Cloud Operations Center

User Guide

Issue	01
Date	2023-11-30

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 Enabling COC and Granting Permissions

1.1 Enabling COC

Upon the first login, you need to obtain the agency permissions to access other cloud services to use COC to perform automated O&M and fault management on cloud service resources. To use COC, create agencies named **ServiceLinkedAgencyForCOC** and **ServiceAgencyForCOC**. For details about permissions contained in the agency, see **Table 1** and **Table 2**.

Figure 1-1 Enabling COC

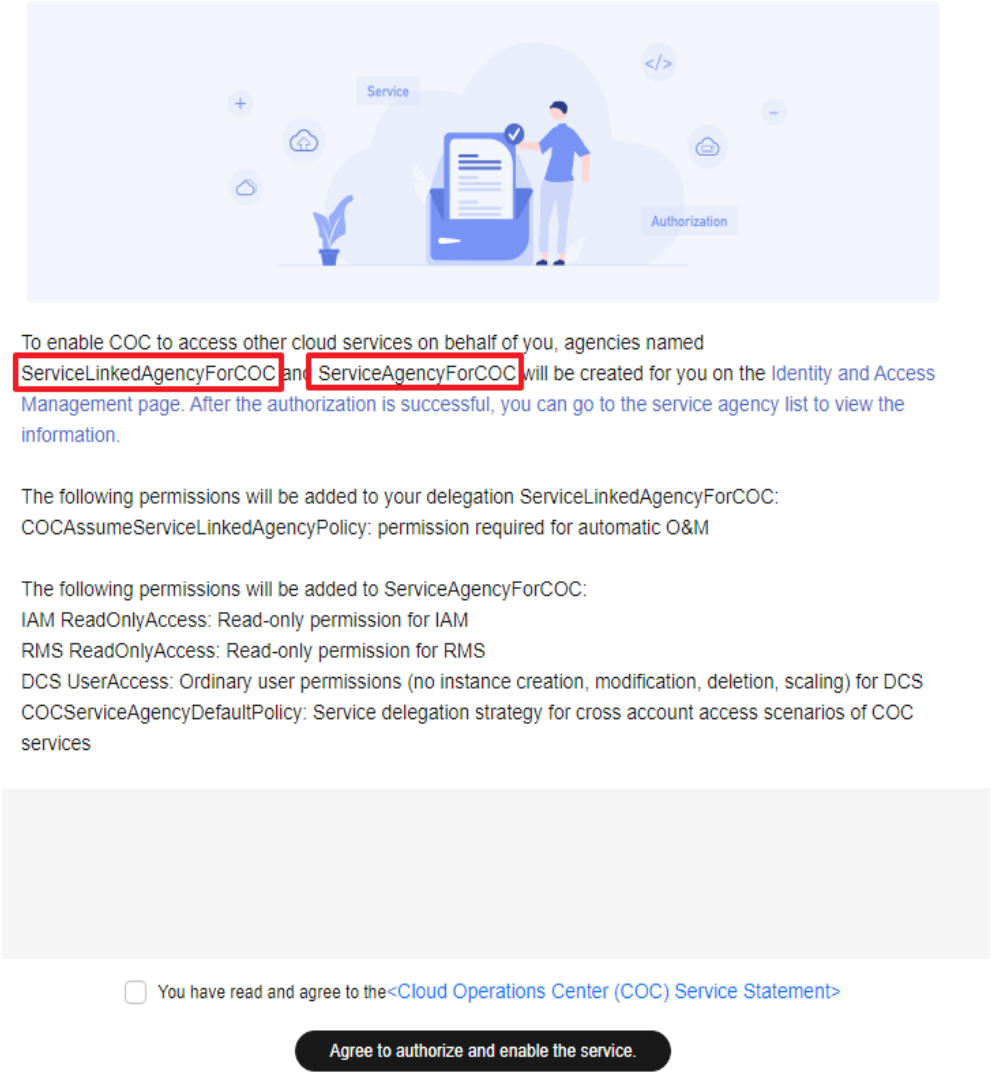


Table 1-1 Permissions in ServiceAgencyForCOC

Permission	Description	Project [Region]	Application Scenario
IAM ReadOnlyAccess	Read-only permissions for IAM	Global service [Global]	Used to read personnel information under an IAM account in the personnel management module.

Permission	Description	Project [Region]	Application Scenario
RMS ReadOnlyAccess	Read-only permissions for RMS	Global service [Global]	Used to synchronize managed cloud service resources in the resource management module.
DCS UserAccess	Common user permissions for DCS, excluding permissions for creating, modifying, deleting DCS instances and modifying instance specifications.	Permissions on all resources (including new projects in the future)	Used to inject faults into DCS resources during chaos drills.
COCServiceAgencyDefaultPolicy	Service agency policy for cross-account access to COC	Permissions on all resources (including new projects in the future)	Used to perform batch resource operations, such as batch restarting ECS and RDS service instances and changing OSs.

Table 1-2 Permissions in ServiceLinkedAgencyForCOC

Permission	Action	Application Scenario
Delivering an agent job	aom:uniagentJob:create	Used to execute scripts, jobs, and scheduled tasks during automated O&M.
Querying logs of an agent job	aom:uniagentJob:get	Used to view the logs of scripts, jobs, and scheduled tasks during automated O&M.
Querying the user list	IdentityCenter:user:list	Used to synchronize personnel information during personnel management.
Creating a topic	smn:topic:create	Used to add notification subscription information during personnel management.
Querying the list of topics	smn:topic:listTopic	Used to send notifications in scenarios such as fault management and automated O&M.
Updating a topic	smn:topic:updateTopic	Used to modify notification subscription information during personnel management.

Permission	Action	Application Scenario
Querying details of a topic	smn:topic:get	Used to send notifications in scenarios such as fault management and automated O&M.
Deleting a topic	smn:topic:delete	Used to delete notification subscription information during personnel management.
Querying a topic policy	smn:topic:listAttributes	Used to send notifications in scenarios such as fault management and automated O&M.
Deleting a topic policy	smn:topic:deleteAttribute	Used to delete notification subscription information during personnel management.
Updating a topic policy	smn:topic:updateAttribute	Used to modify notification subscription information during personnel management.
Creating a subscription for a topic	smn:topic:subscribe	Used to add notification subscription information during personnel management.
Querying the subscription list of a specified topic	smn:topic:listSubscriptionsByTopic	Used to send notifications in scenarios such as fault management and automated O&M.
Querying the subscription list of all topics	smn:topic:listSubscriptions	Used to send notifications in scenarios such as fault management and automated O&M.
Deleting the subscription information from a specified topic	smn:topic:deleteSubscription	Used to delete notification subscription information during personnel management.
Sending a message	smn:topic:publish	Used to send notifications in scenarios such as fault management and automated O&M.
Listing IAM users	iam:users:listUsersV5	Used to synchronize personnel information during personnel management.
Obtaining Information about an IAM user	iam:users:getUserV5	Used to synchronize personnel information during personnel management.
Deleting a service-linked agency	iam:agencies:deleteServiceLinkedAgencyV5	Used to delete an agency associated with a service from IAM.

Permission	Action	Application Scenario
Viewing all the resource lists of a user	rms:resources:list	Used to synchronize the resource lists of a managed account in the resource management module.
Querying parameter details	coc:parameter:*	Used by the automated O&M function to reference parameters in the parameter center.
Obtaining the server password pair	ecs:serverKeypairs:get	Used to reinstall or change an OS, and set the password pair.
Obtaining the server password pair list	ecs:serverKeypairs:list	Used to reinstall or change an OS, and query the password pair list.
Stopping ECSs in batches	ecs:cloudServers:stop	Used to stop ECSs in batches during resource O&M.
Restarting ECSs in a batch	ecs:cloudServers:reboot	Used to restart ECSs in batches during resource O&M.
Starting ECSs in batches	ecs:cloudServers:start	Used to start ECSs in batches during resource O&M.
Changing the OS of an ECS	ecs:cloudServers:changeOS	Used to change the ECS OSs in batches during resource O&M.
Reinstalling ECS OSs	ecs:cloudServers:rebuild	Used to reinstall ECS OSs in batches during resource O&M.
Obtaining ECS information	ecs:servers:get	Used to obtain cloud service information during batch operations in resource O&M.
Listing accounts in an organization	organizations:accounts:list	Used to query accounts in the current organization in the cross-account scenario.
Listing delegated administrator accounts	organizations:delegatedAdministrators:list	Used to query delegated administrator accounts in the current organization in the cross-account scenario.
Getting organization information	organizations:organizations:get	Used to query information about the current organization in the cross-account scenario.
Listing organization units	organizations:ous:list	Used to query organization units in the cross-account scenario.
Listing trusted services	organizations:trustedServices:list	Used to query the list of trusted services enabled for the current organization in the cross-account scenario.

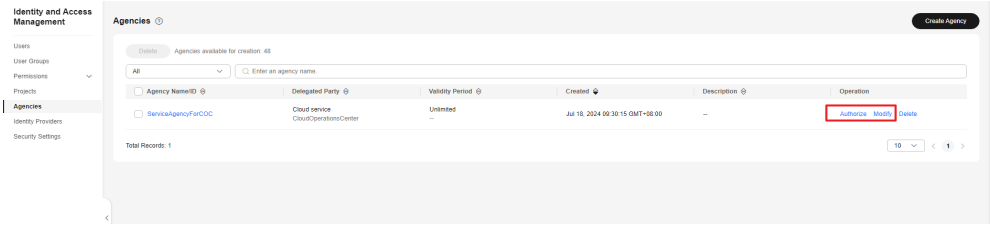
Permission	Action	Application Scenario
Listing roots of an organization	organizations:roots:list	Used to query organization roots in the cross-account scenario.

Modifying or deleting agency permissions

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

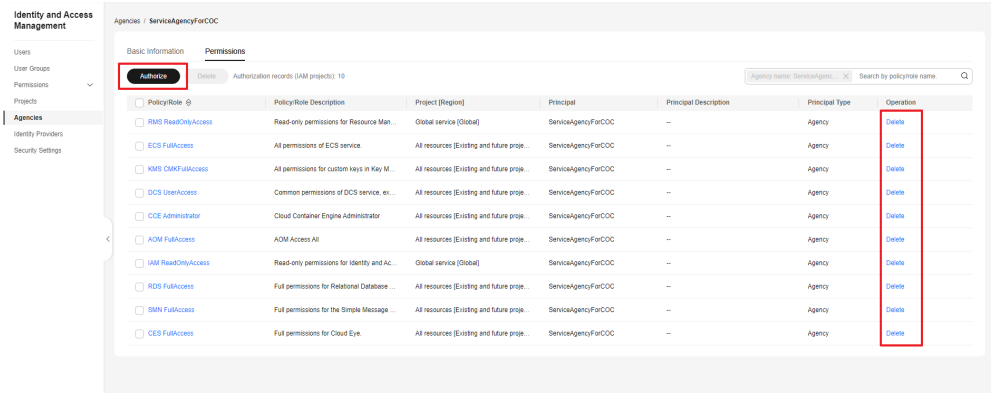
To modify the permissions, validity period, and description of an agency, click **Modify** in the row containing the agency you want to modify.

Figure 1-2 Agencies



On the authorization record page, you can authorize the agency or delete the authorized permissions.

Figure 1-3 Permission granting records



NOTE

- You can change the cloud service, validity period, description, and permissions of cloud service agencies, except the agency name and type.
- Modifying the permissions of cloud service agencies may affect the usage of certain functions of cloud services. Exercise caution when performing this operation.
- For more information about agencies, visit **IAM**.

1.2 Tutorials for RBAC

This section describes how to use **Identity and Access Management (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, see **Permissions Management**. 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 a user** and add it to a user group.

   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**.

   You can create custom policies in either of the following ways:
   - Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
   - JSON: Create a JSON policy or edit an existing one.

