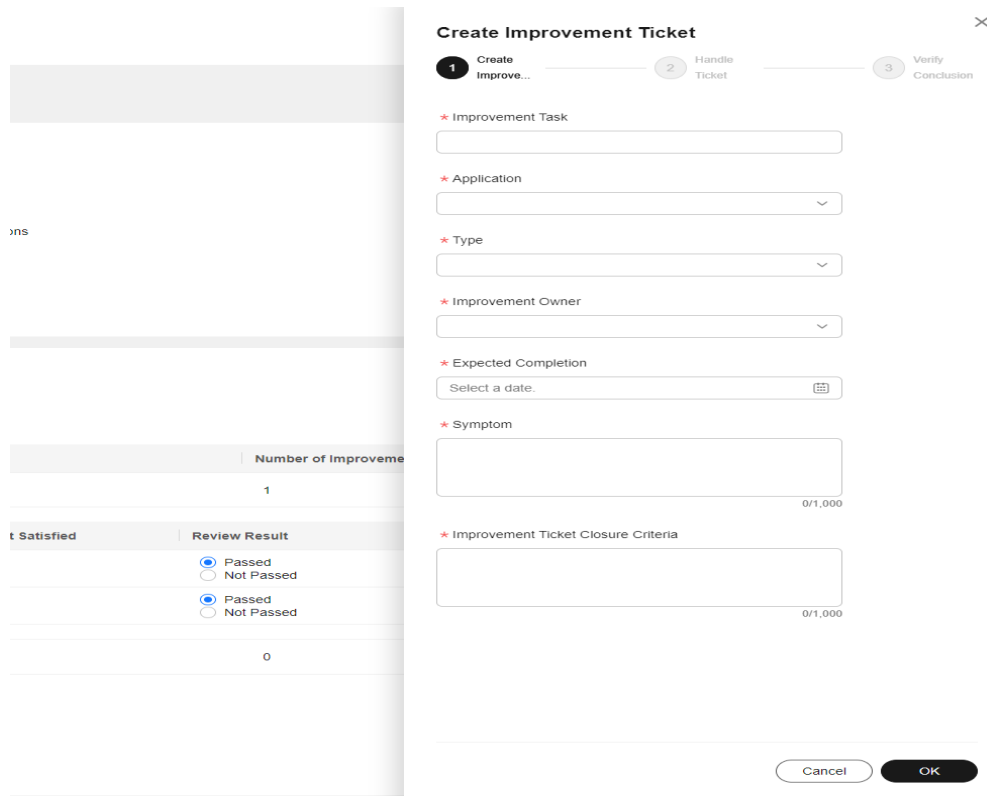
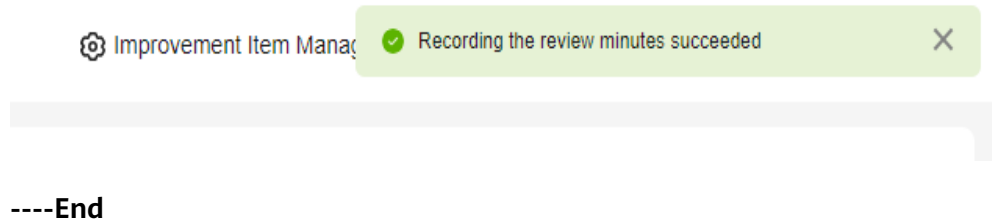


Table 9-7 Improvement ticket parameters

| Parameter | Description |
|-------------------------------------|--|
| Improvement Task | Improvement ticket name |
| Application | Application the improvement ticket belongs to |
| Type | Type of the improvement ticket |
| Improvement Owner | Owner of the improvement ticket |
| Expected Completion | Expected time when the improvement ticket ends |
| Symptom | Issue symptom |
| Improvement Ticket Closure Criteria | Criteria for the closure of the improvement ticket |

Step 6 Click **OK**.

Figure 9-87 Review minutes recorded

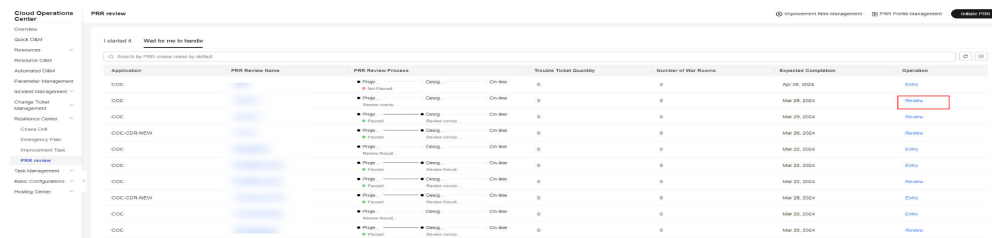


Recording the Review Conclusion

Step 1 Log in to **COC**.

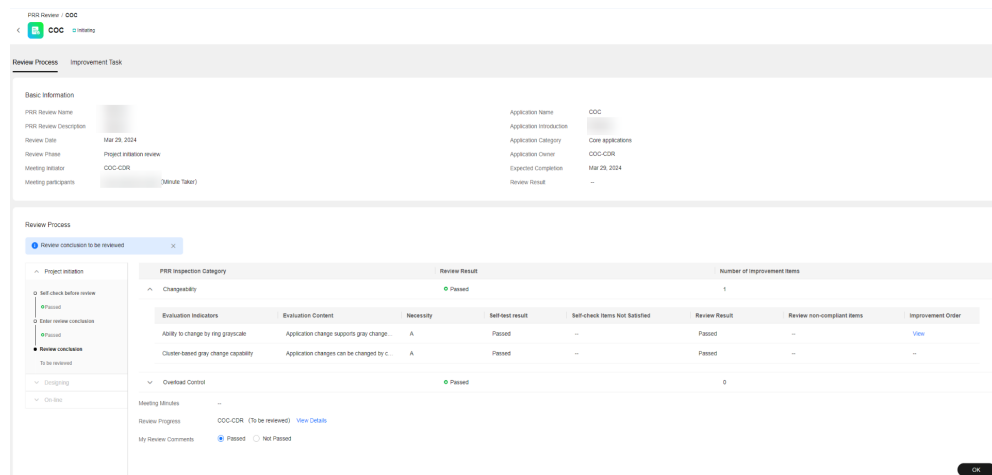
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**. On the displayed page, click the **Wait for me to handle** tab.

Figure 9-88 PRR to be processed



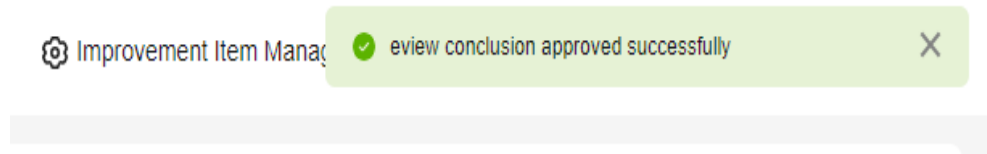
Step 3 Locate the target PRR record, and click **Review** in the **Operation** column. On the displayed page, enter the review conclusion.

Figure 9-89 Recording the review conclusion



Step 4 Click **OK**.

Figure 9-90 Review conclusion recorded



----End

Continuing to Initiate PRR

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**.

Figure 9-91 PRR list

| Application | PRR Review Name | PRR Review Process | Trouble Ticket Quantity | Number of War Rooms | Expected Completion | Operation |
|--------------|-----------------|------------------------|-------------------------|---------------------|---------------------|-----------------|
| COC-CCR-NET | | ● Stage: Review Result | 0 | 0 | Apr 10, 2024 | Continue Review |
| COC | | ● Stage: Not Started | 0 | 0 | Apr 09, 2024 | Continue Review |
| COC | | ● Stage: Passed | 0 | 0 | Mar 29, 2024 | Continue Review |
| COC | | ● Stage: Review Result | 0 | 0 | Mar 29, 2024 | Continue Review |
| Meta-app-IMP | | ● Stage: Review Result | 0 | 0 | Mar 28, 2024 | Continue Review |
| COC-CCR-NET | | ● Stage: Review Result | 0 | 0 | Mar 26, 2024 | Continue Review |
| COC | | ● Stage: Review Result | 0 | 0 | Mar 22, 2024 | Continue Review |
| COC | | ● Stage: Review Result | 0 | 0 | Mar 22, 2024 | Continue Review |

Step 3 Locate the target PRR record, click **Continue Review** in the **Operation** column to initiate the review of the next phase. (The review of the next phase can be initiated only after the review of the previous phase is passed.)

Figure 9-92 Continuing to initiate PRR

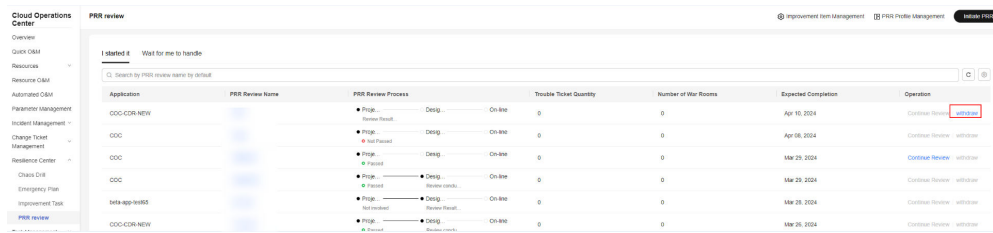
----End

Canceling the PRR

Step 1 Log in to **COC**.

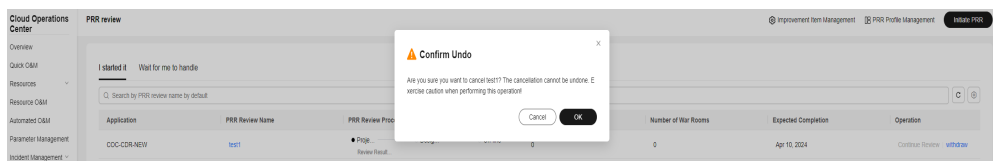
Step 2 In the navigation pane on the left, choose **Resilience Center > PRR review**.

Figure 9-93 PRR list



Step 3 Locate the target PRR record, and click **withdraw**.

Figure 9-94 Canceling the PRR



----End

10 Task Management

10.1 Execution Records

10.1.1 Script Tickets

You can view and manage script tickets.

Prerequisites

If you deliver a script execution task, the system generates a script ticket.

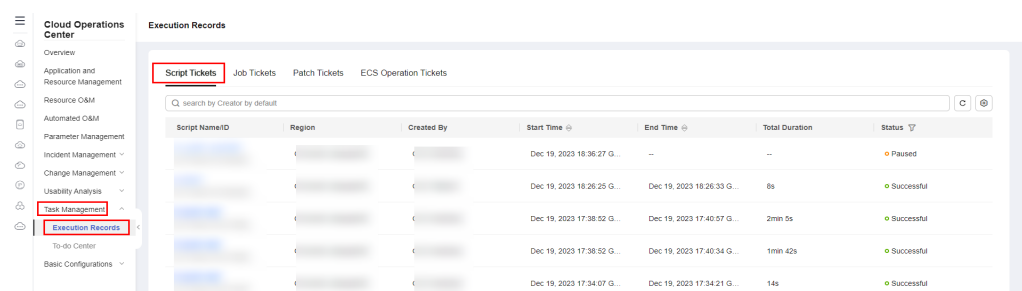
Scenarios

View script tickets on the **Cloud Operations Center** page.

Procedure

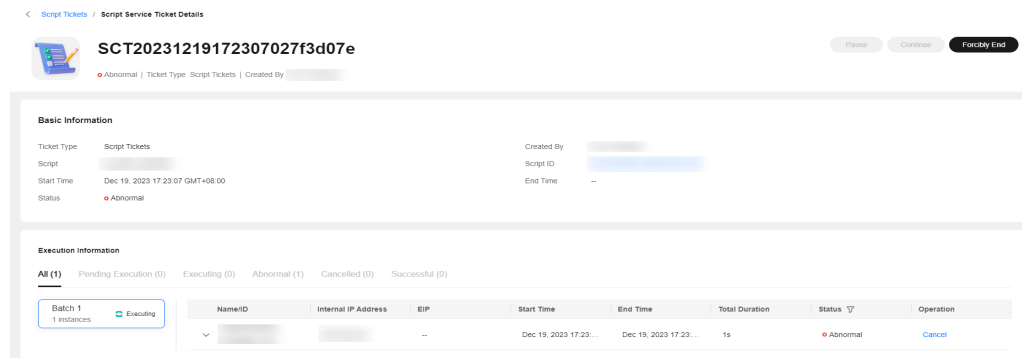
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Task Management > Execution Records** and click the **Script Tickets** tab.

Figure 10-1 Script Tickets



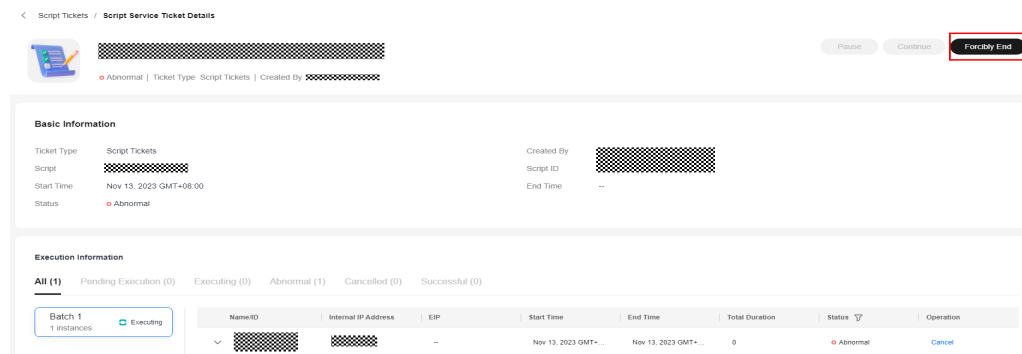
- Step 3** Select a script ticket in the **Abnormal** state.

Figure 10-2 Selecting a script ticket in the **Abnormal** state



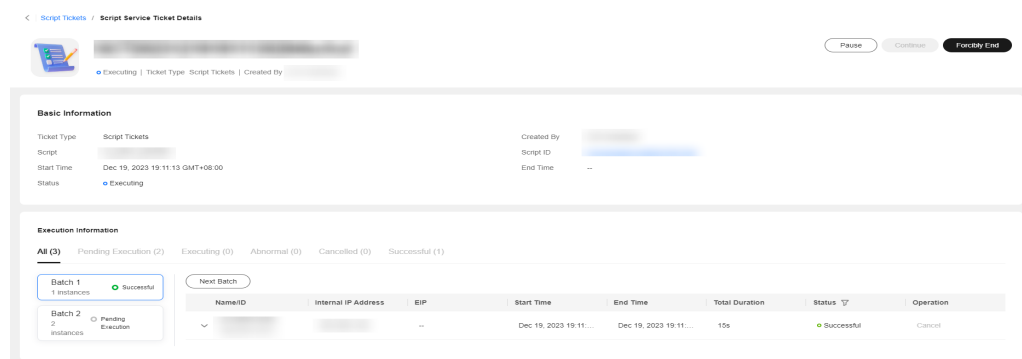
Step 4 Click **Forcibly End** to end the abnormal script ticket.

Figure 10-3 Closing an abnormal script ticket



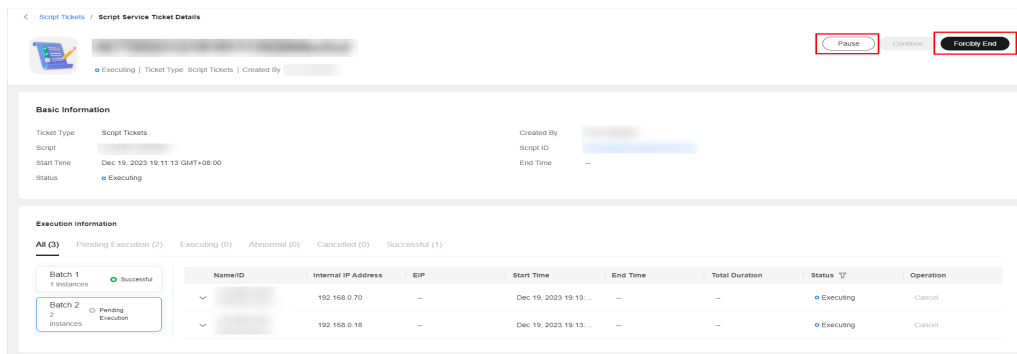
Step 5 Select a script ticket in the **Executing** state.

Figure 10-4 Selecting a script ticket in the **Executing** state



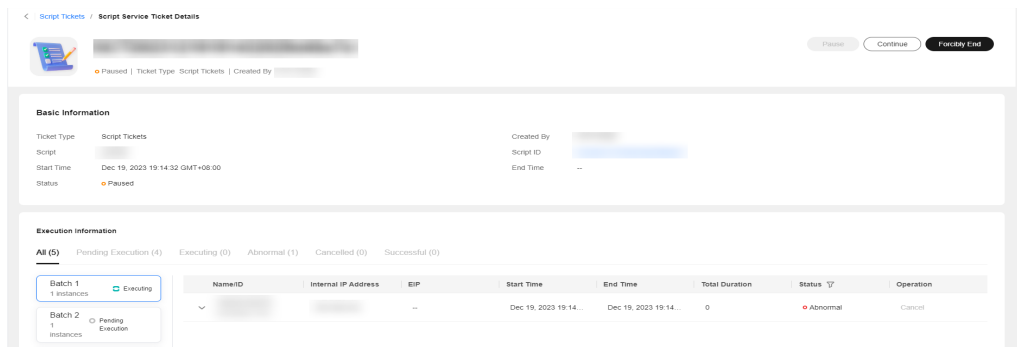
Step 6 Click **Pause** or **Forcibly End** to pause or end the script ticket.

Figure 10-5 Pausing or closing a script ticket



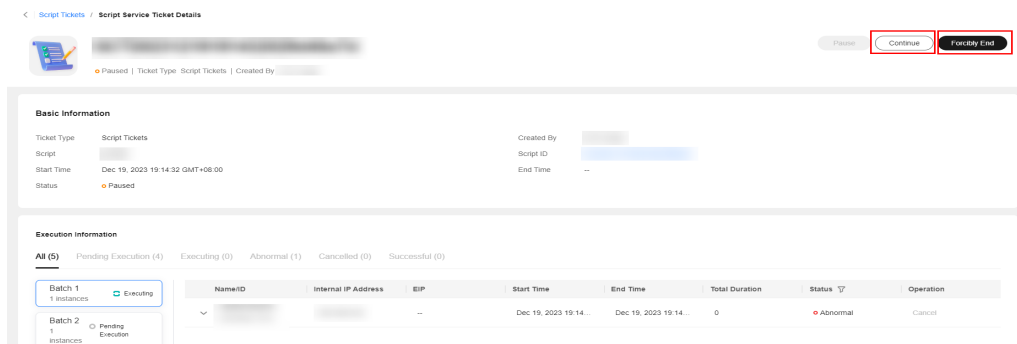
Step 7 Select a script ticket in the **Paused** state.

Figure 10-6 Selecting a script ticket in the **Paused** state



Step 8 Click **Continue** or **Forcibly End** to continue or end the script ticket.

Figure 10-7 Continuing or pausing a paused script ticket



----End

10.1.2 Job Tickets

You can view and manage job orders.

Prerequisites

If you deliver a job execution task, the system generates a job ticket.

Scenarios

View job tickets on the **Cloud Operations Center** page.

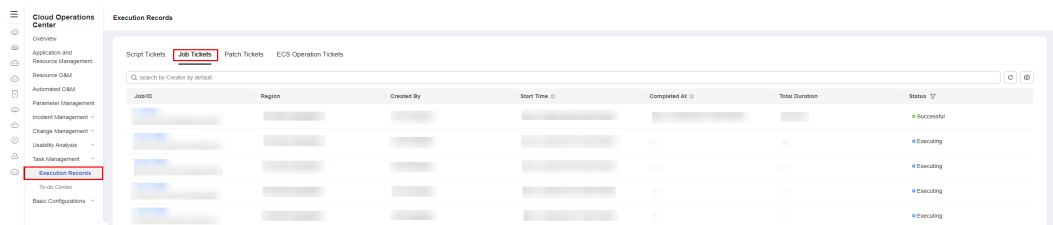
Procedure

Step 1 Log in to **COC**.

Step 2 Choose **Task Management > Execution Records**, and click the **Job Tickets** tab.

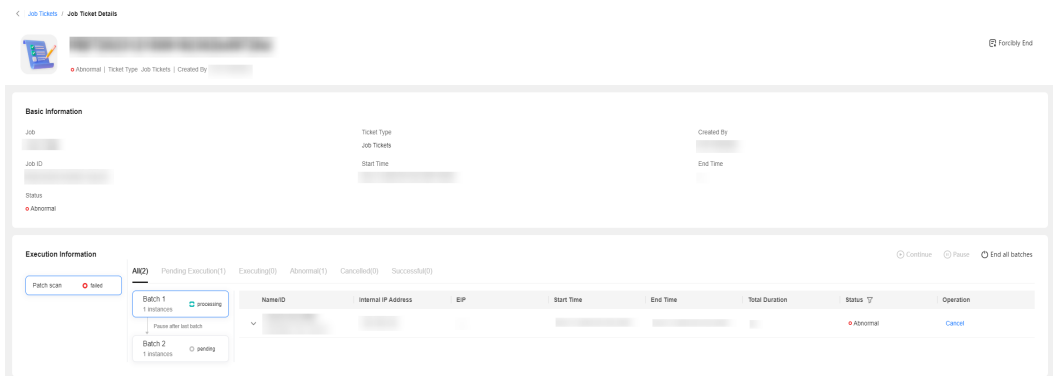
- Cloning a ticket: Click **Clone** of a job ticket to go to the **Execute Job** page. You can execute the job again by following the instructions provided in [Executing a Custom Job](#).
- Editing a tag: Modify job tags by following the instructions provided in [Managing Tags](#).

Figure 10-8 Job tickets



Step 3 Select a job ticket in the **Executing, Abnormal, or Paused** state.

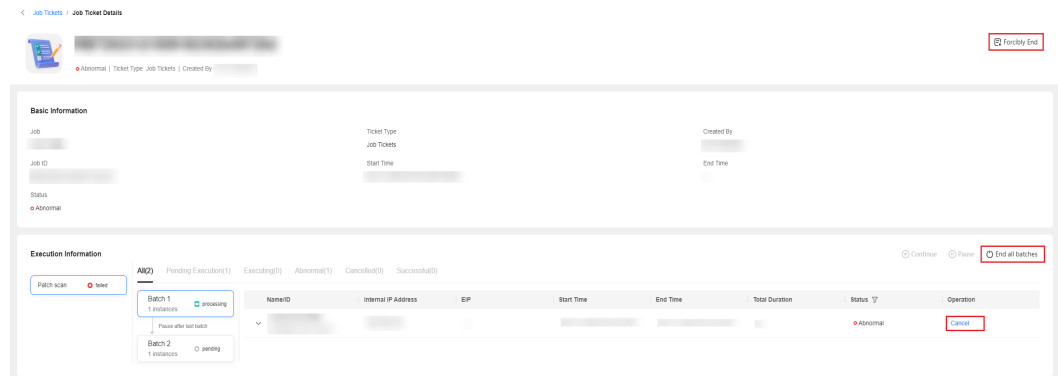
Figure 10-9 Job ticket details



Step 4 You can perform the following operations on a job ticket:

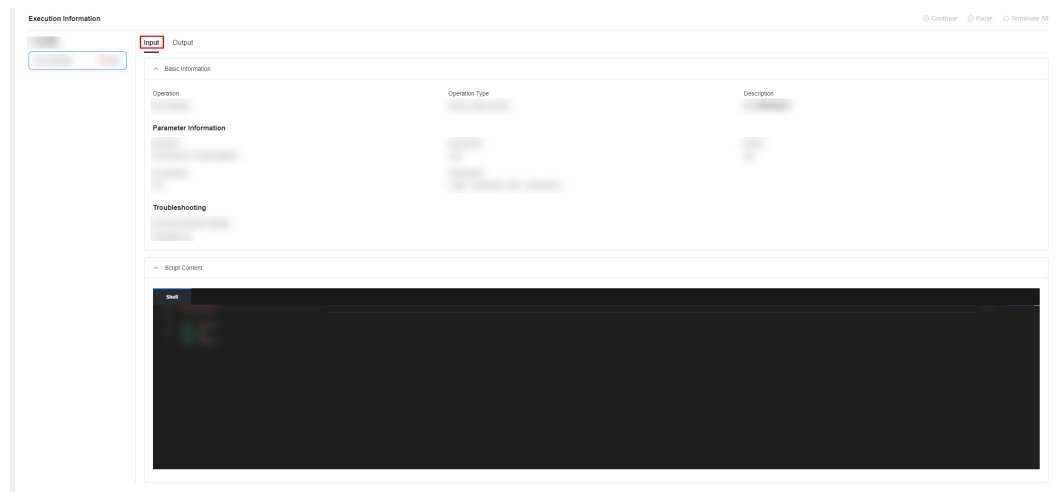
- **Forcibly End:** Forcibly end all tasks of the current job.
- **Terminate All:** End all batches in the current step.
- **Cancel:** Stop the execution jobs of a single instance.
- Editing a tag: Modify job tags by following the instructions provided in [Managing Tags](#).

Figure 10-10 Managing a job ticket



Step 5 On the job details page, click the **Input** tab to view the basic information about the job and the script content of the customized atomic job.

Figure 10-11 Viewing the job details



----End

10.1.3 Patch Tickets

You can view and manage patch tickets.

Prerequisites

If you use the patch management function, the system generates a patch ticket.

Scenarios

View patch tickets on the **Cloud Operations Center** page.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Task Management > Execution Records** and select a patch ticket.

Step 3 You can search for tickets by ID, region, ticket type, start time, and end time.

Figure 10-12 Patch ticket list

| ID | Ticket Type | Scenario Type | Region | Created By | Start Time | End Time | Total Duration | Status | Operation |
|----------------------------|-------------|-----------------|--------|------------|----------------|----------------|----------------|-------------|----------------------|
| OST20231114094146022e68c13 | Scan | Virtualized ... | | | Nov 14, 202... | -- | -- | o Cancelled | Compliance Reporting |
| OST20231114091529028830006 | Repair | Virtualized ... | | | Nov 14, 202... | -- | -- | o Cancelled | Compliance Reporting |
| OST2023111409135802c4a87ce | Scan | Virtualized ... | | | Nov 14, 202... | -- | -- | o Cancelled | Compliance Reporting |
| OST20231110112811021940910 | Scan | Virtualized ... | | | Nov 10, 202... | -- | -- | o Abnormal | Compliance Reporting |
| OST202311092022000210437fd | Scan | Virtualized ... | | | Nov 09, 202... | -- | -- | o Abnormal | Compliance Reporting |
| OST2023110915273602e9a2894 | Scan | Virtualized ... | | | Nov 09, 202... | Nov 09, 202... | 1min 13s | o Cancelled | Compliance Reporting |
| OST2023110914475902f7088c | Scan | Virtualized ... | | | -- | -- | -- | o Cancelled | Compliance Reporting |
| OST202311061541500201444b6 | Scan | Virtualized ... | | | Nov 06, 202... | Nov 07, 202... | 1d 7h 8min ... | o Cancelled | Compliance Reporting |
| OST202311021806310225128b6 | Scan | Virtualized ... | | | Nov 02, 202... | Nov 03, 202... | 21h 17min ... | o Cancelled | Compliance Reporting |
| OST2023110116452402783887d | Repair | Virtualized ... | | | Nov 01, 202... | Nov 02, 202... | 18h 6min 57s | o Cancelled | Compliance Reporting |

NOTE

Ticket type: **Scan** and **Repair**

Step 4 You can click a ticket ID to view the ticket details.

- If a ticket is in the **Paused** state, you can click **Continue** to continue it.
- If a ticket is in the **Executing** state, you can click **Pause** to pause it.
- If a ticket is not completed, you can click **Forcibly End** to stop it.

Figure 10-13 Service ticket details

Basic Information

Ticket Type: Scan
Start Time: Oct 30, 2023 GMT+08:00
Status: o Successful

Created By: [Redacted]
End Time: Oct 30, 2023 GMT+08:00

Execution Information

All (1) Pending Execution (0) Executing (0) Successful (1) Cancelled (0) Paused (0) Abnormal (0)

| NameID | Internal IP Address | EIP | Start Time | End Time | Total Duration | Status | Operation |
|------------|---------------------|-----|------------------------|------------------------|----------------|--------------|-----------|
| [Redacted] | | -- | Oct 30, 2023 GMT+08:00 | Oct 30, 2023 GMT+08:00 | 8s | o Successful | Cancel |

Total Records: 1

----End

10.1.4 Resource Operation Tickets

You can view resource operation tickets.

Prerequisites

If you perform operations on ECSs and RDS DB instances, the system generates a corresponding operation ticket.

Scenarios

View ESC and RDS DB instance operation tickets on the **Cloud Operations Center** page.

Procedure

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Task Management > Execution Records** and click the **Resource Operation Tickets** tab.
- Step 3** You can search for tickets by ID, ticket type, start time, and status.

Figure 10-14 Resource operation Tickets

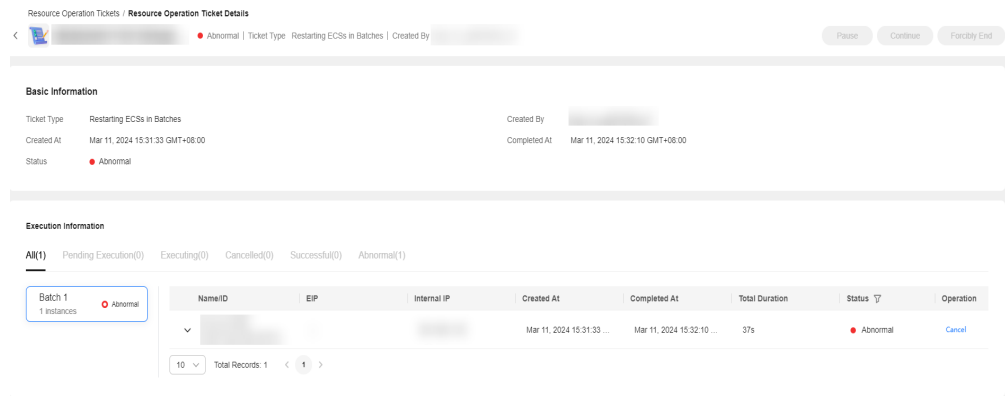
| ID | Ticket Type | Region | Created By | Created At | Completed At | Total Duration | Status |
|----|----------------------------|--------|------------|---------------------------|---------------------------|----------------|------------|
| EC | Restarting ECSs in Bat... | | | Apr 09, 2024 20:07:31 ... | Apr 09, 2024 20:08:10 ... | 39s | Successful |
| EC | Restarting ECSs in Bat... | | | Apr 09, 2024 14:54:51 ... | Apr 09, 2024 14:55:30 ... | 39s | Successful |
| EC | Starting ECSs in Batches | | | Apr 09, 2024 10:34:34 ... | Apr 09, 2024 10:35:10 ... | 36s | Successful |
| RC | Enabling RDS in Batches | | | Apr 08, 2024 15:22:50 ... | Apr 08, 2024 15:27:10 ... | 4min 20s | Successful |
| RC | Stopping RDS in Batches | | | Apr 08, 2024 15:17:27 ... | Apr 08, 2024 15:21:00 ... | 3min 33s | Successful |
| EC | Restarting ECSs in Bat... | | | Apr 08, 2024 14:04:13 ... | Apr 08, 2024 14:04:50 ... | 37s | Successful |
| EC | Starting ECSs in Batches | | | Apr 08, 2024 09:59:15 ... | Apr 08, 2024 09:59:50 ... | 35s | Successful |
| EC | Starting ECSs in Batches | | | Apr 08, 2024 09:30:18 ... | Apr 08, 2024 09:30:50 ... | 32s | Successful |
| RC | Restarting RDS in Batic... | | | Apr 03, 2024 17:24:11 ... | Apr 03, 2024 17:25:00 ... | 49s | Successful |
| RC | Restarting RDS in Batic... | | | Apr 03, 2024 17:21:36 ... | Apr 03, 2024 17:22:10 ... | 34s | Successful |

NOTE

Status: Paused, pending executing, cancelled, successful, and abnormal

- Step 4** You can click a ticket ID to view the ticket details.
 - If a ticket is in the **Paused** state, you can click **Continue** to continue it.
 - If a ticket is in the **Executing** state, you can click **Pause** to pause it.
 - If a ticket is not completed, you can click **Forcibly End** to stop it.

Figure 10-15 Details about a resource operation ticket



----End

10.2 To-do Center

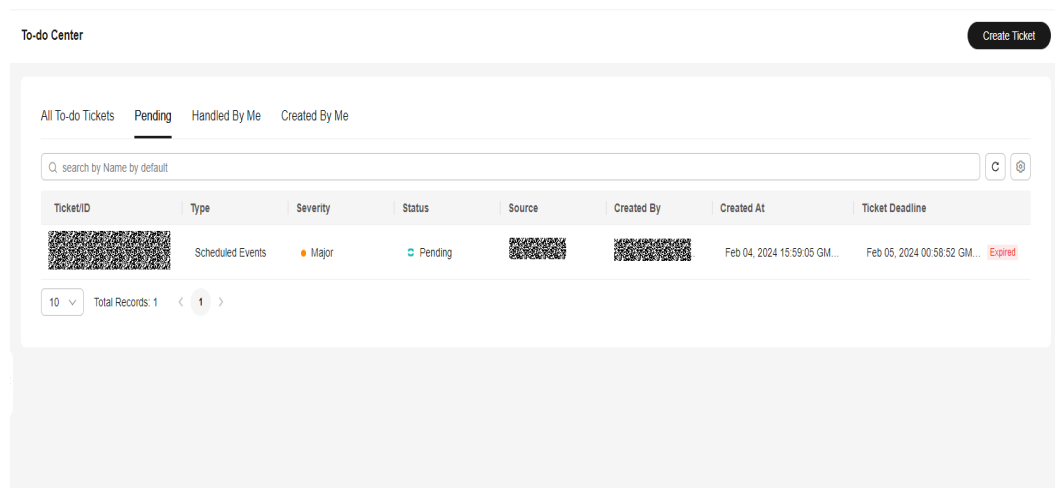
Overview

Main function of To-do Center: You can use a HUAWEI ID (primary SRE of the tenant) to create tasks for IAM users (sub-SREs of the tenant). For example, a company can create IAM accounts for different departments.

Adding a To-do Ticket

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Task Management > To-do Center**.

Figure 10-16 Viewing the to-do center list



- Step 3** Click **Create Ticket**. The **Create Ticket** page is displayed.
- Step 4** Specify the to-do ticket name, description, type, severity, and other mandatory parameter, as shown in [Table 10-1](#).