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

Example Custom Policies

- 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"
      ]
    }
  ]
}
```

1.3 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.

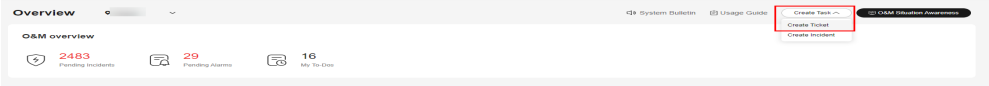
Figure 2-1 Statistical quantity

Step 3 Expand the **Create Task** drop down list, and click **Create Ticket** to **create a ticket**.

Figure 2-2 Creating a to-do task

Step 4 Click **Create Incident** to **create an 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.

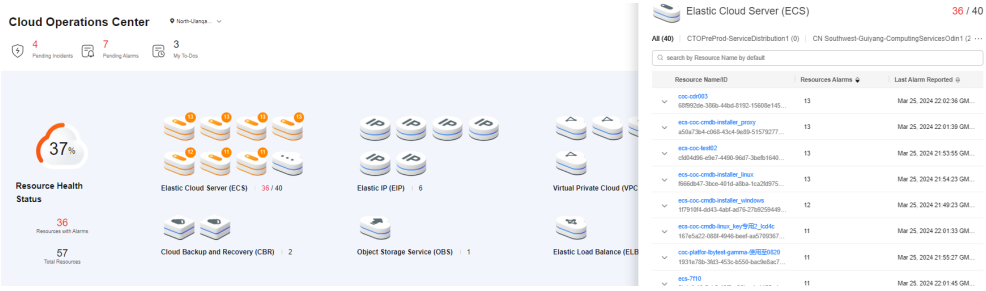
Figure 2-4 Resource information

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.

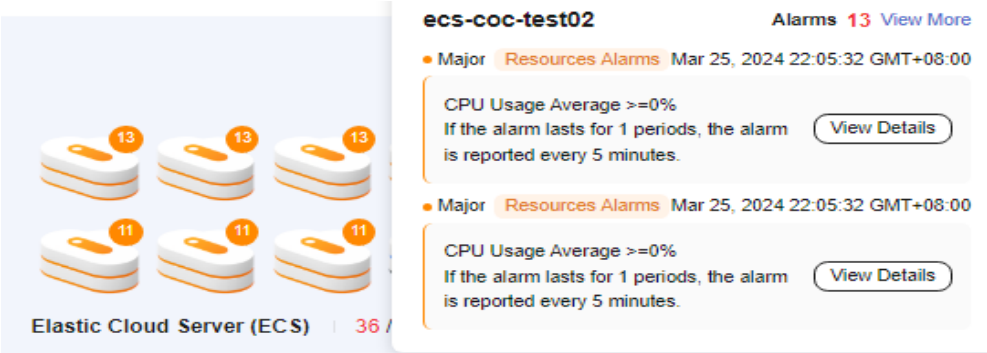
Step 5 In the global view, click  to query all resource information of the corresponding resource type in different regions.

Figure 2-5 Resources in different regions



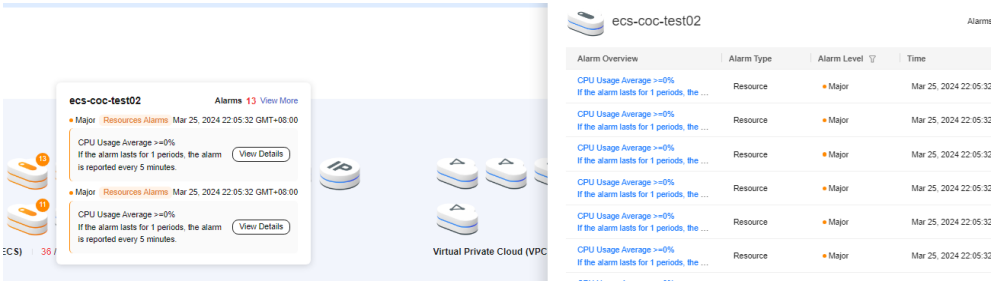
Step 6 Move your cursor to resources that are marked by alarms to view alarm details of the resources.

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 of this area to refresh resource and alarm information.

----End

2.3 Resource Monitoring

You can view resources monitored by CES.

Scenarios

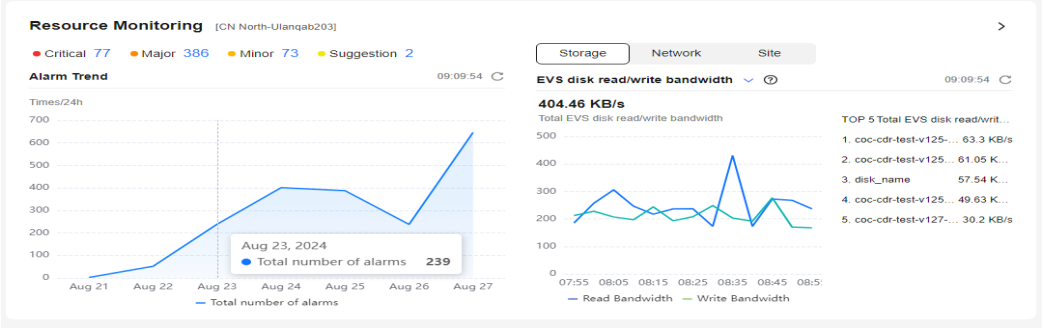
View resources monitored by CES on COC.

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 the **Storage**, **Network**, and **Site** tabs to view different monitoring information.

Step 4 Click the arrow in the upper right corner of the area to access the Cloud Eye page and view the original monitoring information.

----End

2.4 Application Monitoring

You can view custom application monitoring information.

Scenarios

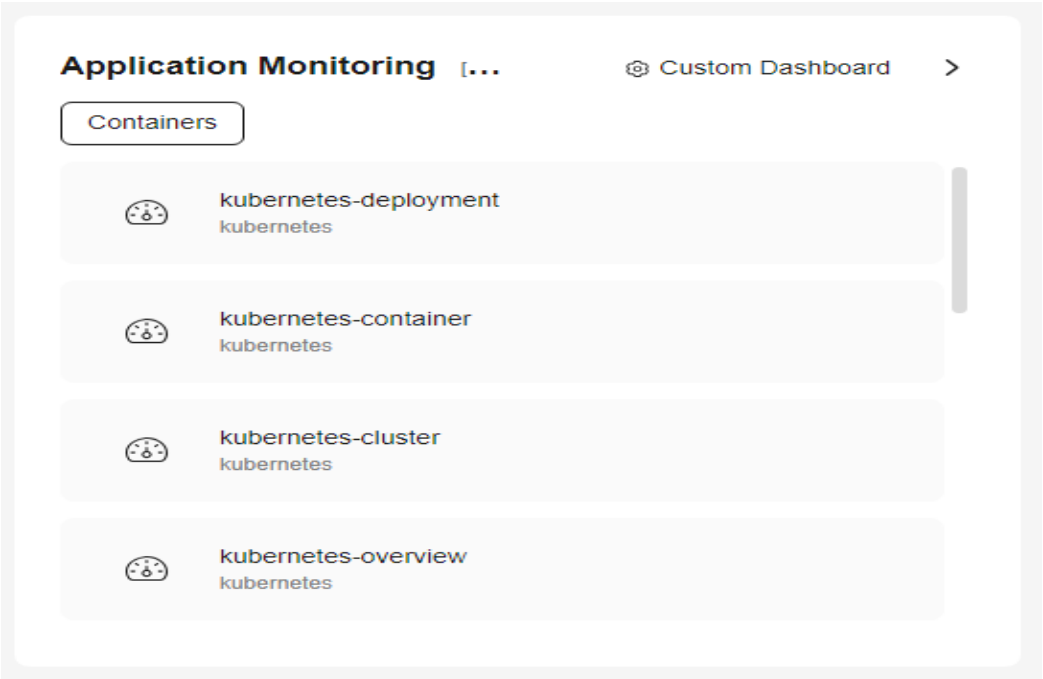
View the information on the dashboard of Application Operations Management (AOM) on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 On the **Overview** page of COC, you can view monitoring information about applications.

Figure 2-9 Application monitoring information



----End

2.5 Security Overview

You can view the security monitoring information from SecMaster.

Scenarios

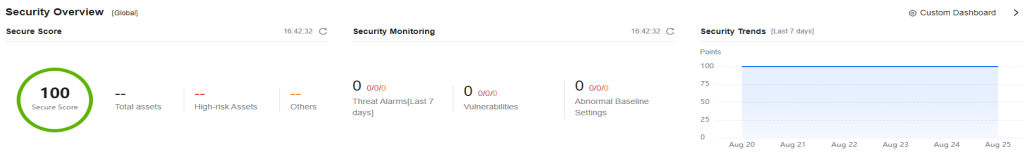
View the security monitoring information provided by SecMaster on COC.

Procedure

Step 1 Log in to **COC**.

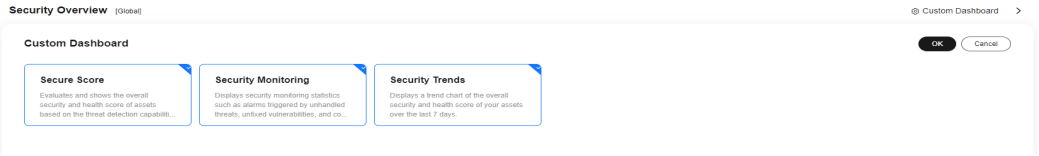
Step 2 On the **Overview** page of COC, you can view the security monitoring information provided by SecMaster.

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

2.6 O&M Situational Awareness

COC provides O&M situational awareness capabilities through monitoring of changes, incidents, alarms, service level objectives (SLOs), production readiness reviews (PRRs), and more. In this module, you can view the overall O&M situation from macro to micro on an enterprise-level O&M sandbox.

- The dedicated O&M BI dashboard caters to various O&M roles, aiding in O&M optimization, insights, and decision-making.
- 30+ O&M metrics are preset, presenting O&M situations of your cloud resources or applications on 7 perspective-based dashboards and a comprehensive enterprise-level O&M sandbox.

Scenarios

View O&M statuses of your applications on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 On the Overview page of COC, click **O&M Situation Awareness**.

Step 3 On the **O&M Situational Awareness** sandbox, filter the O&M data by region, application, or a specified duration as required.

----End

O&M Overview

The O&M overview page consists of four modules: overview, risk reporting, PRR summary, and top 5 incidents. The overview module enables you to observe the O&M situation from the global perspective, facilitating O&M optimization, insights, and decision-making. The risk reporting module displays the O&M statuses and risks reported through P3 or more severe incident tickets, WarRoom requests, faults triggered by changes, and critical alarms. The PRR summary module provides the review statuses of your applications before they are released or put into commercial use. The top 5 incidents module displays the top 5 incidents that have the most severe impacts on your services to help you quickly identify major fault scenarios. For details about the metrics included, see **Table 2-1**.

Figure 2-12 O&M overview

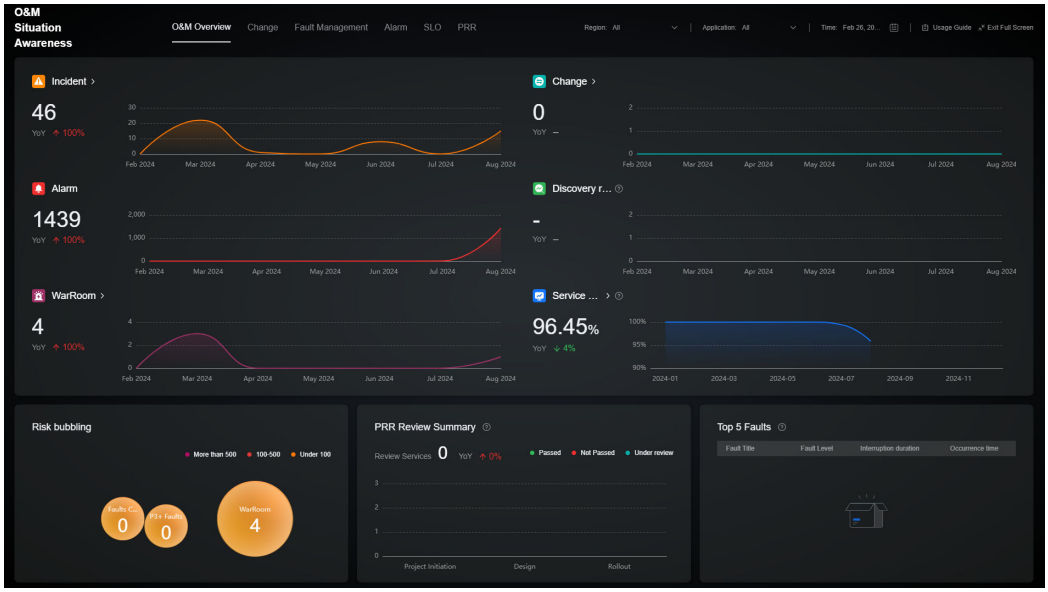


Table 2-1 Metrics in the O&M overview

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Overview	Incidents	Incident center	Collects the trend of the incident ticket quantity.	Collect the number of incident tickets created in a selected period.	Day or month	Count
	Alarms	Alarm center	Collects the alarm quantity trend.	Collect the number of alarms generated in a selected period.	Day or month	Count
	WarRoom Requests	WarRoom	Collects the WarRoom request quantity trend.	Collect the number of WarRoom requests initiated in a selected period.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Monitoring Discovery Rate	Alarm center	Collects the proportion of incidents that trigger specified alarms.	Monitoring discovery rate = Number of incidents that meet the filter criteria and trigger specified alarms/Total number of incidents that meet the filter criteria	Day or month	%
	Changes	Change management	Collects the change ticket quantity trend.	Collect the number of change tickets created in a selected period.	Day or month	Count
	Cloud Service SLO	SLO management	Collects the change trend of the actual SLO value of a cloud service.	Cloud service SLO = 1 – (Unavailability duration of the cloud service/Total duration of the cloud service) x 100%	Day or month	%
Risk reporting	Change-triggered Incidents	Incident management	Collects the number of incidents caused by changes.	Collect the number of incident tickets whose incident type is change.	Day or month	Count
	Critical Alarms in Last 7 Days	Alarm center	Collects the number of critical alarms in the last 7 days.	Collect the number of critical alarms in the last 7 days.	Last 7 days	Count
	P3 or More Severe Incidents	Incident management	Calculates the number of P3 or more severe incidents.	Collect the total number of P1, P2, and P3 incidents, including unhandled incidents.	Day or month	Count
	WarRoom Requests	Alarm center	Collects the number of WarRoom requests.	Collect the number of WarRoom requests initiated in a selected period.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
PRR summary	PRR	PRR	Collects the number of services that are covered by a PRR.	Collect the number of services that are covered by a PRR.	Day or month	Count
	PRR Passing	PRR	Collects the number of services passed or failed a PRR in each PRR phase.	Collect the number of services passed or failed a PRR in each PRR phase.	Day or month	Count
Top 5 incidents	Top 5 Incidents	Incident management	Collects the top 5 most severe incidents.	Collect the number of handled P3 or more severe incidents in a specified period, rank the incidents by severity first and then by interruption duration to obtain the top 5 most severe incidents.	Day or month	Incident information

Changes

The **Changes** page consists of three modules: data overview, change overhead, and change risks, comprehensively displaying change statuses of your applications or cloud services using core change metrics. The data overview module encompasses various metrics, inducing change duration, success rate, and automated change rate. COC uses these metrics to present the overall change statistics of your services on change trend charts that are bolstered by required change data. The change risk module displays the faults caused by changes and provides the change success rate, as well as the change level and change method distribution charts. The change overhead module shows the trends of the labor required and time consumed by your services in a specified period so that you can control your change overhead as required. For details about the metrics included, see **Table 2-2**.

Figure 2-13 Changes

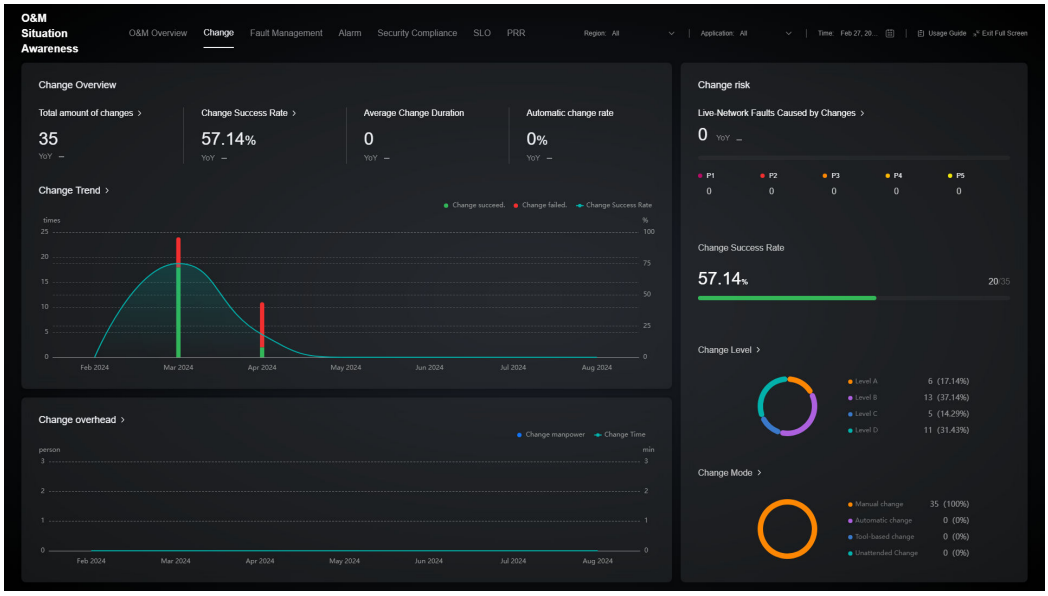


Table 2-2 Metrics on the Changes page

Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Change-caused Incidents on the Live Network	Change management	Collects the number of change-caused incidents of each level on the live network.	Collect the number of incident tickets created for each level of incidents that are caused by changes within a selected time range.	Day or month	Count
Change Level	Change management	Collects the number of change tickets for each level of changes.	Collect the number of change tickets for each level of changes in a selected period.	Day or month	Count
Change Method	Change management	Collects the number of change tickets that employ different change methods, such as automated and manual changes, respectively.	Collect the number of change tickets for each change method.	Day or month	Count

Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Total Changes	Change management	Collects the number of change tickets.	Collect the number of change tickets completed in a selected period.	Day or month	Count
Change Success Rate	Change management	Collects the success rate of change tickets.	Change success rate = Number change tickets that are handled/Total number of change tickets that are handled and failed x 100%	Day or month	%
Average Change Duration	Change management	Collects the average duration for handling change tickets.	Average change duration = Total duration required by handled change tickets in a selected period/Number of handled change tickets x 100%	Day or month	ddhhmm
Automatic Change Rate	Change management	Collects the proportion of automatic changes in all change tickets.	Automatic change rate = Number of automatic changes/Total number of change tickets x 100%	Day or month	%
Change Trend	Change management	Collects the number of successful and failed changes and change success rate trend.	Collect the number of successful and failed changes and change success rate trend.	Day or month	Count
Change Manpower	Change management	Collects the number of O&M engineers required in changes.	Change labor = Number of change coordinators + Number of change implementers	Day or month	Person-time

Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Change Duration	Change management	Collects the average handling duration of change tickets.	Average change handling duration = Total duration required by handled change tickets in a selected period/Number of handled change tickets x 100%	Day or month	ddhhmm

Fault Management

Incident Management consists of three modules: incident statistics, WarRoom, and backtracking and improvement. These modules leverage core metrics of the entire incident management process to manage and handle incidents efficiently. Backed by metrics such as incident quantity, closure rate, handling duration, and number of damaged applications, the incident statistics module presents incident risks of your cloud services and applications on incident risk trend charts and top/bottom ranking charts with change data marked. The WarRoom module encompasses damaged applications, levels and time windows of incidents that trigger WarRoom request initiation, warning the occurrence of major fault scenarios and representing the fault handling. The backtracking and improvement module includes the fault closure rate and trend analysis of fault backtracking and improvement to ensure that experience in handling known faults is accumulated, reducing the frequency and handling duration of similar faults. For details about the metrics included, see **Table 2-3**.

Figure 2-14 Fault management

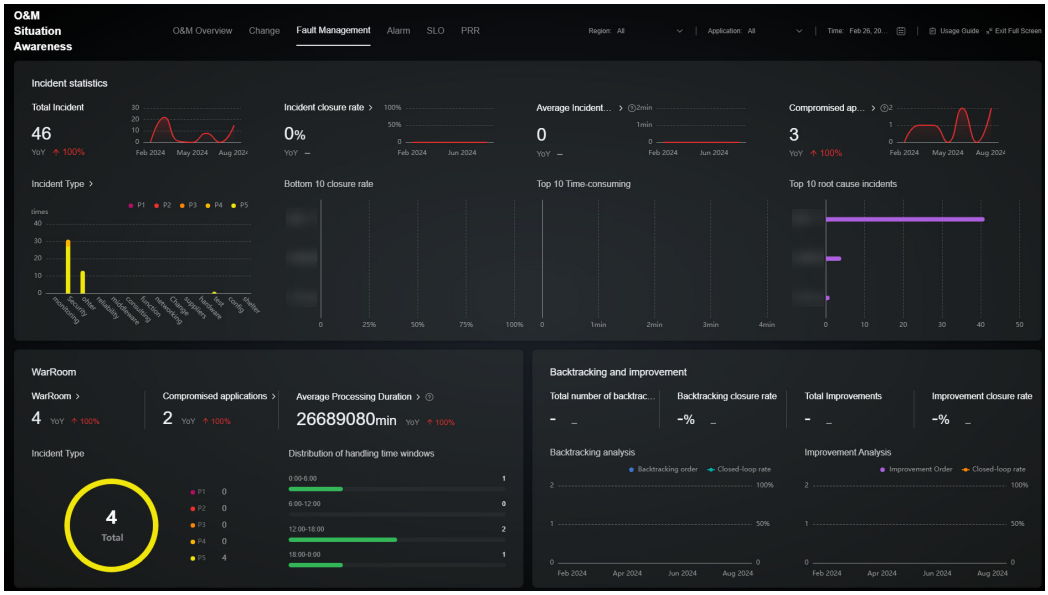


Table 2-3 Incident management data dictionary

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Incident statistics	Total Incidents	Incident management	Collect the total number of incident tickets.	Collect the number of incident tickets created in a selected period.	Day or month	Count
	Incident Level	Incident management	Collects the number of incident tickets of each type and level.	Collects the number of incident tickets of each type and level within a selected time range.	Day or month	Count
	Incident Closure Rate	Incident management	Collects the closure rate incident tickets.	Incident ticket closure rate = Number of closed incident tickets within a selected time range/Total number of incident tickets x 100%	Day or month	%
	Incident Duration	Incident management	Collects the average handling duration of incident tickets.	Incident handling duration = Total handling duration of closed incidents/ Number of closed incidents x 100%	Day or month	ddhhmm
	Affected Applications	Incident management	Collects the number of applications affected by an incident ticket.	Collect the number of affected applications (including deleted applications) of an incident ticket after deduplication.	Day or month	Count
WarRoom	WarRoom Requests	WarRoom	Collects the number of all WarRoom requests.	Collect the number of WarRoom requests initiated in a selected period.	Day or month	Count
	Fault Level	Incident management	Collects the number of incidents of each level for a WarRoom request.	Calculate the number of incidents of each level for a WarRoom request.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Affected Applications	WarRoom	Collects the number of affected applications for a WarRoom request.	Calculate the number of affected applications for a WarRoom request after deduplication.	Day or month	Count
	Average Recovery Duration	WarRoom	Collects the average duration for fault recovery from a WarRoom request.	Average WarRoom recovery duration = Total duration required by handled WarRoom requests within a selected time range/ Number of handled WarRoom requests	Day or month	ddhhmm
	Distribution of Handling Time Windows	WarRoom	Collects the number of times WarRoom requests are initiated in each time window.	Collect the number of times WarRoom request are initiated in each time window.	Day or month	Count
Backtracking and improvement	Backtracking Tickets	Issue Management	Collects the number of backtracking tickets.	Total number of backtracking tickets in a statistical period	Day or month	Count
	Closure Rate of Backtracking Tickets	Issue Management	Collects the closure rate of backtracking tickets.	Closure rate of backtracking tickets = Number of closed backtracking tickets/ Total number of backtracking tickets x 100%	Day or month	%
	Total Improvement Tickets	Issue Management	Collects the number of improvement tickets.	Collect the total number of improvement tickets in a statistical period.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Improvement Ticket Closure Rate	Issue Management	Collects the closure rate of improvement tickets.	Closure rate of improvement tickets = Number of closed improvement tickets/ Total number of improvement tickets x 100%	Day or month	%

Monitoring and Alerting

The alerting and monitoring package displays alarm information in charts, helping O&M engineers quickly learn about the overall service status. The altering and monitoring package consists of three modules: alarm analysis, alarm costs, and alarm quality, reflecting core metrics of alarm management. Alarm analysis provides the metrics for calculating the total number of alarms, alarm severity, top 10 applications, alarm reduction, and alarm trend. By analyzing historical alarm data, the O&M supervisor can understand the trend and mode of service alarms and detect potential performance problems or potential faults. The alarm cost statistics include the alarm manpower and automatic handling rate. The O&M supervisor can effectively control the labor cost of changes based on the alarm cost. The alarm quality statistics function collects statistics on incident ticket- and war room-triggered alarm detection rates, helping O&M supervisors evaluate the validity of current alarms and optimize alarm configurations in a timely manner. For details about the metrics included, see **Table 2-4**.

Figure 2-15 Monitoring and alerting

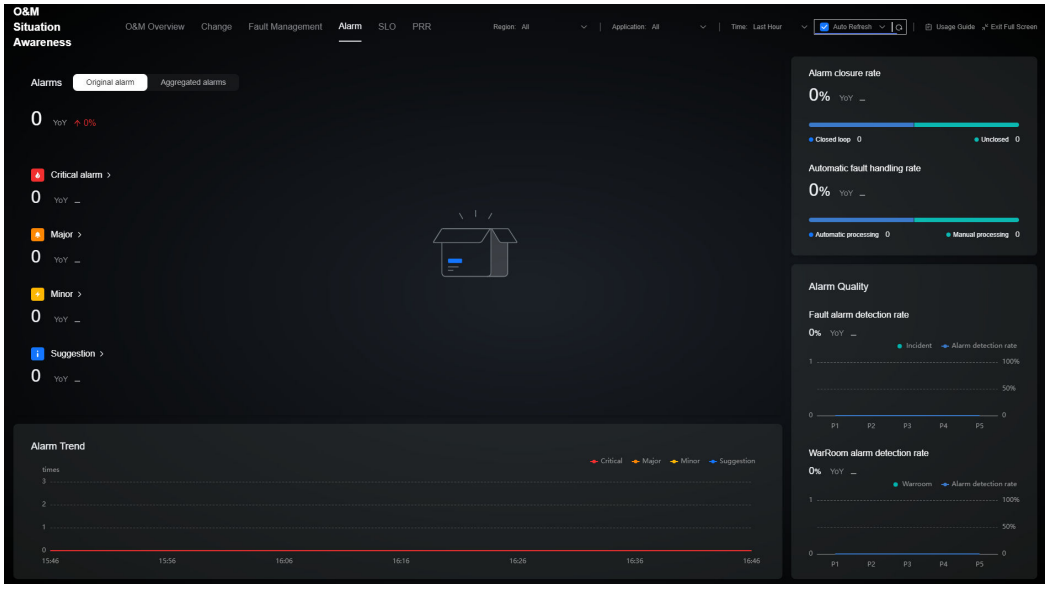


Table 2-4 Monitoring alarm data dictionary

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Alarm analysis	Alarms	Alarms	Collects the total number of alarms.	Collects the number of alarms generated in a selected period.	Day/Month	Count
	Alarm Severity	Alarms	Collects the number of alarms of each severity.	Number of alarms of each severity within the selected time range	Day/Month	Count
	Alarm Trend	Alarms	Collects the trend of the number of alarms of each severity within the selected time range.	Number of alarms of each severity within the selected time range	Day/Month	Count
Alerting Cost	Persons Involved	Alarms	Collects the number of alarm handling participants.	Number of owners (deduplicated) for integrated alarms	Day/Month	Person
	Alarms Handled Per Capita	Alarms	Collects the number of alarms handled by per person.	Total number of alarms in the selected time range/Number of alarm handling participants in the selected time range	Day/Month	Person
	Automatic Alarm Handling Rate	Alarms	Collects statistics on automatic alarm handling.	Number of automatically handled alarms in the selected time range/Total number of alarms x 100%	Day/Month	%
Alarm Quality	Fault alarm detection rate	Incident Management	Collects statistics on the number of incident tickets triggered by alarms.	Number of incident tickets converted from alarms in the selected time range/Total number of incident tickets in the selected time range x 100%	Day/Month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	War Room Alarm Detection Rate	WarRoom	Collects the number of war rooms triggered by alarms.	Number of war rooms triggered by incidents converted from alarms in the selected time range/War rooms Total quantity x 100%	Day/Month	%
Alarms Reported	Alarms Reported	Alarms	Displays alarm risks reported by application.	Weighted calculation and sorting based on the severity and quantity of alarms reported for an application	Day/Month	N/A

SLO Dashboard

The service level objective (SLO) dashboard covers the overall SLO achievement, application-dimension SLO statistics, and error budget management. In the **Overall SLO Achievement** area, you can view SLO values by year and month and the overall service level trend. In the **SLO Statistics by Application** area, you can view SLO values by time and application and evaluate the service level of each application. The **Error Budgets** module shows the error budget based on the SLO values of each application to provide guidance for changes or other high-risk operations. For details about the metrics included, see **Table 2-5**.

Figure 2-16 SLO dashboard

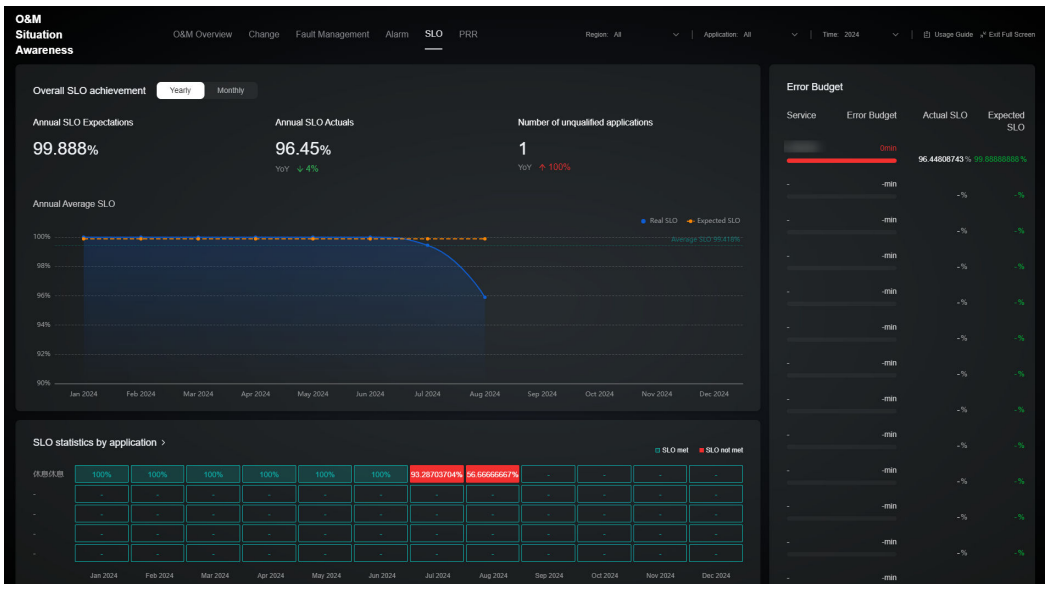


Table 2-5 SLO dashboard data dictionary

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
SLO achievement	Annual Expected SLO Value	SLO management	Expected SLO value of applications in a year	Expected SLO value = Expected SLO value set in the SLO management module Expected SLO value of multiple applications = Average expected SLO value of applications	Year	%
	Annual Actual SLO Value	SLO management	Actual SLO value achieved in a year	Actual SLO value in a year = 1 – (Annual service unavailability duration/Total service duration in a year) x 100% Actual SLO value of multiple applications in a region = Average actual SLO value of these applications in a year Actual SLO value of an application in several regions in a year = Minimum actual SLO value of the application in multiple regions in a year Actual SLO value of multiple applications in multiple regions = Average actual SLO value of these applications in multiple regions in a year	Day or month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Applications That Do Not Meet Exceptions	SLO management	Collects the number of applications that do not meet SLO expectations.	Calculate the number of applications that fail to achieve the SLO expectation. If all regions are selected and the actual SLO value of applications in any region in a year is less than the annual expected SLO value, the SLO exception is not met.	Day or month	Count