Figure 10-17 Creating a to-do ticket

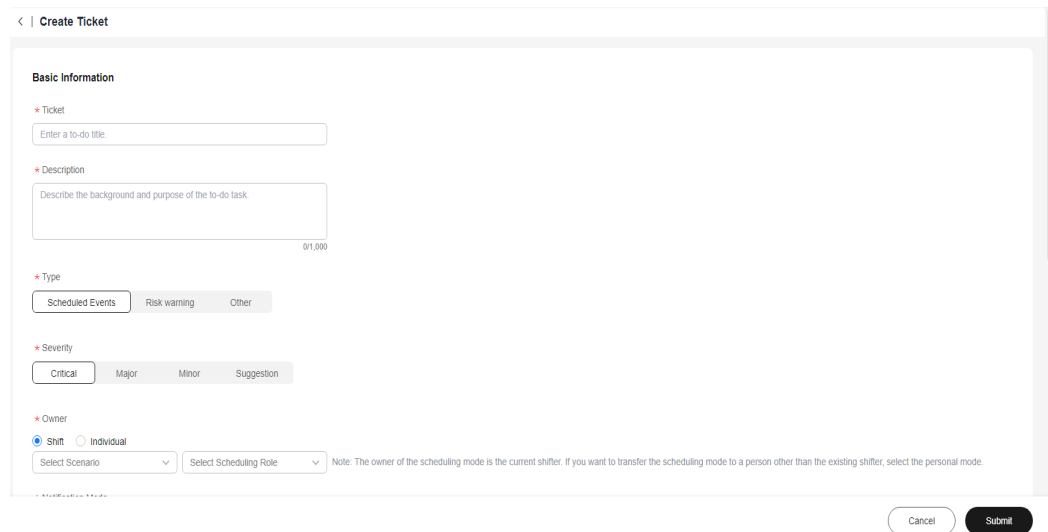


Table 10-1 Parameters

| Parameter | Description |
|-------------|---|
| Ticket | <p>Mandatory.</p> <ul style="list-style-type: none"> The ticket name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). Start with a letter or number. Cannot end with a period (.). |
| Description | <p>Mandatory.</p> <p>The description can contain a maximum of 1,000 characters, including letters, numbers, and special characters.</p> |
| Type | <p>Mandatory.</p> <p>To-do ticket type. The options are as follows:</p> <ul style="list-style-type: none"> Scheduled incidents Risk warning Other |

| Parameter | Description |
|----------------------|--|
| Severity | Mandatory. Severity of a to-do ticket. The options are as follows: <ul style="list-style-type: none"> • Critical • Major • Minor • Suggestion |
| Owner | Mandatory. The owner of a to-do ticket can be: <ul style="list-style-type: none"> • Shift • Individual |
| Notification Mode | Mandatory. Notification mode. The options are as follows: <ul style="list-style-type: none"> • Default • SMS • Enterprise WeChat • DingTalk • Email • No notification |
| Ticket Deadline | Mandatory. Time when a to-do ticket needs to be closed |
| Label | Optional. |
| Recommended Solution | Mandatory. The description can contain a maximum of 1,000 characters, including letters, numbers, and special characters. |

Step 5 Specify optional parameters such as **Label** and **Add File**.

Step 6 Click **Submit**. If "To-do task created" is displayed in the upper right corner, the creation is successful.

 **NOTE**

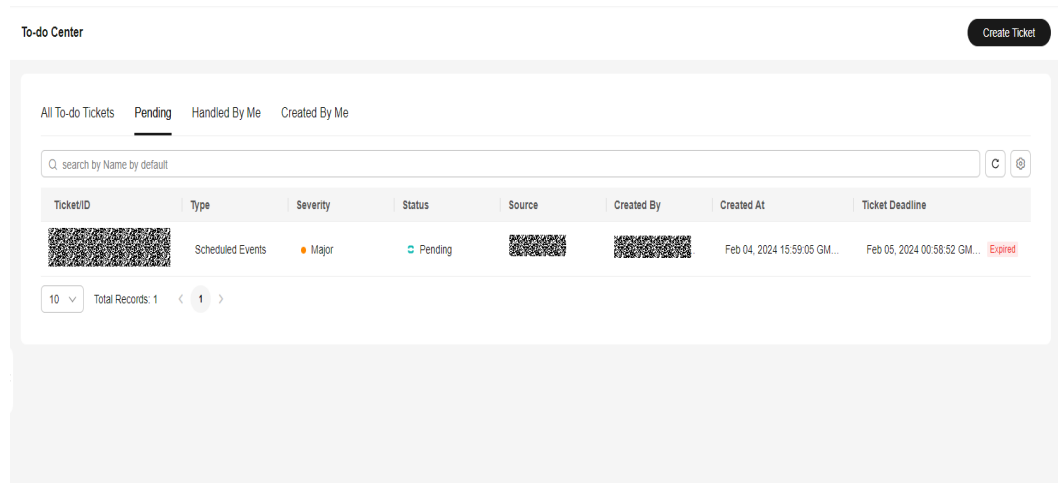
You can select **Shift** or **Individual** for **Owner**. The size of a file to be uploaded must be less than 50 MB. Various formats are supported.

----**End**

To-do Ticket List

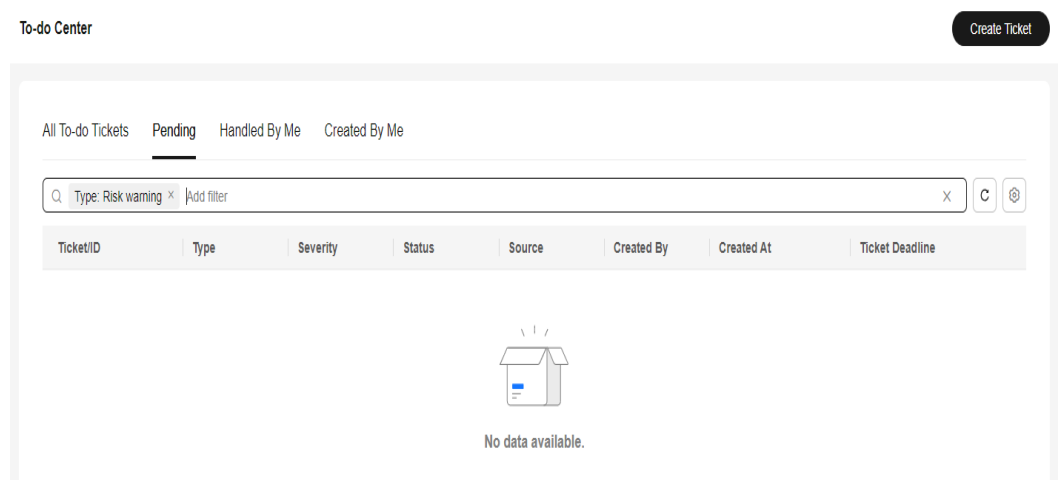
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Task Management > To-do Center**. The to-do ticket list is displayed.

Figure 10-18 Viewing the to-do center list



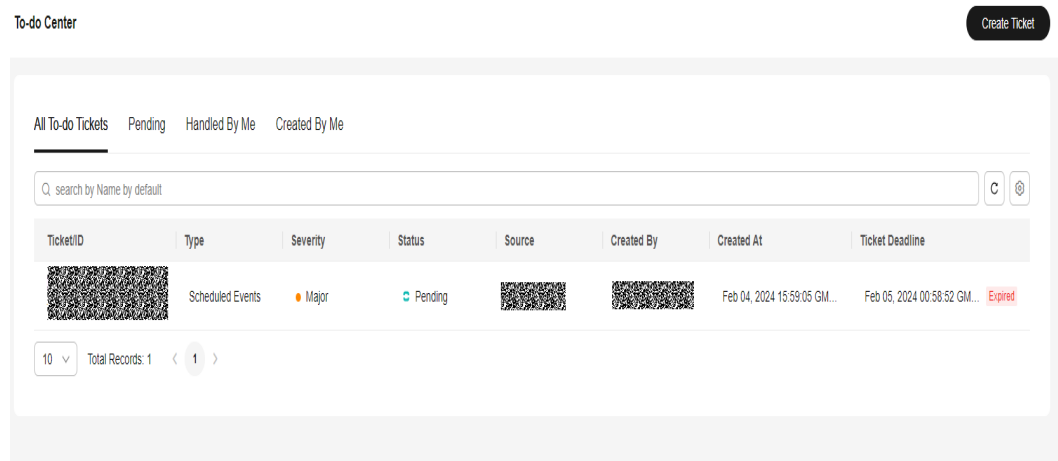
- Step 3** Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data.
- Step 4** You can click the icons next to the search box to refresh the list data and set the fields to be displayed in the list.

Figure 10-19 Adding search criteria



- Step 5** Click the **All To-do Tickets**, **Pending**, **Handled By Me**, or **Created By Me** tabs. The corresponding to-do ticket list is displayed.

Figure 10-20 To-do ticket list



NOTE

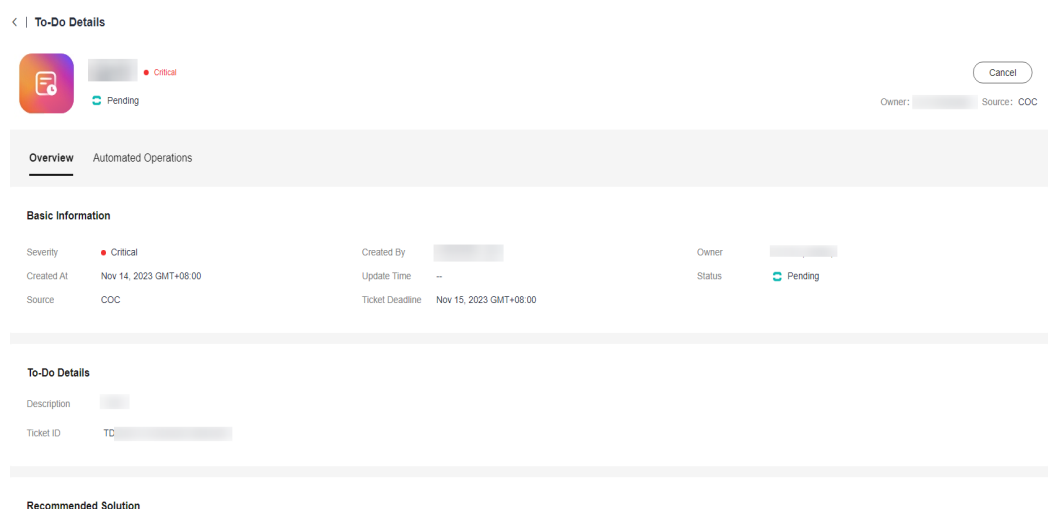
An IAM user can only view the tickets related to this user on the **All To-do Tickets** tab page, and cannot view those related to other IAM users on this tab page.

----End

Viewing Pending Tickets

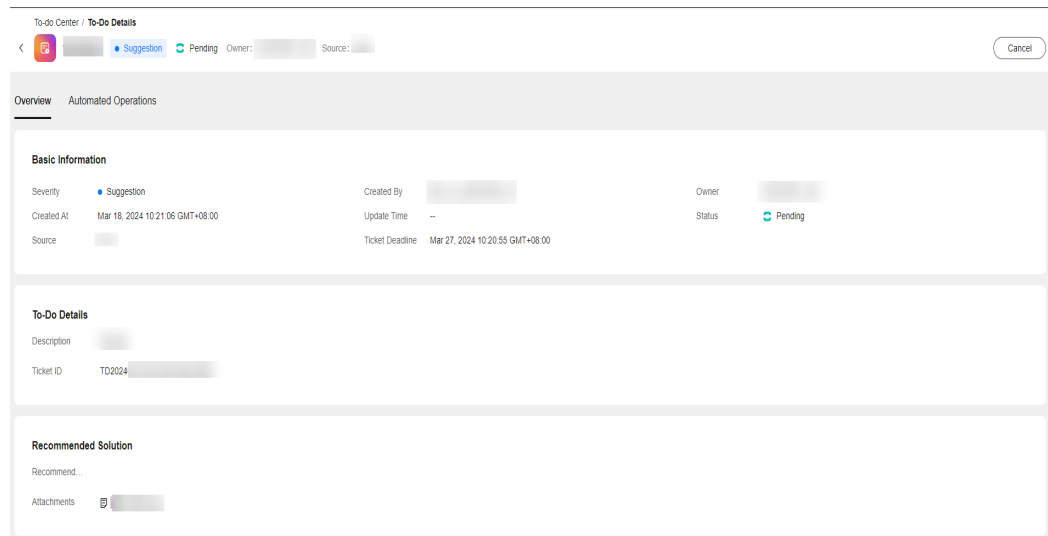
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane, choose **Task Management > To-do Center**. The to-do ticket list is displayed.
- Step 3** Click a to-do ticket name in the list. The to-do ticket details are displayed.

Figure 10-21 To-do ticket details



- Step 4** On the details page, click the attachment name to download the attachment.

Figure 10-22 Downloading an attachment



NOTE

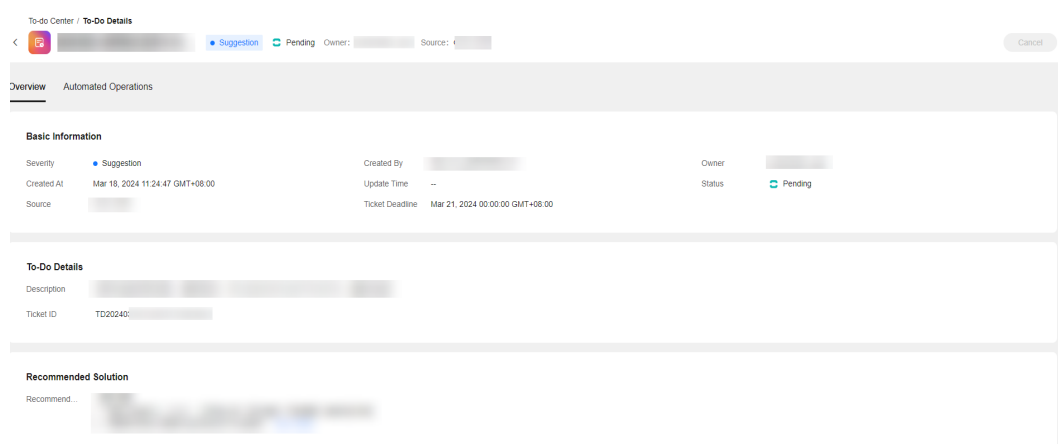
The attachment download traffic is limited. After downloading an attachment, the next download can be performed after 5 seconds.

----End

Handling To-do Tickets

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Task Management > To-do Center**. On the displayed page, click the **Pending** tab.
- Step 3** Click a to-do ticket name in the list to go to the to-do ticket details page. Click **Accept** in the upper right corner to complete the handling.

Figure 10-23 Handling a to-do ticket



 **NOTE**

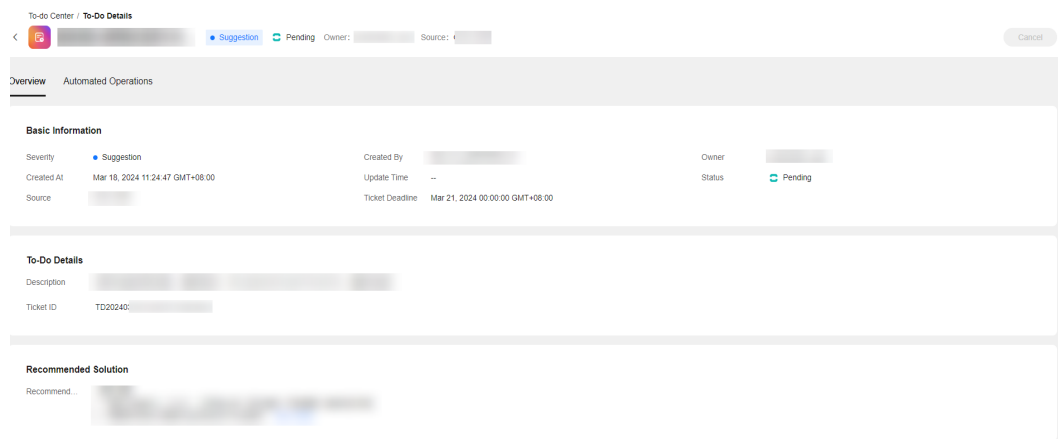
The current login user can handle only the to-do tickets whose owner is himself/herself.

----End

Canceling a To-Do Ticket

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Task Management > To-do Center**. On the displayed page, click the **Created By Me** tab. In the displayed list, filter to-do tickets in the **Pending** state.
- Step 3** Click a to-do ticket name in the list to go to the ticket details page.
- Step 4** Click **Cancel** in the upper right corner.

Figure 10-24 Canceling a to-do task



 **NOTE**

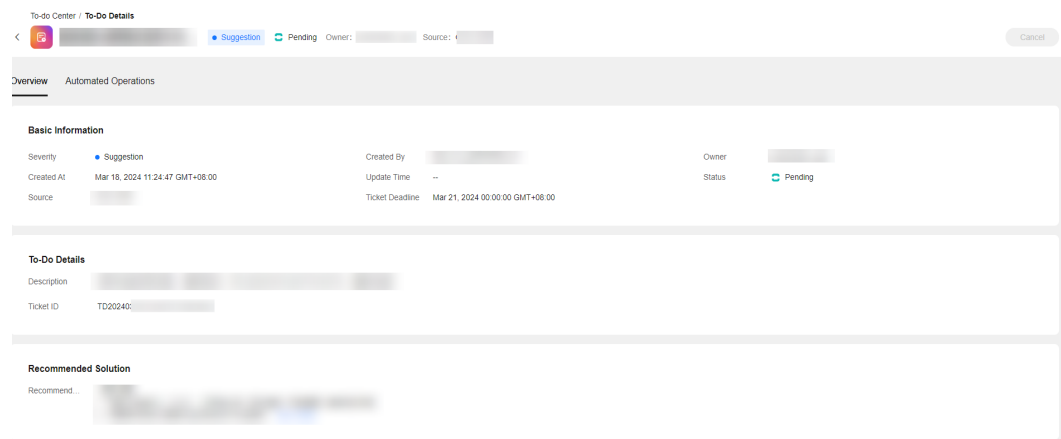
The current login user can cancel only the to-do tickets that are created by or owned by this user.

----End

Closing a To-do Ticket

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Task Management > To-do Center**. On the displayed page, click the **Handled By Me** tab. In the displayed to-do list, filter to-do tickets in the **Processing** state.
- Step 3** Click a to-do ticket name in the list. On the to-do ticket details page that is displayed, click **Close** in the upper right corner.

Figure 10-25 Closing a to-do ticket



 **NOTE**

The current login user can close only the to-do tickets whose owner is himself/herself.

----End

11 Basic Configurations

11.1 O&M Engineer Management (COC)

11.1.1 O&M Engineer Management Overview

Cloud O&M Center supports unified management of O&M engineers. You can manage users of the current tenant on the **O&M Engineer Management** page. The basic user data in the **O&M Engineer Management** page is synchronized from IAM and is used by multiple basic functional modules, such as to-do task creation, scheduled O&M, notification management, and incident center.

- On the **O&M Engineer Management** page, you can manually add and manage user information.
- If you edit the information of an existing user, the system background creates a corresponding subscription mode after you specify a communication method, such as mobile number, email address, enterprise WeChat, or DingTalk.
- On the **O&M Engineer Management** page, the notification methods in gray indicates that the user does not subscribe to the notification methods or does not confirm the subscriptions. The notification methods in black indicates that the user has subscribed to the notification methods and has confirmed the subscriptions.

11.1.2 O&M Engineer Management Usage

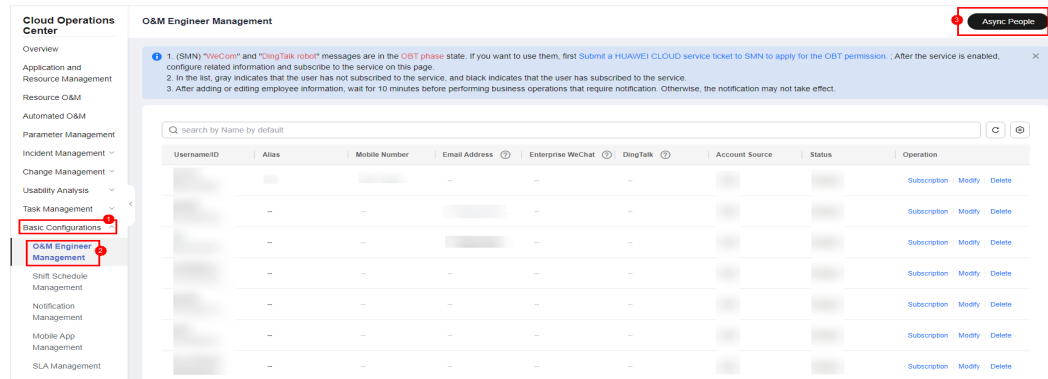
This section describes how to use the **O&M Engineer Management** module.

Adding a User

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > O&M Engineer Management**. On the displayed **O&M Engineer Management** page, click **Async People** in the upper right corner.

Figure 11-1 Synchronizing people



----End

Editing User Information

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > O&M Engineer Management**. On the displayed **O&M Engineer Management** page, locate the target username and click **Modify** in the **Operation** column.

Figure 11-2 Modifying personal information

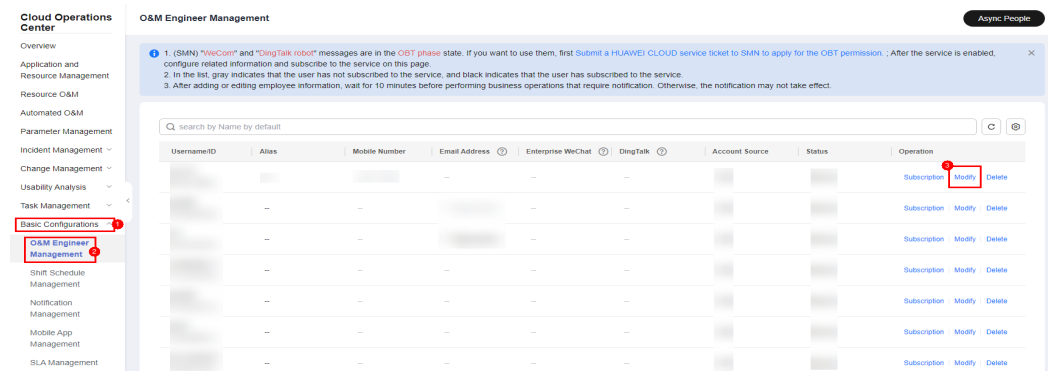
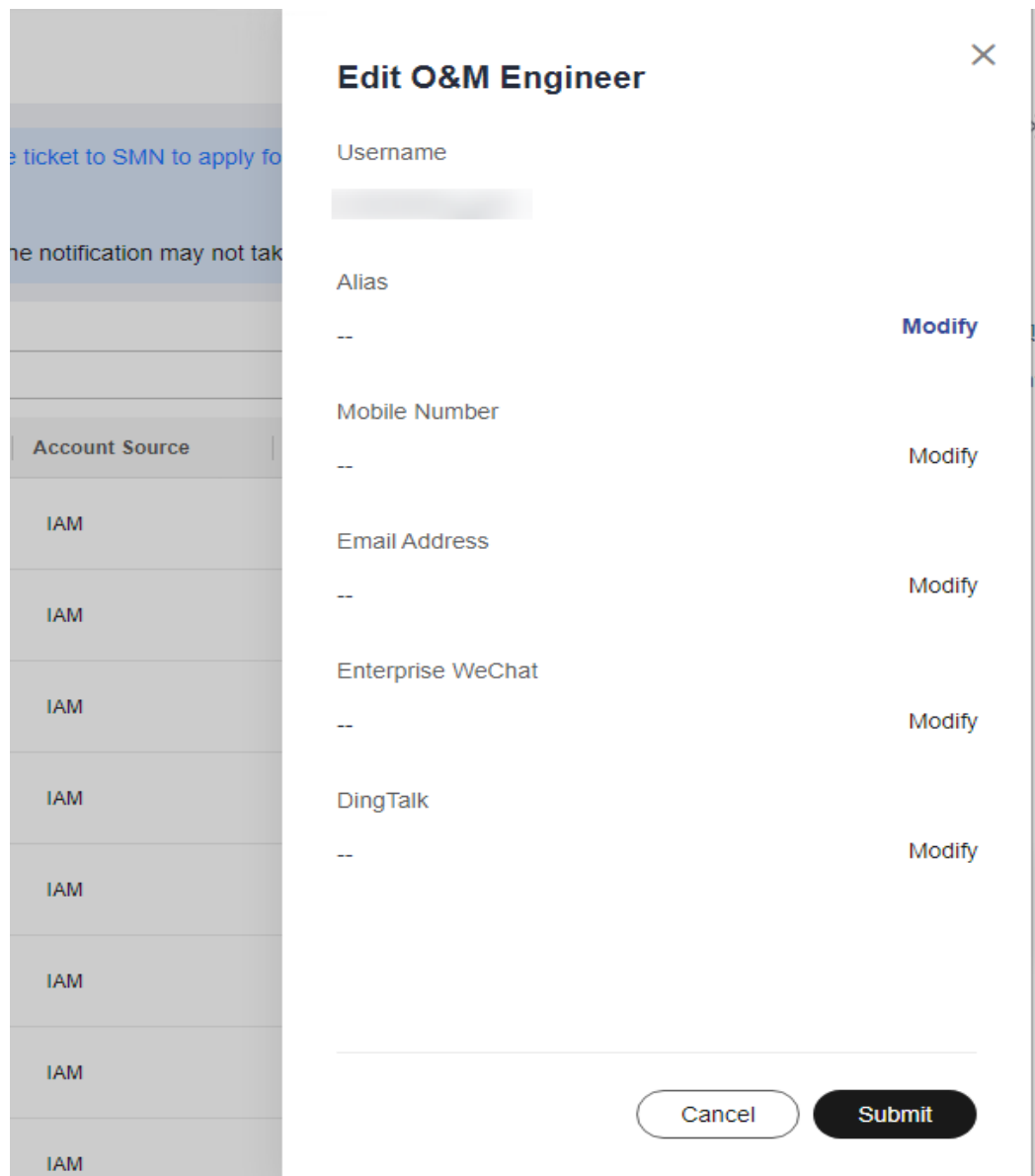


Figure 11-3 Modifying details



- **Alias:** Alias of the current user.
- **Mobile Number:** The mobile number of the current user.
- **Email Address:** The Email address of the current user.
- **Enterprise WeChat:** The webhook address of the enterprise WeChat group chatbot.
- **DingTalk:** The webhook address of the DingTalk group chatbot.

NOTE

The usage of the communication methods in the personnel information:

After the communication methods are edited 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.
- **Enterprise WeChat** can be used without subscription.
- **DingTalk** can be used without subscription.

Notes:

- The current version supports the following notification methods: SMS, enterprise WeChat, voice, DingTalk, and email. Enterprise WeChat, DingTalk, and voice notifications 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 **Personnel Management** page.
- After the DingTalk and enterprise WeChat information is saved, the system can use them without subscription.
- After the subscription of the message, voice, or email services are confirmed, the subscription status is automatically synchronized 10 minutes later and the corresponding message notification methods can be used.

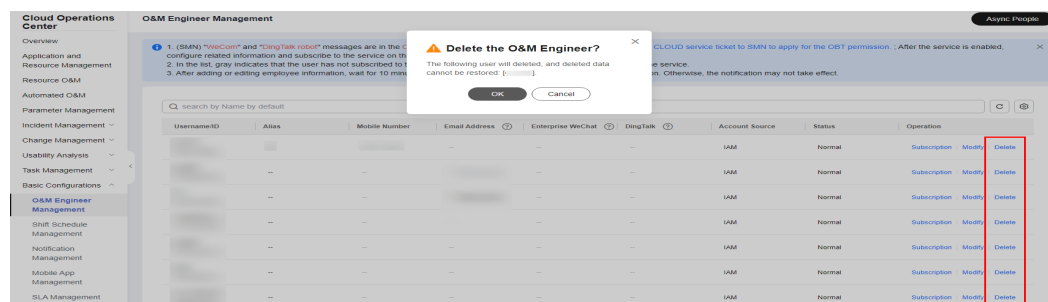
----End

Deleting a User

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > O&M Engineer Management**. On the displayed **O&M Engineer Management** page, locate the target username and click **Delete** in the **Operation** column.

Figure 11-4 Deleting a member



----End

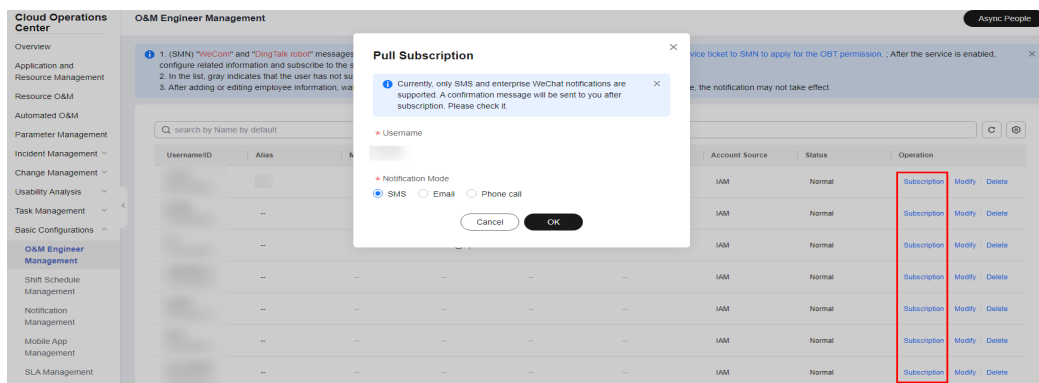
Subscribing to a User

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 on the left, choose **Basic Configurations > O&M Engineer Management**. On the displayed **O&M Engineer Management** page, locate the target username and click **Subscription** in the **Operation** column.

Figure 11-5 Subscription



NOTE

The usage of subscription in personnel management is as follows:

- After you click **Subscription**, 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 on 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.

----End

11.2 Shift Schedule Management

11.2.1 Overview

Schedule management allows you to centrally manage O&M engineers and customize shift schedules. You can create scheduling scenarios and roles, and add O&M engineers to schedules.

- When you need to set or obtain O&M engineers in a schedule, go to the **Shift Schedule Management** page to configure or query a shift schedule.
- The created shift schedules can be directly used to set personnel parameters in O&M services such as **Incident Forwarding Rules**, **Incident Center**, **Automated O&M**, **Notification management**, and **Change Ticket Management**.

Scheduling Scenarios

Multiple shift schedules can be used for a scheduling scenario. When creating a scheduling scenario, you need to specify the scheduling mode and dimension. The configuration varies according to your selection.

Roles

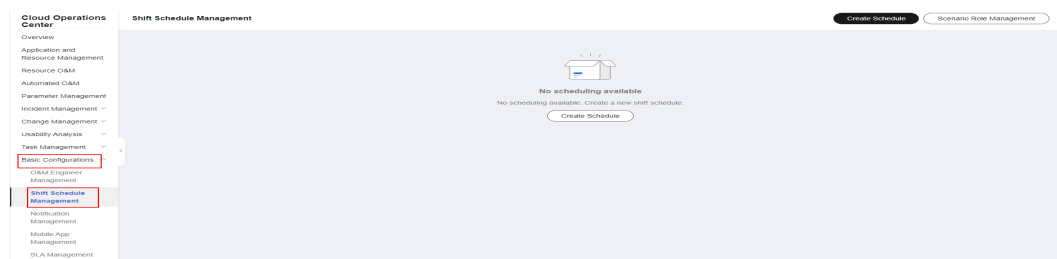
A scheduling role is the minimum unit for setting a schedule. Multiple roles can be created in a scheduling scenario, and each role can be attached to multiple O&M engineers.

11.2.1.1 Creating a Schedule

Step 1 Log in to **COCCOC**.

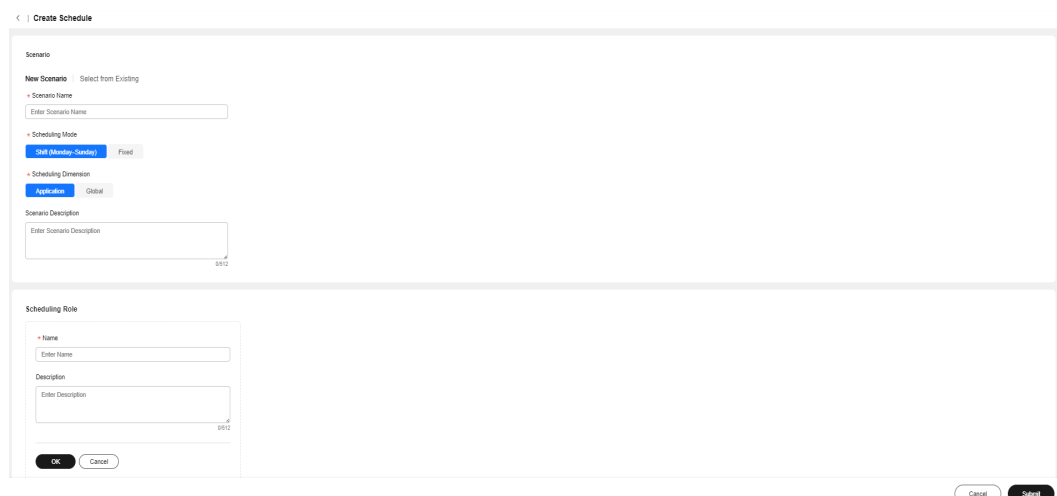
Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the **Shift Schedule Management** page, click **Create Schedule**.

Figure 11-6 Schedule management page



Step 3 On the page for creating a schedule, enter schedule scenario information, add a schedule role, and click **Submit**. If there already is a scheduling scenario and a scheduling role, you can select the existing scenario on the page for creating a schedule and view the roles in the scenario.

Figure 11-7 Page for creating a schedule



- **Scenario Name:** name of a scenario

- **Scheduling Mode:** scheduling mode. The options are **Fixed** and **Shift (Monday–Sunday)**.
- **Scheduling Dimension:** impact scope of the schedule. The options are **Application** or **Global**.
- **Scenario Description:** detailed description of the scenario
- **Name:** name of a scheduling role
- **Scenario:** In the **Scenario** pane, click **Select form Existing** to specify a scenario for the role.
- **Description:** detailed description of the scheduling role

 **NOTE**

Scheduling Mode

- **Fixed:** Engineers work within fixed working hours.
- **Shift (Monday–Sunday):** Engineers work different shifts depending on the schedule.

Scheduling Dimension

- **Global:** The schedule is globally used regardless of applications.
- **Application:** The schedule is created for an application in a specific region (optional).

Step 4 Click **O&M Roles** on the page indicating that the schedule is created. The method of adding engineers varies according to the scheduling mode and dimension. For details, see [Adding O&M Engineers](#).

----End

11.2.1.2 Adding O&M Engineers

Prerequisites

Before adding O&M engineers to your schedule, you need to add them to a list on the **O&M Engineer Management** page, and then create a schedule scenario and roles.