	Monthly Expected SLO Value	SLO management	SLO value expected to be achieved by services in a month	Expected SLO value = Expected SLO value set in the SLO management module Expected SLO value of multiple applications = Average expected SLO value of applications	Day or month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Monthly Actual SLO Value	SLO management	Actual monthly SLO value achieved by services	Actual SLO value in a month= 1 – (Monthly service unavailability duration/Total service duration in a month) x 100% Actual monthly SLO value of multiple applications in a region = Average actual SLO value of these applications in a month Actual SLO value of an application in several regions = Minimum actual SLO value of the application in multiple regions in a month Actual SLO value of multiple applications in multiple regions = Average actual SLO value of these applications in multiple regions in a year	Day or month	%

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

PRR Dashboard

The PRR dashboard encompasses the review service summary, evaluation radar distribution, service review, and improvement task closure. The review service summary module shows the review phase of each service before the service is put into production and the review status. The evaluation radar distribution module shows the distribution of review items that do not meet service requirements. The service review and improvement module presents the rectification statuses of the

items that do not meet the review requirements. For details about the metrics included, see **Table 2-6**.

Figure 2-17 PRR dashboard

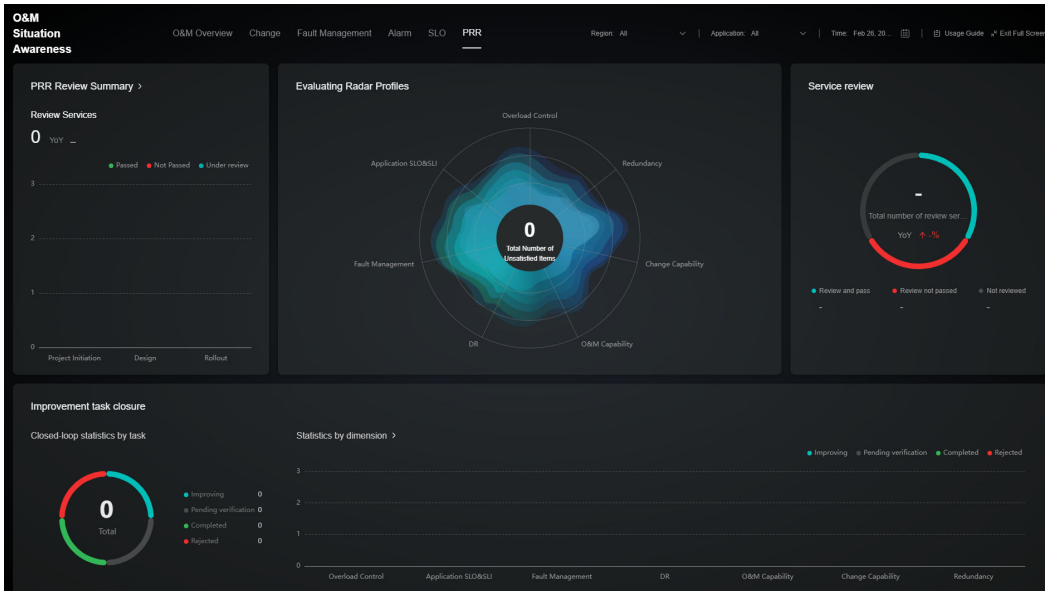


Table 2-6 PRR dashboard data dictionary

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Service PRR Summary	Total Review Services	PRR	Collects the number of services that are included in the PRR.	Collect the total number of services are covered by the PRR within a selected time range.	Day or month	Count
	Service PRR summary	PRR	Collects the number of services that are included in each PRR phase and the approval status.	Collect the number of sources included in each PRR phase and the approval status within a selected time range.	Day or month	Count

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Evaluation radar distribution chart	Evaluation Radar Distribution	PRR	Collects the distribution of PRR items that fail to be met.	Collect the number of review items that are not met in a selected time range.	Day or month	Count
Service review	Services to Be Reviewed	PRR	Collects the total number of services to be reviewed and the approval status.	Collect the total number of services to be reviewed and service approval status within a selected time range.	Day or month	Count
Closure of improvement tasks	Task Closure Statistics	PRR	Collects the number of improvement tasks and their closure statuses.	Collect the number of improvement tasks and the closure statuses of the tasks within a selected time range.	Day or month	Count
	Improvement Tasks	PRR	Collects the number of improvement tasks in each dimension and their closure statuses.	Collect the number of improvement tasks by review item and the closure statuses of these tasks.	Day or month	Count

3 Application and Resource Management

Based on resources and centered on applications, all resource objects and applications are managed in a unified manner. This feature provides multi-view resource management views for different service scenarios, offering accurate, timely, and consistent resource configuration data for upper-layer O&M services.

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.

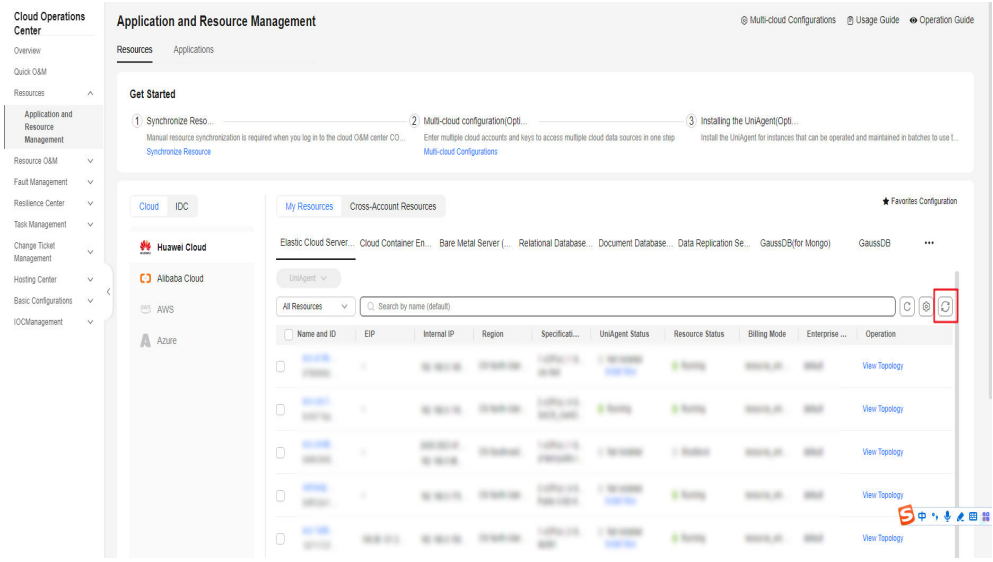
Procedure

Step 1 Log in to **COC**.

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

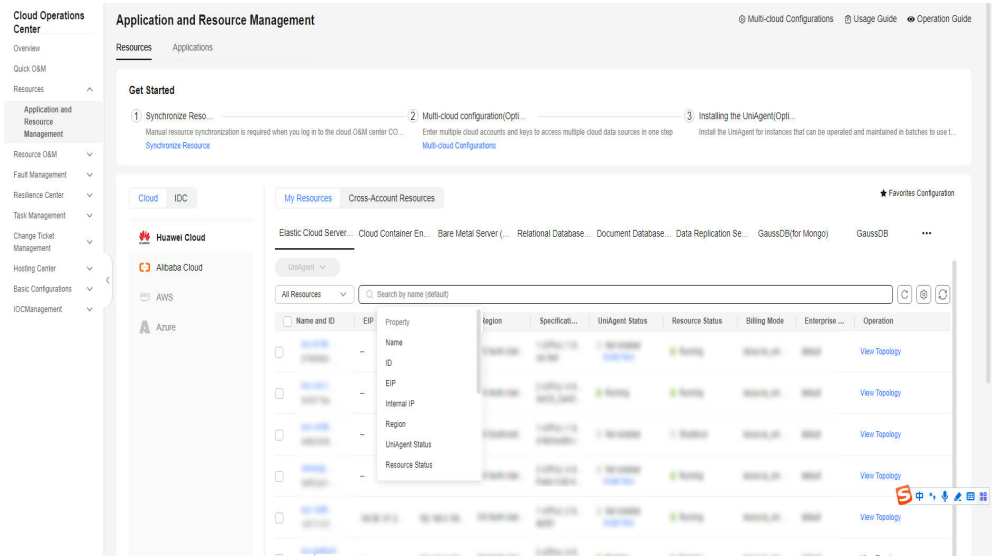
resources you want synchronize **(Elastic Cloud Server (ECS)** is selected by default), and click **Synchronize Resource**.

Figure 3-1 Synchronizing resources



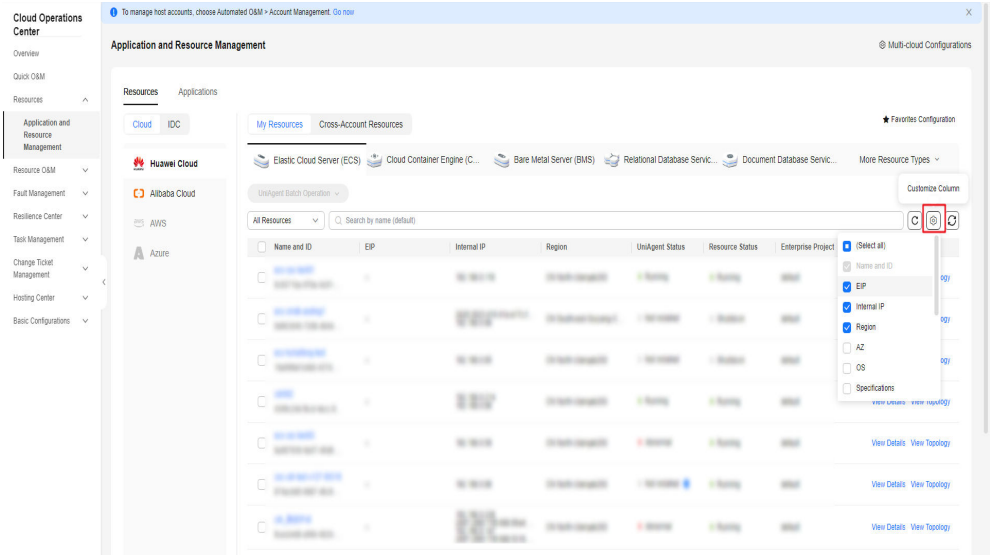
Step 3 In the search box above the resource list, select search criteria to quickly search for resources.

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, reinstall, and upgrade a UniAgent on and uninstall a UniAgent from corresponding nodes.

Scenarios

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

Precautions

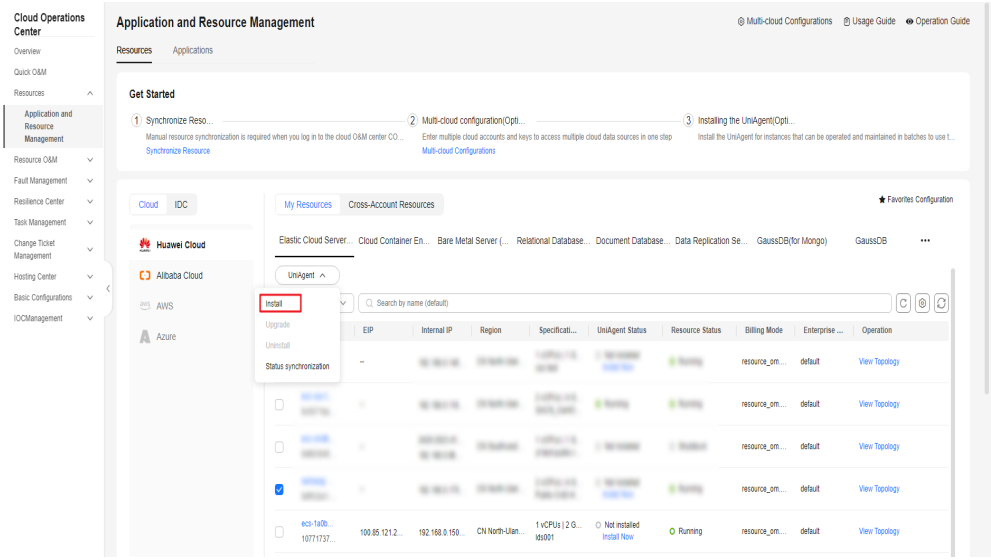
Currently, you can only perform operations on UniAgent for ECSs.

Procedure

Step 1 Log in to **COC**.

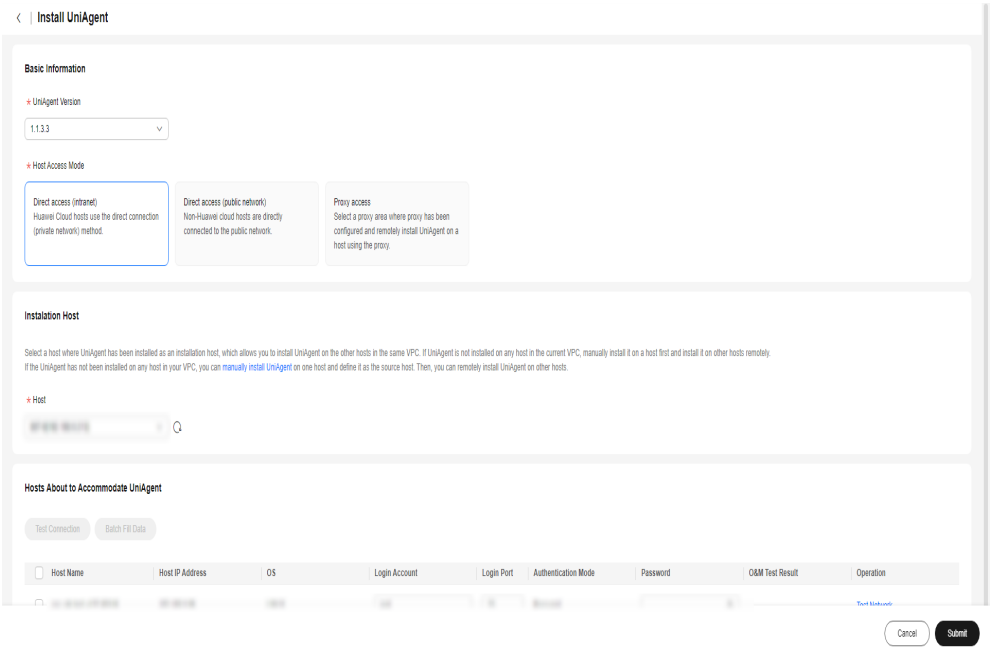
Step 2 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Resources** tab page, above the resource list, select the desired instances and choose **UniAgent > Install**.

Figure 3-4 Installing a UniAgent



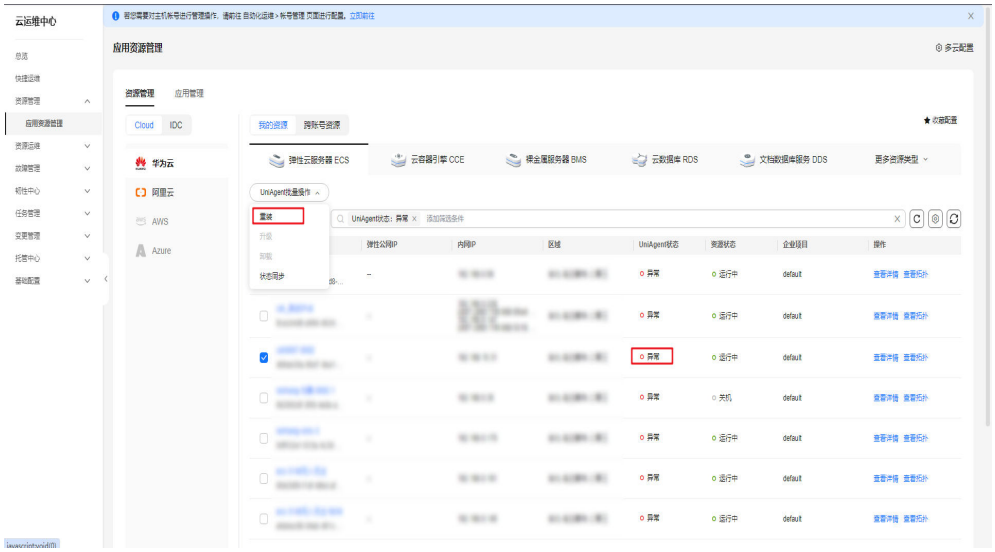
Step 3 On the displayed **Install UniAgent** page, specify required information by referring to **Table 3-1** and click **Submit** to trigger the automated installation process. Wait until the installation is complete.

Figure 3-5 Setting parameters



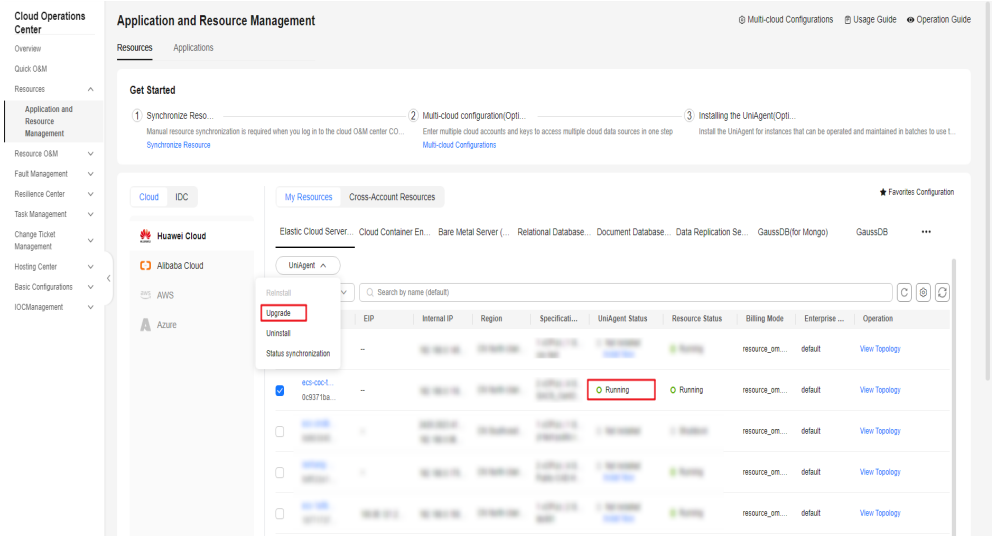
Step 4 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. Click the **Resources** tab, select the instances whose UniAgent status is **Abnormal**, **Not installed**, or **Installation failed**, and choose **UniAgent** > **Reinstall**.

Figure 3-6 Reinstalling a UniAgent



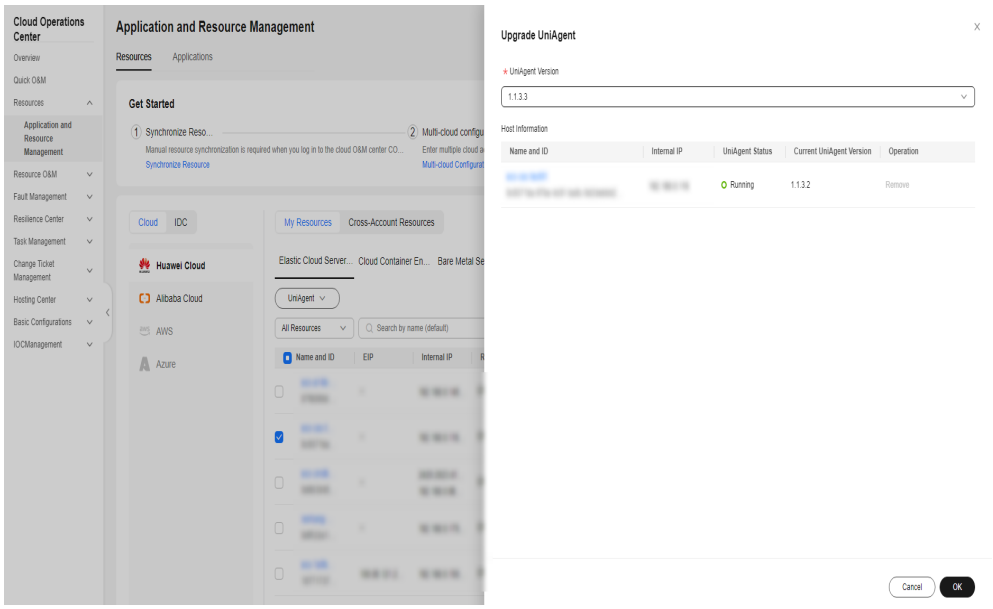
Step 5 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. On the displayed **Resources** tab page, above the resource list, select the instances with UniAgents installed and choose **UniAgent** > **Upgrade**.

Figure 3-7 Upgrading a UniAgent



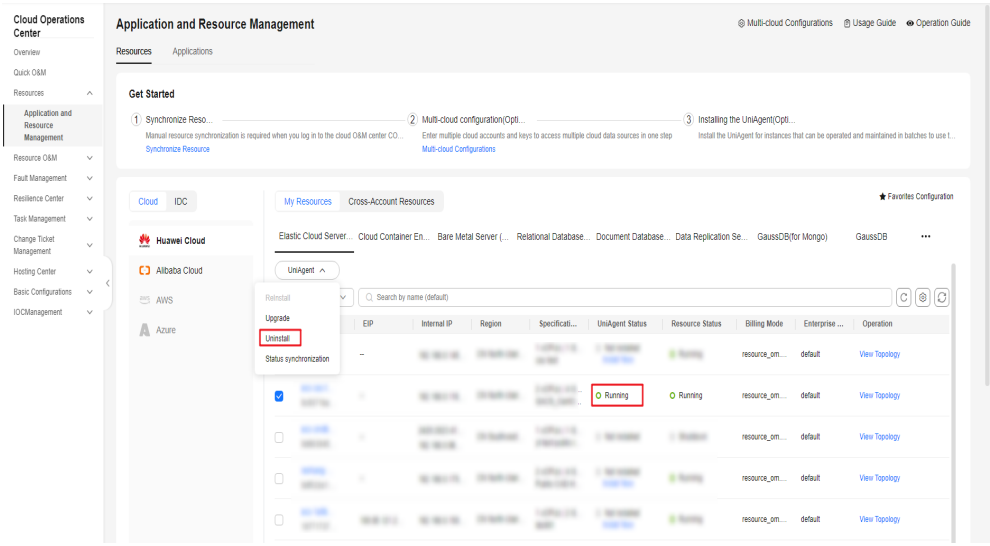
Step 6 In the drawer that is displayed on the right, select the UniAgent to be upgraded and click **OK** to trigger the automatic upgrade process. Wait until the operation is complete.

Figure 3-8 Parameters for upgrading a UniAgent



Step 7 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Resources** tab page, above the resource list, select the instances with UniAgents installed and choose **UniAgent > Uninstall**.

Figure 3-9 Uninstalling a UniAgent



Step 8 In the drawer that is displayed, click **OK** to trigger the automatic uninstallation 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

Parameter	Description	Example Value
Host Access Mode	There are three access modes: **Direct access (private network)**, **Direct access (public network)**, and **Proxy access**. ● **Direct access (intranet)**: intended for Huawei cloud hosts. ● **Direct access (public network)**: intended for non-Huawei Cloud hosts. ● **Proxy access**: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy.	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.	-
Installation Host	An installation host is used to execute commands for remote installation. This parameter is mandatory. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. 2. Access the AOM service to configure the installation host.	-

Parameter	Description	Example Value
Hosts About to Accommodate UniAgents	Detailed information about the host where the UniAgent is to be installed. This parameter is mandatory. Specify the following information: ● **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 **NOTE** The hosts that run Windows do not support connectivity tests.	-

----End

3.1.3 Viewing Resource Details

You can view resource details.

Scenarios

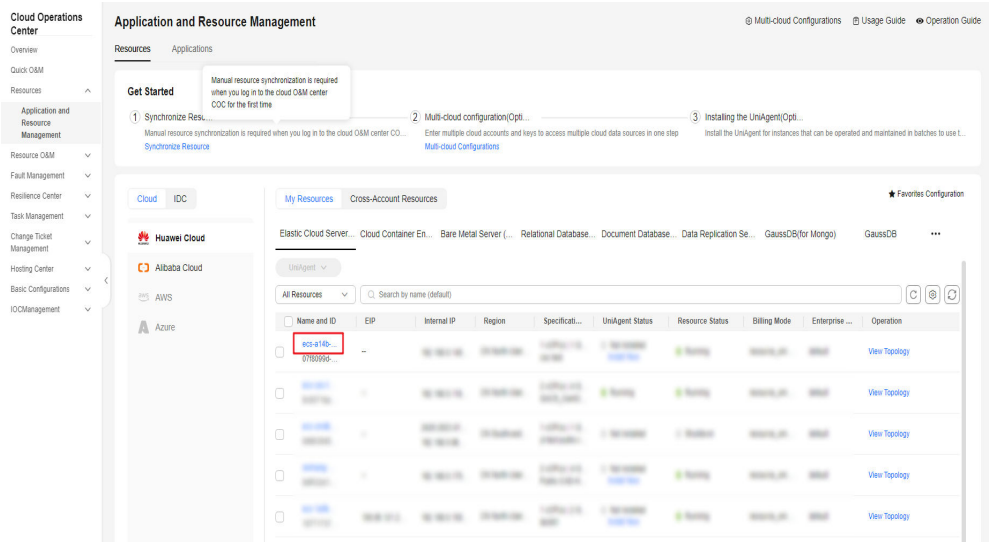
View resource details on COC.

Procedure

Step 1 Log in to **COC**.

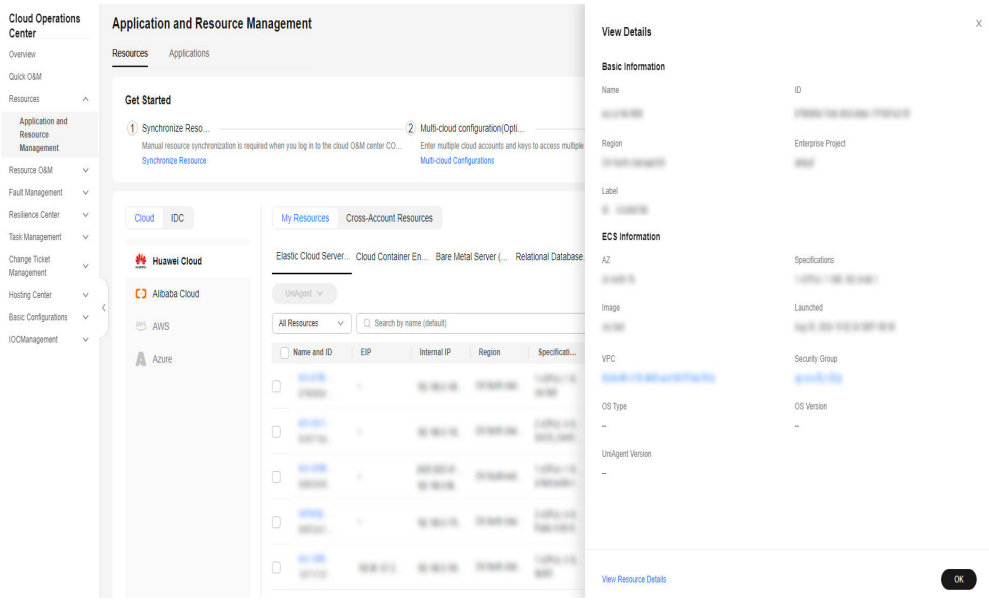
Step 2 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Resources** tab page, above the resource list, select the instances whose details you want to check and click **View Details** in the **Operation** column.

Figure 3-10 Viewing details



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

Figure 3-11 Resource details



----End

3.1.4 Viewing Resource Topologies

You can view resource topologies.

Scenarios

View resource topologies on COC.

Precautions

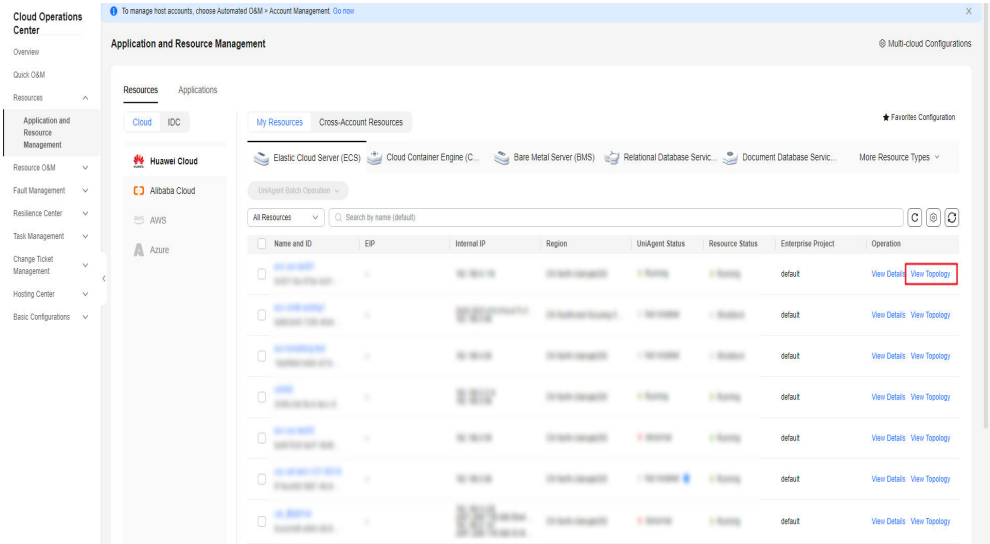
Currently, only the topologies of instances of Elastic Cloud Servers (ECS), MapReduce Services (MRS) instance, Bare Metal Server (BMS), and Cloud Container Engine (CCE) can be viewed.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. On the displayed **Resources** tab page, above the resource list, select the instances whose resource topology you want to check and click **View Topology** in the **Operation** column.

Figure 3-12 Viewing resource topologies



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

Figure 3-13 Topology relationship

----End

3.2 Application Management

Application Management manages the relationship between applications and cloud resources, and provides unified and timely resource environment management services for follow-up resource monitoring and automatic O&M.

3.2.1 Creating an Application

You can create an application to facilitate resource management by service logic unit.

Scenarios

Create an application on COC.

Precautions

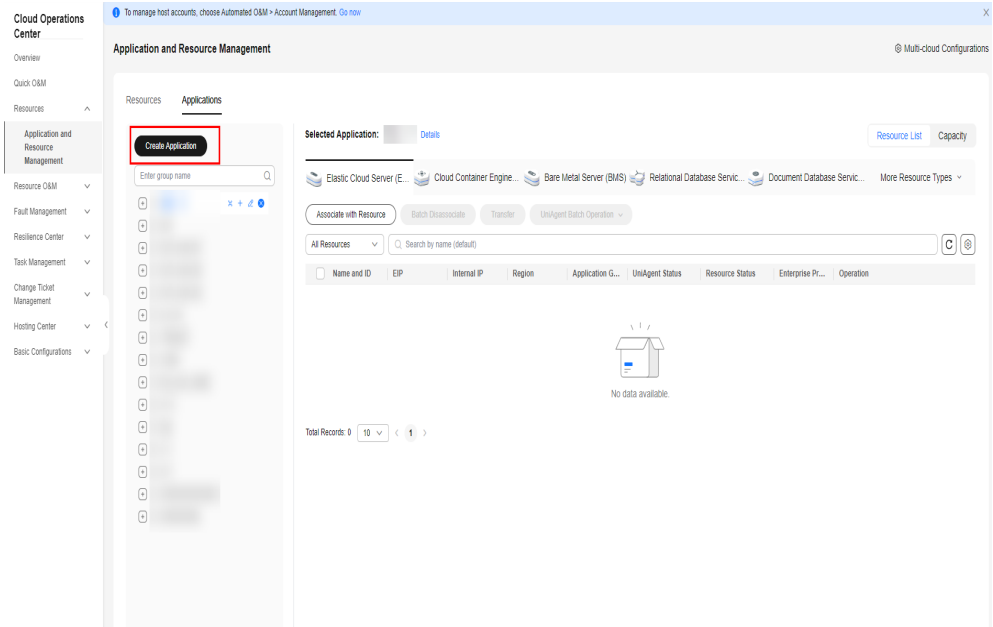
An application cannot contain both sub-applications and components.

Procedure

Step 1 Log in to **COC**.

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

Figure 3-14 Creating an application



Step 3 On the **Create Application** page, configure required information and click **Submit**. For details, see **Table 3-2**.

Figure 3-15 Setting parameters

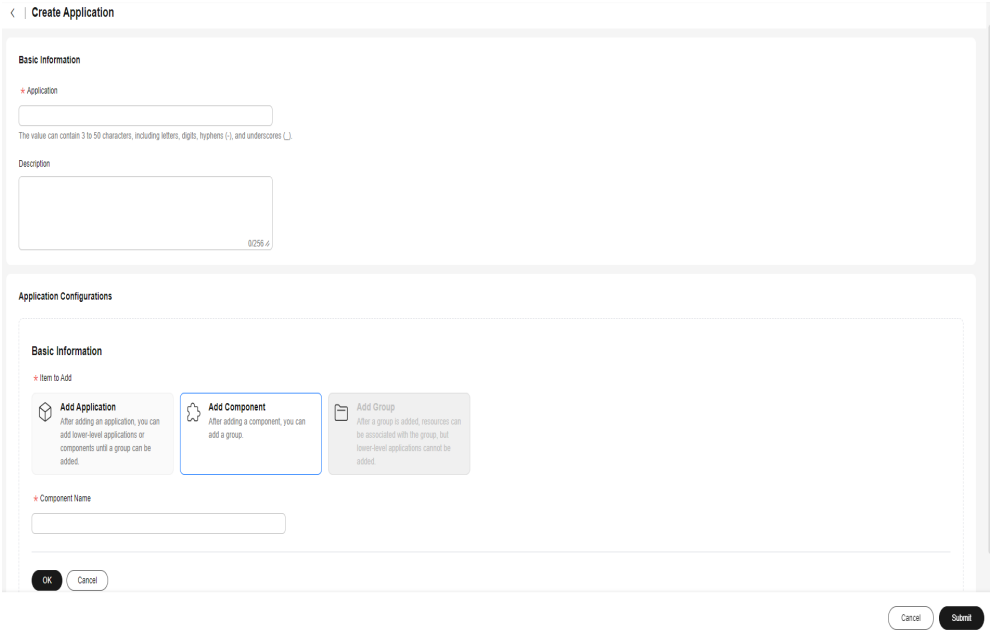


Table 3-2 Parameters for creating an application

Parameter	Description	Example Value
Application ID	(Mandatory) In the **Basic Information** area, enter an application ID.	testApplication

Parameter	Description	Example Value
Application	(Mandatory) In the **Basic Information** area, enter the application name.	Test Application
Enterprise Project	(Mandatory) In the **Basic Information** area, specify the enterprise project, which the application belongs to.	default
Description	(Optional) In the **Basic Information** area, provide important information about the application.	-