Scenarios

The methods of adding engineers vary depending on scheduling modes and scheduling dimensions. Click the links in the following table to see detailed procedures.

| Schedule Type | Fixed Shifts | Rotating Shift (Monday-Sunday) |
|----------------------|--|---|
| Global | Adding engineers to a global schedule of fixed shifts | Adding engineers to a global schedule of rotating shifts |
| Application-specific | Adding engineers to an application-specific schedule of fixed shifts | Adding engineers to an application-specific schedule of rotating shifts |

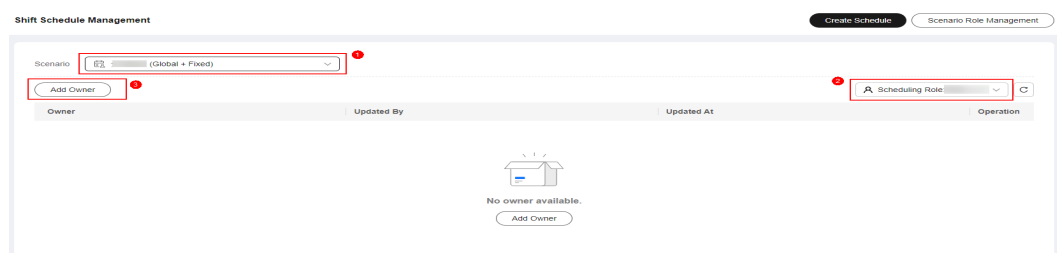
Global Schedule of Fixed Shifts

Application scenario: These schedules are applied to all applications. O&M engineers are fixed in a day.

Step 1 Log in to [COCCOC](#).

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a created schedule scenario (**Global + Fixed** is displayed next to the scenario name) and a scheduling role, and click **Add Owner**.

Figure 11-8 Adding the owner of a **Global + Fixed** scenario



----End

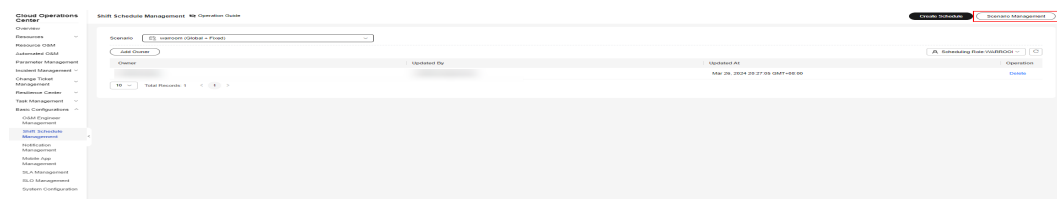
Global Schedule of Rotating Shifts

Application scenario: These schedules are applied to all applications. O&M engineers work various shifts over a period.

Step 1 Log in to [COCCOC](#).

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a created schedule scenario (**Global + Shift (Monday-Sunday)** is displayed next to the scenario name), and click **Schedule**.

Figure 11-9 Adding a schedule



Step 3 Enter the information about the schedule and click **OK**.

Figure 11-10 Specifying schedule information

ScheduleX

i Note that the original shifts of all services will be overwritten. Changing the switch time may result in unscheduled shifts in some time periods. Exercise caution when performing this operation. X

* Start Time

Select a date.📅

* End Time

Select a date.📅

* Shift Number

Select Shift Number▼

CancelOK

- **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.

NOTE

All shifts are displayed, and you need to specify the start and end time of each shift and set the owners of specific scheduling roles for each shift.

You can select multiple owners for each shift.

Step 4 Select the scenario and a date in the upper right corner to view the engineers in a shift.

----End

Application-specific Schedule of Fixed Shifts

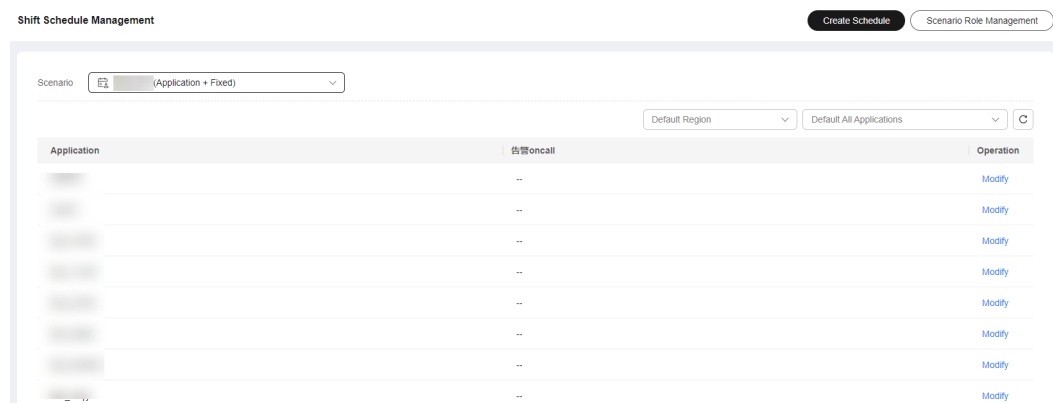
Application scenario: These schedules are applied to specific applications. O&M engineers are fixed in a day.

Prerequisites: An application has been created on the **Mobile App Management** page.

Step 1 Log in to [COCCOC](#).

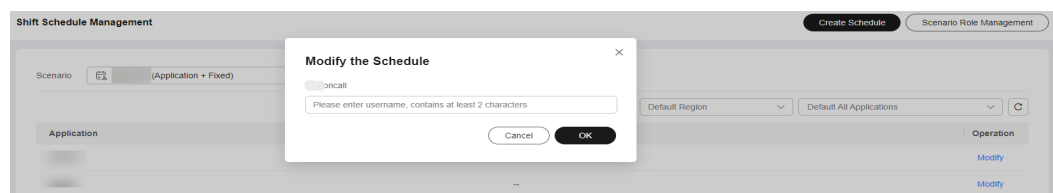
Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a created scenario (**Application + Fixed** is displayed next to the scenario name), region, and application.

Figure 11-11 Applications where the schedules are applied



Step 3 Click **Modify** in the **Operation** column of the list, select a user, and click **OK**. You can view the added engineer in the list.

Figure 11-12 Adding an engineer



----End

Application-specific Schedule of Rotating Shifts

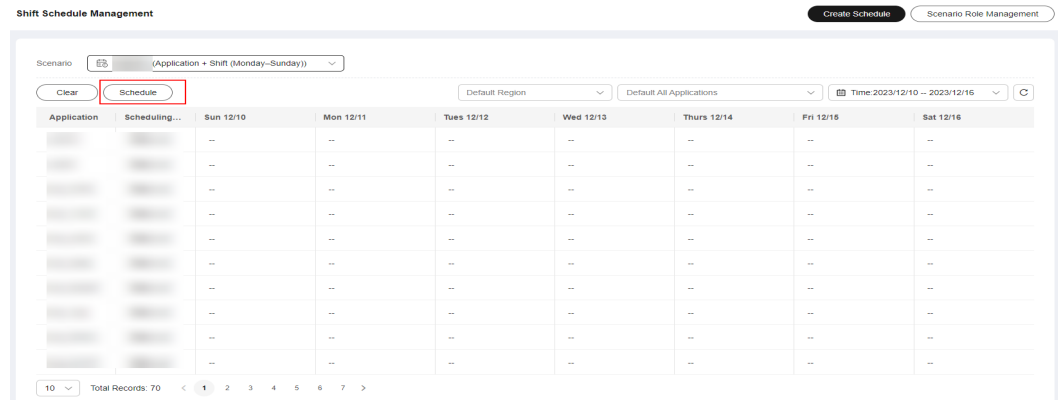
Application scenario: These schedules are applied to specific applications.

Prerequisites: An application has been created on the **Mobile App Management** page.

Step 1 Log in to [COCCOC](#).

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a created scenario (**Application + Shift (Monday–Sunday)** is displayed next to the scenario name), region, and application.

Figure 11-13 Applications where the schedules are applied



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 is no regional differences.

Step 3 Click **Schedule**, specify detailed shift information, and click **OK**. Added engineers are displayed.

Figure 11-14 Adding engineers

Schedule X

i Note that the original shifts of all services will be overwritten. Changing the switch time may result in unscheduled shifts in some time periods. Exercise caution when performing this operation. X

Region

Default v

* Application

Select Application v

* Start Time

Select a date. 📅

* End Time

Select a date. 📅

* Shift Number

Select Shift Number v

CancelOK

- **Region:** Region where this schedule is applied. You can select multiple regions or leave this option blank.
- **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.

----End

11.2.1.3 Managing O&M Engineers

You can query, modify, and delete O&M engineers in different shifts.

Scenarios

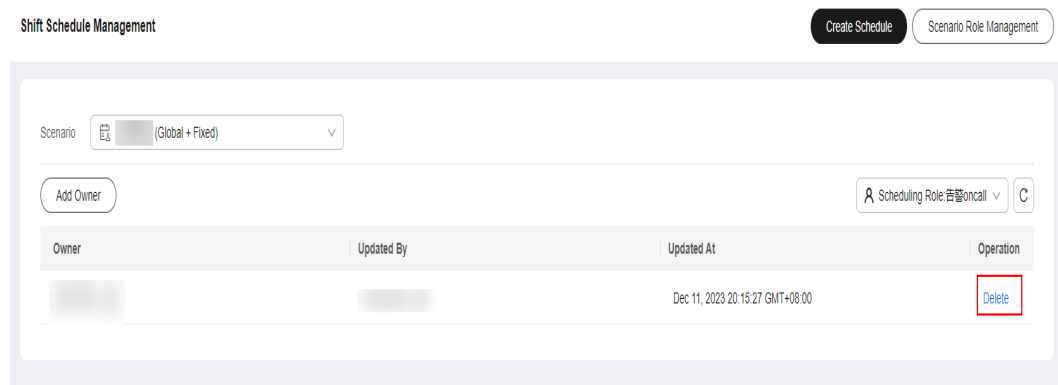
When the engineers in a schedule change, you can modify or delete the information about the changes. The method of changing the engineers varies according to the scenario.

Global Schedule of Fixed Shifts

Step 1 Log in to COCCOC.

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a scenario and role, and click **Delete** in the **Operation** column.

Figure 11-15 Deleting an engineer



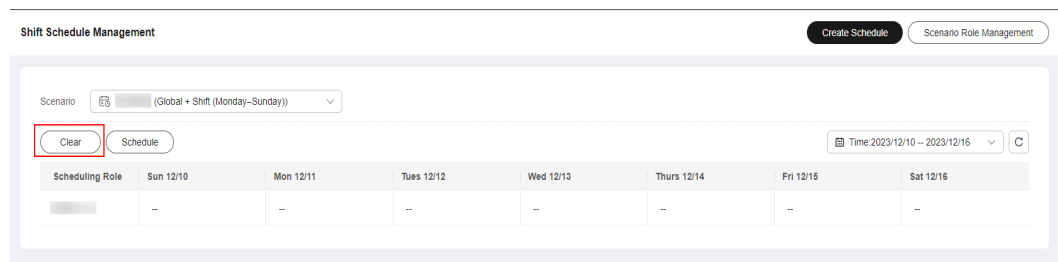
----End

Global Schedule of Rotating Shifts

Step 1 Log in to COCCOC.

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a scenario and click **Clear**.

Figure 11-16 Deleting engineers



Step 3 In the **Clear** pane, enter the start time and end time, select a scheduling role, and click **OK**.

Figure 11-17 Clearing a schedule

Clear ✕

ℹ The expired shifts will not be cleared. ✕

* Start Time
Select a date. 📅

* End Time
Select a date. 📅

* Scheduling Role
Select Scheduling Role ▾

Cancel OK

----End

Application-specific Schedule of Fixed Shifts

- Step 1** Log in to [COCCOC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a scenario, region, and applications, and click **Modify** in the **Operation** column to add or delete engineers.

Figure 11-18 Modifying a fixed shift

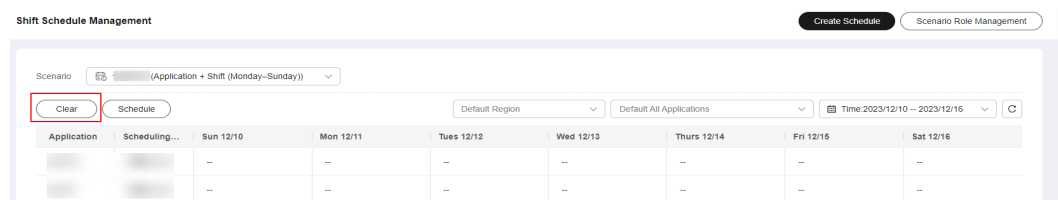


----End

Application-specific Schedule of Rotating Shifts

- Step 1** Log in to [COCCOC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, select a scenario and click **Clear**.

Figure 11-19 Clearing schedules



- Step 3** In the **Clear** pane, select regions and applications, enter the start time and end time, select a scheduling role, and click **OK**.

Figure 11-20 Clearing schedules

Clear ×

i The expired shifts will not be cleared. ×

Region
Default ▾

* Application
Select Application ▾

* Start Time
Select a date. 📅

* End Time
Select a date. 📅

* Scheduling Role
Select Scheduling Role ▾

Cancel OK

----End

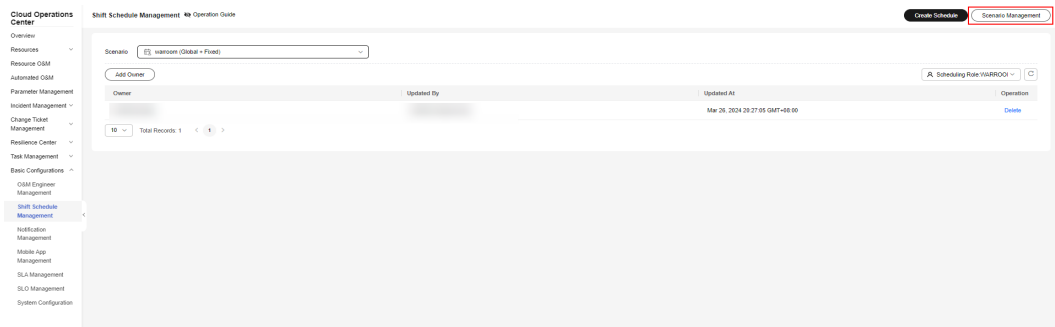
11.2.2 Managing Scheduling Scenarios

This topic describes how to manage scheduling scenarios and scheduling roles.

Creating a Scheduling Scenario

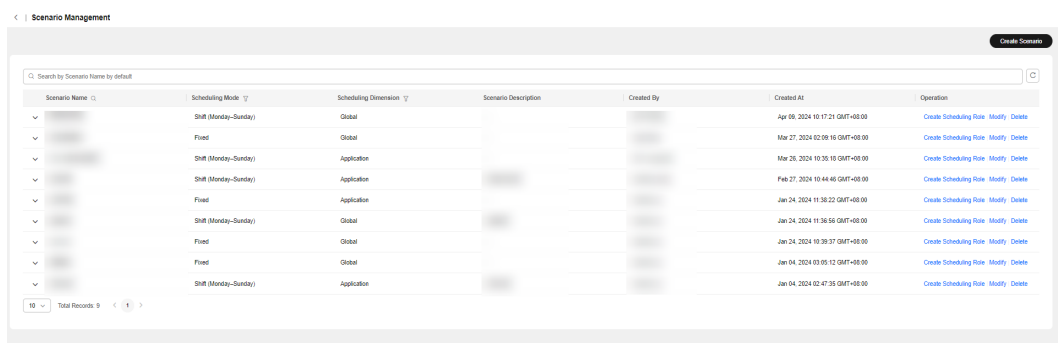
- Step 1** Log in to [COCCOC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, click **Scenario Management**.

Figure 11-21 Scenario management



Step 3 Click **Create Scenario**.

Figure 11-22 Scenario list



Step 4 Enter the basic information about the scenario, and then click **OK**.

Figure 11-23 Creating a scheduling scenario

Create Scenario X

* Scenario Name

Enter Scenario Name

* Scheduling Mode

Shift (Monday-Sunday) Fixed

* Scheduling Dimension

Application Global

Scenario Description

Enter Scenario Description

0/512

Cancel OK

- **Scenario Name:** name of a scheduling scenario
- **Scheduling Mode:** shift type. The options are **Shift (Monday-Sunday)** and **Fixed**.
 - **Fixed:** Engineers work within fixed working hours.
 - **Shift (Monday-Sunday):** Engineers work different shifts depending on the schedule.
- **Scheduling Dimension:** use scope of schedules in this scenario. The options are **Application** and **Global**.

- **Global:** The schedule is globally used regardless of applications.
- **Application:** The schedule is created for and applied to a specific application.
- **Scenario Description:** detailed description of the scheduling scenario

Step 5 Click **Create Scheduling Role** in the **Operation** column of a scenario.

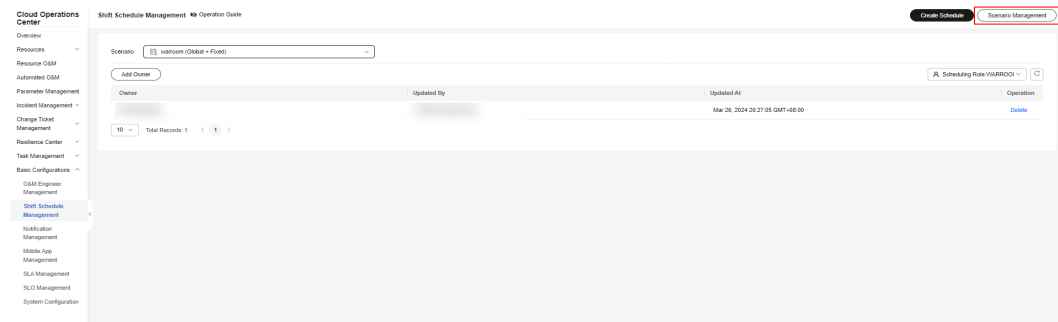
----End


Querying a Scheduling Scenario

Step 1 Log in to **COCCOC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, click **Scenario Management**.

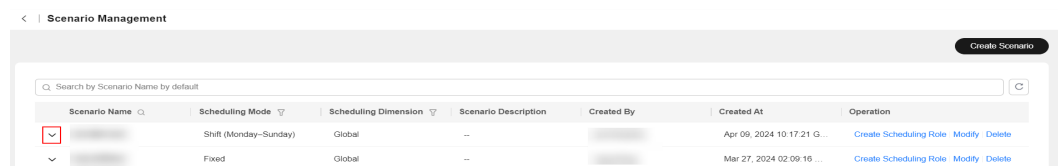
Figure 11-24 Scenario management



Step 3 In the **Scenario** tab, enter a query condition, and click  on the left or press **Enter**.

Step 4 Click  in the scheduling scenario list to view roles of the scenario.

Figure 11-25 View roles



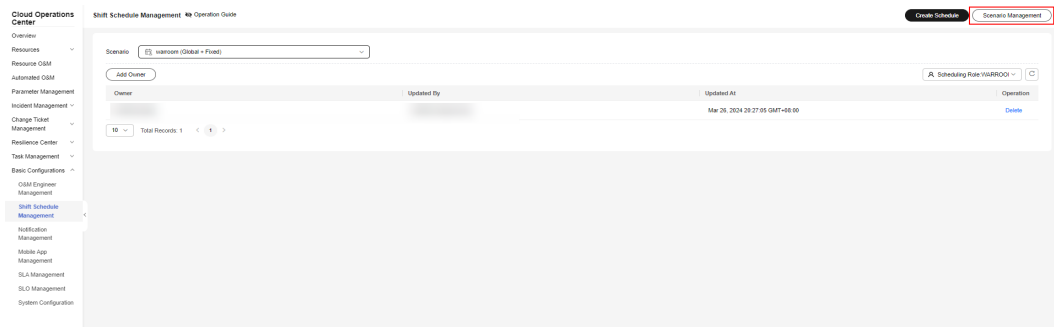
----End

Modifying a Scheduling Scenario

Step 1 Log in to **COCCOC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, click **Scenario Management**.

Figure 11-26 Scenario management



Step 3 In the **Scenario** tab, locate the scheduling scenario you want to modify and click **Modify**.

Step 4 In the displayed dialog box, modify the scenario name and description, and click **OK**.

Figure 11-27 Modifying a scenario

Modify the Scenario

✕

* Scenario Name

* Scheduling Mode

Shift (Monday–Sunday)Fixed

* Scheduling Dimension

ApplicationGlobal

Scenario Description

Enter Scenario Description

0/512

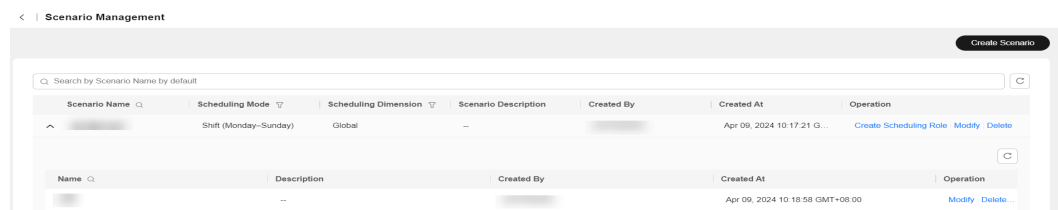
CancelOK

NOTE

The scheduling mode and scheduling dimension in a scenario cannot be modified. You can create a new schedule to specify the mode and dimension you need.

Step 5 Click followed by a scenario name, locate the role you want to modify, and click **Modify** in the **Operation** column of the role.

Figure 11-28 Modifying a scheduling role

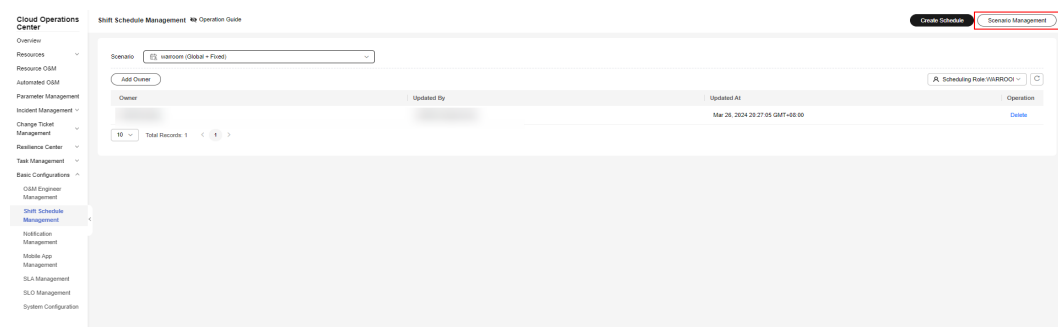


----End

Deleting a Scheduling Scenario

- Step 1** Log in to [COCCOC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Shift Schedule Management**. On the displayed page, click **Scenario Management**.

Figure 11-29 Scenario management



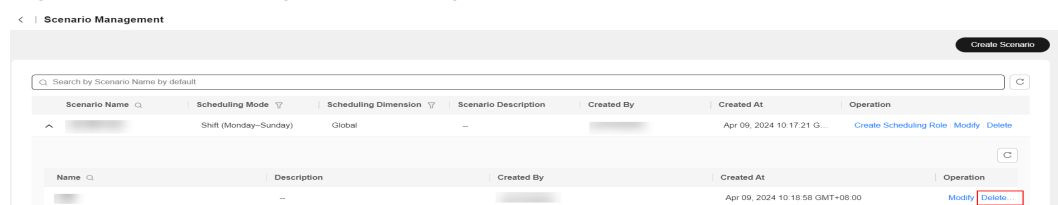
- Step 3** In the **Scenario** tab, locate the scheduling scenario you want to delete and click **Delete**.
- Step 4** In the displayed dialog box, click **OK**.

NOTE

A scheduling scenario can be deleted only when no scheduling role is used in that scheduling scenario.

- Step 5** To delete a scheduling role in a scenario, click **▼** followed by the scenario name and click **Delete** in the **Operation** column of the scheduling role.

Figure 11-30 Deleting a scheduling role



----End

11.2.3 Managing Scheduling Roles

11.3 Notification Management

Notification Management allows users to create notification rules. Notification rules include notification scenarios and incident matching rules. When an incident ticket is generated, the notification rule first matches the incident information, then provides the O&M engineers to be notified, the notification content, and notification method, and finally sends the notification messages.

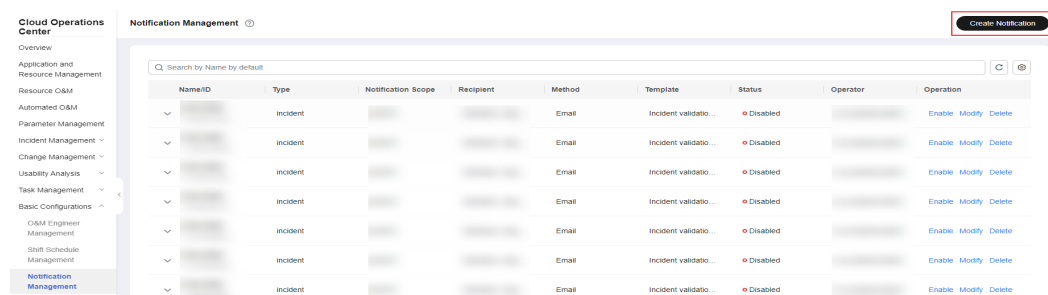
Notification templates are system built-in, including incident creation, incident rejection, incident forwarding, incident verification, incident verification failure, incident completion, and incident rejection completion templates. You can select a notification template based on your scenario.

Creating a Notification

Create a notification rule. After an incident ticket triggers the corresponding scenario, a notification is automatically sent.

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, click **Create Notification**.

Figure 11-31 Clicking Create Notification



- Step 3** Enter the parameters for creating a notification and click **OK**. [Table 11-1](#) describes the parameters for creating a notification.

Figure 11-32 Entering the notification parameters

Table 11-1 Notification parameters

| Parameter | Mandatory | Radio/Checkbox | Description |
|--------------------|-----------|----------------|--|
| Name | Yes | / | Notification name of a notification instance. Fuzzy search can be performed based on the notification name. |
| Type | Yes | Radio | Currently, Incident Notification is the default value. |
| Template | Yes | Checkbox | Notification content template is system built-in. The template list varies depending on the notification type. After a template is selected, the notification template details are displayed. |
| Notification Scope | Yes | Checkbox | Select a service. For example, if service A is selected and service A is displayed in the incident ticket, the subscription takes effect and a notification is sent based on the subscription instance without considering other matching rules. |

| Parameter | Mandatory | Radio/Checkbox | Description |
|---------------------------------------|-----------|--|--|
| Recipient | Yes | If Shift is selected, you can select single scenario and multiple roles. If Individual is selected, you can select multiple users. | Objects to be notified. If Shift is selected, the notification module automatically obtains the list of personnel in the current schedule mode and sends notifications to the corresponding personnel. If Individual is selected, the notification module directly sends notifications to the corresponding users. |
| Notification Rule | / | / | For example, if the value of rule <i>A</i> is set to <i>a</i> , in an incident ticket, the value of rule <i>A</i> is <i>a</i> , 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 <i>A</i> in the incident ticket is <i>b</i> , the subscription instance will not take effect, and no notification is sent. |
| Notification Rule - Level | Yes | Checkbox | Level of an incident ticket. There are five levels: P1 to P5. For details about the incident ticket levels, see section "Creating an Incident". |
| Notification Rule - Incident Category | Yes | Checkbox | Category of an incident ticket. Multiple values are available. |
| Notification Rule - Source | Yes | Checkbox | Source of an incident ticket. Manual creation indicates that the incident ticket is created in the incident ticket center. Transfer creation indicates that the incident ticket is generated during the transfer. |
| Notification Rule - Region | No | Checkbox | Region of an incident ticket. Multiple regions can be selected. |
| Method | Yes | Checkbox | Notification channel. |

CAUTION

In the shift scenario, duplicated users 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.

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.

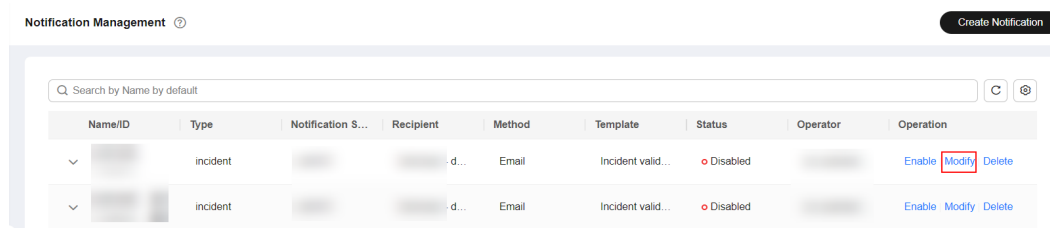
----End

Editing Notifications

Modify an existing notification instance.

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, locate the notification to be modified and click **Modify** in the **Operation** column.

Figure 11-33 Modifying notifications



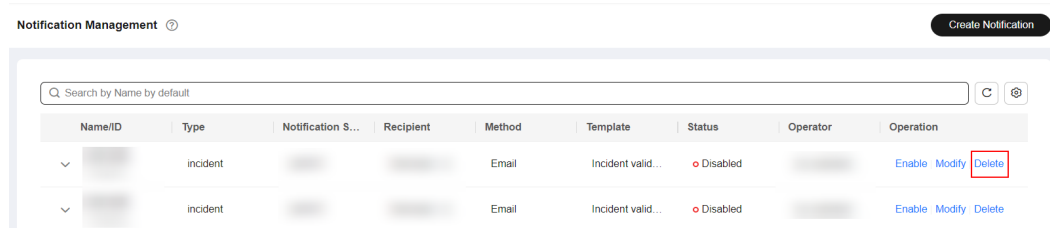
- Step 3** Modify the notification instance and save the modification. For details, see [Step 3](#).

----End

Deleting a Notification

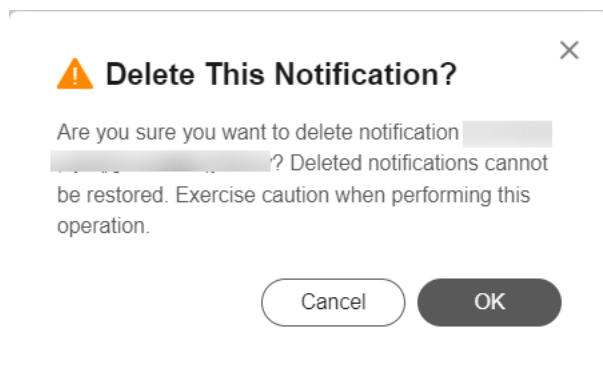
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, locate the notification to be deleted and click **Delete** in the **Operation** column.

Figure 11-34 Deleting a notification



- Step 3** In the displayed confirmation dialog box, click **OK** to delete the notification instance. After the notification instance is deleted, it is not displayed in the list.

Figure 11-35 Confirming the deletion

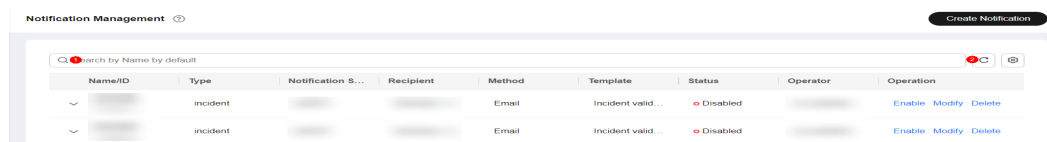


----End

Searching for a Notification Instance

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, click the search box, enter the target notification information, and press **Enter**.

Figure 11-36 Searching for notifications



NOTE

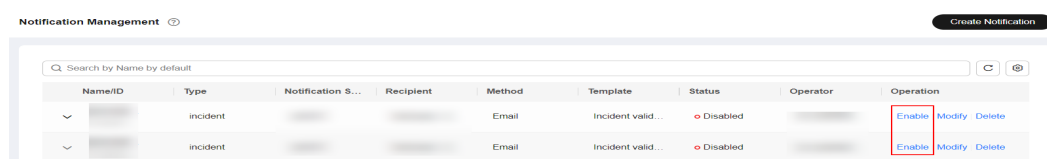
The search box supports search by notification type and notification name (fuzzy search). The search results can be displayed on multiple pages (10, 20, 50, or 100 records per page). Click the drop-down arrow on the left of each notification instance displays details.

----End

Enabling and Disabling a Notification Instance

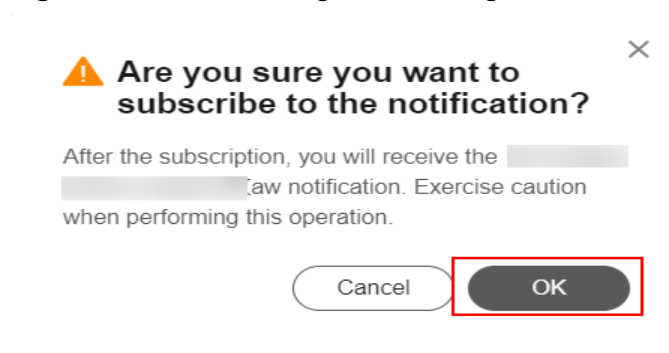
- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, locate the notification to be enabled or disabled, click **Enable** or **Disable** in the **Operation** column.

Figure 11-37 Enabling/Disabling Notifications



Step 3 The confirmation dialog box is displayed. Click **OK**.

Figure 11-38 Confirming the enabling



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 change triggers multiple notifications, and the subscriber or other conditions of multiple notifications are the same, the notification module deduplicates the recipients, ensuring that the recipients receive only one notification when an incident ticket change occurs.

2. Notification Template Description

Different templates correspond to different scenarios. When an incident ticket matches a scenario, a notification can be sent. The notification templates are described as follows:

- Incident creation: A notification needs to be sent after an incident is created.
- Event rejection: A notification is sent after an event is rejected.
- Incident forwarding: A notification is sent after an incident is forwarded.
- Incident verification: A notification is sent when an incident enters the to-be-verified state after being resolved.
- Incident completion: A notification is sent after an incident is processed and verified.
- Incident verification failed: A notification is sent when an incident enters the to-be-verified state and fails to pass the verification.
- Incident close after rejection: After an incident is rejected, a notification is sent after the incident is closed.

11.4 Mobile Application Management

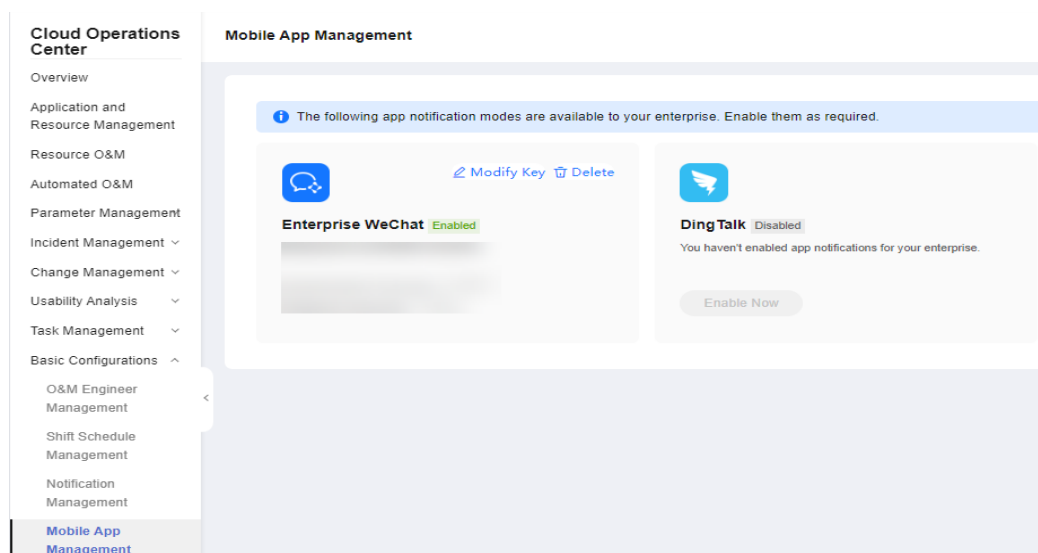
Mobile Application Management is used to manage the enterprise WeChat configuration information required for creating an enterprise WeChat WarRoom.