Component ID	(Mandatory) In the **Application Configuration** area, enter the ID of the component you want to create.	testComponent
Component	(Mandatory) In the **Application Configuration** area, enter the name of the component you want to create.	Test Component
Group ID	(Mandatory) Group of the component you created. Enter a valid group ID.	testGroup
Group	(Mandatory) Group of the component you created. Enter a valid group name.	Test Group
Resource Association Method	(Mandatory) Method that is used to associate resources with the group you created. There are two association methods: manual association and intelligent association. ● Manual: You can manually associate resources with the group you created for unified management. ● Intelligent: You can add all resources with the same tag in an enterprise project to a resource group.	Manual
Tag Key	(Mandatory) This parameter is displayed if the intelligent resource association method is used.	testKey
Tag Value	(Optional) This parameter is displayed if the intelligent resource association method is used.	testValue

----End

3.2.2 Modifying an Application

You can modify applications to facilitate resource management by service logic unit.

Scenarios

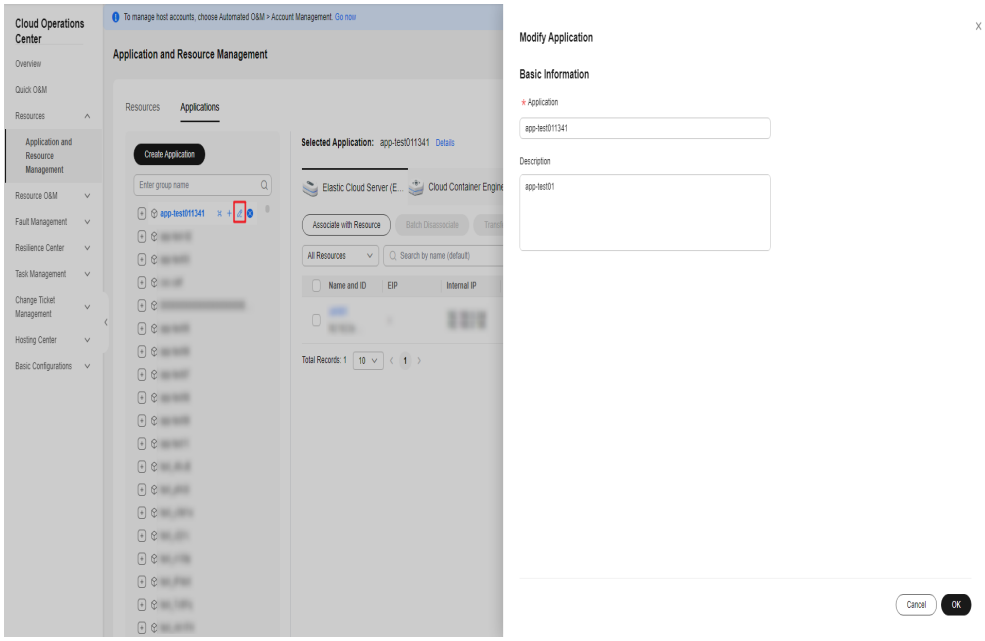
Modify application configurations on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose the application you want to update in the resource tree on the left, and click .

Figure 3-16 Editing an application



Step 3 Set parameters in the **Modify Application** drawer by referring to **Table 3-3** and click **OK**.

Table 3-3 Parameters for updating application configurations

Parameter	Description	Example Value
Application	(Mandatory) In the **Basic Information** area, enter the application name.	Test Application
Description	(Optional) In the **Basic Information** area, provide important information about the application.	-

----End

3.2.3 Deleting an Application

You can delete applications that are no longer needed.

Scenarios

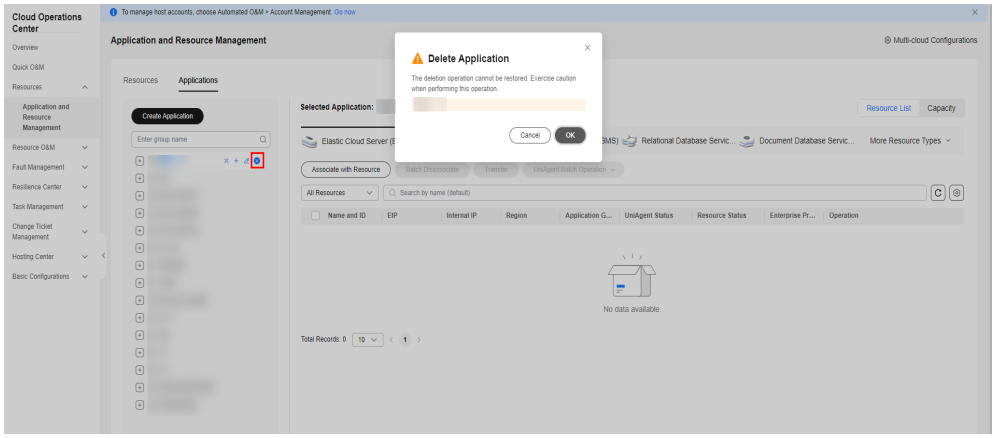
Delete an application on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose the application you want to delete in the resource tree on the left, and click .

Figure 3-17 Deleting an application



Step 3 Click **OK**.

----End

3.2.4 Editing an Application Topology

You can edit the application topology and edit component invoking connections.

Scenarios

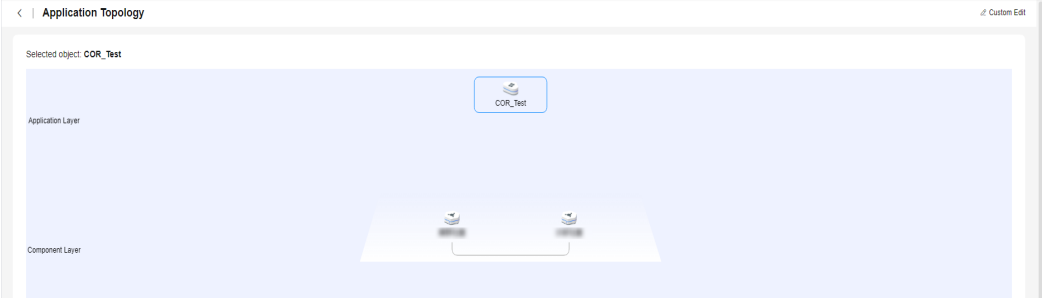
Check the application topology and edit the component invoking connections on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose a desired application in the resource tree on the left, and click .

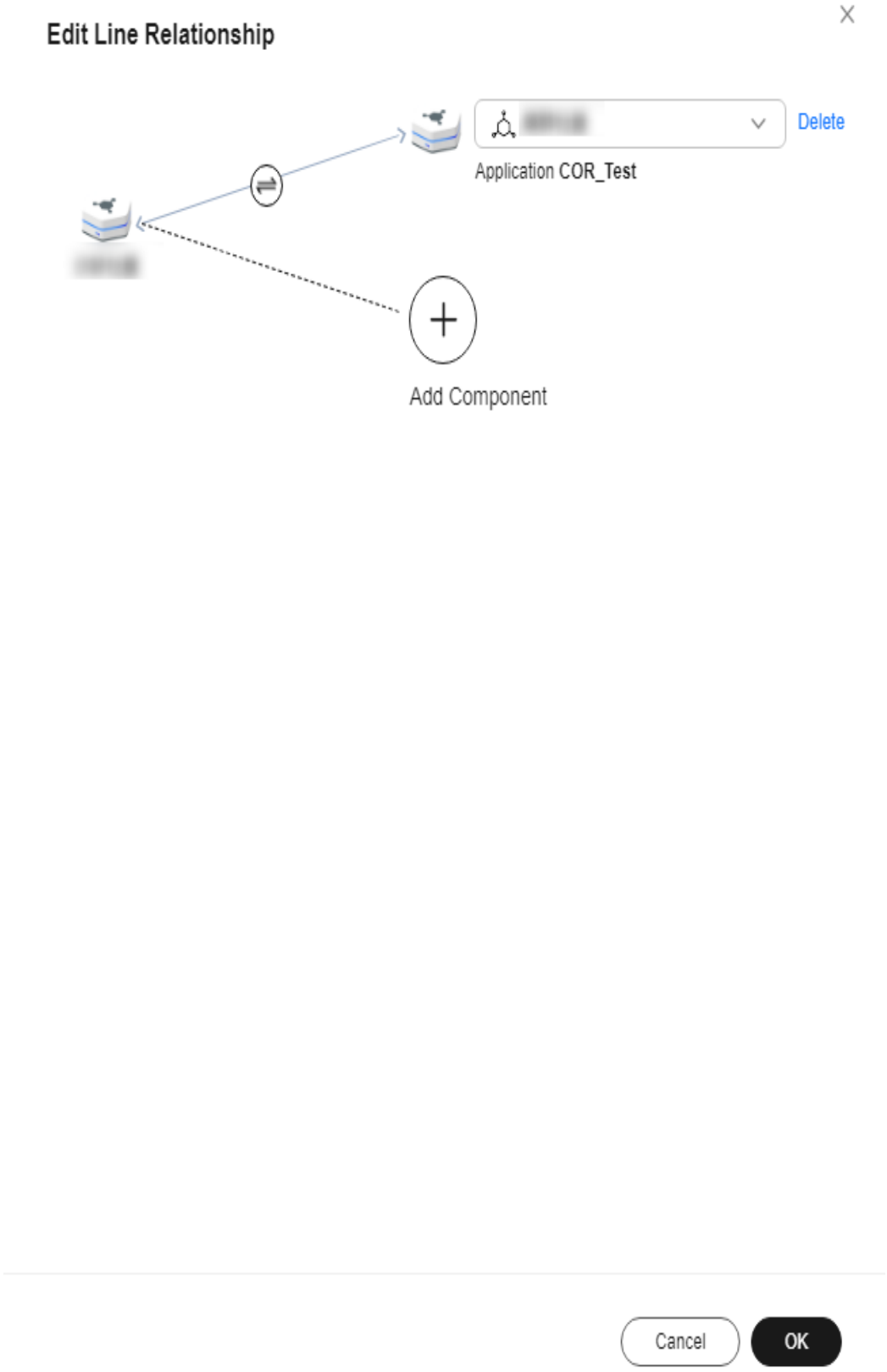
Figure 3-18 Application topology



Step 3 Click **Custom Edit** in the upper right corner to enter the topology editing mode.

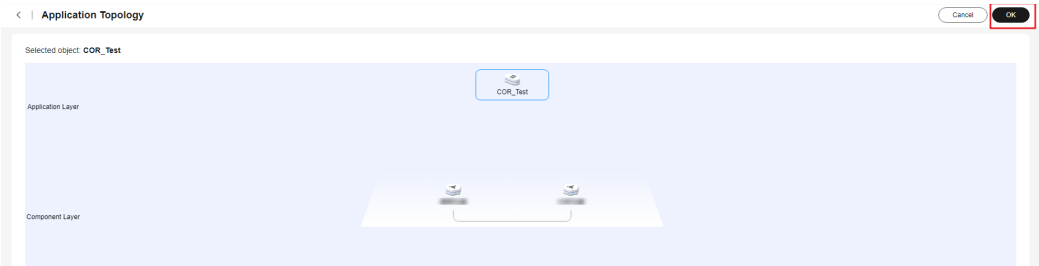
Step 4 Select a component, edit the component invoking connections, and click **OK**.

Figure 3-19 Editing component connections



Step 5 Click **OK** to exit the editing mode.

Figure 3-20 Exiting the editing state.



----End

3.2.5 Creating a Component

You can create a component to facilitate resource management by service logic unit.

Scenarios

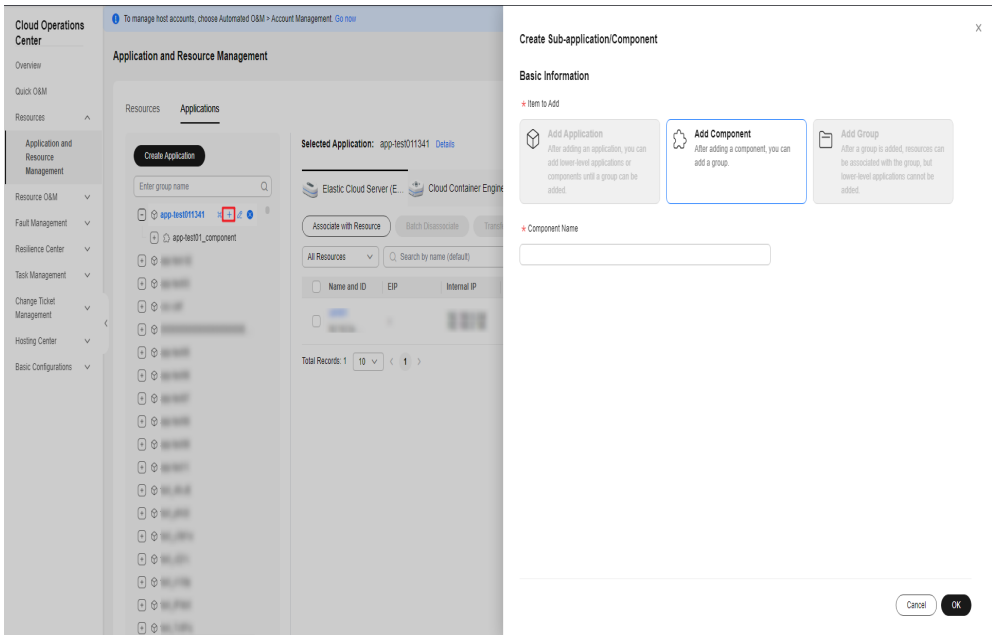
Create a component on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose the application for which you want to create a component in the application tree on the left, and click the plus sign (+).

Figure 3-21 Creating a component



Step 3 Set parameters in the **Create Sub-application/Component** drawer by referring to **Table 3-4** and click **OK**.

Table 3-4 Parameters for creating a component

Parameter	Description	Example Value
Component ID	(Mandatory) In the **Basic Information** area, enter the ID of the component you want to create.	testComponent
Component	(Mandatory) In the **Basic Information** area, enter the name of the component you want to create.	Test Component

----End

3.2.6 Modifying a Component

You can modify a component as required.

Scenarios

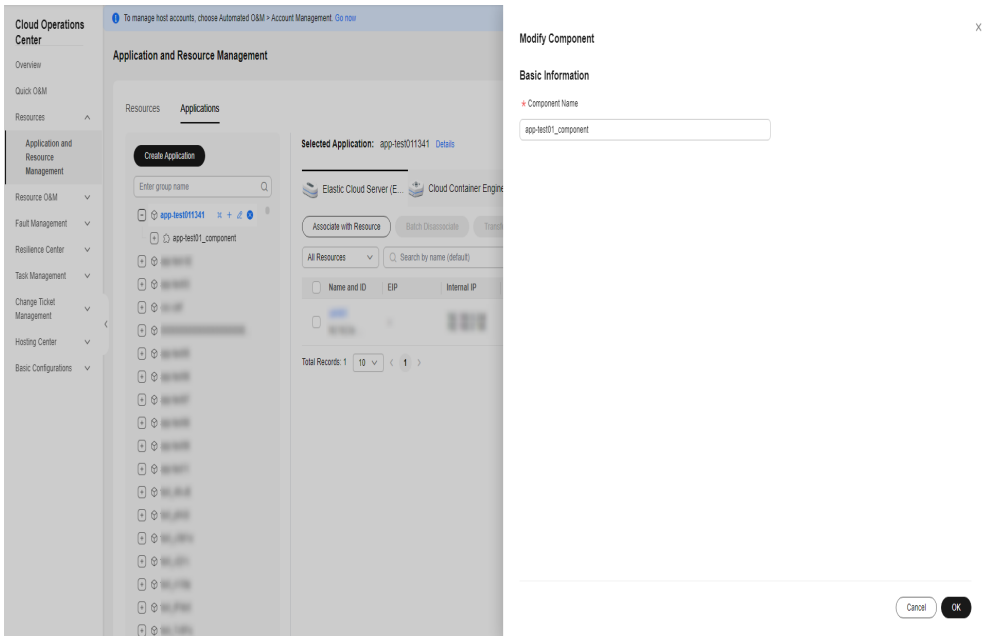
Modify a component on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**. On the displayed page, click the **Applications** tab, choose the application for which you want to modify the component in the resource tree on the left, and click .

Figure 3-22 Editing a component



Step 3 Set parameters in the **Modify Component** drawer by referring to **Table 3-5** and click **OK**.

Table 3-5 Parameters for modifying a component

Parameter	Description	Example Value
Component	(Mandatory) In the **Basic Information** area, enter the name of the component you want to create.	Test Component

----End

3.2.7 Deleting a Component

You can delete components as required.

Scenarios

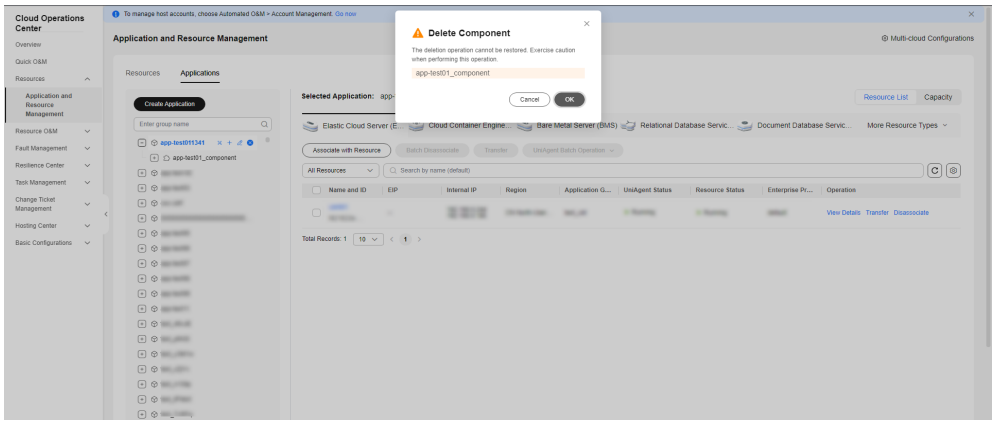
Delete a component on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose the application for which you want to delete a component in the resource tree on the left, and click ⊗.

Figure 3-23 Deleted a component



Step 3 Click **OK**.

----End

3.2.8 Creating a Group

You can create a group to facilitate resource management by service logic unit.

Scenarios

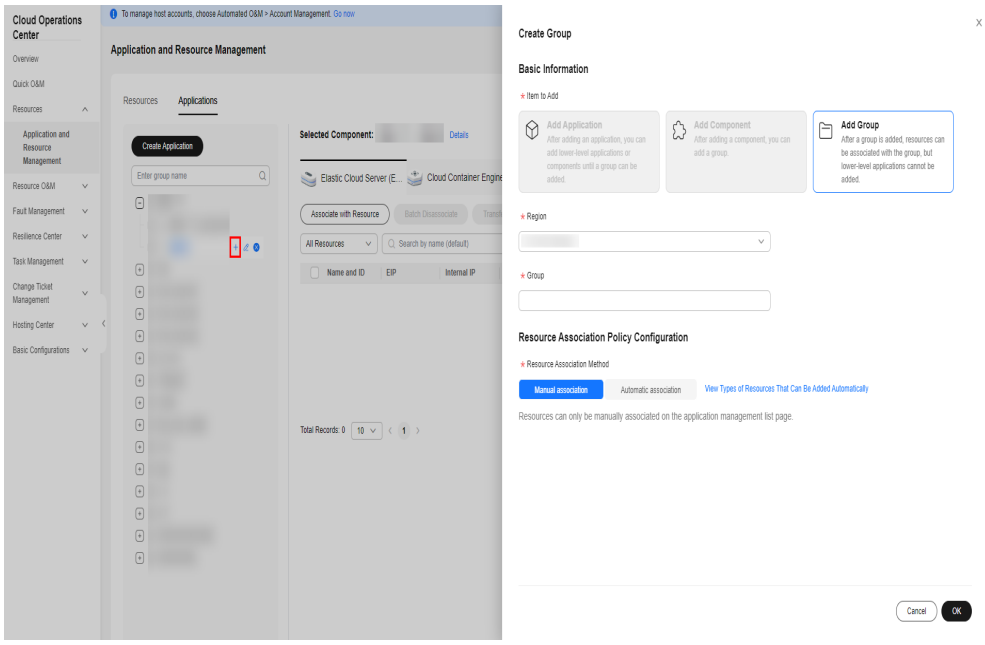
Create a group on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tag, choose a desired component in the resource tree on the left, and click the plus sign (+).

Figure 3-24 Creating a group



Step 3 Set parameters in the **Create Group** drawer by referring to **Table 3-6** and click **OK**.

Table 3-6 Parameters for creating a component

Parameter	Description	Example Value
Group ID	(Mandatory) Group of the component you created. Enter a valid group ID.	testGroup
Group	(Mandatory) Group of the component you created. Enter a valid group name.	Test Group
Resource Association Method	(Mandatory) Method that is used to associate resources with the group you created. There are two association methods: manual association and intelligent association. ● Manual: You can manually associate resources with the group you created for unified management. ● Intelligent: You can add all resources with the same tag in an enterprise project to a resource group.	Manual
Tag Key	(Mandatory) This parameter is displayed if the intelligent resource association method is used.	testKey
Tag Value	(Optional) This parameter is displayed if the intelligent resource association method is used.	testValue

----End

3.2.9 Modifying a Group

You can modify a group as required.

Scenarios

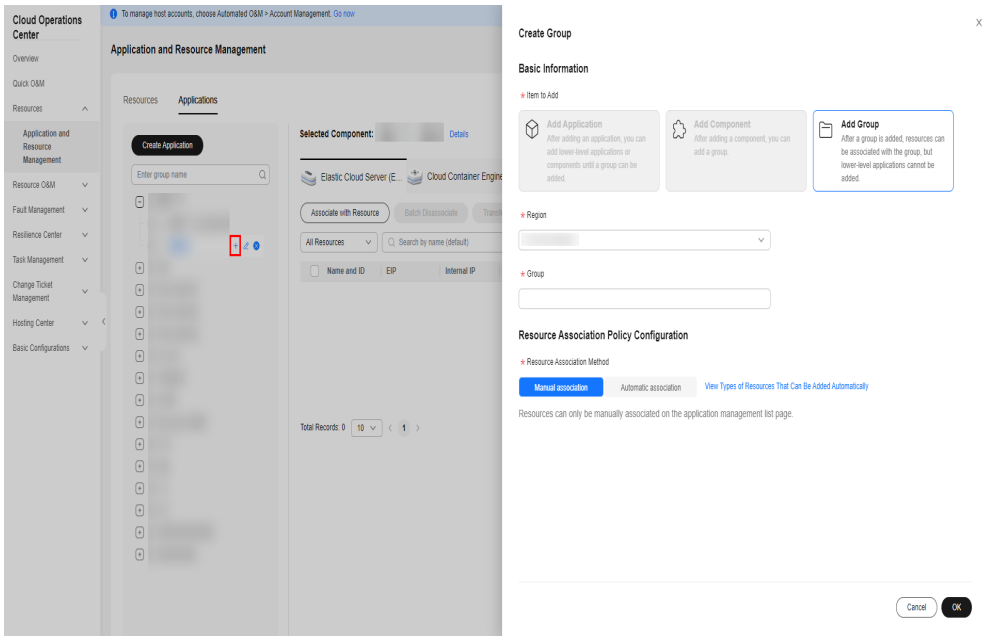
Modify a group on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose a desired group in the resource tree on the left, and click .

Figure 3-25 Modifying a group



Step 3 Set parameters in the **Modify Group** drawer by referring to **Table 3-7** and click **OK**.

Table 3-7 Parameters for modifying a group

Parameter	Description	Example Value
Group	(Mandatory) Group of the component you created. Enter a valid group name.	Test Group
Resource Association Method	(Mandatory) Method that is used to associate resources with the group you created. There are two association methods: manual association and intelligent association. • Manual: You can manually associate resources with the group you created for unified management. • Intelligent: You can add all resources with the same tag in an enterprise project to a resource group.	Manual
Tag Key	(Mandatory) This parameter is displayed if the intelligent resource association method is used.	testKey
Tag Value	(Optional) This parameter is displayed if the intelligent resource association method is used.	testValue

----End

3.2.10 Deleting a Group

You can delete groups as required.

Scenarios

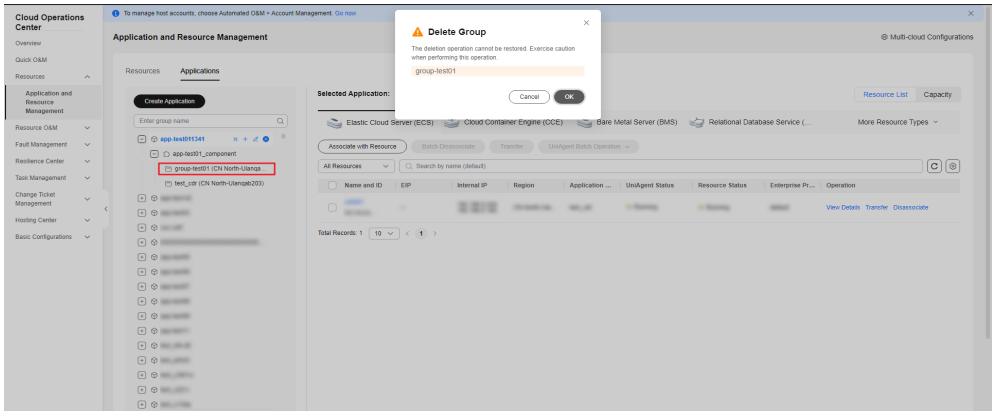
Delete a group on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, choose a desired group in the resource tree on the left, and click .

Figure 3-26 Deleting a group



Step 3 Click **OK**.

----End

3.2.11 Associating Resources with an Application Group

You can associate resources with an application group for unified resource management.

Scenarios

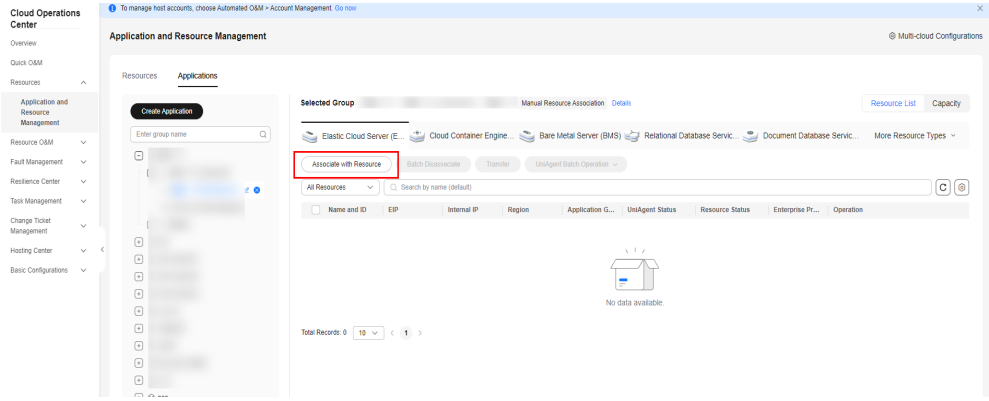
Associate resources with a specified application group.

Procedure

Step 1 Log in to **COC**.

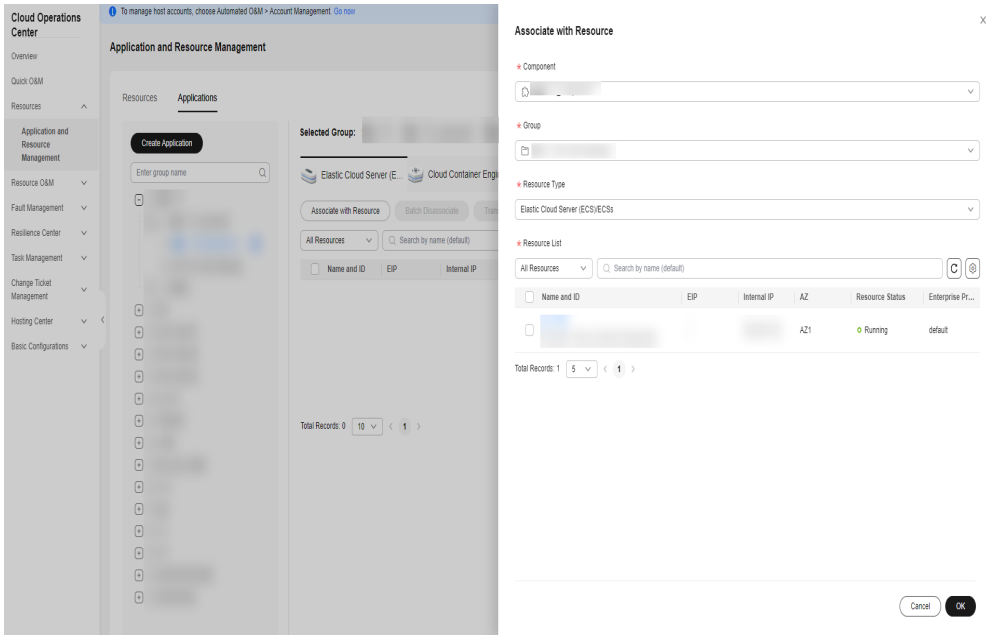
Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab and click **Associate with Resource**.

Figure 3-27 Manually associating resources with a group



Step 3 Configure parameters for associating resources in the drawer that is displayed, select the resources to be associated with the group, and click **OK**.

Figure 3-28 Selecting the resources to be associated with the group



----End

3.2.12 Intelligently Associating Resources with an Application Group

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

Scenarios

Associate resources with a specified application group.

Precautions

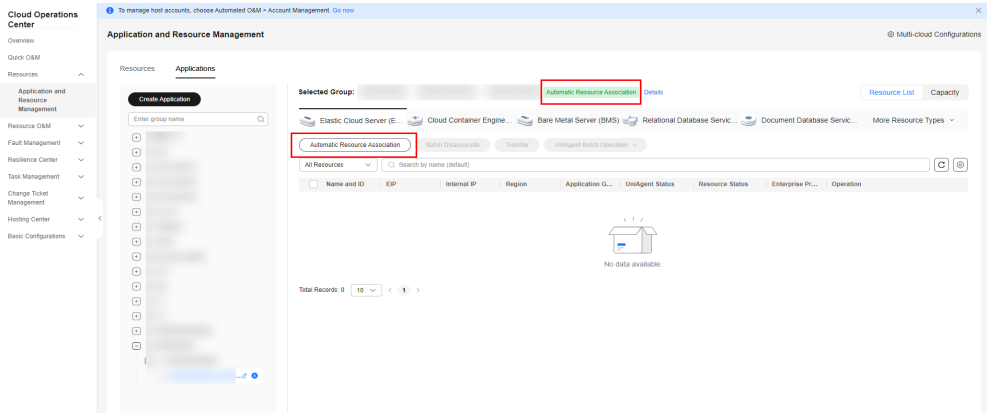
1. Only after you select a group and click the **Intelligent resource association** button above the resource list, can this operation take effect.
2. After intelligent resource association is triggered, wait until the synchronization task is executed. Time the association takes depends on the total number of resources to be associated.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab and choose a group in the resource tree in the left and click **Associate with Resource**.

Figure 3-29 Intelligently associating resources with a group



----End

3.2.13 Transferring Resources

You can transfer associated resources to other groups for management.

Scenarios

Transfer associated resources to a specified application group on COC.

Precautions

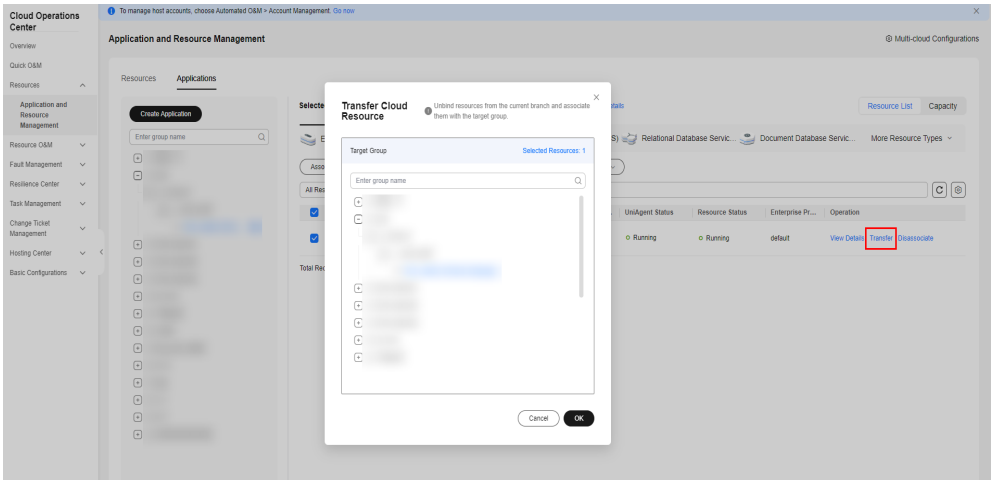
Resources can be transferred to application groups only when they belong to the same enterprise project as the application.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, locate the resource you want to transfer to other groups, and click **Transfer** in the **Operation** column.

Figure 3-30 Transferring a resource