Viewing Mobile Application Management

Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Basic Configurations > Mobile App Management**. If a tenant has been bound to an enterprise WeChat account, the binding information is displayed. If a tenant is not bound to an enterprise WeChat account, the page for adding an enterprise WeChat key is displayed.

Figure 11-39 Mobile application management



NOTE

Currently, only enterprise WeChat is supported.

----End

Adding a Mobile Application

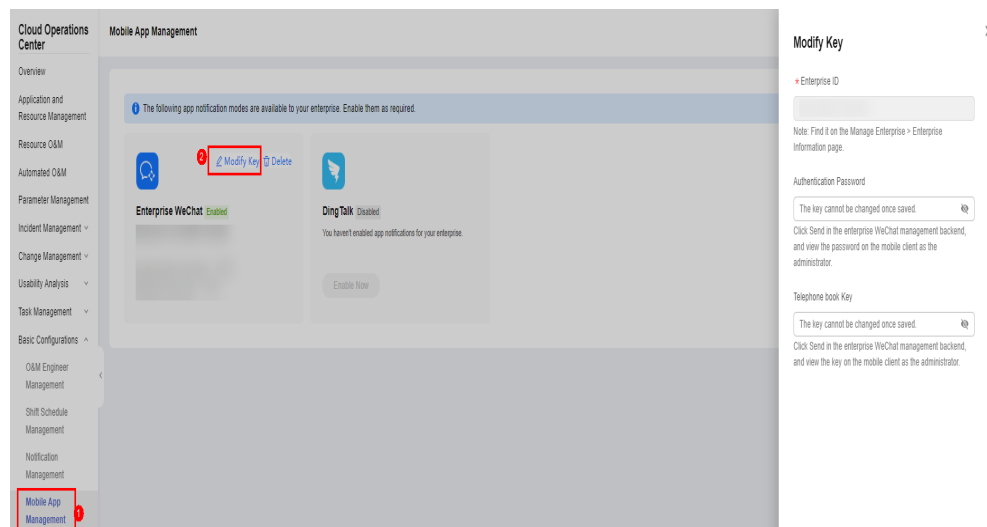
Step 1 Log in to [COC](#).

Step 2 In the navigation pane on the left, choose **Basic Configurations > Mobile App Management**. If a tenant is not bound to an enterprise WeChat account, the page for adding an enterprise WeChat key is displayed.

Step 3 Click **Enable Now** and enter the enterprise WeChat application ID, enterprise key, and address book key.

Step 4 Click OK. If the message is displayed indicating that the mobile application is created successfully, the mobile application is created successfully.

Figure 11-40 Creating a mobile application

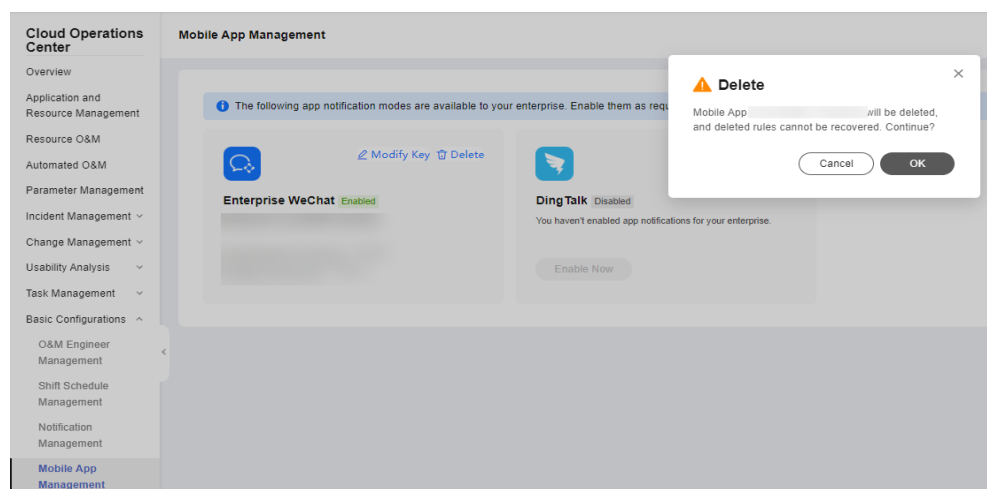


----End

Deleting a Mobile Application

- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > Mobile App Management**.
- Step 3** If the tenant ID has been bound to an enterprise WeChat key, the key information page is displayed.
- Step 4** Click **Delete**. In the displayed dialog box, click **OK**.

Figure 11-41 Deleting a Mobile Application



----End

11.5 SLA Management

Overview

SLA provides ticket timeliness management for customers. When a ticket triggers an SLA rule, customer will be notified to handle the ticket in time and the SLA triggering details will be recorded.

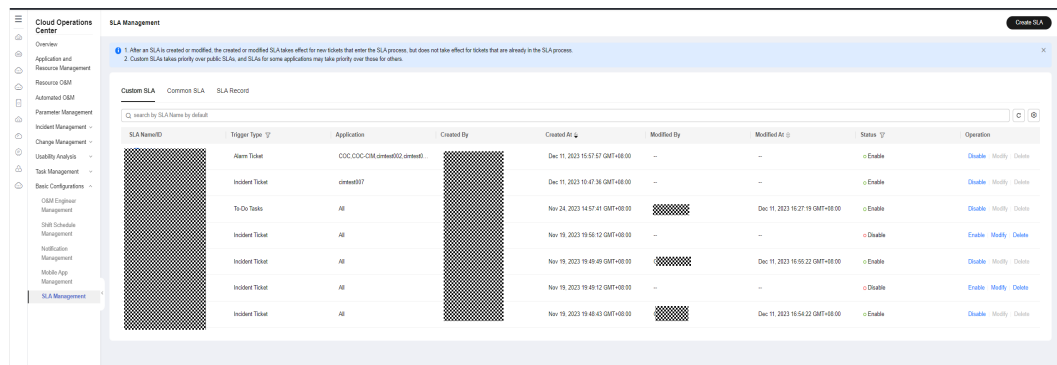
11.5.1 Custom SLA

Tenants can customize SLA as required.

Querying a Custom SLA

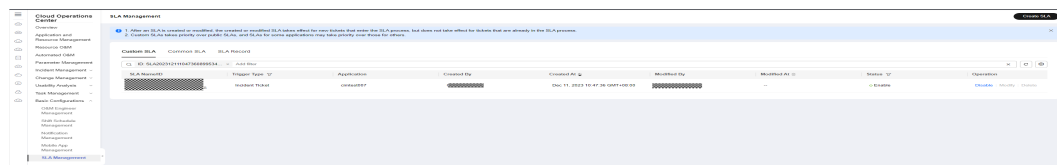
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > SLA Management**.
- Step 3** Click the **Custom SLA** tab.

Figure 11-42 SLA list



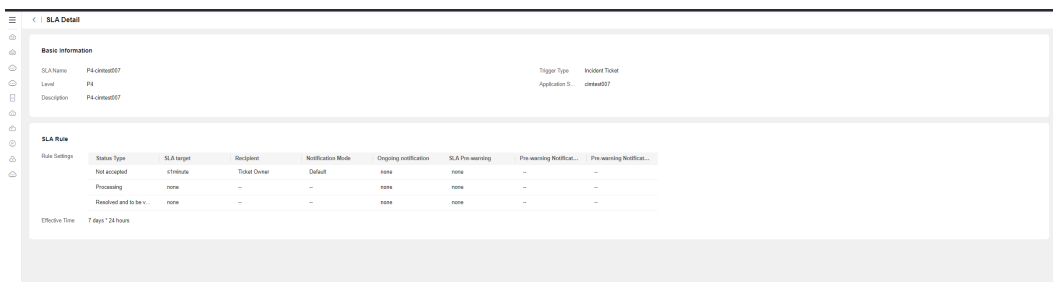
- Step 4** Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 11-43 Filtering SLA rules



- Step 5** Click an SLA name in the list to go to the SLA details page.

Figure 11-44 Viewing SLA details



NOTE

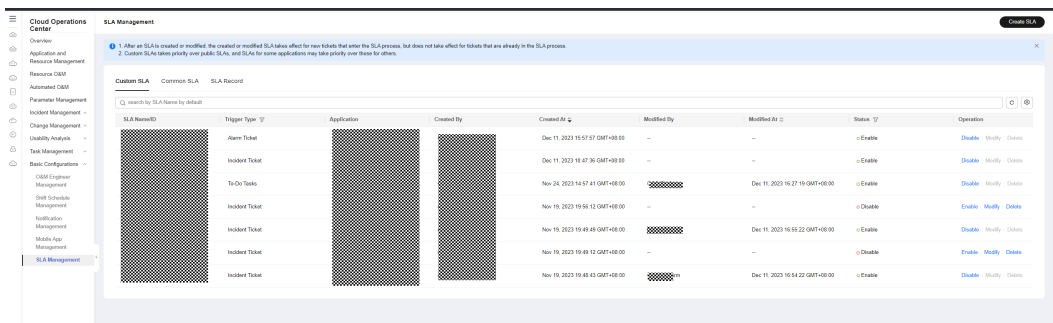
Tenant isolation is implemented in the system. You can view only the custom SLAs created by the current tenant account and its subaccounts.

----End

Creating a Custom SLA

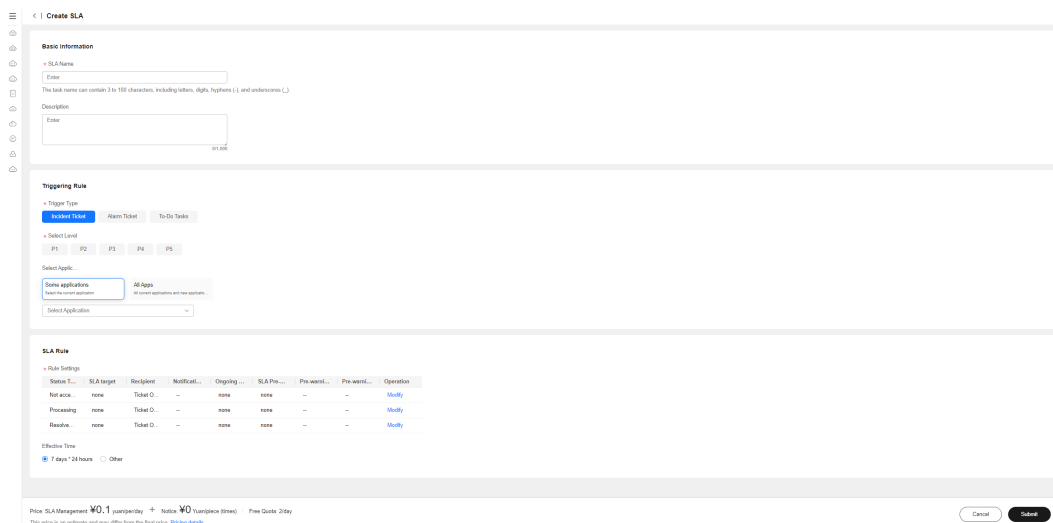
- Step 1** Log in to [COC](#).
- Step 2** In the navigation pane on the left, choose **Basic Configurations > SLA Management**.
- Step 3** Click the **Custom SLA** tab.

Figure 11-45 Querying the SLA List



- Step 4** Click **Create SLA** in the upper right corner.

Figure 11-46 Creating a custom SLA



Step 5 Enter the SLA name, description, trigger type, level, and application information. If **Some applications** is selected, search for and select applications from the drop-down list box. Multiple or all applications can be selected. [Table 11-2](#) describes the required parameters.

Figure 11-47 Selecting applications

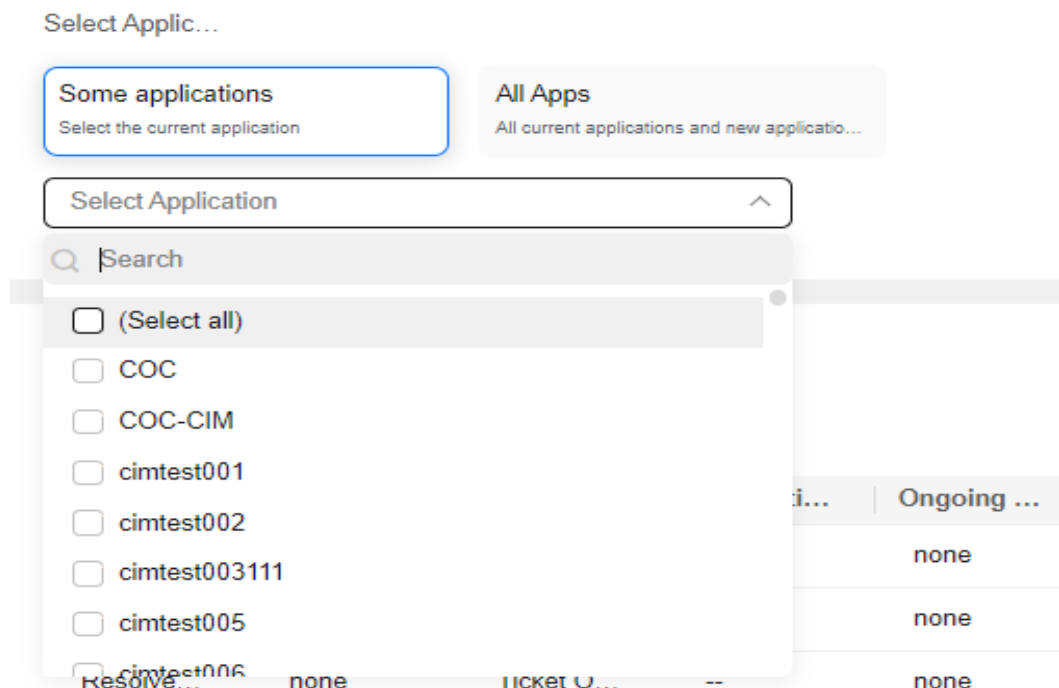


Table 11-2 Description

| Parameter | Description |
|--------------------|---|
| SLA Name | Mandatory The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_). |
| Description | The value can contain a maximum of 1000 characters, including letters, digits, and special characters. |
| Trigger Type | Mandatory Trigger types include: <ul style="list-style-type: none"> ● Incident Ticket ● Alarm Ticket ● To-Do Task |
| Select Level | When the trigger type is incident ticket, the levels are as follows: <ul style="list-style-type: none"> ● P1 ● P2 ● P3 ● P4 ● P5 When the trigger type is Alarm Ticket, the levels include: <ul style="list-style-type: none"> ● Critical ● Major ● Minor ● Suggestion When the trigger type is To-Do Task, the levels include: <ul style="list-style-type: none"> ● Critical ● Major ● Minor ● Suggestion |
| Select Application | Options: <ul style="list-style-type: none"> ● Some applications ● All Apps |

Step 6 Click **Modify** in **Operation** column of the **SLA Rule** table.

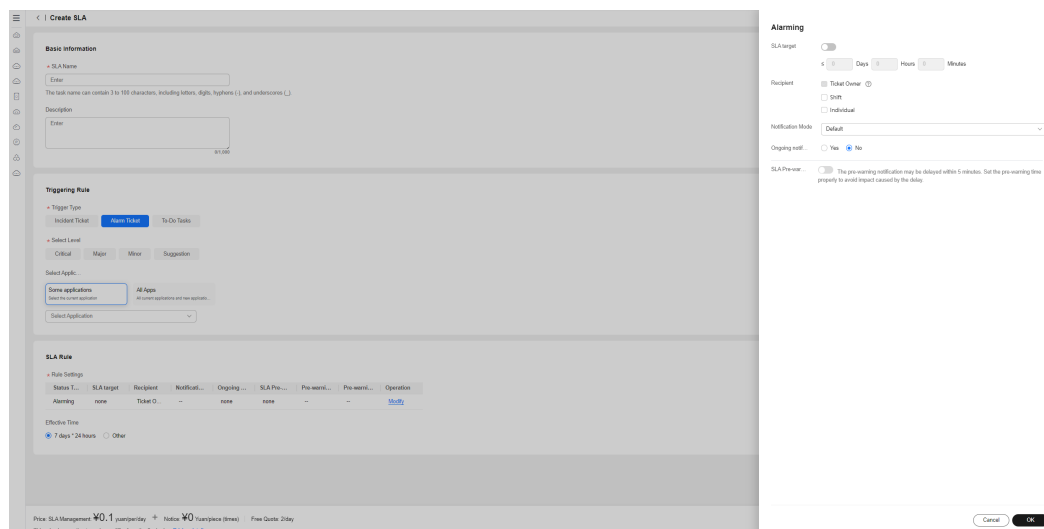
Step 7 Set SLA target, notification object, and notification channel in the dialog box that is displayed.

Table 11-3 Description

| Parameter | Description |
|----------------------|--|
| SLA Status Type | <p>When the trigger type is incident ticket, the status types are as follows:</p> <ul style="list-style-type: none"> • Not yet accepted • Processing • To-be-verified <p>When Trigger Type is set to Alarm Ticket, the status types are as follows:</p> <ul style="list-style-type: none"> • In alarm <p>When Trigger Type is set to Alarm Ticket, the status types are as follows:</p> <ul style="list-style-type: none"> • Pending processing • Processing |
| SLA target | <p>The SLA target can be enabled. After the SLA target is enabled, a maximum of seven days can be set.</p> |
| Notification Objects | <p>Notification objects are classified into the following types:</p> <ul style="list-style-type: none"> • Ticket owner. • Shift • Individual <p>The case owner is the default notification.</p> |
| Notification Mode | <p>Notification mode. The options are as follows:</p> <ul style="list-style-type: none"> • Default • SMS • Enterprise WeChat • DingTalk • Email • No notification |

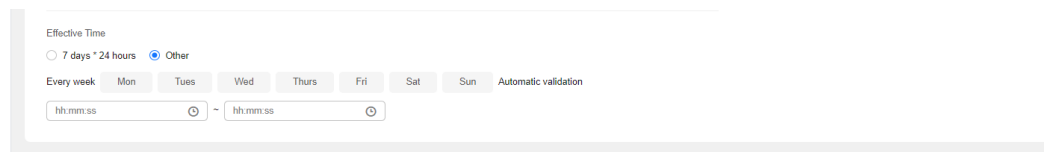
Step 8 Click OK to modify the SLA rule.

Figure 11-48 Configure an SLA Rule



Step 9 By default, **Effective Time** is set to **7 days * 24 hours**. SLA takes effect at any time. When you select **Other**, the time option is displayed. You can select the date when the SLA takes effect and the valid duration.

Figure 11-49 Setting effective time



Step 10 After all SLA information is entered, click **Submit**.

NOTE

1. Only custom SLAs can be created. Common SLA is automatically preset in the system. Tenants can only enable, disable, and view common SLA.
2. After an SLA is created or modified, the new SLA takes effect for the tickets that just enter the SLA process. For those that have been in the SLA process, the new SLA does not take effect.
3. SLA templates with the same SLA type, application, and importance cannot be created repeatedly.

----End

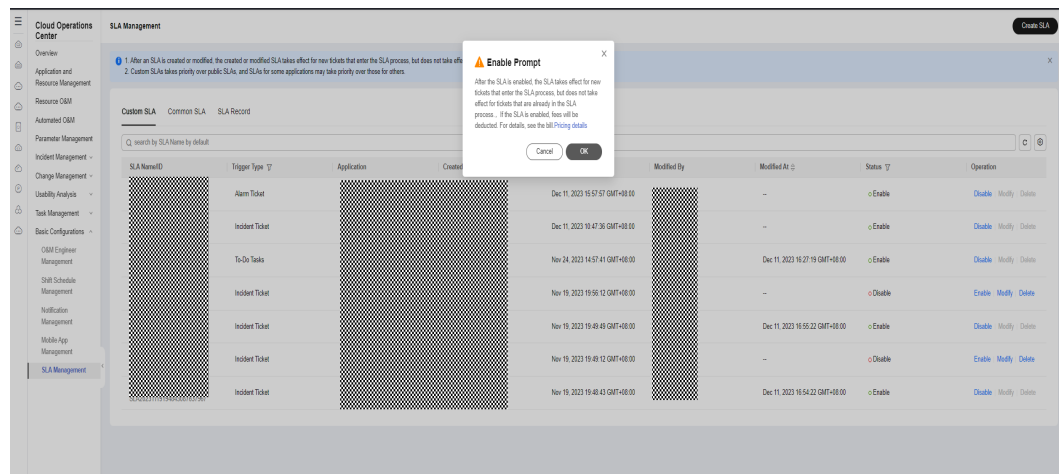
Enabling or Disabling a Custom SLA

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > SLA Management**. On the displayed page, click the **Custom SLA** tab.

Step 3 Locate the target SLA record in the list and click **Enable** or **Disable** in the **Operation** column. In the confirmation dialog box that is displayed, click **OK**.

Figure 11-50 Enabling or disabling an SLA



NOTE

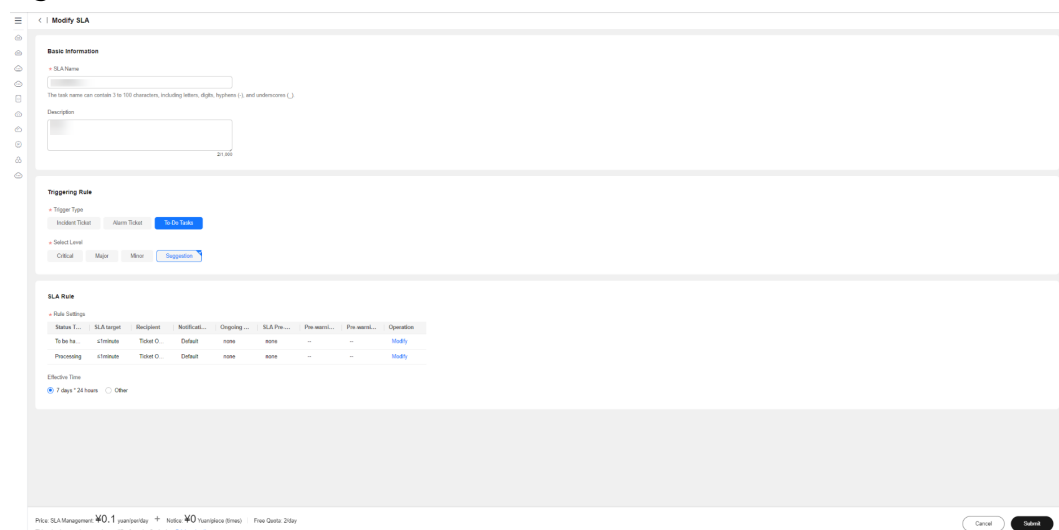
- After an SLA is created, it is disabled by default. You need to enable it manually
- When multiple SLA rules match a new service ticket, the priority of the custom SLA is higher than that of the common SLA, and the priority of some applications is higher than that of all applications.
- By default, common SLA is disabled. After you click **Enable**, SLA management is enabled for the ticket.

----End

Modifying SLA

- Step 1** Log in to **COC**.
- Step 2** In the navigation pane on the left, choose **Basic Configurations > SLA Management**.
- Step 3** Locate a target SLA record, click **Modify** in the **Operation** column to modify the SLA information.

Figure 11-51 SLA details



Step 4 After modifying the basic information, click **Submit**.

NOTE

- Only custom SLAs in the **Disabled** state can be modified.
- After an SLA is modified, enable it. The new SLA will take effect for the tickets that just enter the SLA process. For those that have been in the SLA process, the new SLA does not take effect.

----End

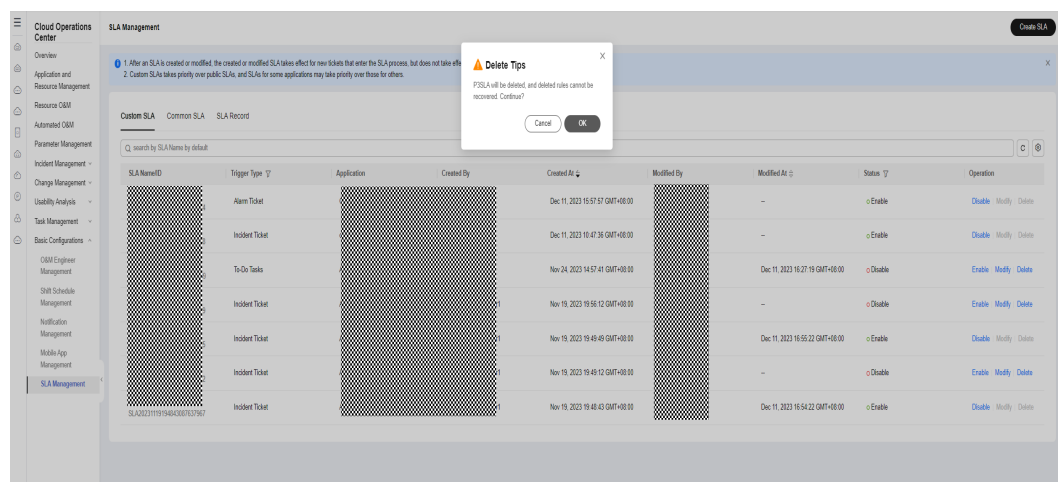
Deleting SLA

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > SLA Management**.

Step 3 Locate the target SLA and click **Delete** in the **Operation** column. In the confirmation dialog box that is displayed, click **OK**.

Figure 11-52 Deleting SLA



NOTE

Only custom SLA templates in the **Disabled** state can be deleted.

----End

11.5.2 Common SLA

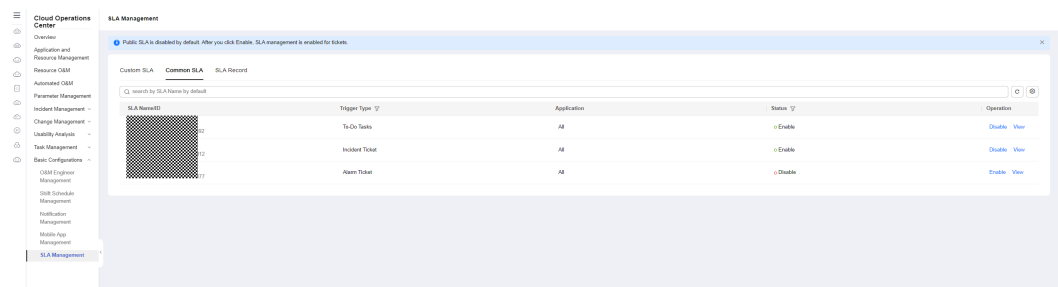
Querying Common SLA

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > SLA Management**.

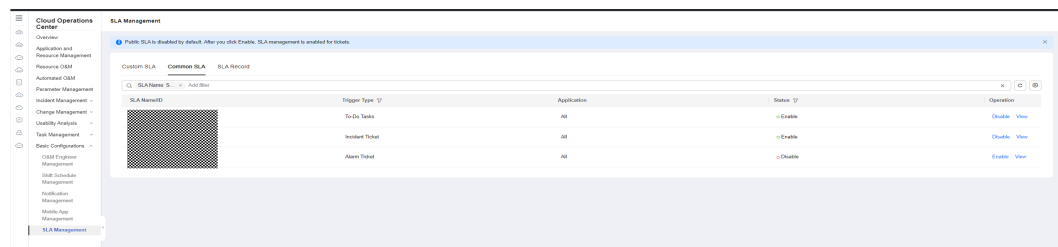
Step 3 Click the **Common SLA** tab.

Figure 11-53 Viewing the SLA list



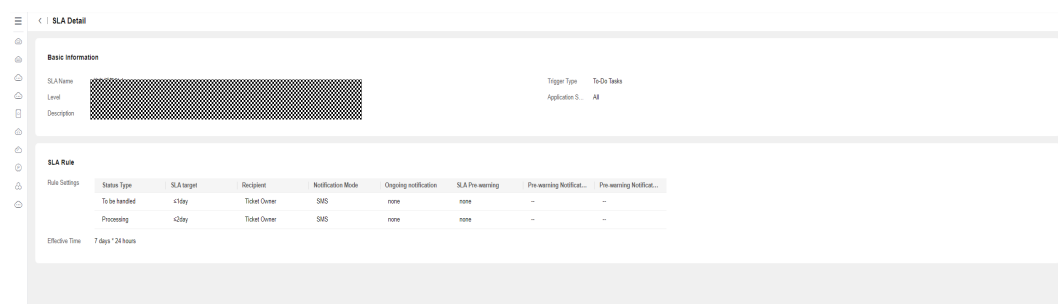
Step 4 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 11-54 Searching for a common SLA templates



Step 5 Click an SLA name in the list to go to the SLA details page.

Figure 11-55 Viewing common SLA details



NOTE

All users can view the preset common SLA.

----End

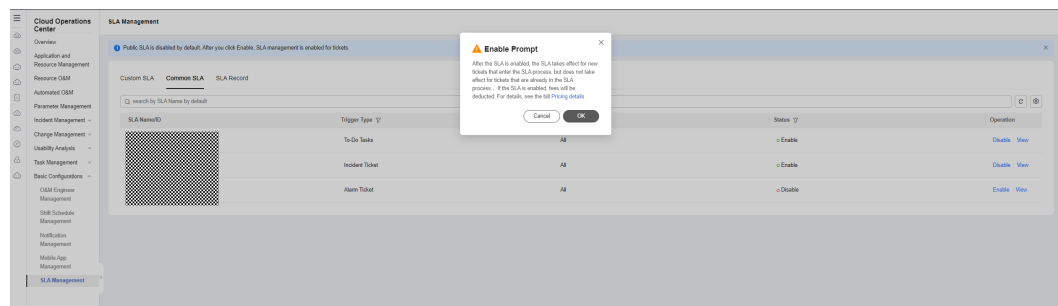
Enabling or Disabling Common SLAs

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > SLA Management**. Click the **Common SLA** tab.

Step 3 Locate the target SLA record in the list and click **Enable** or **Disable** in the **Operation** column. In the confirmation dialog box that is displayed, click **OK**.

Figure 11-56 Enabling or Disabling a common SLA



Step 4 Click **Pricing details** in the dialog box that is displayed to view the COC billing description document.

----End

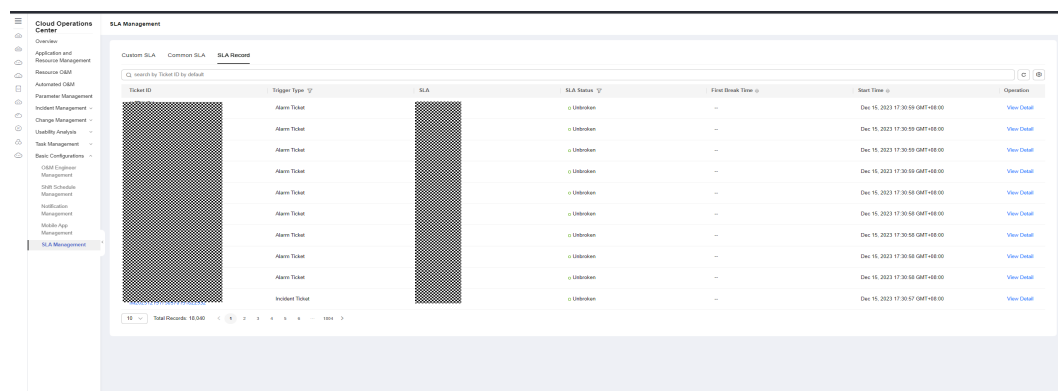
11.5.3 Managing SLA Records

Viewing SLA Records

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Basic Configurations > SLA Management**. Click the **SLA Record** tab.

Figure 11-57 Querying SLA records



Step 3 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Step 4 Click the value in the **SLA** column to view the corresponding SLA template.

Step 5 Click the value in the **Ticket ID** column or **View Detail** in the **Operation** column to view the SLA record details.

Step 6 Click **x** in the upper right corner of the dialog box to exit.

Figure 11-58 Querying SLA record details

| Status Type | Duration | SLA target | SLA Status | SLA Break Time | Owner | Recipient | Notification Mode | Notification Time | Ongoing notification | SLA Pre warning | Pre warning Notification | Post warning Notification |
|-------------|----------|------------|------------|----------------------------------|---------|--------------|-------------------|----------------------------------|----------------------|-----------------|--------------------------|---------------------------|
| Alerting | 30m SLA | 3Minute | Has Broken | Dec 15, 2023 17:31:53 GMT +08:00 | By_test | Ticket Or... | Default | Dec 15, 2023 17:31:53 GMT +08:00 | none | none | -- | -- |

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

12 Viewing Logs

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 WarRoom | WarRoom | createWarRoom |
| Creating a WarRoom initiation rule | MeetingRule | createMeetingRule |
| Deleting a WarRoom initiation rule | MeetingRule | deleteMeetingRule |
| Modifying a WarRoom initiation rule | MeetingRule | updateMeetingRule |
| Modifying WarRoom information | WarRoom | modifyWarRoomInfo |
| Sending notifications using WarRoom | NotificationBriefing | sendNotificationBriefing |
| Adding WarRoom members | WarRoom | addWarRoomMember |
| Removing a WarRoom member | WarRoom | deleteWarRoomMember |
| Creating the WarRoom affected applications | ImpactApplication | createImpactApplication |
| Modifying the WarRoom affected applications | ImpactApplication | updateImpactApplication |
| Deleting the WarRoom affected applications | ImpactApplication | deleteImpactApplication |
| Executing actions | Ticket | actionTicket |

| Action | Resource | Trace |
|--|-------------------|-----------------------------|
| 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 a transferring rule | TransferRule | createTransferRules |
| Modifying a transferring rule | TransferRule | updateTransferRules |
| Deleting a transferring rule | TransferRule | deleteTransferRules |
| Disabling a transferring rule | TransferRule | disableTransferRules |
| Enabling a transferring 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 |
| Updating a scheduling scenario | ScheduleScene | updateSceneOncall |

| Action | Resource | Trace |
|---|--------------|-------------------------|
| Creating a shift role | ScheduleRole | createRoleOncall |
| Updating a shift role | ScheduleRole | updateRoleOncall |
| Deleting a shift role | ScheduleRole | deleteRoleOncall |
| Deleting a fixed scheduled user | ScheduleUser | deleteGlobalFixed |
| Adding a user to the global fixed shift | ScheduleUser | createGlobalFixed |
| Updating fixed scheduled users | 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 |
| Executing a public job | Job | ExecutePublicRunbook |

| Action | Resource | Trace |
|----------------------------------|----------|------------------|
| Operating the job service ticket | Job | OperateJobTicket |