Step 3 Select the group to which you want to transfer this resource and click **OK**.

----End

3.2.14 Disassociating a Resource from an Application Group

You can disassociate resources from application groups.

Scenarios

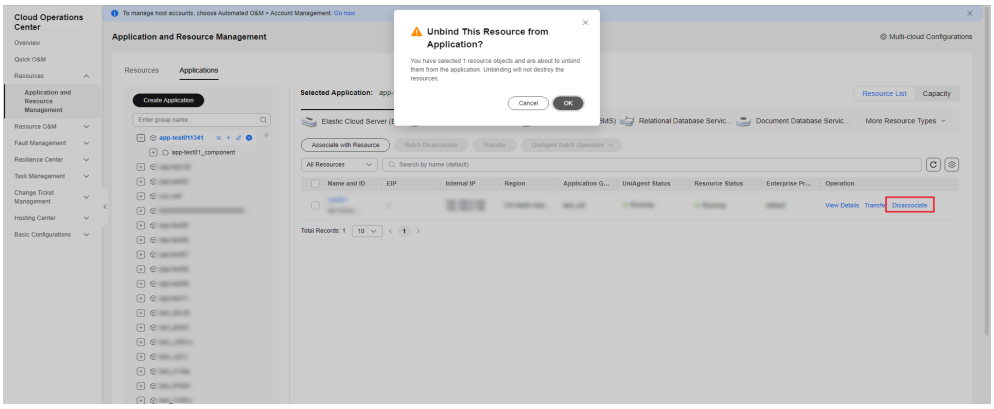
Disassociate resources from groups on COC

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab, locate the application from which you want to disassociate resources, and click **Disassociate** in the **Operation** column.

Figure 3-31 Disassociating a resource from a group



Step 3 Click **OK**.

----End

3.2.15 Performing Operations on a UniAgent

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

Scenarios

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

Precautions

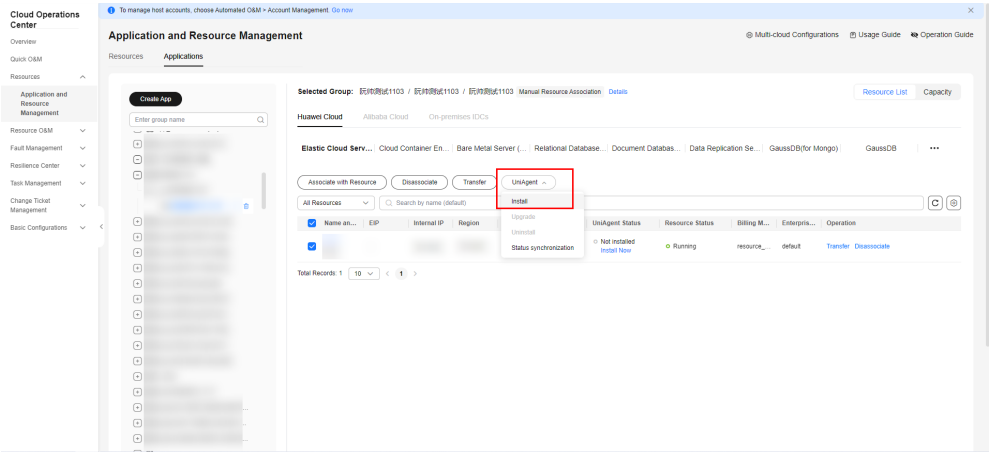
Currently, you can only perform operations on UniAgent for ECSs.

Procedure

Step 1 Log in to **COC**.

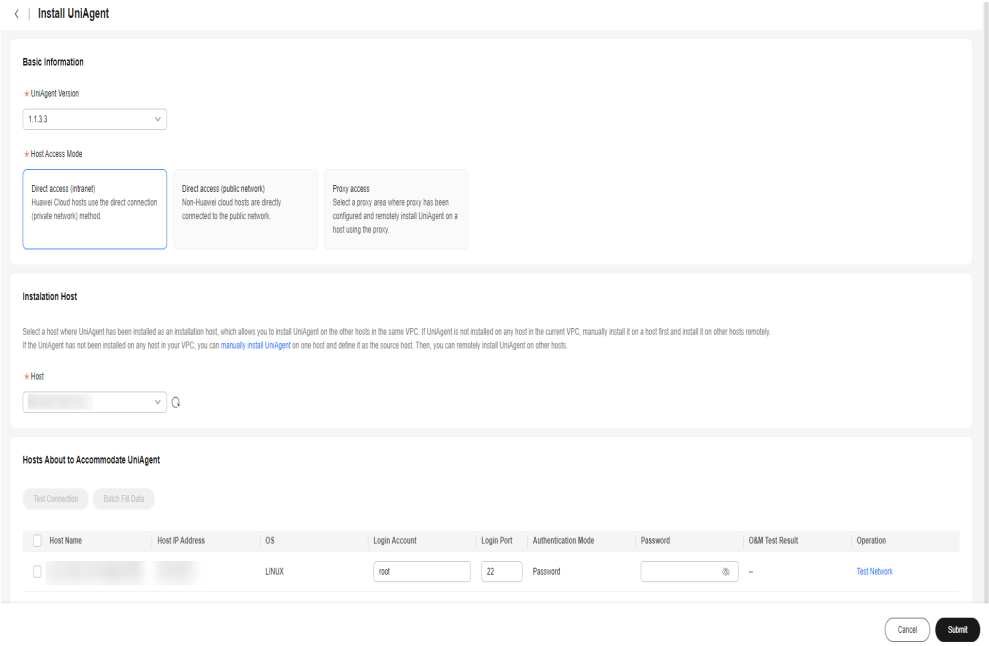
Step 2 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. On the displayed **Applications** > **Elastic Cloud Server (ECS)** tab page, above the resource list, select a desired ECS and choose **UniAgent** > **Install**.

Figure 3-32 Installing a UniAgent



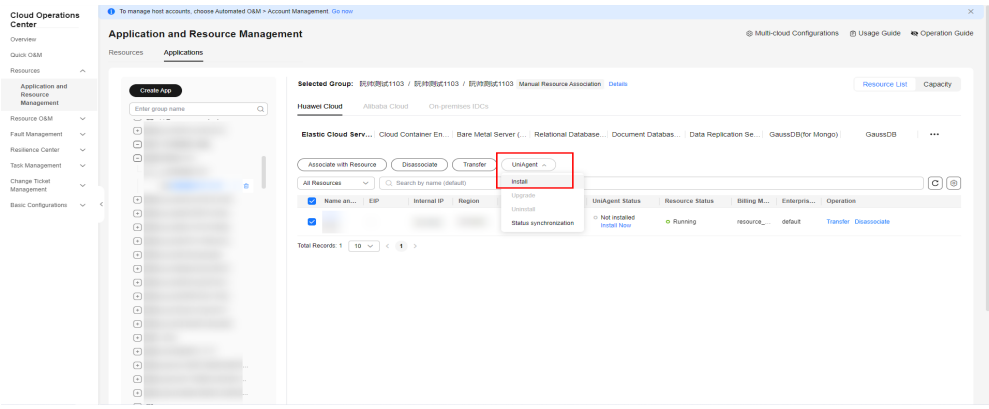
Step 3 On the displayed **Install UniAgent** page, specify required information by referring to **Table 3-8** and click **Submit** to trigger the automated installation process. Wait until the installation is complete.

Figure 3-33 Setting parameters



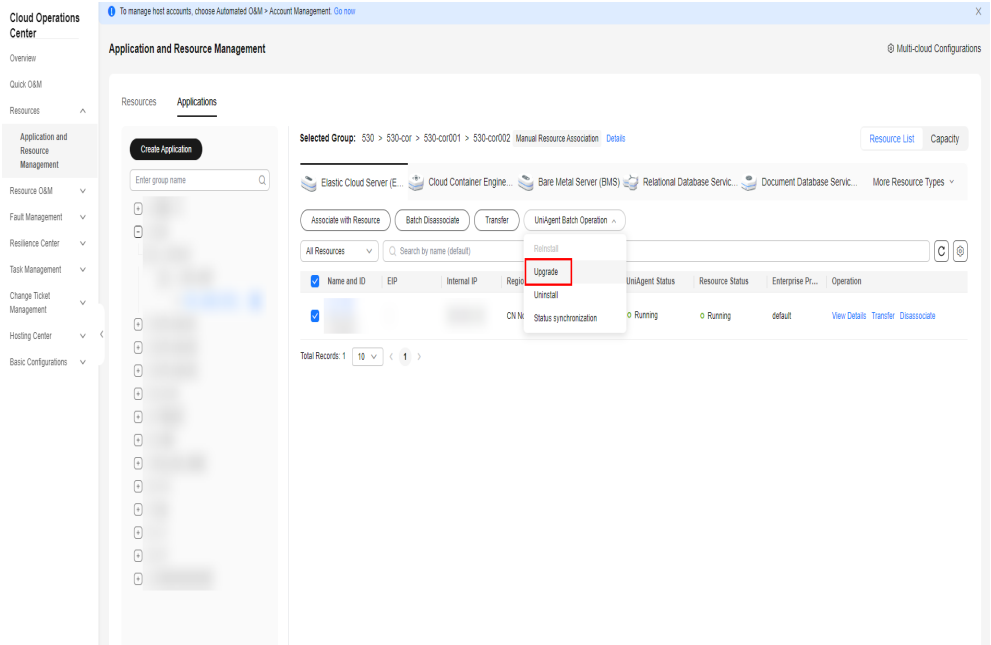
Step 4 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. Click the **Applications** tab, select the instances whose UniAgent status is **Abnormal**, **Not installed**, or **Installation failed**, and choose **UniAgent** > **Reinstall**.

Figure 3-34 Reinstalling a UniAgent



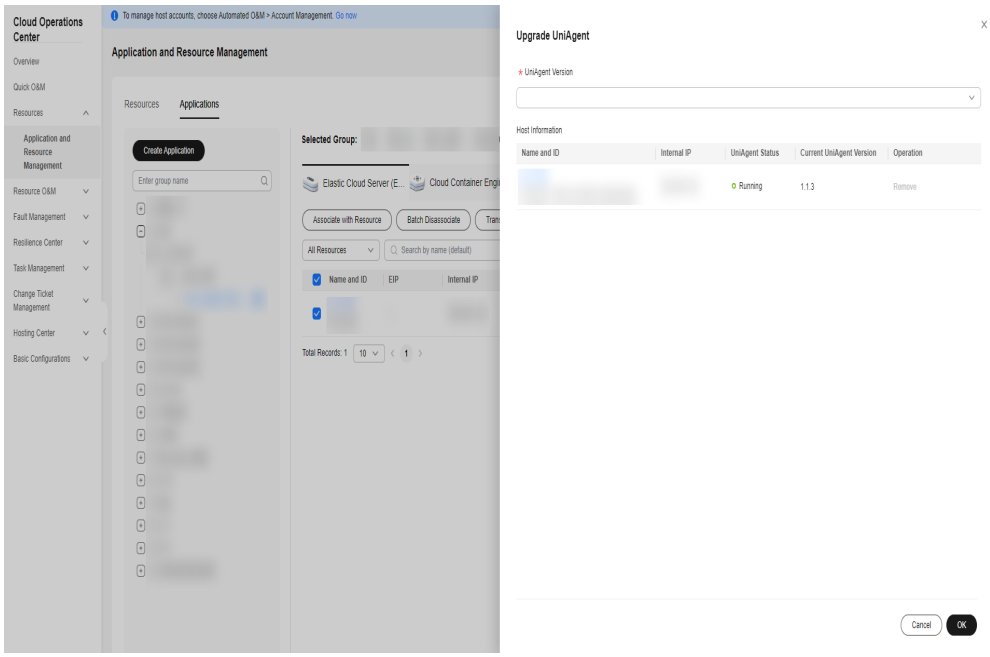
Step 5 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Applications** tab page, above the resource list, select the instances with UniAgents installed and choose **UniAgent > Upgrade**.

Figure 3-35 Upgrading a UniAgent



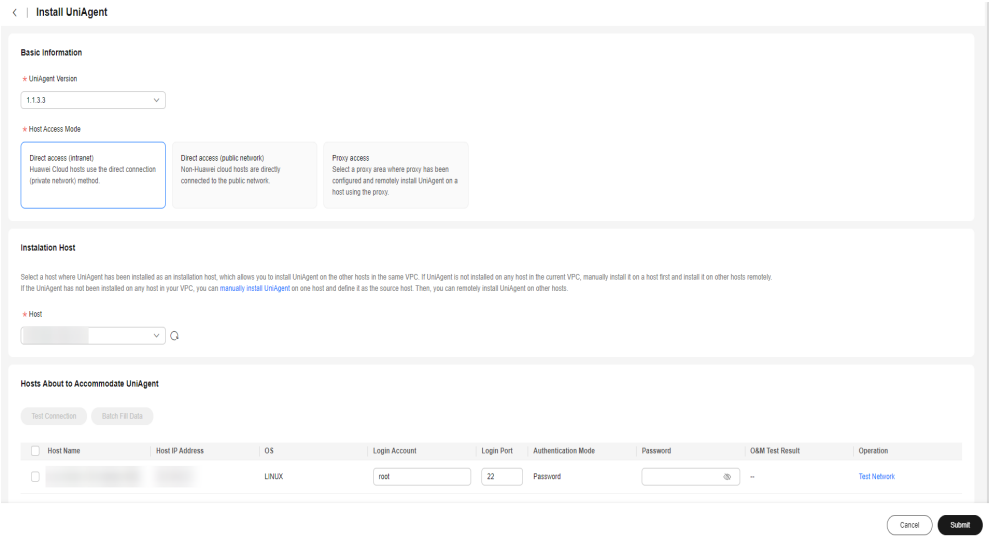
Step 6 In the drawer that is displayed on the right, select the UniAgent to be upgraded and click **OK** to trigger the automatic upgrade process. Wait until the operation is complete.

Figure 3-36 Parameters for Upgrading a UniAgent



Step 7 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Applications** > **Elastic Cloud Server (ECS)** tab page, above the resource list, select the ECS with UniAgents installed and choose **UniAgent > Uninstall**.

Figure 3-37 Uninstalling a UniAgent



Step 8 In the drawer that is displayed, click **OK** to trigger the automatic uninstallation process. Wait until the operation is complete.

Table 3-8 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**. • **Direct access (intranet)**: intended for Huawei cloud hosts • **Direct access (public network)**: intended for non-Huawei Cloud hosts • **Proxy access**: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy.	Direct access (private network)
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	An installation host is used to execute commands for remote installation. This parameter is mandatory. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. 2. Access the AOM service to configure the installation host.	-
Hosts About to Accommodate UniAgents	Detailed information about the host where the UniAgent is to be installed. This parameter is mandatory. Specify the following information: ● **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, you are advised to use the **root** account 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 **NOTE** The hosts that run Windows do not support connectivity tests.	-

----End

3.2.16 Viewing Resource Details

You can view resource details.

Scenarios

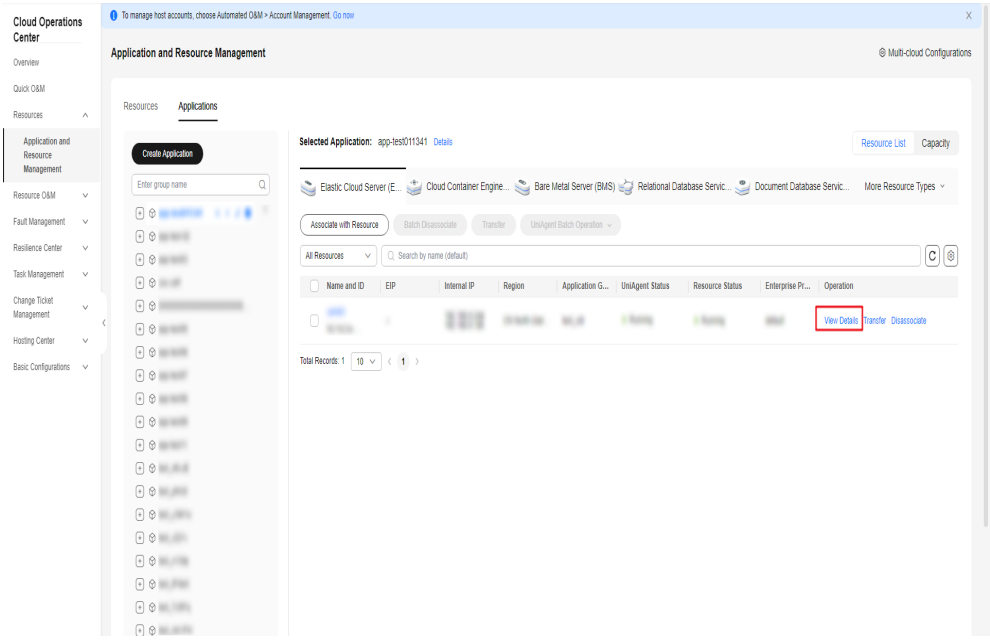
View details about resources associated with applications on COC.

Procedure

Step 1 Log in to **COC**.

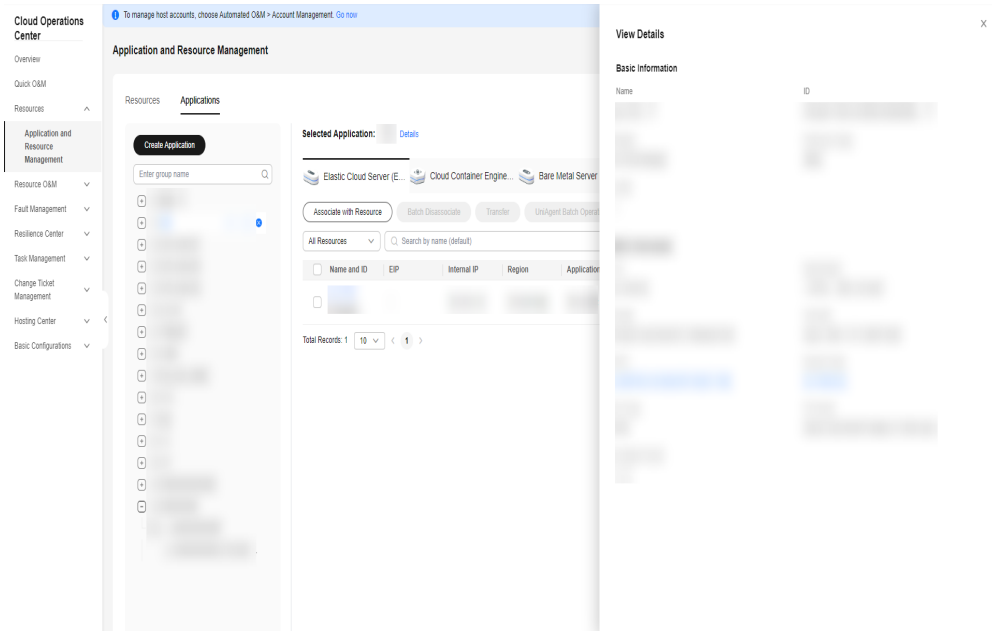
Step 2 In the navigation pane on the left, choose **Resources** > **Application and Resource Management**. On the displayed **Applications** > **Elastic Cloud Server (ECS)** tab page, above the resource list, select the ECSs whose details you want to check and click **View Details** in the **Operation** column.

Figure 3-38 Viewing resource details



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

Figure 3-39 Resource details



----End

3.2.17 Viewing Capacity Rankings

You can view the capacity rankings of associated resources.

Scenarios

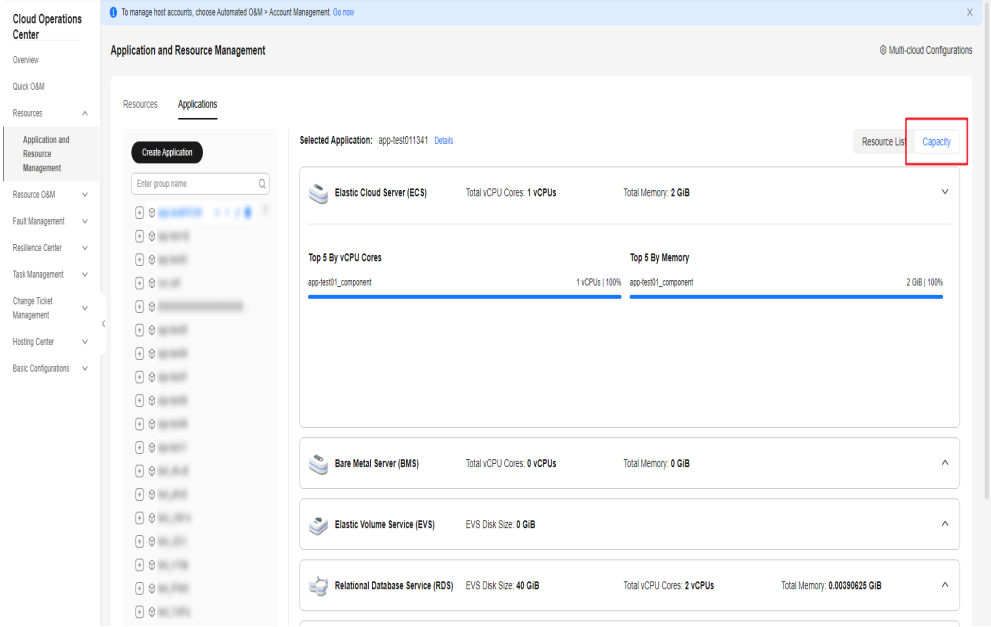
View the capacity rankings of associated resources on COC.

Procedure

Step 1 Log in to **COC**.

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

Figure 3-40 Viewing capacity rankings



----End

3.3 Multi-cloud Configurations

3.3.1 Creating an Account

You can create an account under a cloud vendor to synchronize resources of the account.

Scenarios

Create a cloud vendor account on COC.

Precautions

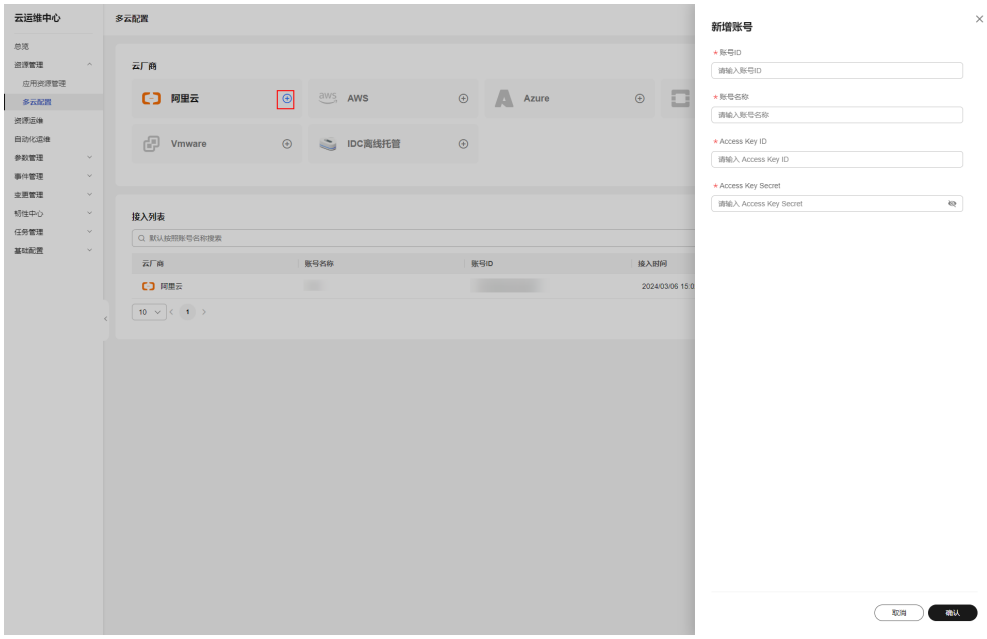
Currently, only Alibaba Cloud accounts can be created.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resource Management** > **Multi-cloud Configurations**. On the displayed page, click plus sign on the right of a desired cloud vendor.

Figure 3-41 Creating an account



Step 3 Enter required information and click **OK**. For details, see **Table 3-9**.

Table 3-9 Parameters for creating an account

Parameter	Description	Example Value
Account ID	(Mandatory) Basic information, which is the account ID.	-
Account	(Mandatory) Basic information, which is the account name.	-
Access Key ID	(Mandatory) Basic information, which is the access key ID.	-
Access Key Secret	(Mandatory) Basic information, which is the access key secret.	-

----End

3.3.2 Editing an Account

You can update existing accounts.

Scenarios

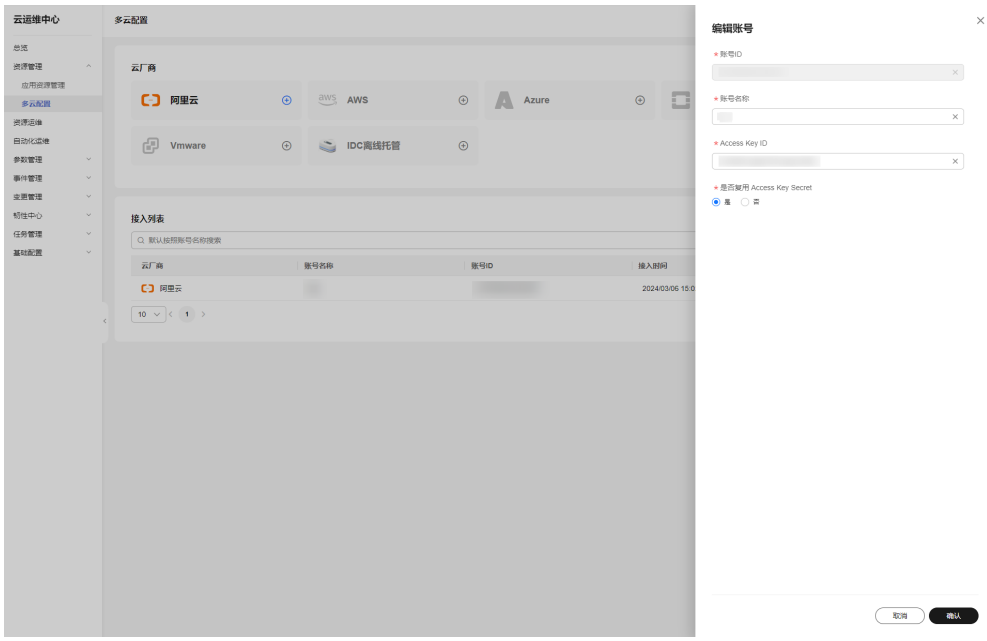
Update a cloud vendor account on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resource Management** > **Multi-cloud Configurations**. On the displayed page, locate the account you want to update and click **Edit** in the **Operation** column.

Figure 3-42 Editing an account



Step 3 Enter required information and click **OK**. For details, see **Table 3-10**.

Table 3-10 Parameters for editing an account

Parameter	Description	Example Value
Account	(Mandatory) Basic information, which is the account name.	-
Access Key ID	(Mandatory) Basic information, which is the AK ID.	-
Reuse Access Key Secret	(Mandatory) Whether to reuse the access key secret If this parameter is set to **Yes**, the latest access key secret is reused. If this parameter is set to **No**, you need to enter a new access key secret.	Yes
Access Key Secret	Basic information, which is the access key secret.	-

----End

3.3.3 Deleting an Account

You can delete cloud vendor accounts.

Scenarios

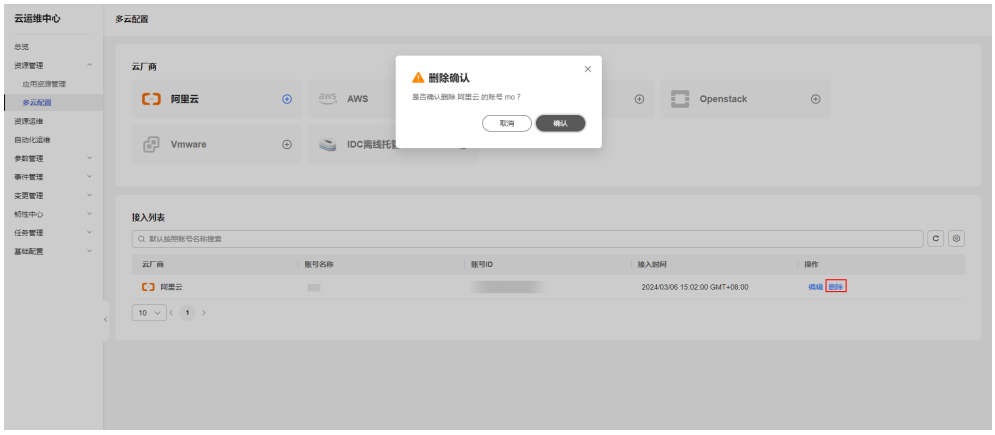
Delete a cloud vendor account on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resource Management** > **Multi-cloud Configurations**. On the displayed page, locate the account you want to update and click **Delete** in the **Operation** column.

Figure 3-43 Deleting an account



Step 3 Click **OK** in the dialog box that is displayed.

----End

4 Resource O&M

4.1 Overview

Resource O&M allows users to manage patches and operate Elastic Cloud Servers (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 Batch ECS operations

You can manage ECSs in batches, including batch starting, stopping, and restarting ECSs, and switching and reinstalling OSs for ECSs.

4.2.1 Starting ECSs

Scenarios

Start ECS instances in batches on COC.

Precautions

Instances that have been started cannot be selected.

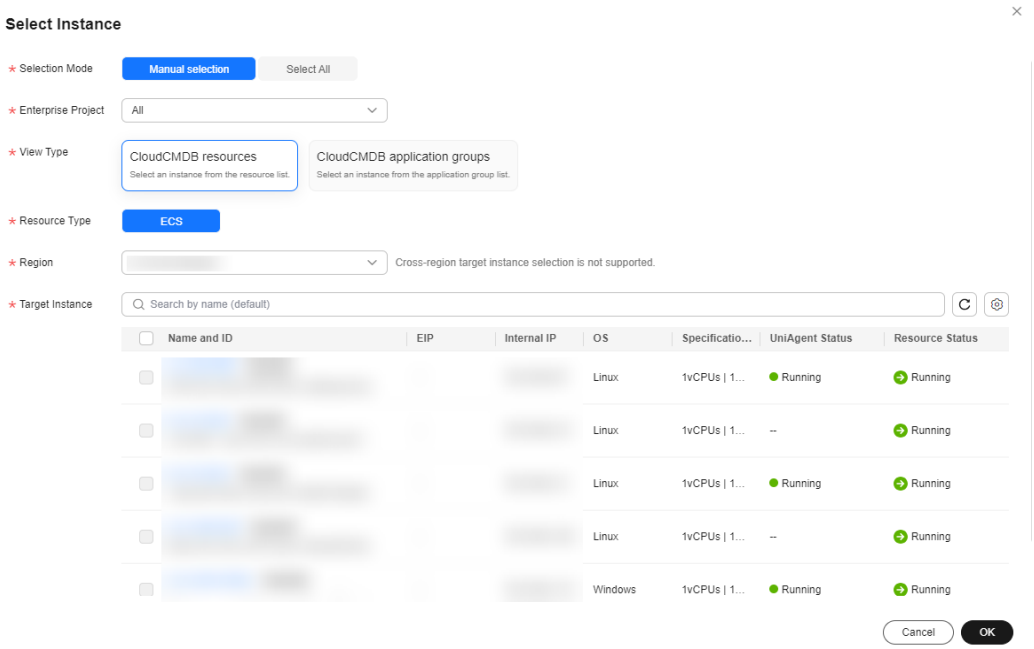
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**, and click **Start ECSs** in **ECS Operations**.

Step 3 On the **Start ECSs** page, click **Add**.

Figure 4-1 Selecting instances



Step 4 Select **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.

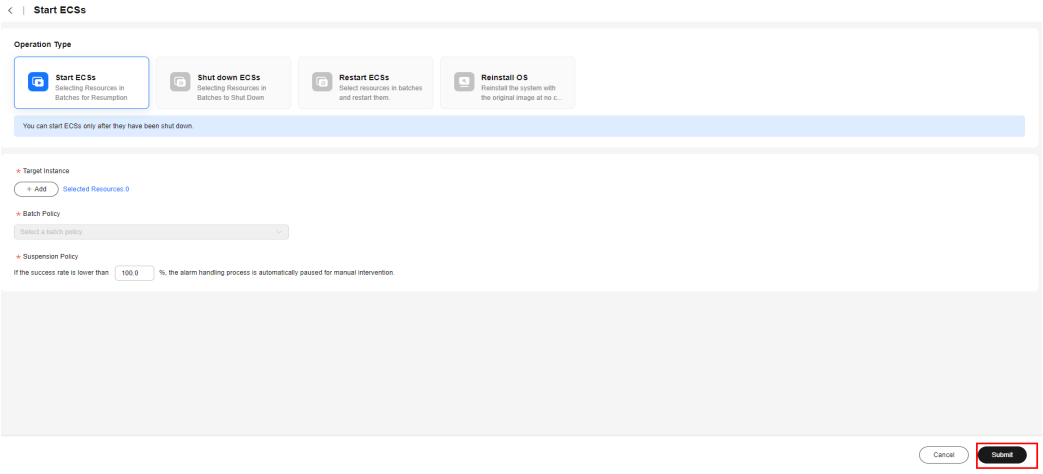
Step 5 Set **Suspension Policy**.

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 range is from 0 to 100 and can be set to one decimal place.

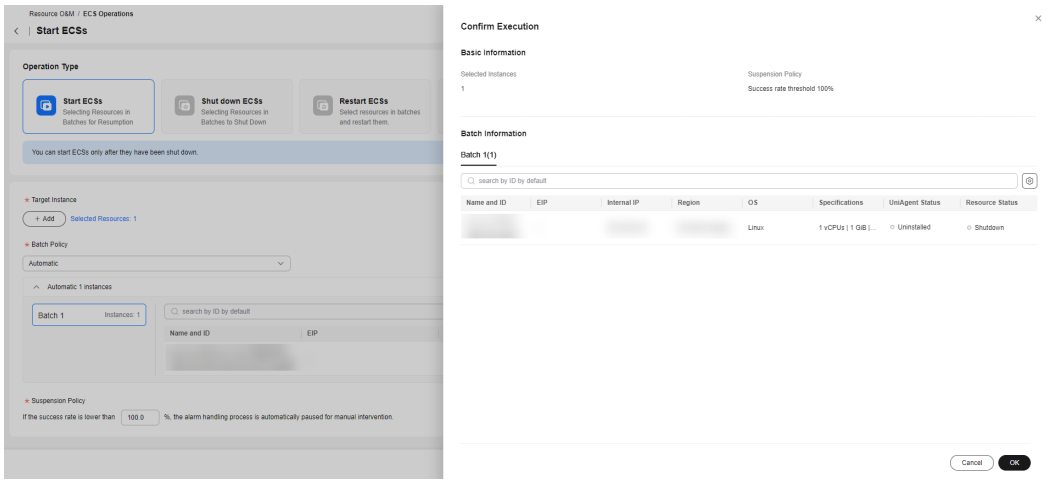
Step 6 Click **Submit**.

Figure 4-2 Starting instances



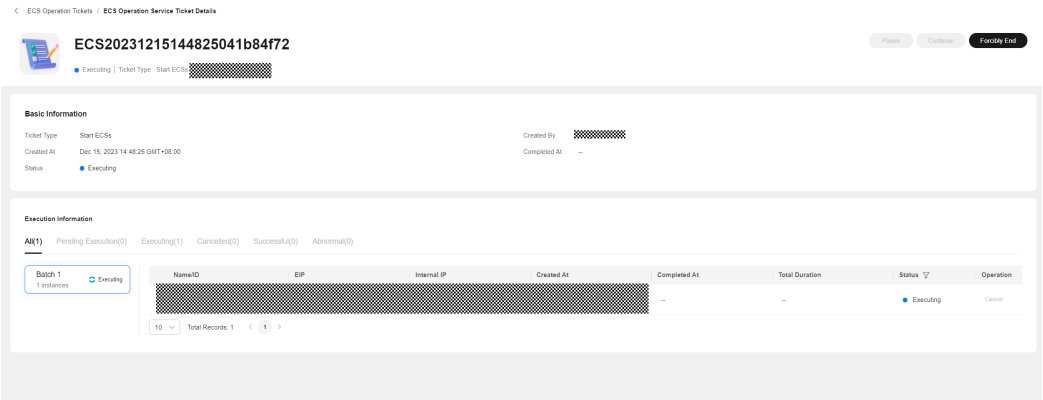
Step 7 In the **Confirm Execution** dialog box, click **OK**.

Figure 4-3 Confirming the execution



Step 8 View the execution result.

Figure 4-4 Viewing the result



----End

4.2.2 Stopping ECSs

Scenarios

Stop ECS instances in batches on Cloud Operations Center.

Precautions

Stopped instances cannot be selected.

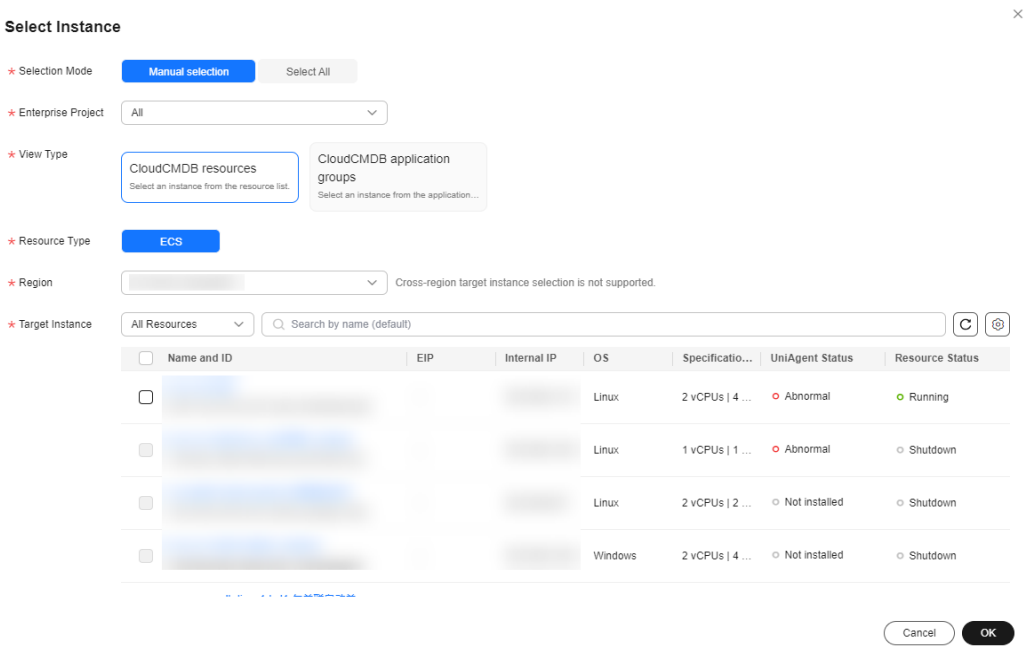
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**, and click **Shut Down ECSs** in **ECS Operations**.

Step 3 On the **Shut Down ECSs** page, click **Add**.

Figure 4-5 Selecting instances



Step 4 Select **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.

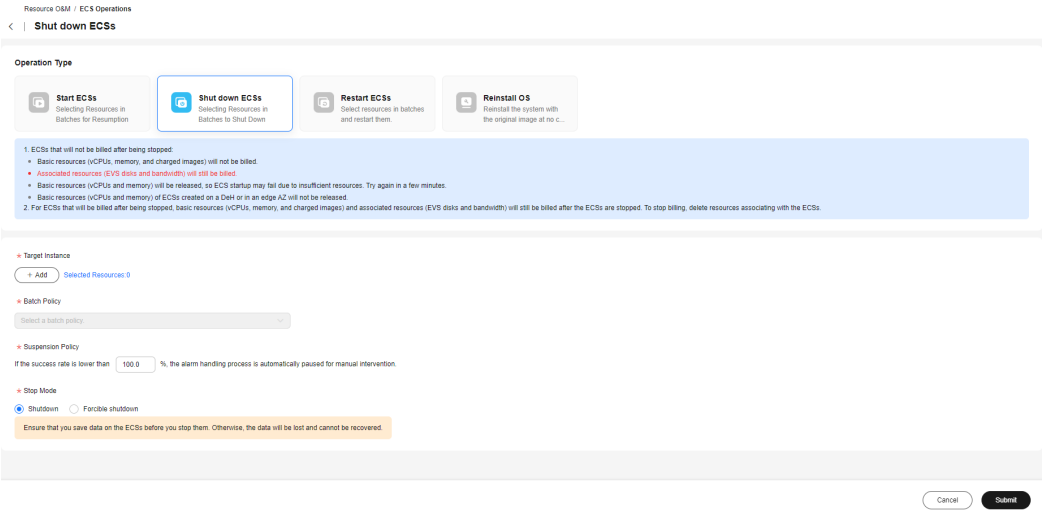
Step 5 Set **Suspension Policy**.

NOTE

- 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.
- The value range is from 0 to 100 and can be set to one decimal place.

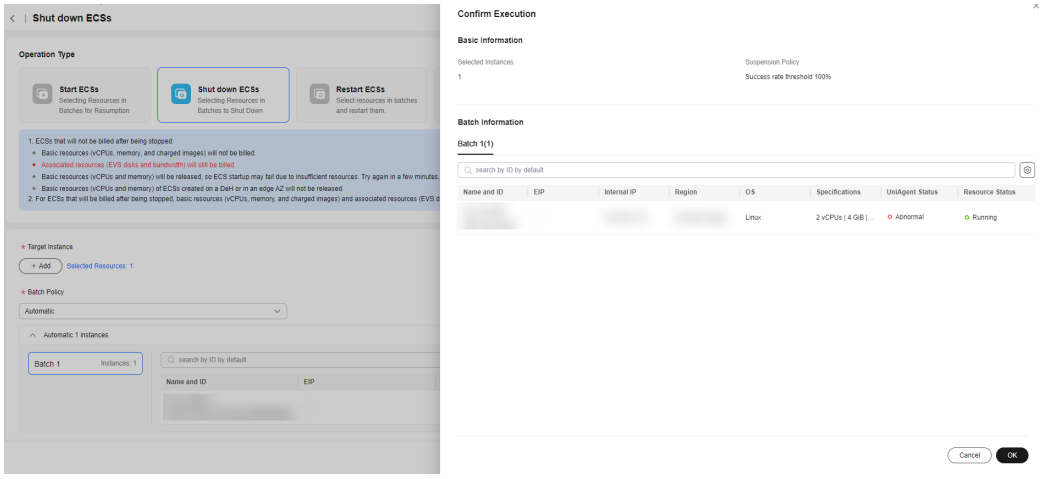
Step 6 Click **Submit**.

Figure 4-6 Stopping instances



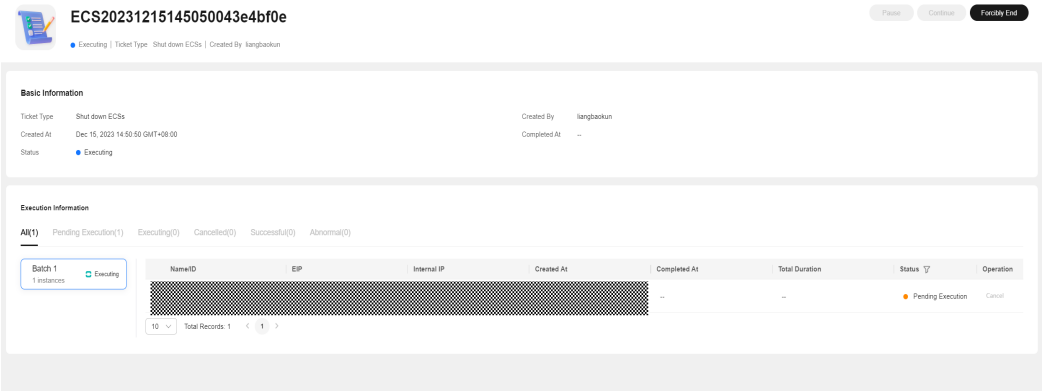
Step 7 In the **Confirm Execution** dialog box, click **OK**.

Figure 4-7 Confirming the execution



Step 8 View the execution result.

Figure 4-8 Viewing the result



----End

4.2.3 Restarting ECSs

Scenarios

Restart ECS instances in batches on COC.

Precautions

Stopped instances cannot be selected.

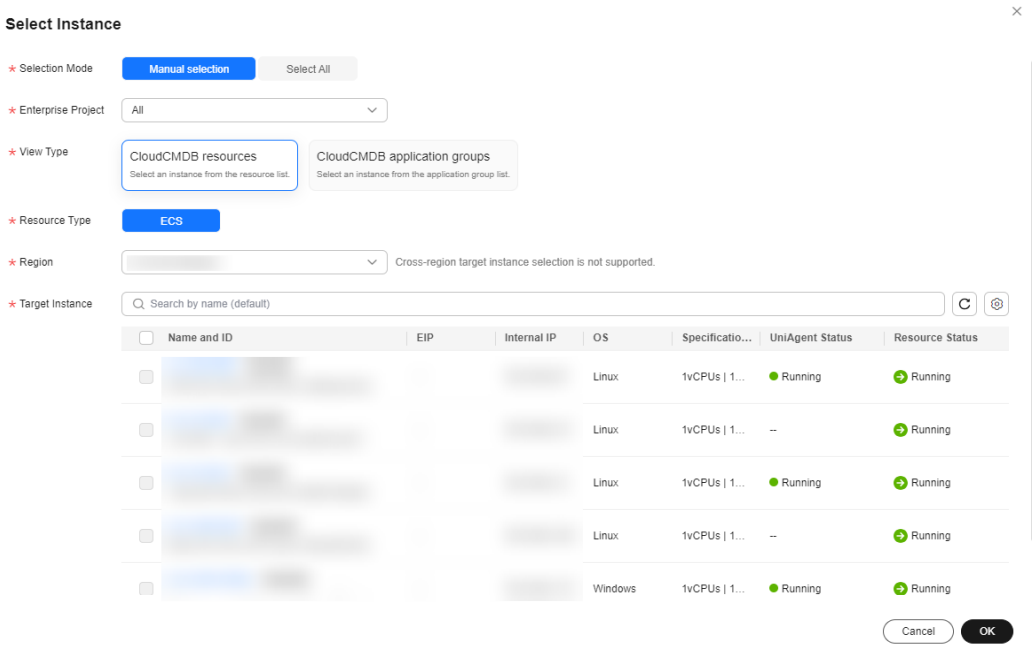
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**, and click **Restart ECSs** in **ECS Operations**.

Step 3 On the **Restart ECSs** page, click **Add**.

Figure 4-9 Selecting host instances



Step 4 Select **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 5 Set **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 range is from 0 to 100 and can be set to one decimal place.

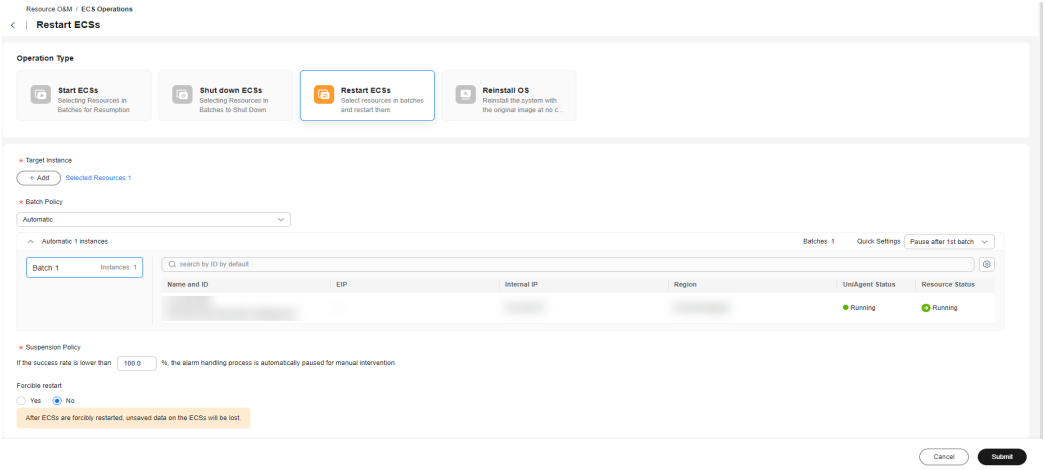
Step 6 Determine whether to forcibly restart ECSs.

NOTE

After **Forcible restart** is enabled, unsaved data on ECSs will be lost.

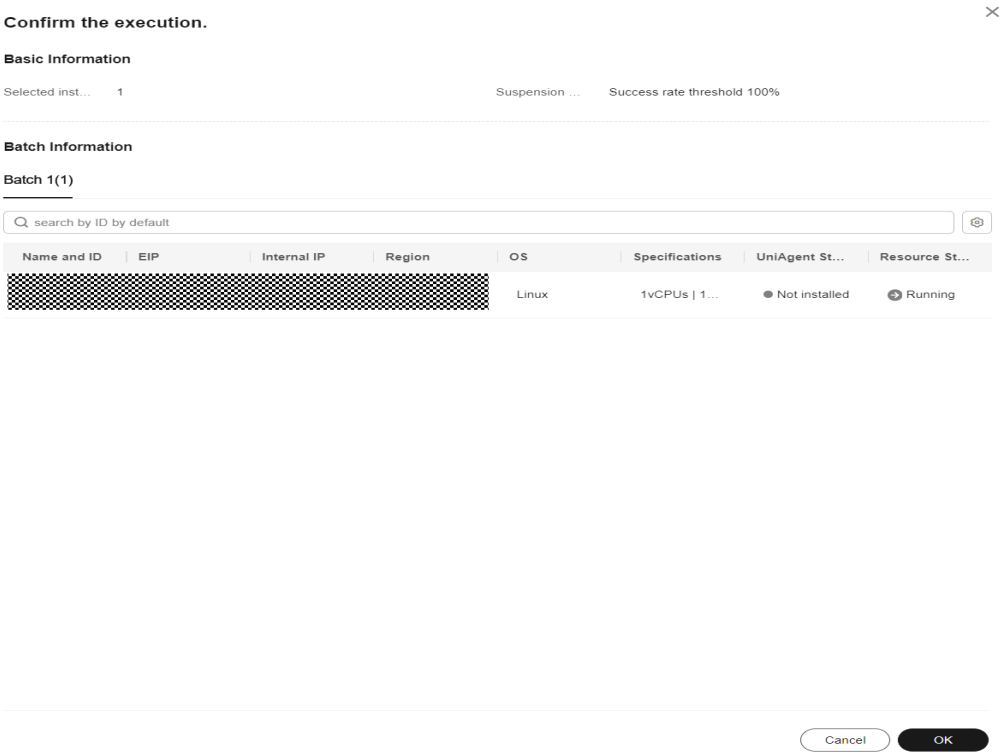
Step 7 Click **Submit**.

Figure 4-10 Restarting instances



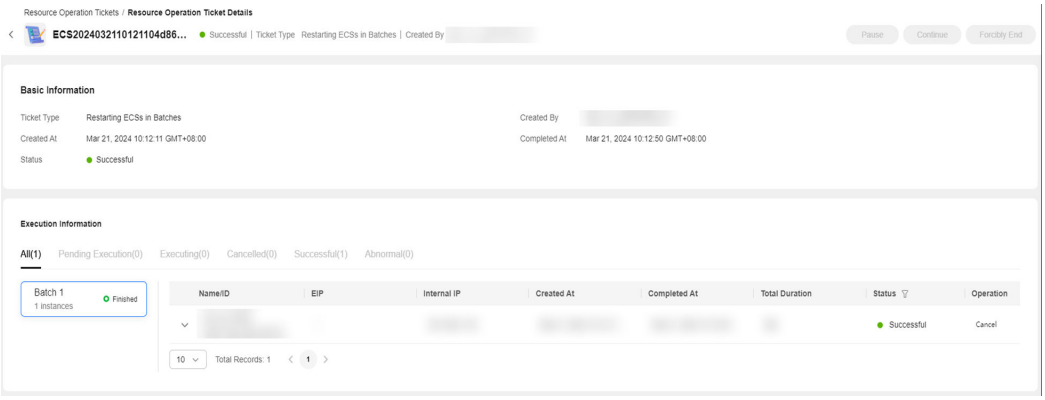
Step 8 In the **Confirm Execution** dialog box, click **OK**.

Figure 4-11 Confirming the execution



Step 9 View the execution result.

Figure 4-12 Viewing the result



----End

4.2.4 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

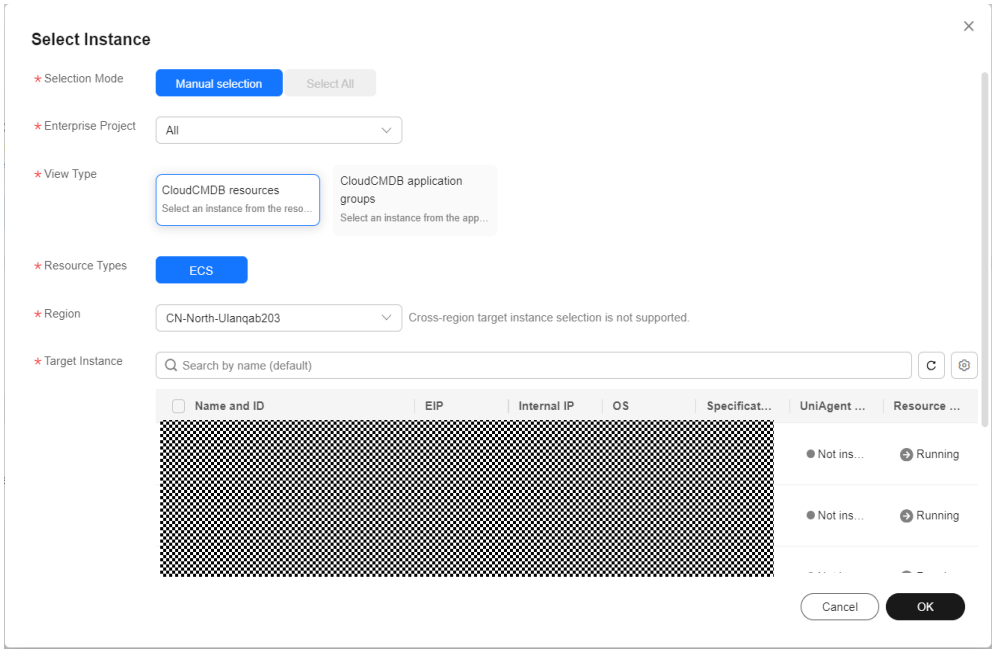
Step 1 Log in to **COC**.

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 4-13 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.

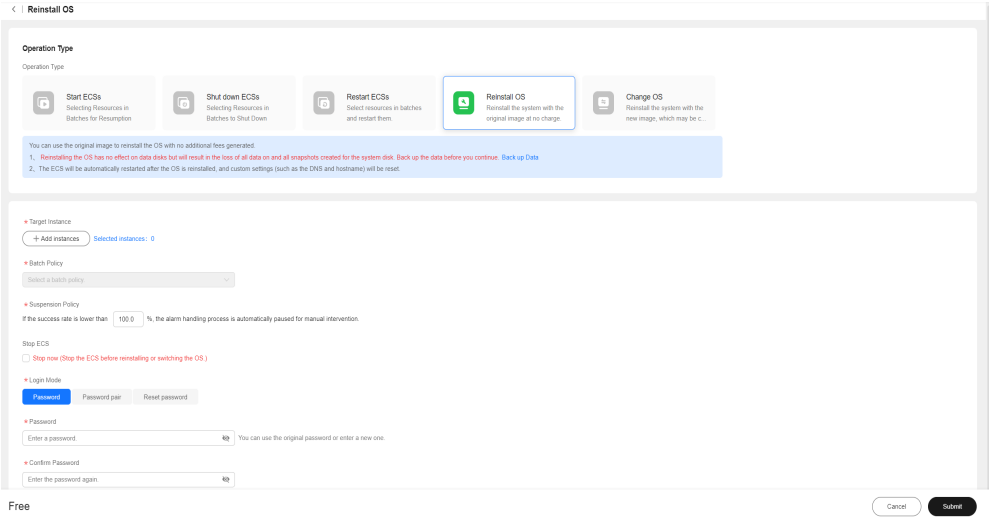
Step 7 Set the login mode.

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.

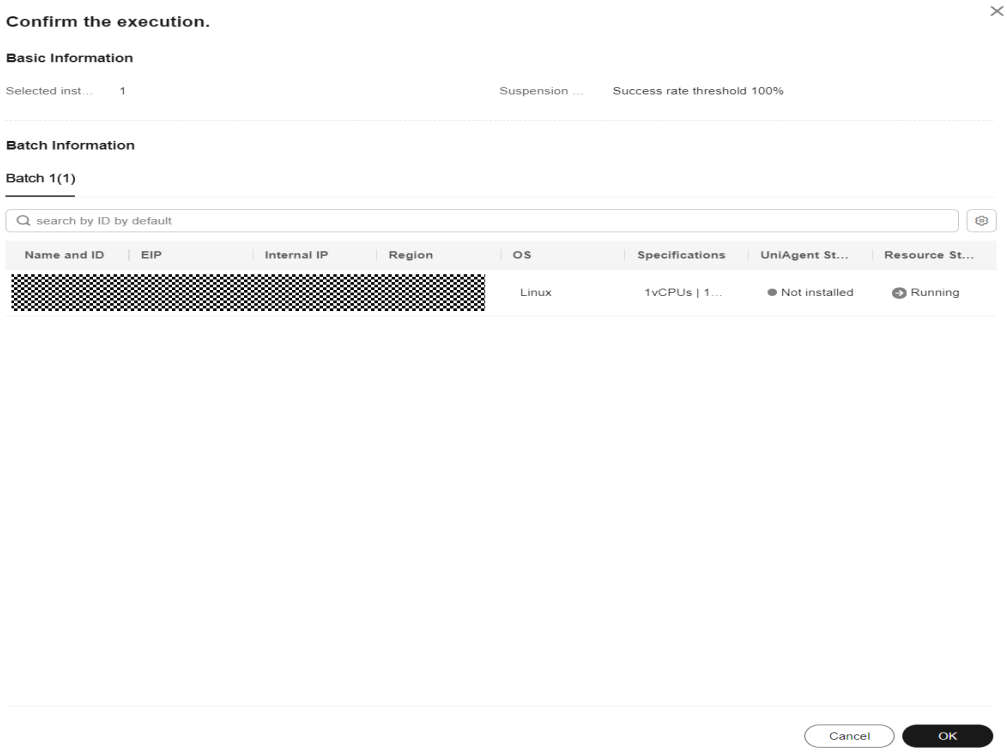
Step 8 Click **OK**.

Figure 4-14 Reinstalling OSs



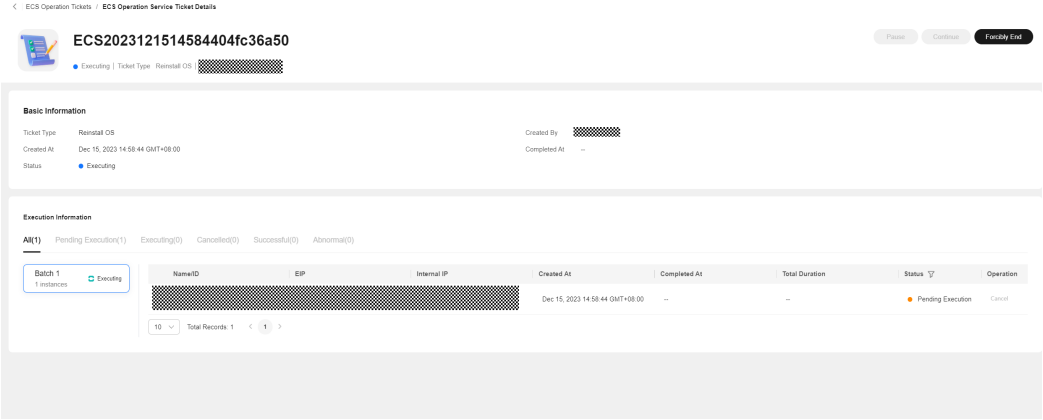
Step 9 Click **OK**.

Figure 4-15 Confirming the execution



Step 10 View the execution result.

Figure 4-16 Viewing the execution result



----End

4.2.5 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

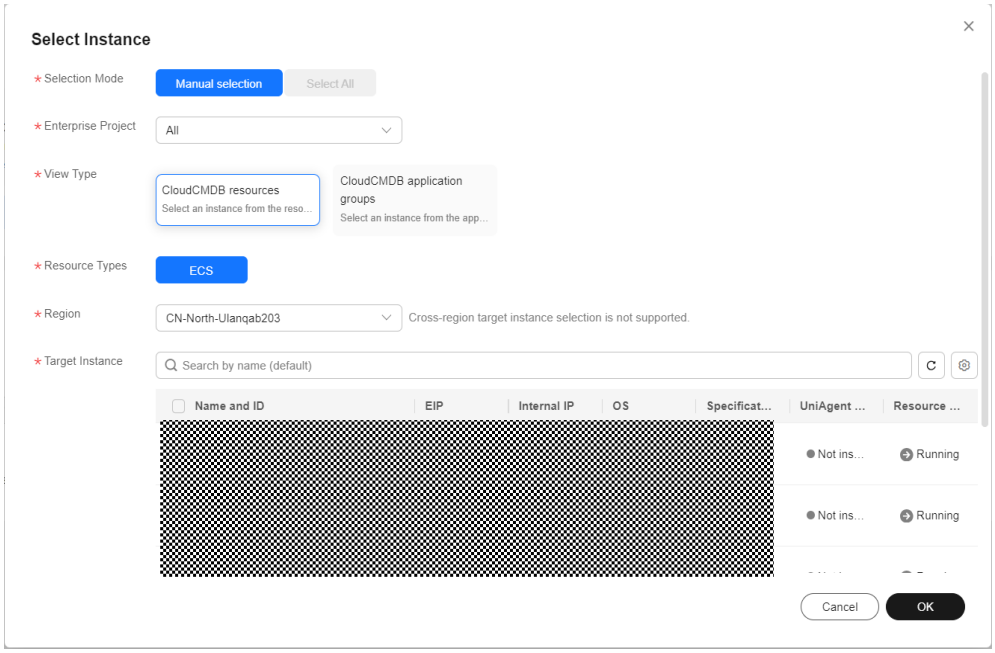
Step 1 Log in to **COC**.

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 4-17 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.

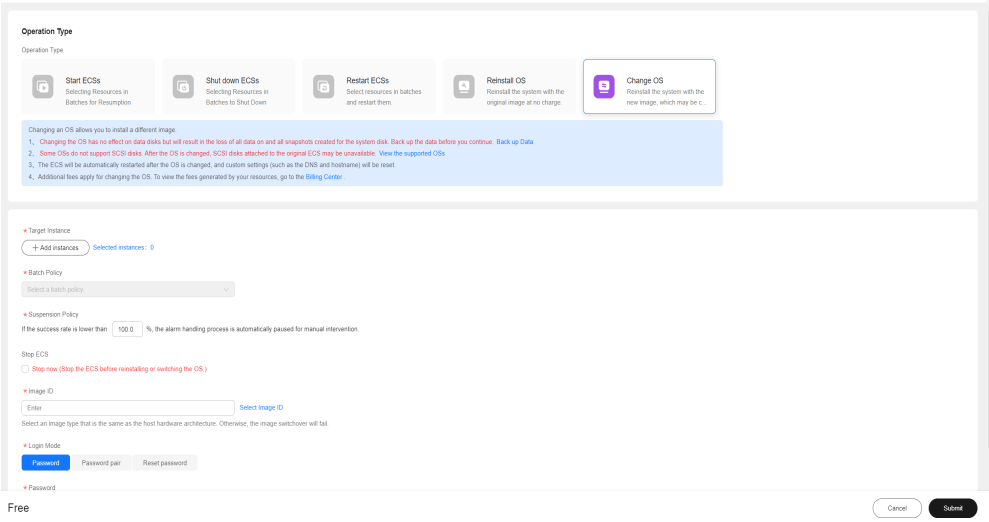
Step 8 Set the login mode.

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.

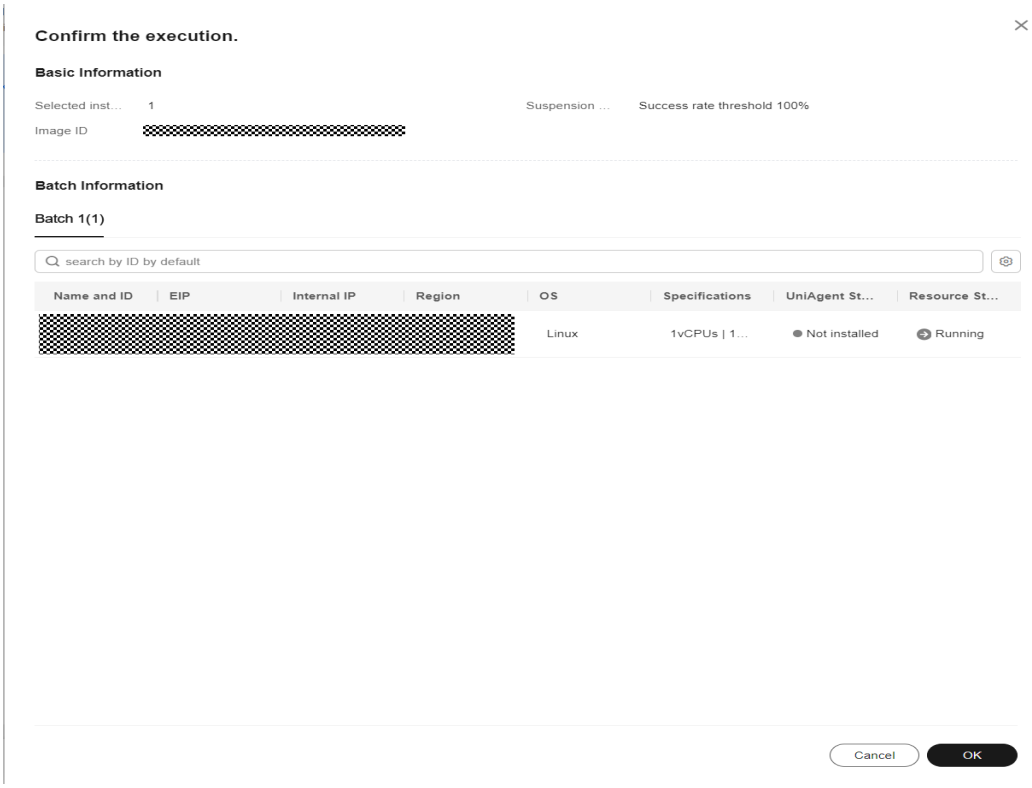
Step 9 Click **OK**.

Figure 4-18 Changing OSs



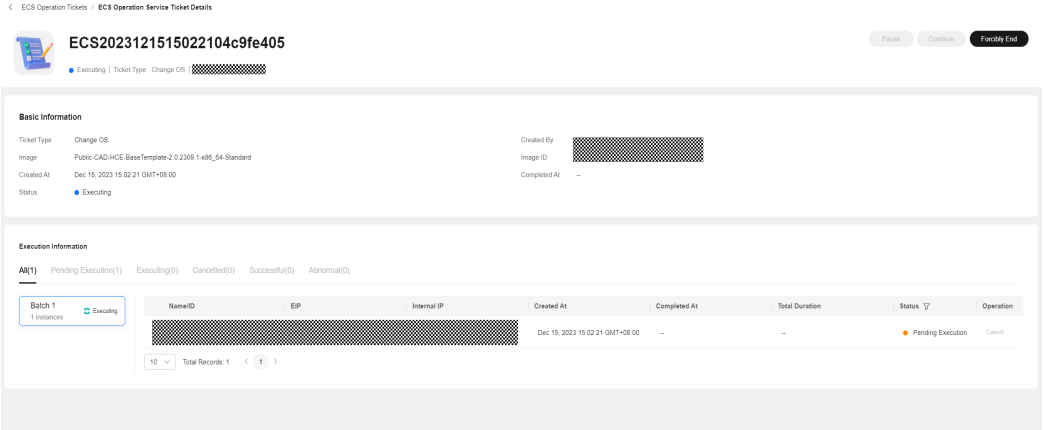
Step 10 Click **OK**.

Figure 4-19 Confirming the execution



Step 11 View the execution result.

Figure 4-20 Execution result



----End

5 Automated O&M

5.1 Patch Management

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

NOTE

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

- **Table 5-1** lists the OSs and versions supported by the patch management feature.
- **Table 5-2** lists the environment on which patch management depends.

Table 5-1 OSs and versions supported by the patch management feature

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

OS	Product
EulerOS	EulerOS 2.2 EulerOS 2.5 EulerOS 2.8 EulerOS 2.9 EulerOS 2.10

Table 5-2 Second-party packages on which the patch management feature depends

Type	Dependency Item
Python environment	Python (Python2 or Python3) DNF software packages (depended by Huawei Cloud EulerOS 2.0, CentOS 8.0 or later, and EulerOS 2.9 or later) YUM software packages (depended by Huawei Cloud EulerOS 1.1, versions earlier than CentOS 8.0 and EulerOS 2.9) lsb-release software package
Software package management tool	RPM

5.1.1 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.

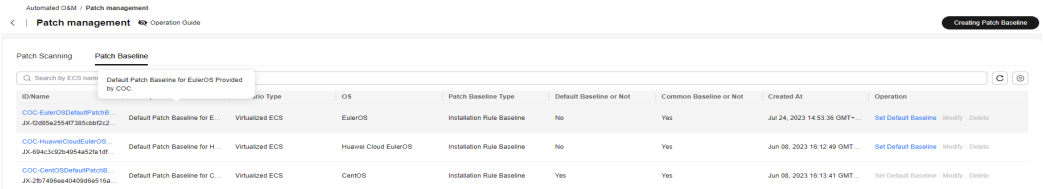
Procedure

Step 1 Log in to **COC**.

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

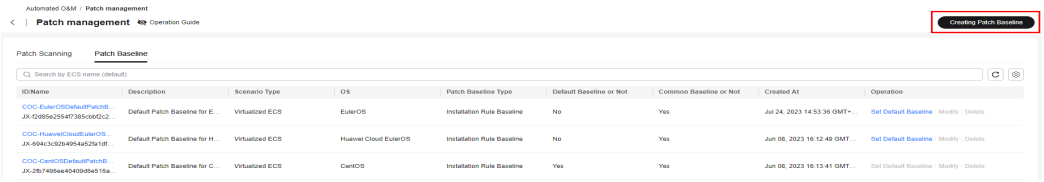
Step 3 Click the **Patch Baseline** tab to view the baseline list.

Figure 5-1 Patch baseline list



Step 4 Click **Creating Patch Baseline**.

Figure 5-2 Creating a patch baseline



Step 5 Set the patch baseline information as prompted.

Figure 5-3 Setting the patch baseline information

NOTE

- **Table 5-3** describes the parameters for creating an installation rule baseline.
- **Table 5-4** describes the parameters for creating a custom baseline.

Table 5-3 OS installation rule baseline

Field	Options	Description
Product	• Huawei Cloud EulerOS – All – Huawei Cloud EulerOS 1.1 – Huawei Cloud EulerOS 2.0 • CentOS – All – CentOS7.2 – CentOS7.3 – CentOS7.4 – CentOS7.5 – CentOS7.6 – CentOS7.7 – CentOS7.8 – CentOS7.9 – CentOS8.0 – CentOS8.1 – CentOS8.2 • EulerOS – 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	• All • Security • Bugfix • Enhancement • Recommended • Newpackage	Category of patches. The patches of the selected category are scanned and repaired.

Field	Options	Description
Severity	• All • Critical • Important • Moderate • Low • None	Severity level of patches. The patches of the selected severity level can be scanned and repaired.
Automatic Approval	• Approve the patch after a specified number of days. • Approve patches released before the specified date.	Automatically approve patches that meet specified conditions.
Specified Days	0 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	• 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	The formats of the software packages of approved patches and rejected patches are as follows: 1. The format of a complete software package name: *example*-**1.0.0-1.r1.hce2.x86_64**. 2. The format of the software package name that contains a single wildcard: *example*-**1.0.0*.x86_64**.

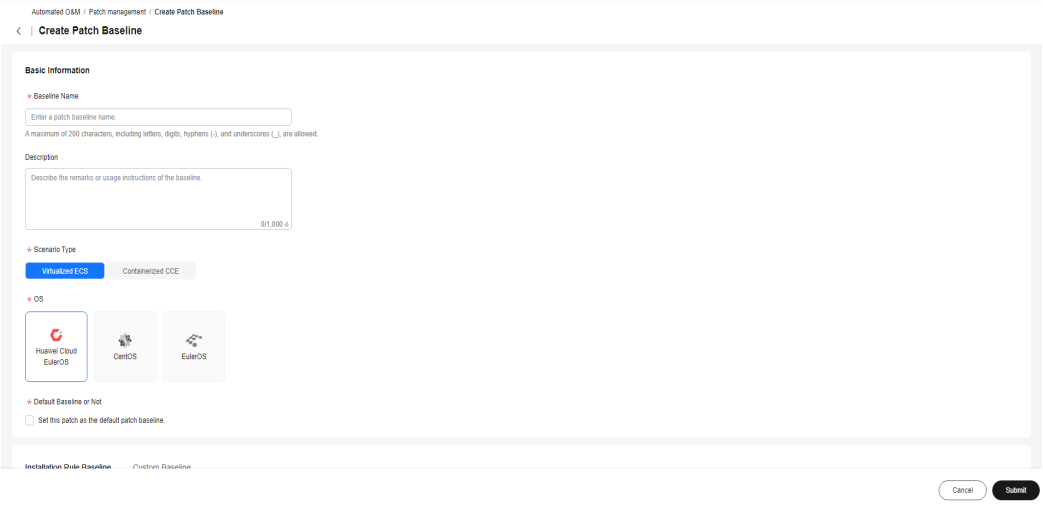
Table 5-4 Customized installation rule

Field	Options	Description
Product	● Huawei Cloud EulerOS – All – Huawei Cloud EulerOS 1.1 – Huawei Cloud EulerOS 2.0 ● CentOS – All – CentOS 7.2 – CentOS 7.3 – CentOS 7.4 – CentOS 7.5 – CentOS 7.6 – CentOS 7.7 – CentOS 7.8 – CentOS 7.9 – CentOS 8.0 – CentOS 8.1 – CentOS 8.2 ● EulerOS – All – EulerOS 2.2 – EulerOS 2.5 – EulerOS 2.8 – EulerOS 2.9 – EulerOS 2.10	Product 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	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. 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 5-4 Creating a customized patching baseline



----End

5.1.2 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.

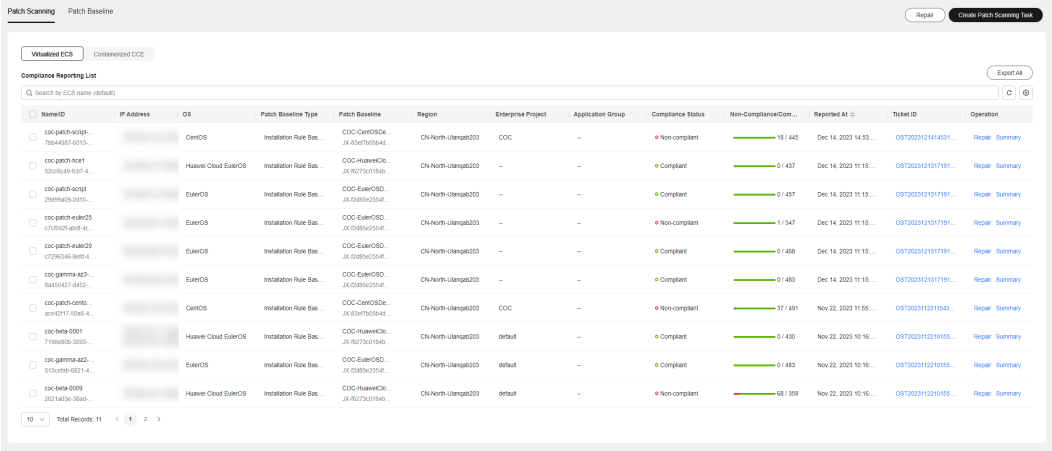
Procedure

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**.

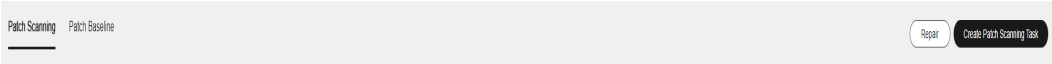
Step 3 On the displayed page, click **Patch Scanning** to view the compliance report list.

Figure 5-5 Compliance report list



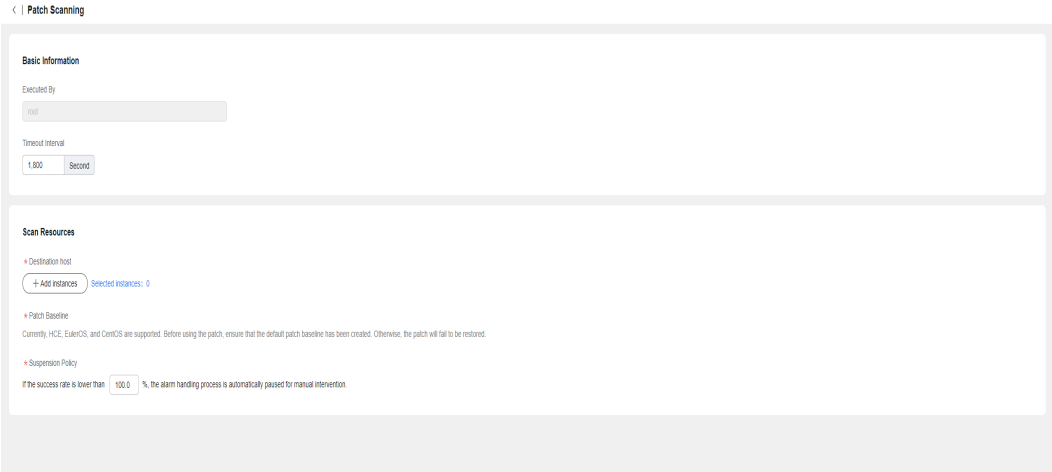
Step 4 Click **Create Patch Scanning Task**.

Figure 5-6 Creating a patch scanning task



Step 5 Click **Add Instances**.

Figure 5-7 Selecting instances



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

Figure 5-8 Selecting the target ECS instances

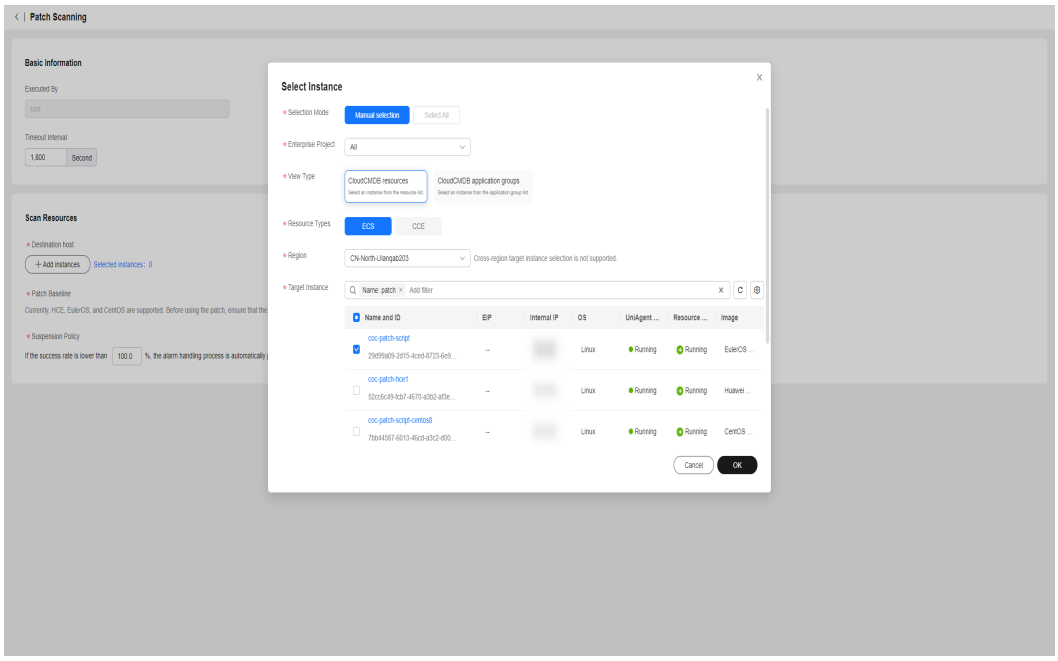
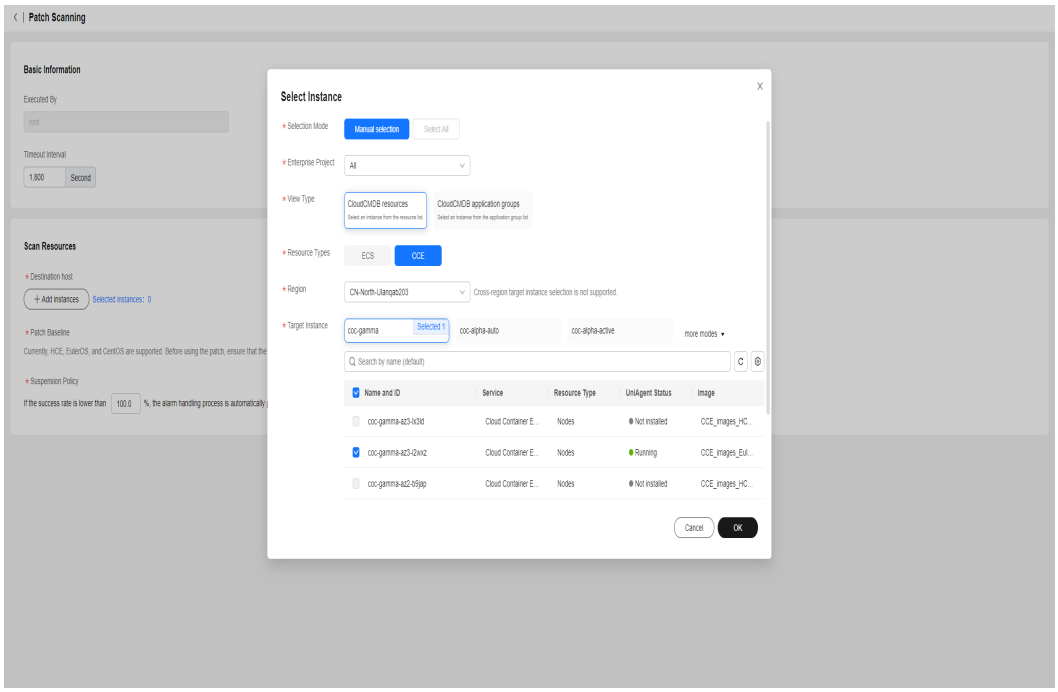


Figure 5-9 Selecting the target CCE instances

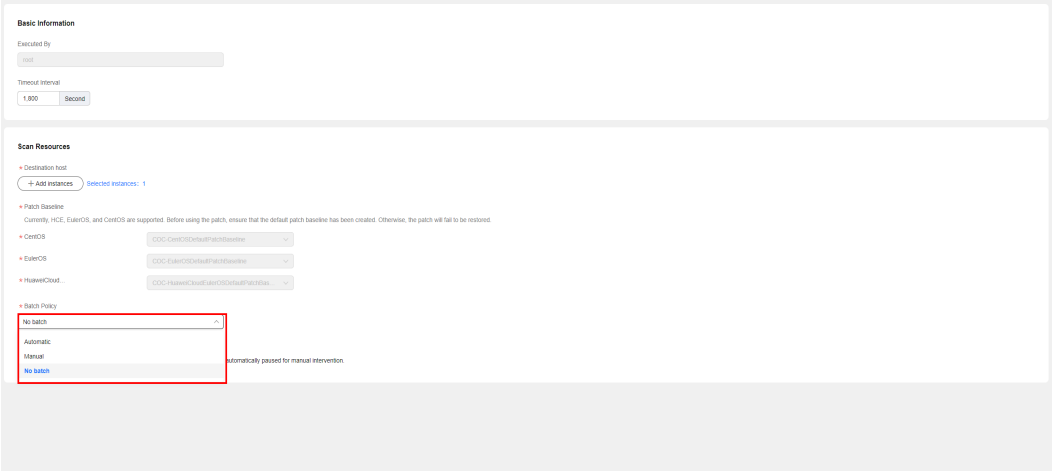


Step 7 Set the batch policy.

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.

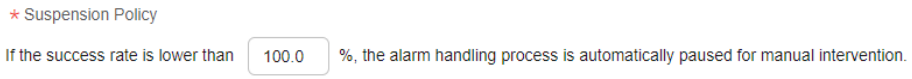
Figure 5-10 Selecting batch policies



Step 8 Configure a suspension policy.

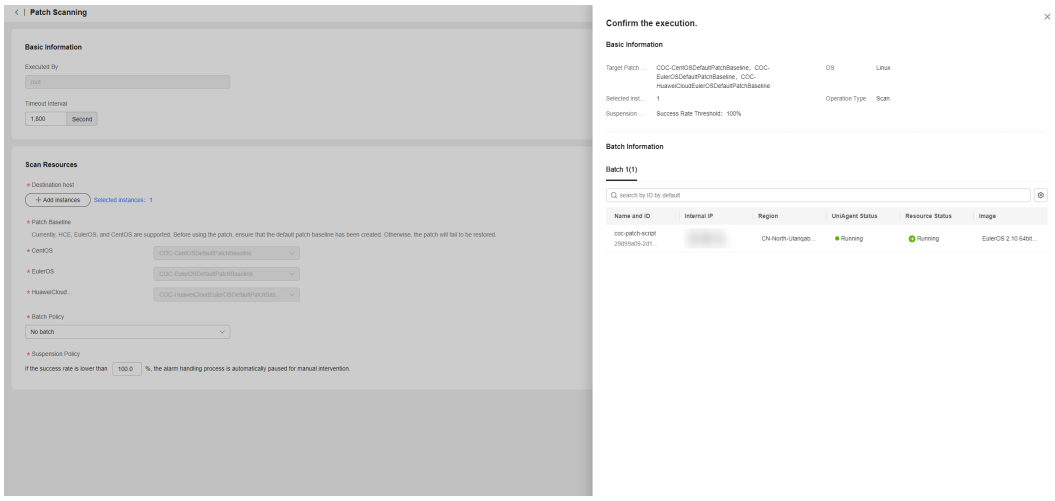
Suspension threshold: You can set the execution success rate. When the number of failed hosts reach the pre-defined suspension threshold, the service ticket status become abnormal and the service ticket will stop being executed.

Figure 5-11 Suspension policy



Step 9 Click **Submit**.

Figure 5-12 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 5-13 Service ticket details

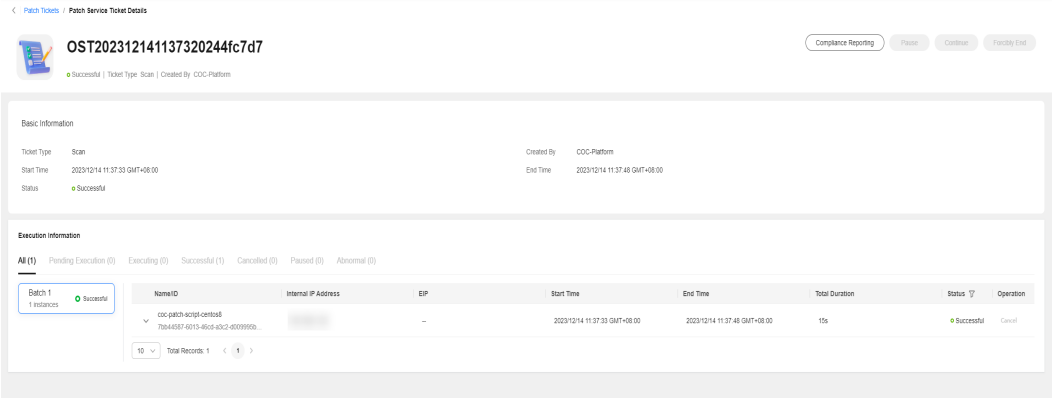
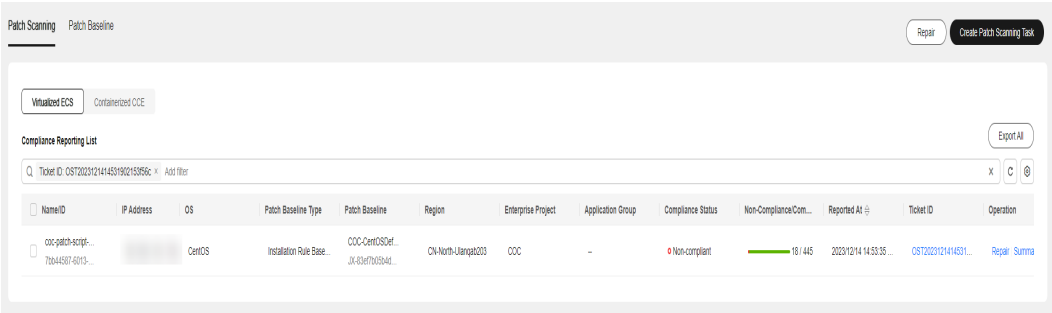


Figure 5-14 Compliance report list



----End

5.1.3 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 COC.

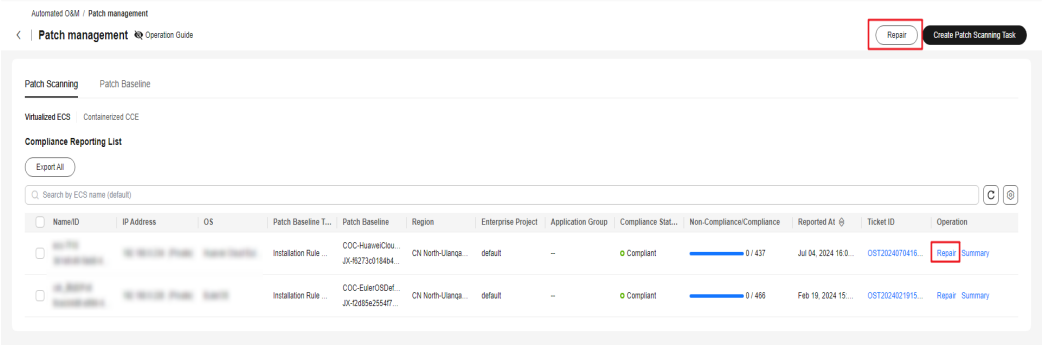
Procedure

Step 1 Log in to **COC**.

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

Step 3 Select the instance whose patch needs to be repaired and click **Repair**.

Figure 5-15 Select the target instances

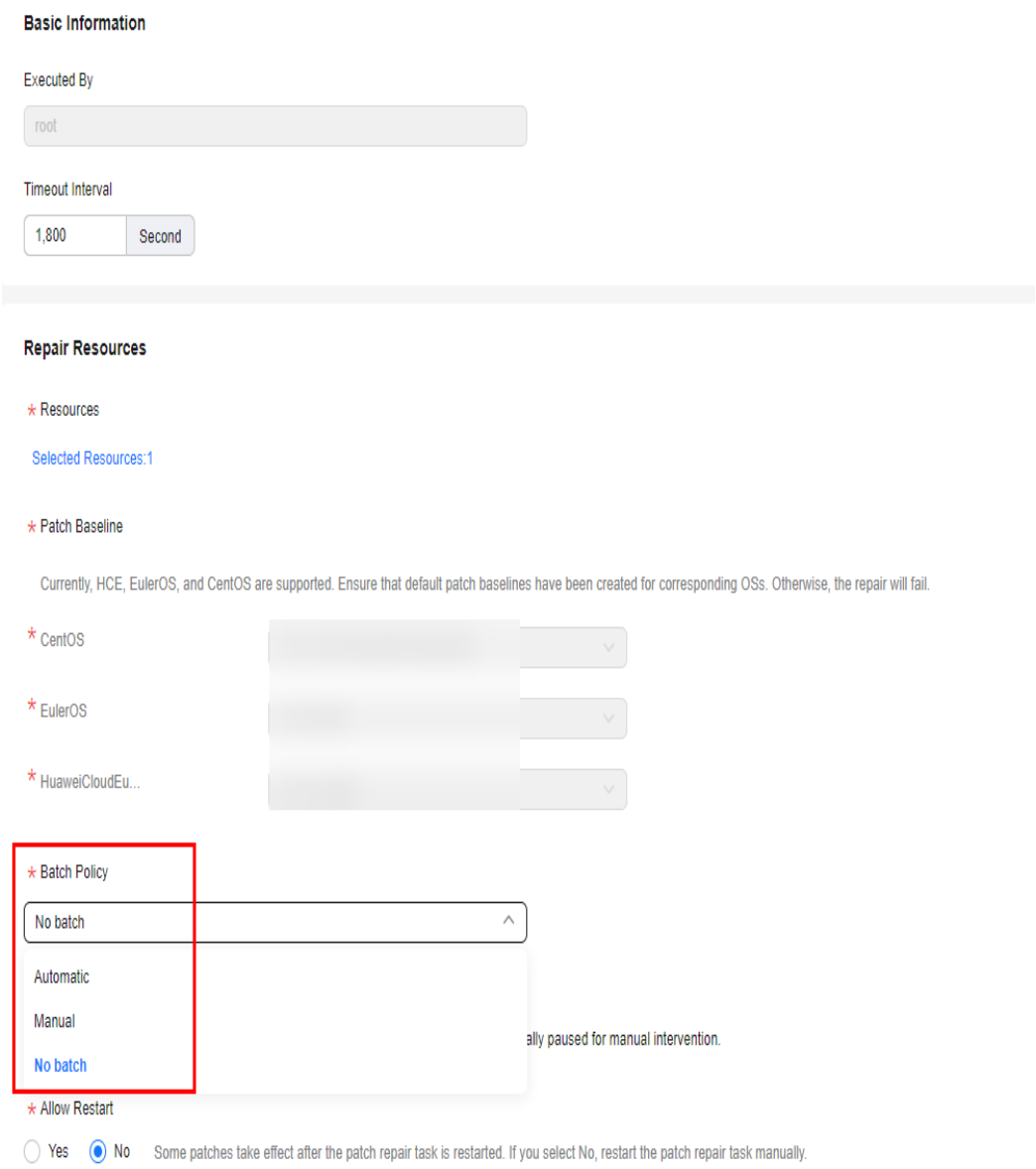


Step 4 Set the batch policy.

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.

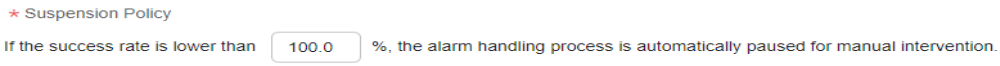
Figure 5-16 Selecting the batch policy



Step 5 Set a suspension policy.

Suspension threshold: You can set the execution success rate. When the number of failed hosts reaches the pre-set suspension threshold figure, the service ticket status becomes abnormal and the service ticket stops being executed.

Figure 5-17 Suspension policy



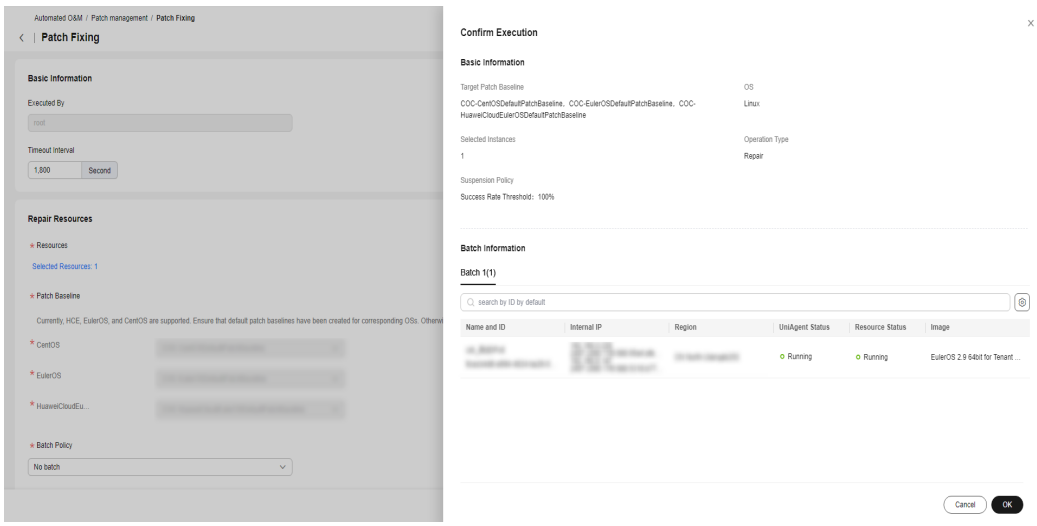
Step 6 Set whether to allow restart.

NOTE

If you select **No**, you need to restart the system at another time due to some patches only taking effect after the system is restarted.

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

Figure 5-18 Execution information page



----End

5.1.4 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

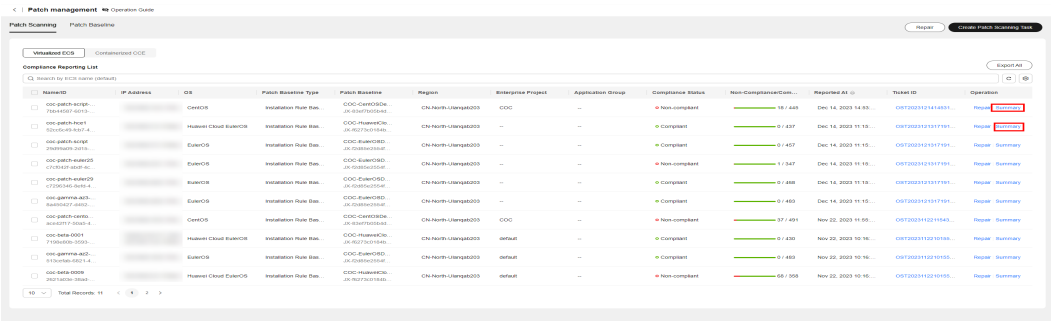
The patch compliance report retains only the scan or repair record at the latest time.

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 5-19 Patch management

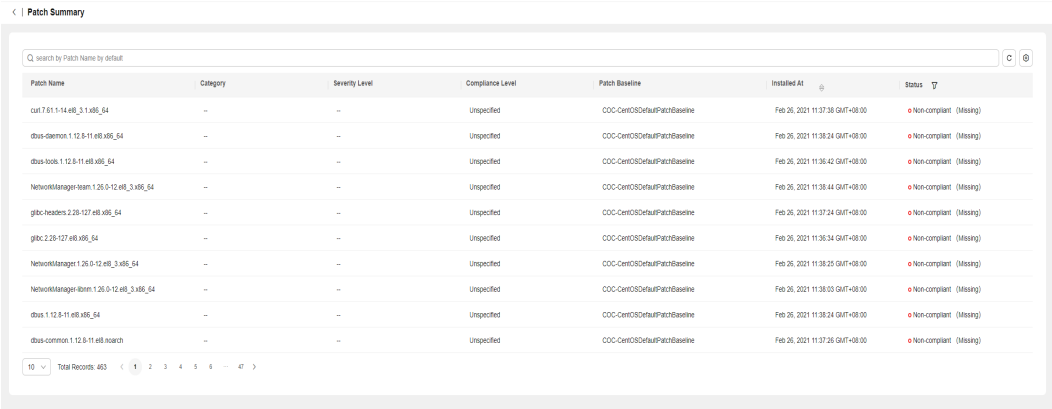


Step 3 Select the patch compliance report to be viewed and click **Summary** in the **Operation** column.

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 5-20 Patch compliance report summary



----End

5.2 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).

5.2.1 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

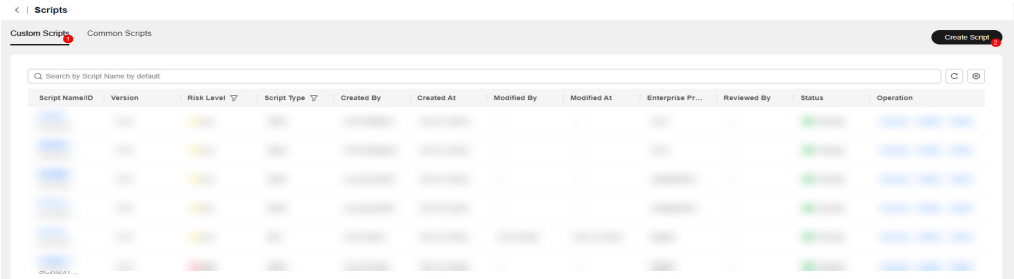
Confirm and complete the risk level of the script content.

Procedure

Step 1 Log in to **COC**.

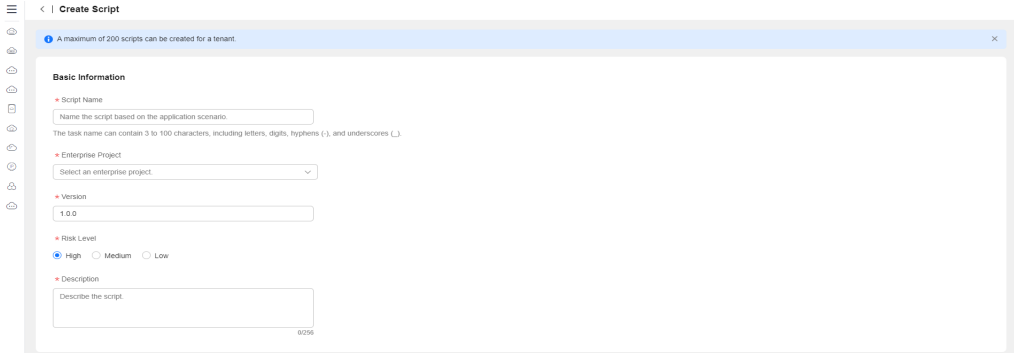
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Scripts**. On the displayed **Scripts** page, click the **Custom Scripts** tab and click **Create Script**.

Figure 5-21 Clicking **Create Script**



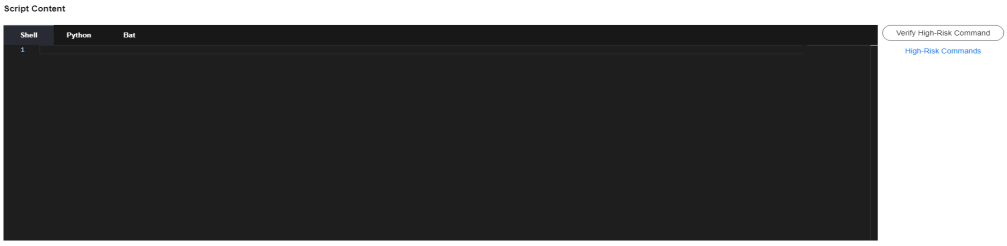
Step 3 Enter the basic script information.

Figure 5-22 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 5-23 Entering the script content



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

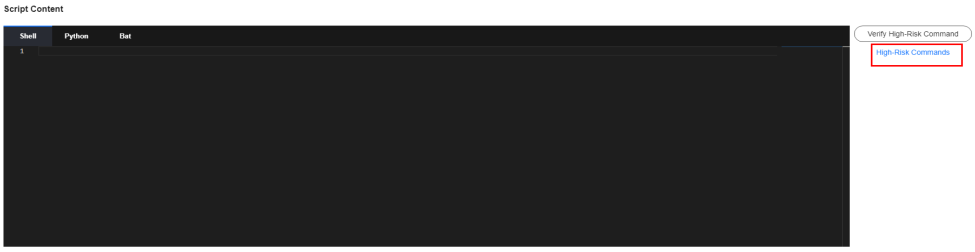
- Verification scope: the high-risk commands involved in the detection. You can click **High-Risk Commands** to view the verification rules.

- 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

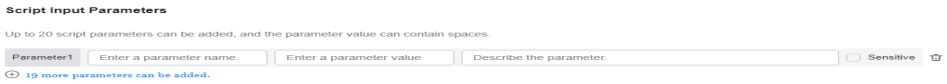
The result of high-risk command verification is used only as a reference for grading the script risk level. The system does not forcibly require the consistency between script risk level and the verification result. Evaluate the risk level based on the actual service impact.

Figure 5-24 Verifying high-risk commands



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

Figure 5-25 Entering script input parameters

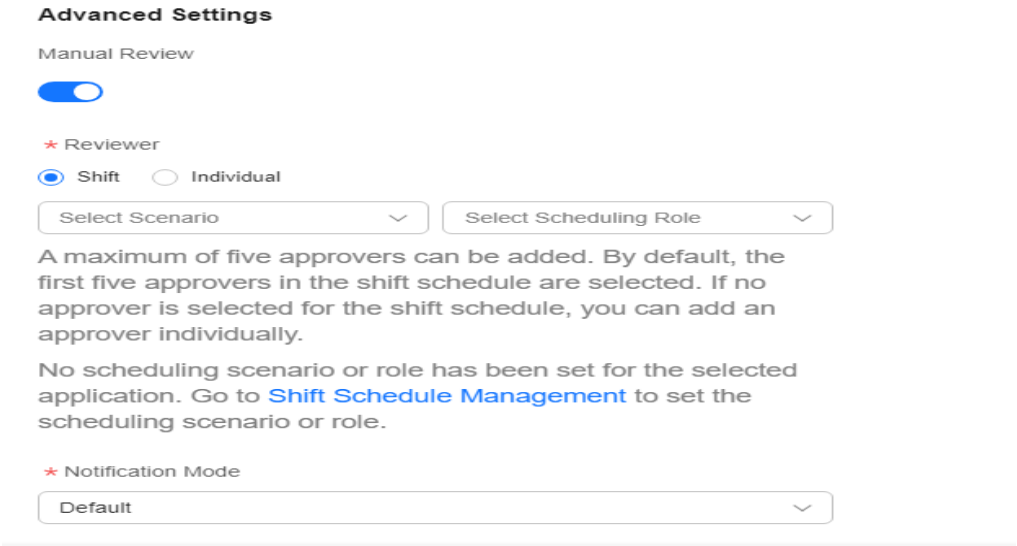


NOTE

Sensitive: parameters are anonymized and encrypted for storage.

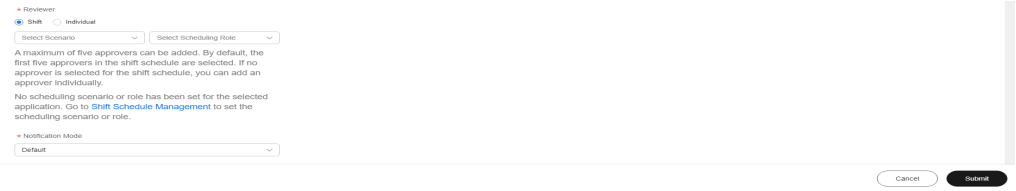
Step 7 Enable **Manual Review**. This switch is enabled automatically for high-risk scripts.

Figure 5-26 Selecting the reviewer and the notification mode



Step 8 Click **Submit**.

Figure 5-27 Click **Submit**.



----End

5.2.2 Managing Custom Scripts

The custom script modification and deletion capabilities are provided.

Scenarios

Modify and delete a custom script to be executed on COC.

Precautions

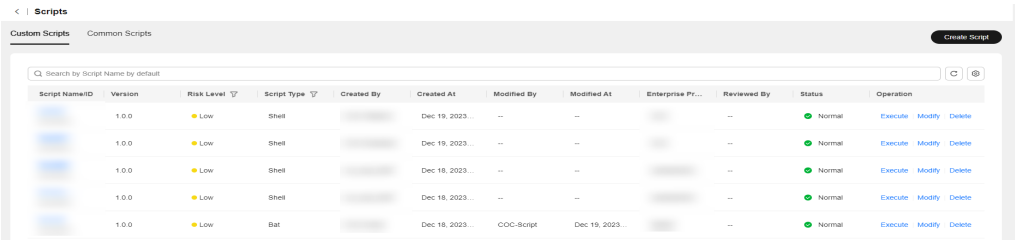
Confirm and complete the risk level of the script content when modifying a script.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-28 Script management



Step 3 Select the operation to be performed 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 5-29 Modifying and deleting a script

----End

5.2.3 Executing Custom Scripts

The custom script execution capability is provided.

Scenarios

Execute a custom script on COC.

Precautions

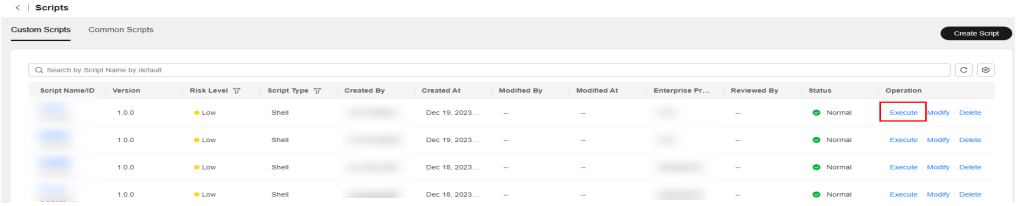
Ensure that you have the permission on the component to which the target VM belongs when executing a script.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-30 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 **Creating a Parameter**.

Figure 5-31 Manually entering script parameters

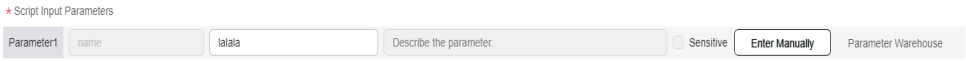


Figure 5-32 Selecting script parameters from the parameter warehouse

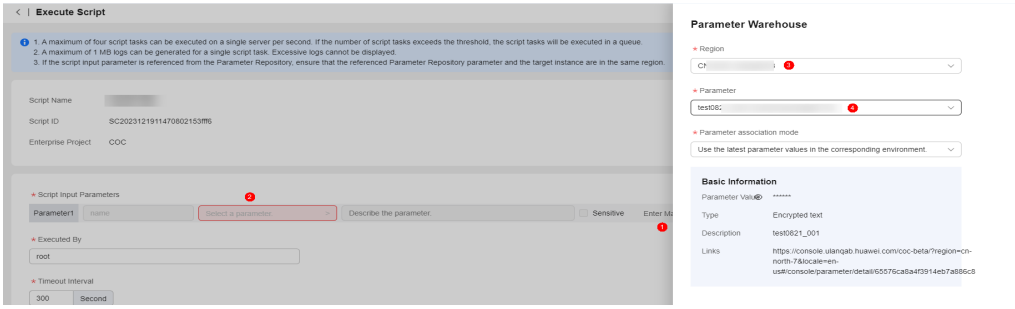


Table 5-5 Parameter association modes

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.

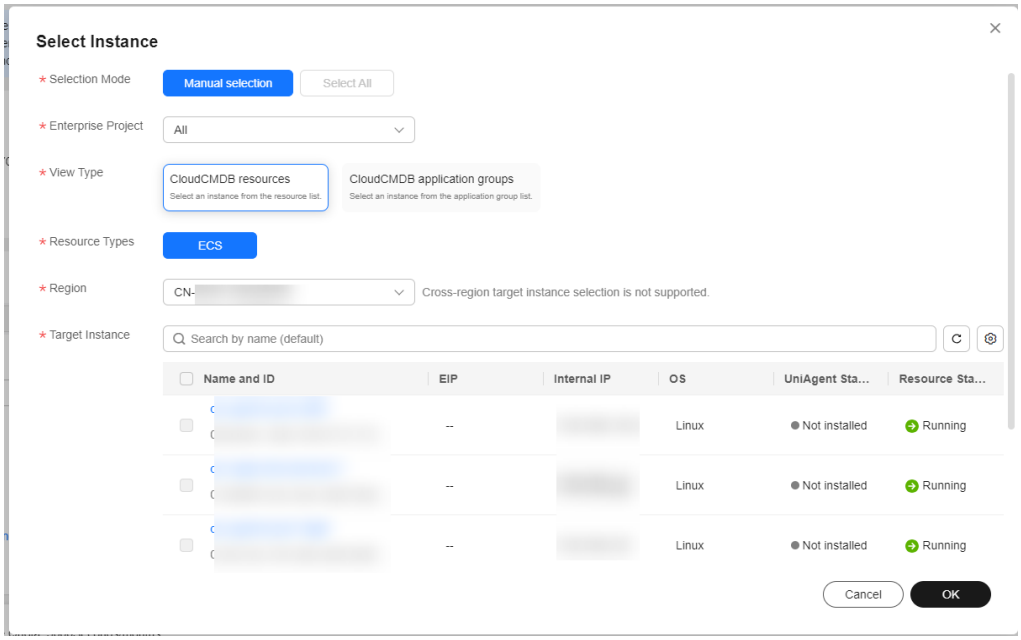
NOTE

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

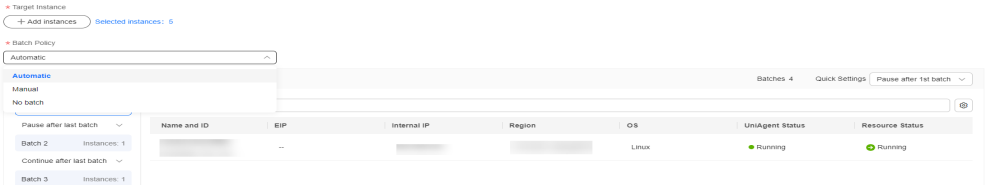
Figure 5-33 Selecting target instances



Step 6 Select **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 target instances are in the same batch.

Figure 5-34 Selecting a batch policy



Step 7 Set **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 5-35 Setting a suspension policy

Step 8 Click **Submit**.

Figure 5-36 Submitting the request

----End

5.2.4 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

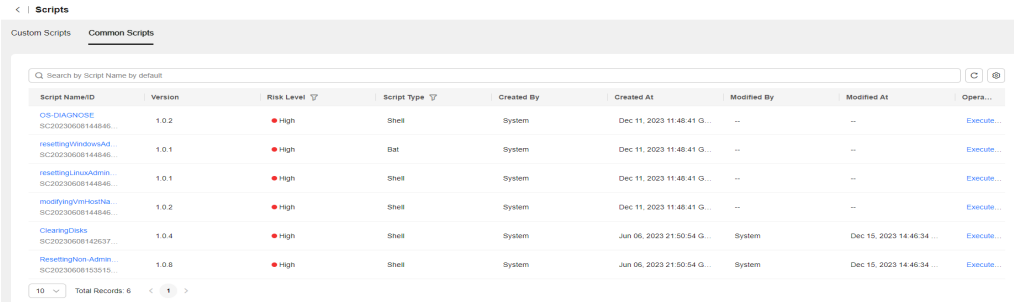
Ensure that you have the permission on the component to which the target VM belongs when executing a script.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-37 Selecting the target common script to be executed



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 selected from 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 **Creating a Parameter**.

Figure 5-38 Manually entering script parameters

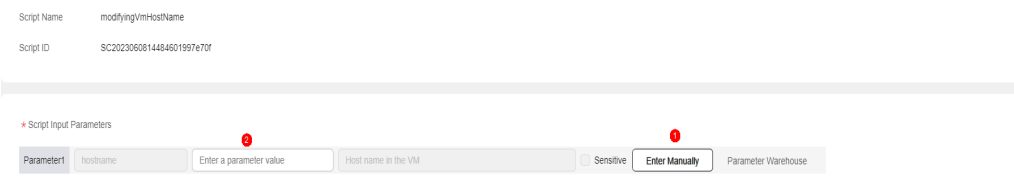


Figure 5-39 Selecting script parameters from repository

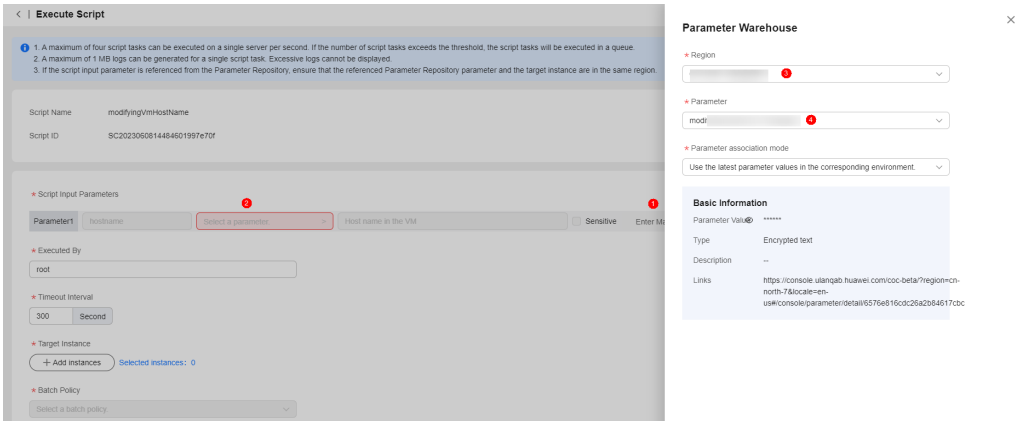
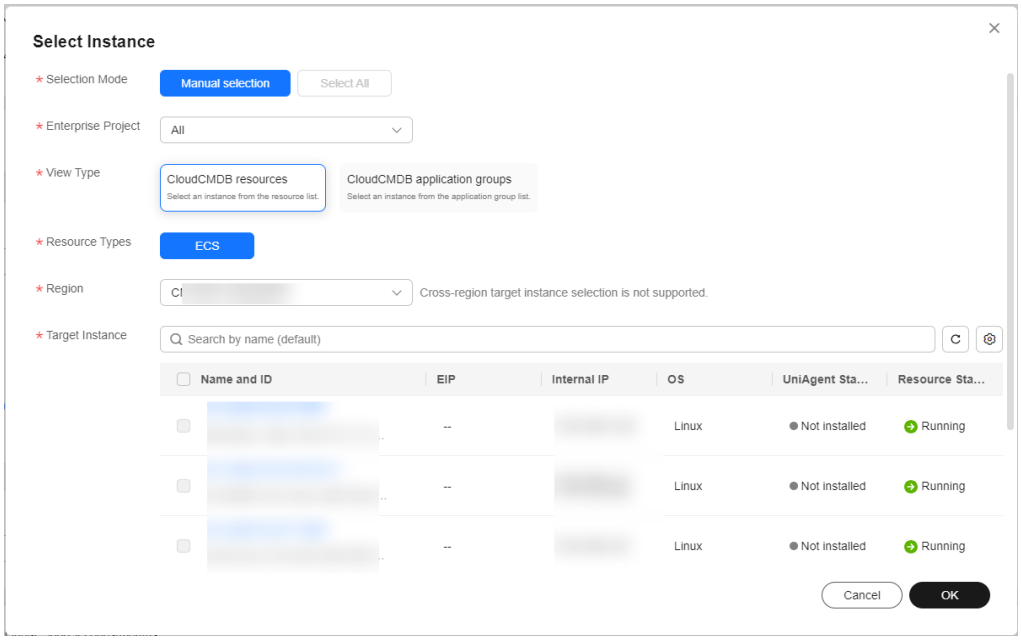


Table 5-6 Parameter association modes

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

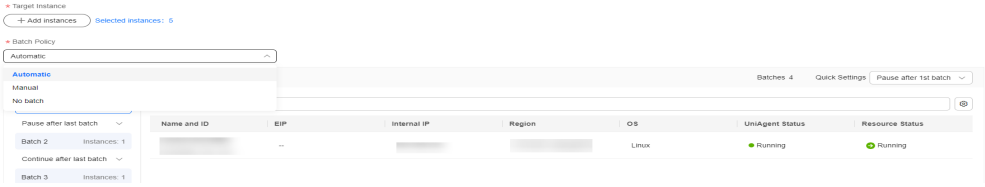
Figure 5-40 Selecting target instances



Step 5 Select **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 target instances are in the same batch.

Figure 5-41 Selecting a batch policy



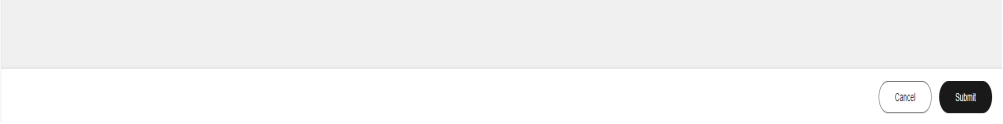
Step 6 Set **Suspension Policy**.

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 5-42 Setting a suspension policy

Step 7 Click **Submit**.

Figure 5-43 Submitting the request



----End

5.3 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).

5.3.1 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

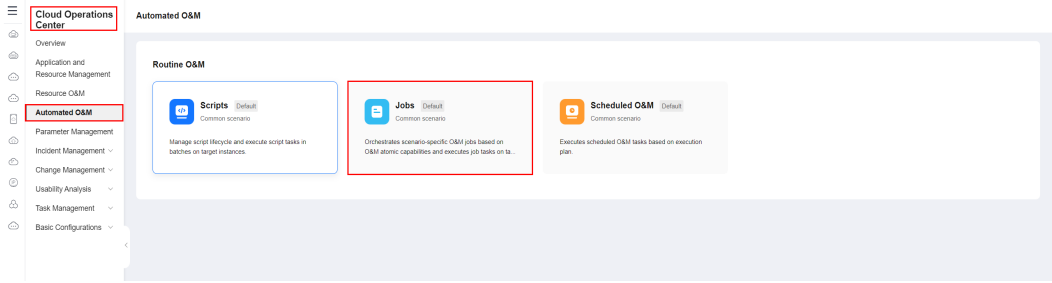
Before executing a common job, ensure that you have the resource permissions of target instances.

Procedure

Step 1 Log in to **COC**.

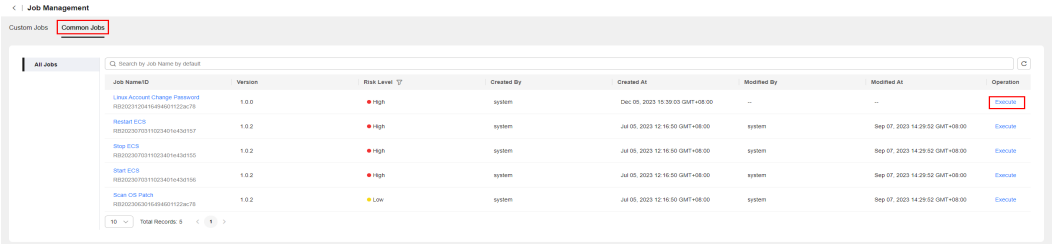
Step 2 In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-44 Clicking **Jobs**



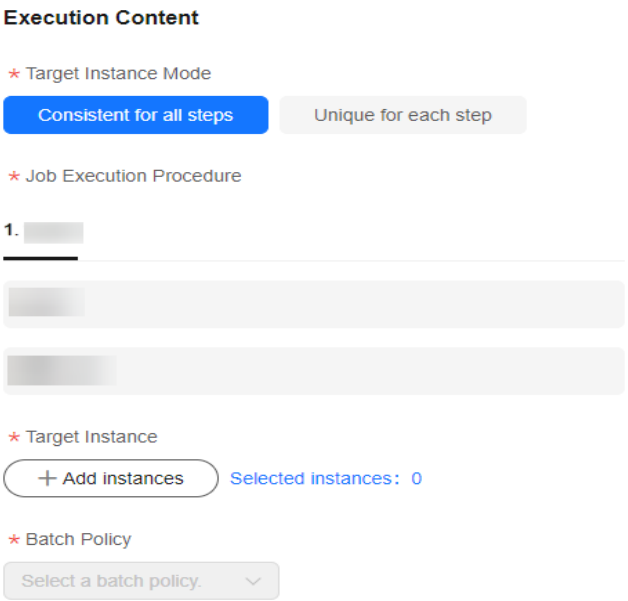
Step 3 Click the **Common Jobs** tab, click **All Jobs**, locate the public job to be executed, and click **Execute** in the **Operation** column.

Figure 5-45 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 5-46 Entering basic execution information



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

Table 5-7 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 5-47 Consistent for all steps

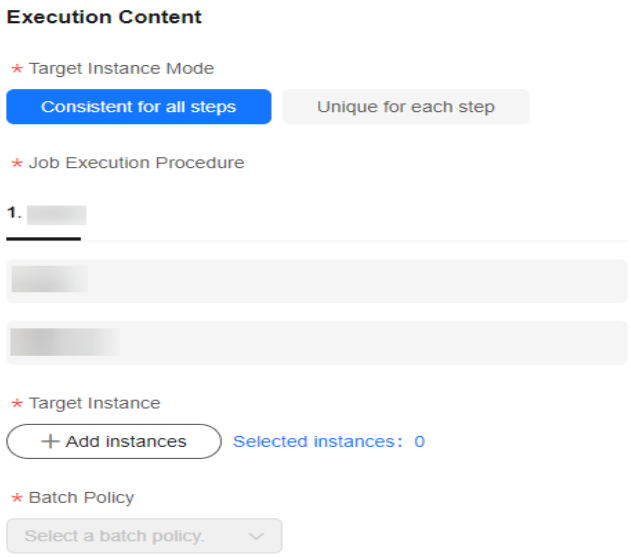
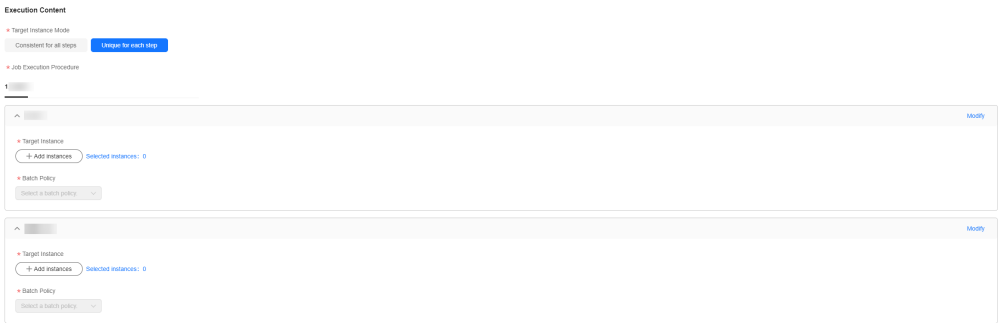
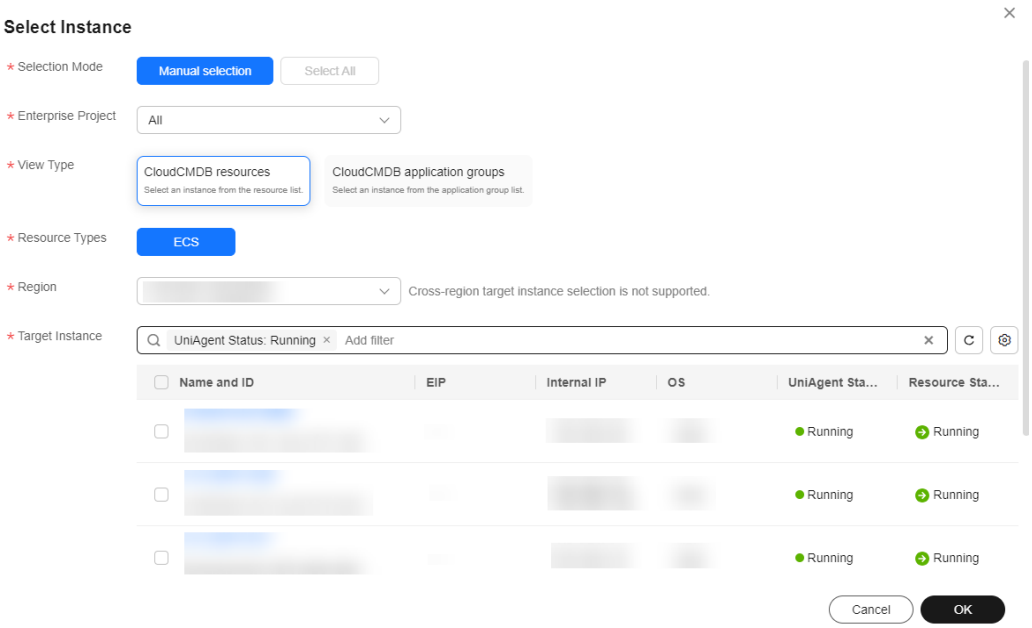


Figure 5-48 Unique for each step



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**.

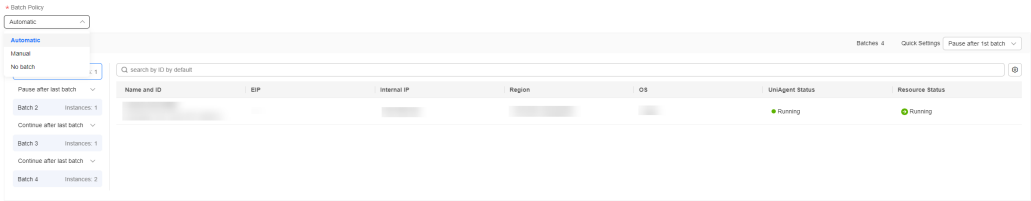
Figure 5-49 Selecting target instances



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 5-50 Selecting a batch policy

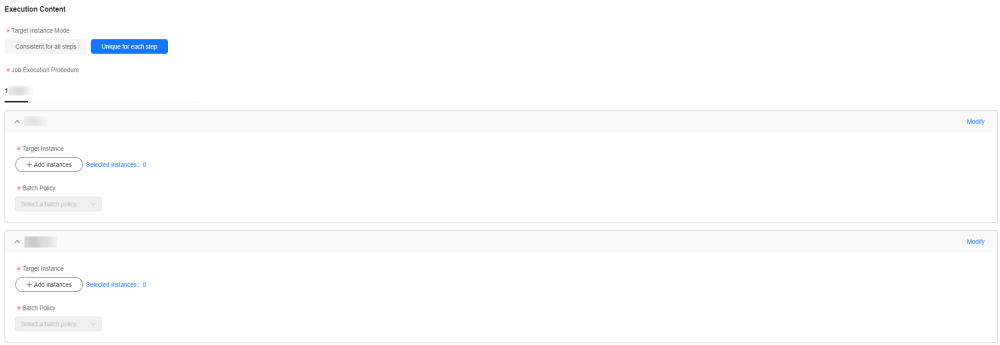


Step 8 Click **Submit** to execute the common job. The **Job Ticket Details** page is displayed. View the execution status of jobs and each batch on the details page.

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 5-51 Job ticket details



----End

5.3.2 Creating a Custom Job

The custom job creation and step compilation capabilities are provided.

Scenarios

Create a custom job on Cloud Operations Center.

Precautions

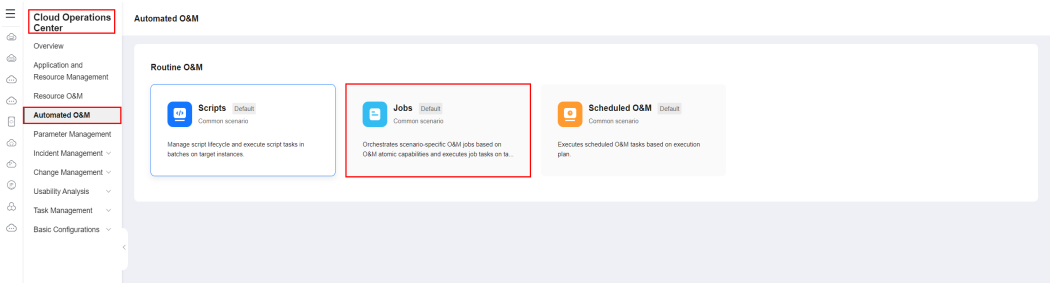
Confirm and fill in the risk level of the operation according to the operation procedure.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-52 Job Management page

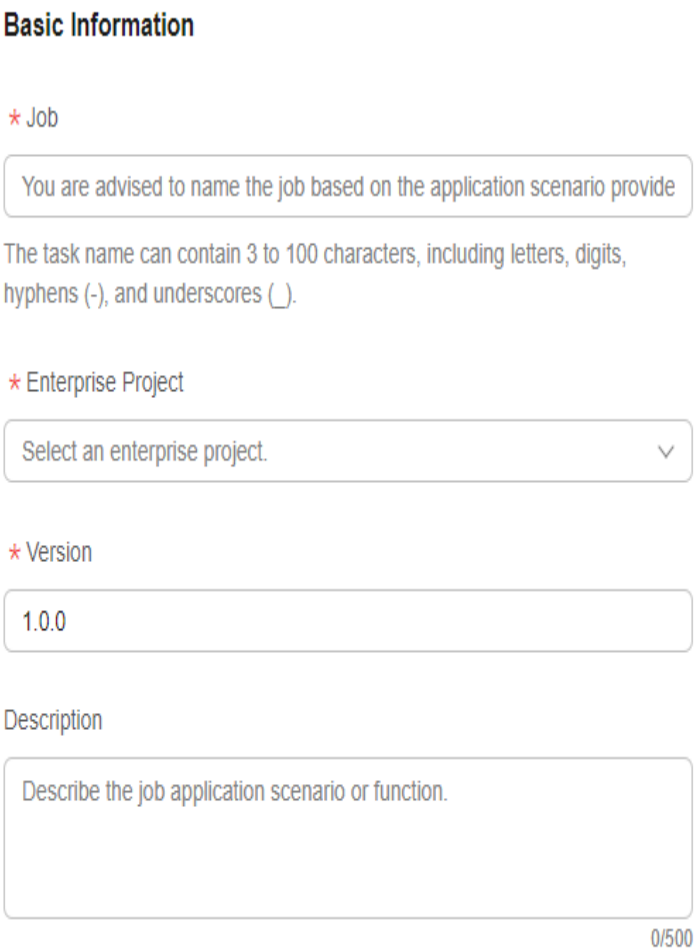


Step 3 Click **Custom Jobs** and click **Create Job**.

Figure 5-53 Clicking **Create Job**

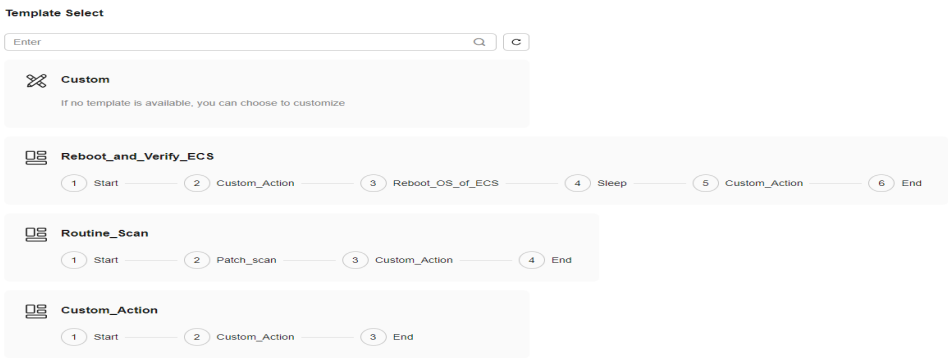
Step 4 Enter the basic job information, including the job name, enterprise project, description, and tag. You can create tags by following the instructions provided in **Tag Management**.

Figure 5-54 Entering basic job information



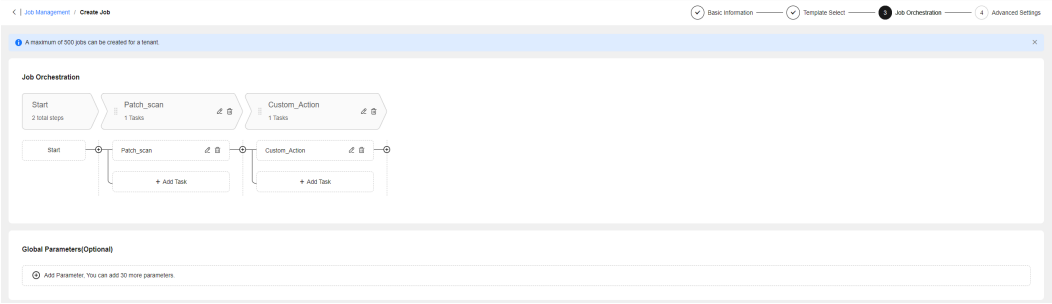
Step 5 Select a job template. If no proper template is available, select **Custom**.

Figure 5-55 Selecting a job template



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

Figure 5-56 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 5-57 Selecting **Custom** and adding global parameters

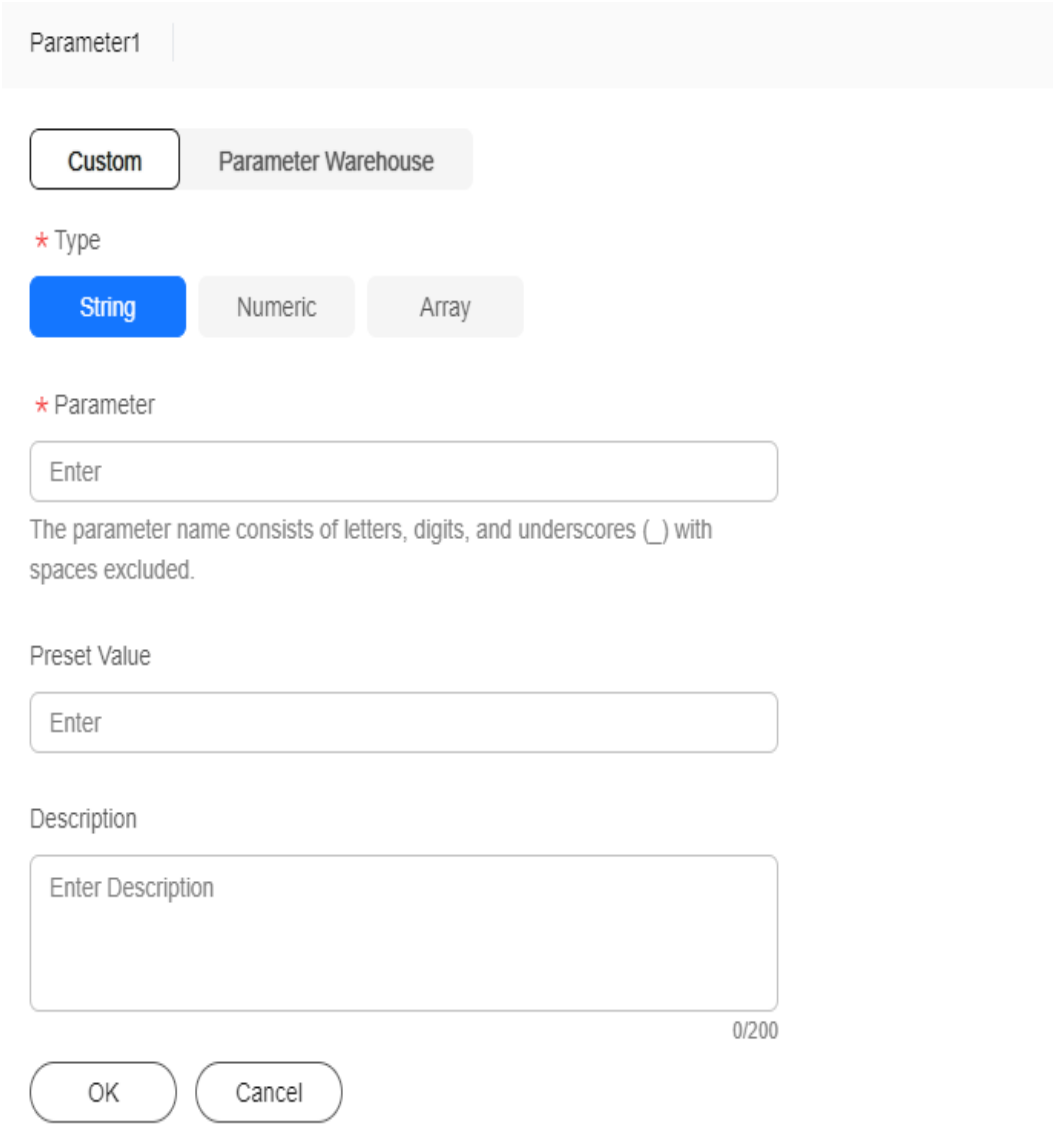


Figure 5-58 Obtaining and adding Global parameters from the parameter warehouse

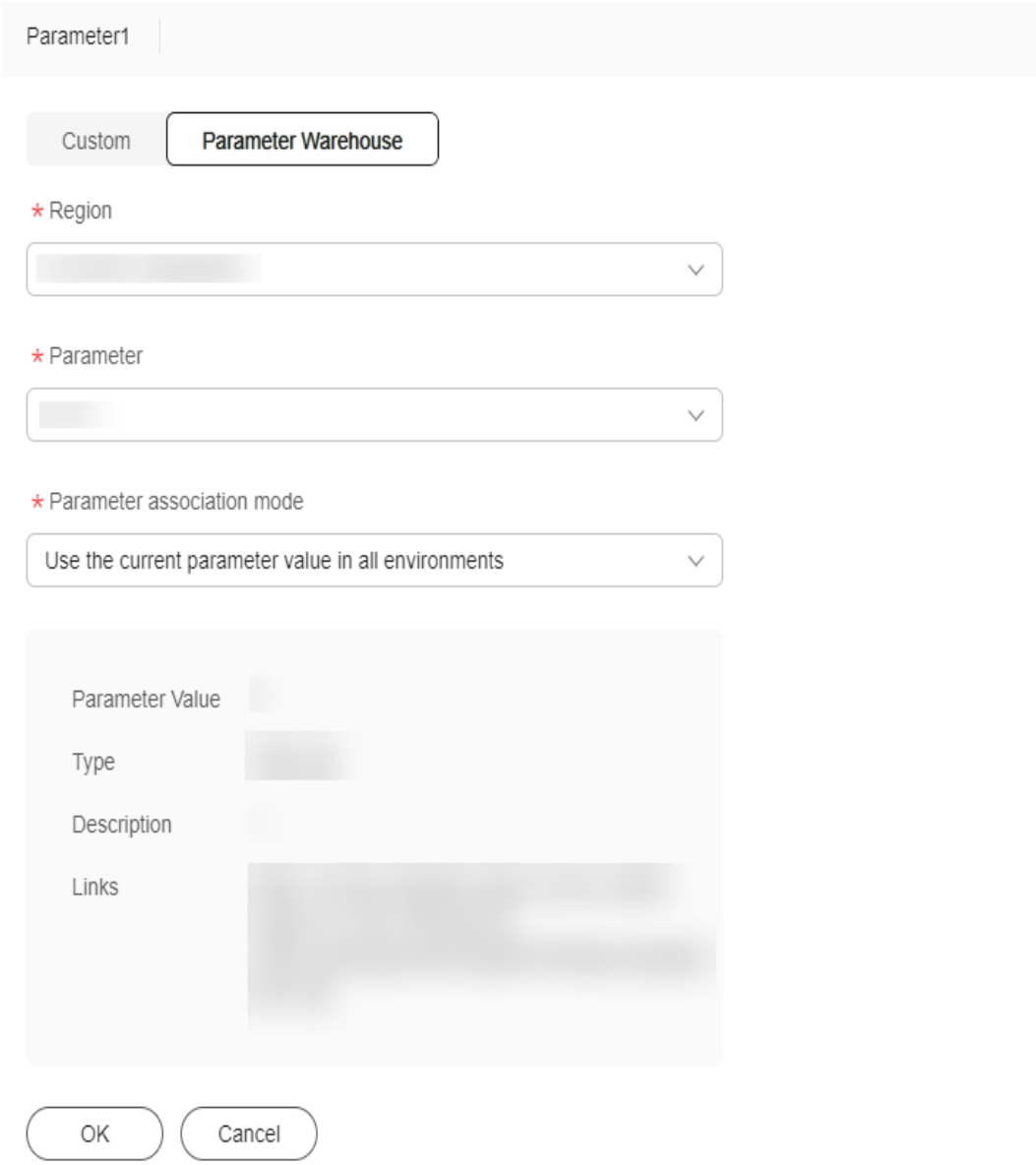


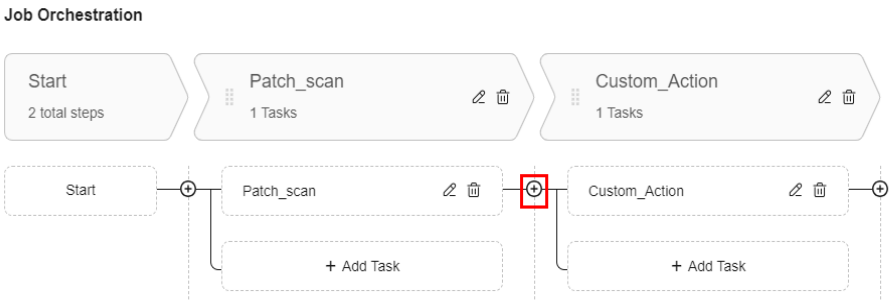
Table 5-8 Parameter association modes

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.

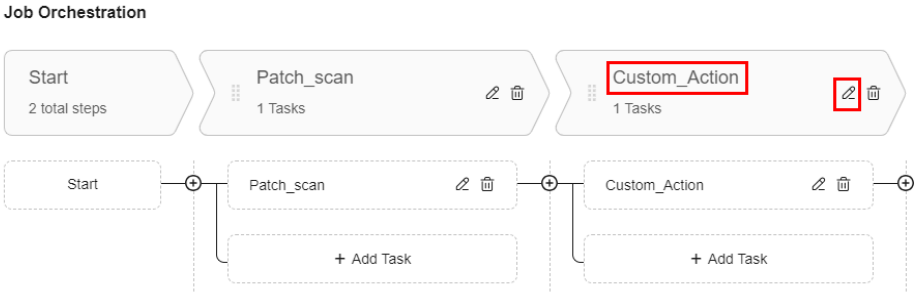
Step 8 Click to add a new step.

Figure 5-59 Adding a step



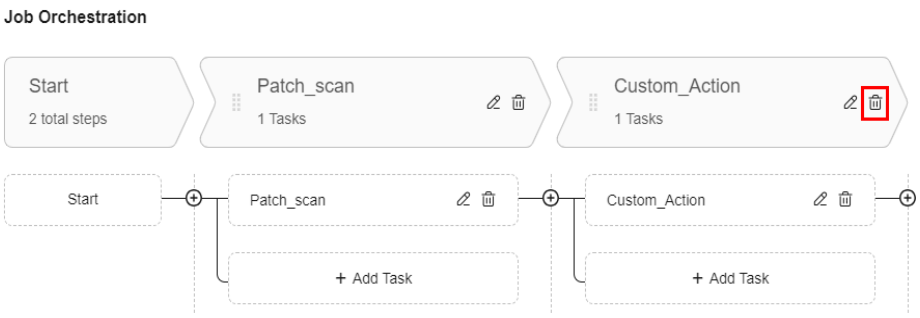
Step 9 Click the step name or to change the step name.

Figure 5-60 Changing the step name



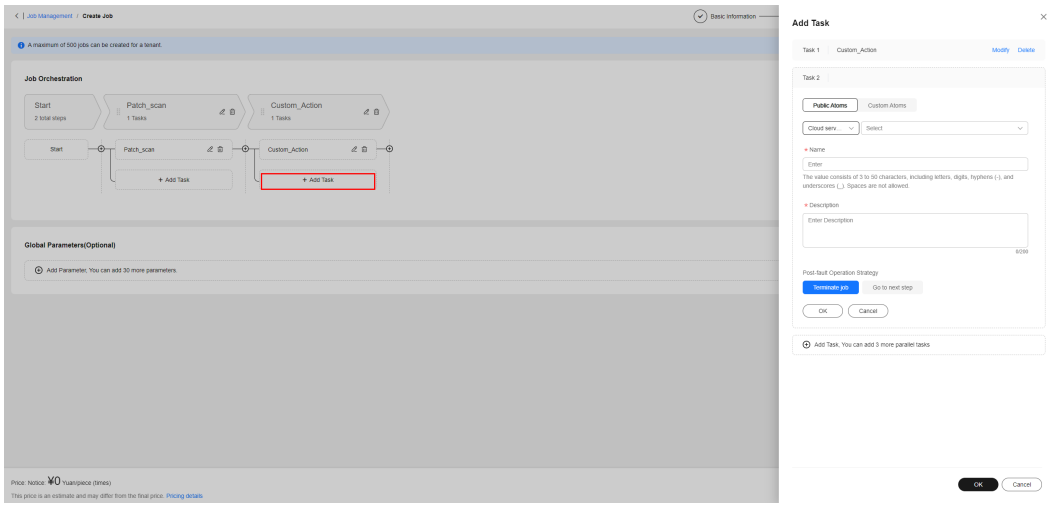
Step 10 If there are unnecessary steps, click to delete them.

Figure 5-61 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**.

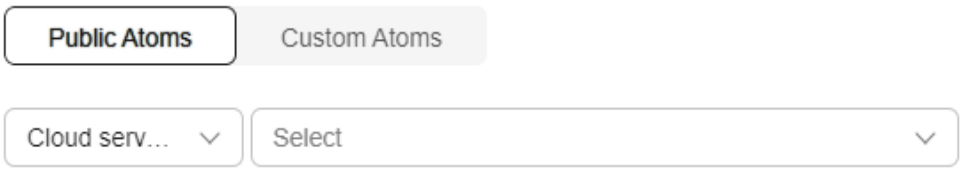
Figure 5-62 Adding tasks



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

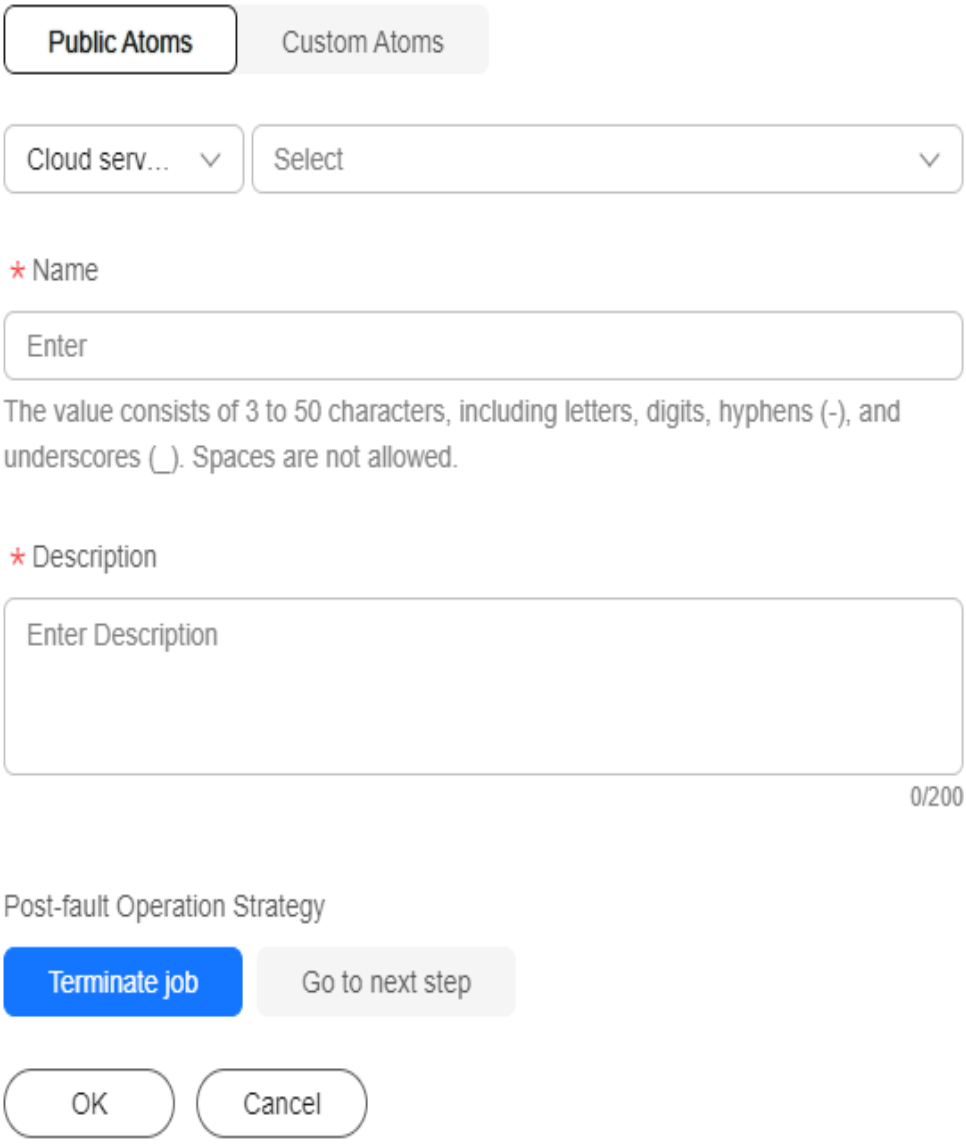
- Public atoms: include control atoms and cloud service API atoms. Cloud service APIs support ECS operation atoms. For details, see ECS Operations.
- Custom atoms: You can select a custom script type. After a custom script is created, a custom atom record is automatically registered.

Figure 5-63 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 5-64 Setting task information



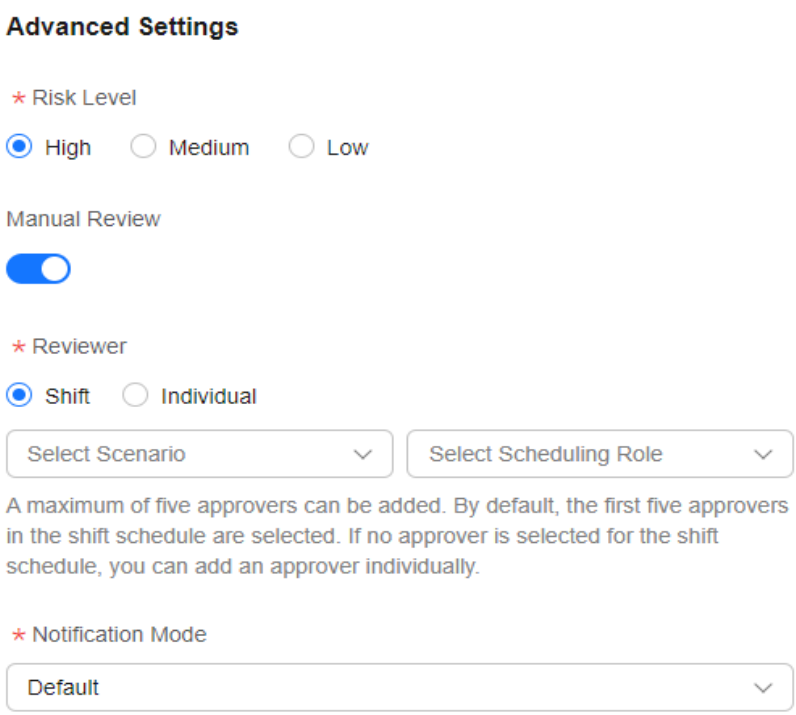
Step 14 After the job orchestration is complete, determine the risk level of the job based on the operation risks.

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 5-65 Advanced settings



----End

5.3.3 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

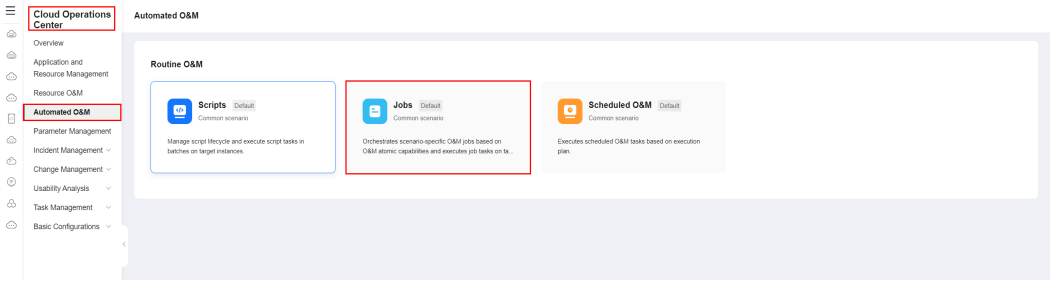
When modifying or cloning a job, determine and fill out the risk level of the job.

Procedure

Step 1 Log in to **COC**.

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

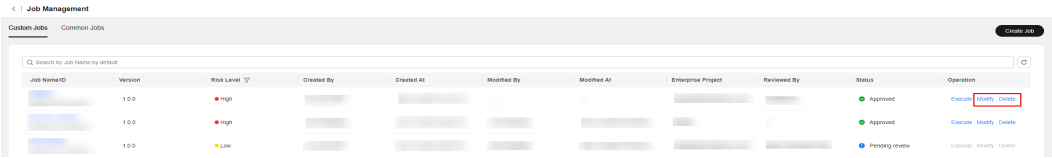
Figure 5-66 Job Management page



Step 3 Locate the target job, and click the operation to be performed on the job, including **Execute**, **Modify**, **Clone**, **Delete.**

- Modifying a job: Click **Modify** in the **Operation** column. For details, see section **Creating a Custom Job**. Click **Cancel** to cancel the modification, and click **Submit** to update 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** to delete a job.
- Modifying a tag: You can modify job tags by following the instructions provided in **Tag Management**.

Figure 5-67 Performing operations on a job



----End

5.3.4 Executing a Custom Job

Execute recorded custom jobs.

Scenarios

Execute a custom job on Cloud Operations Center.

Precautions

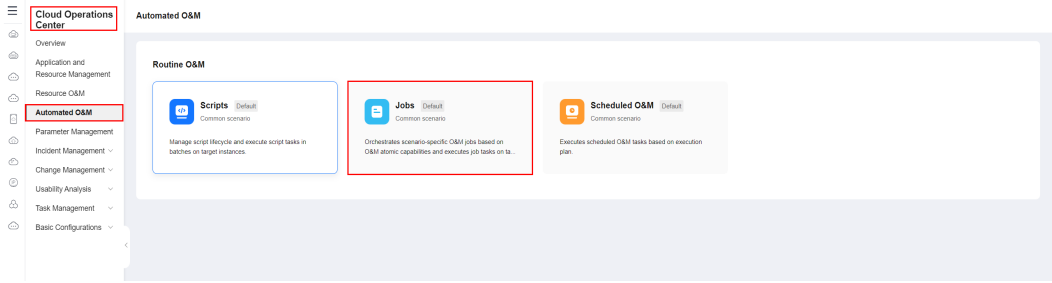
Before executing a job, ensure that you have the resource permissions of target instances.

Procedure

Step 1 Log in to **COC**.

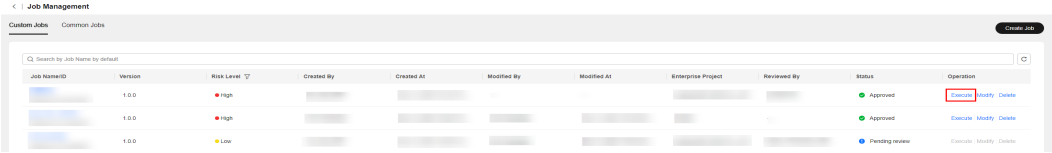
Step 2 In the navigation pane on the left, choose **Automated O&M** and click **Jobs**.

Figure 5-68 Job Management page



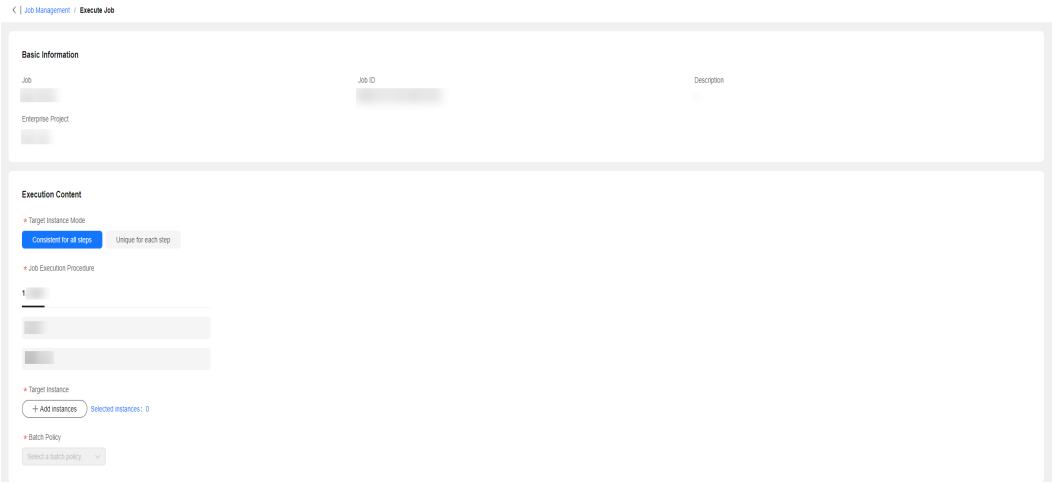
Step 3 Select **Custom Jobs**, select the job to be executed, and click **Execute**.

Figure 5-69 Selecting the job to be executed



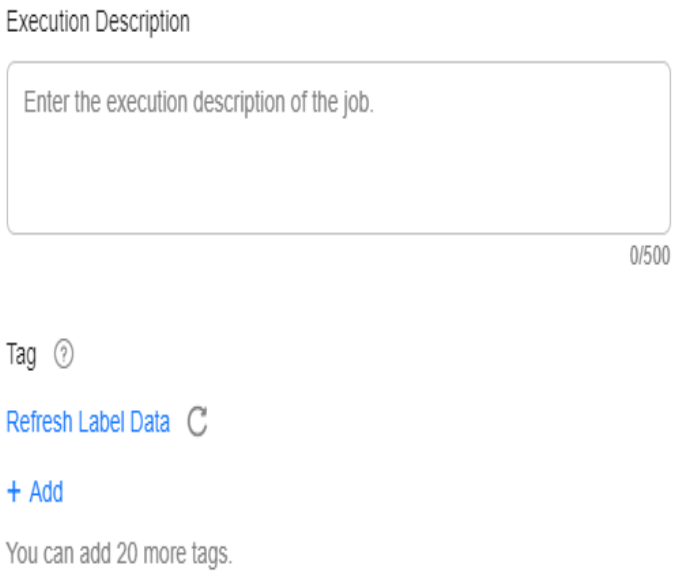
Step 4 Select a job version number and check whether the job steps meet the expectation.

Figure 5-70 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 5-71 Entering basic execution information



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 5-9 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 5-72 Selecting **Consistent for all steps**

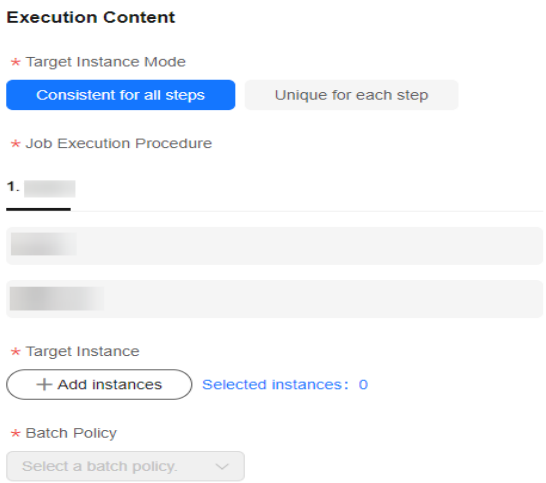
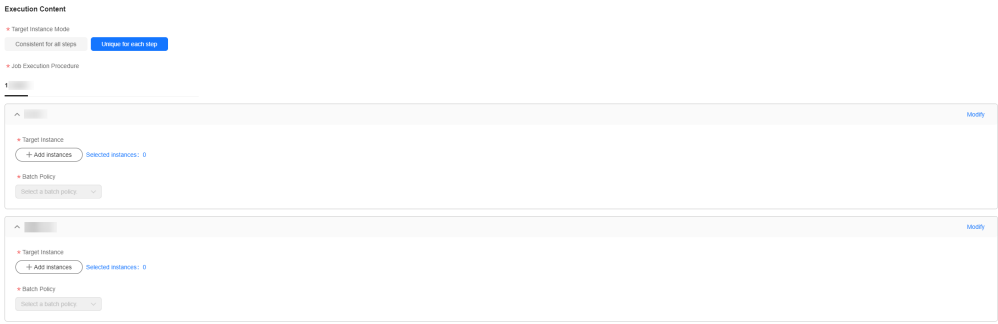
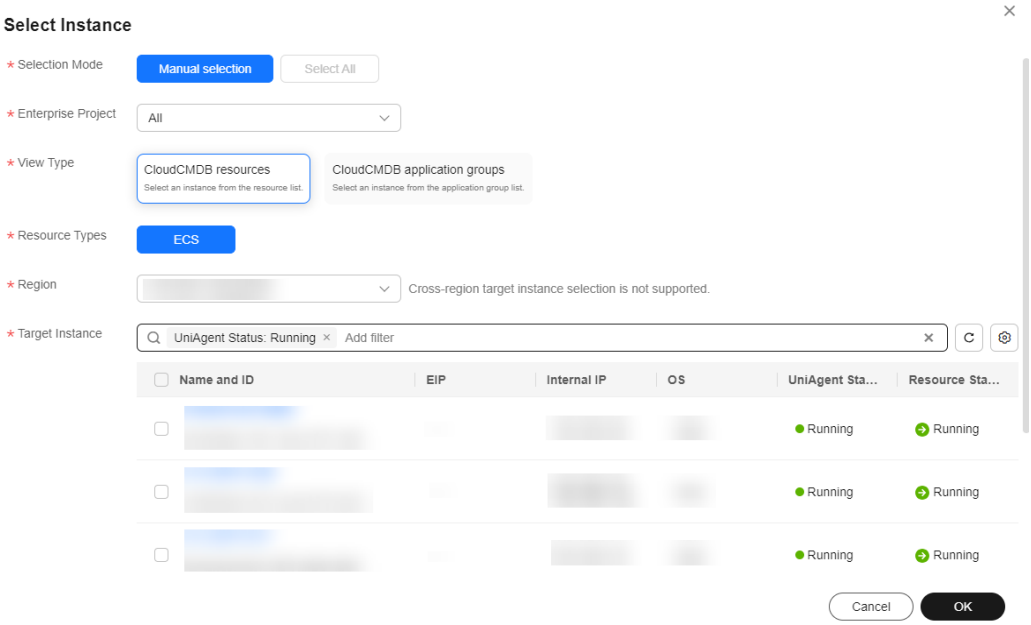


Figure 5-73 Selecting **Unique for each step**



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**.

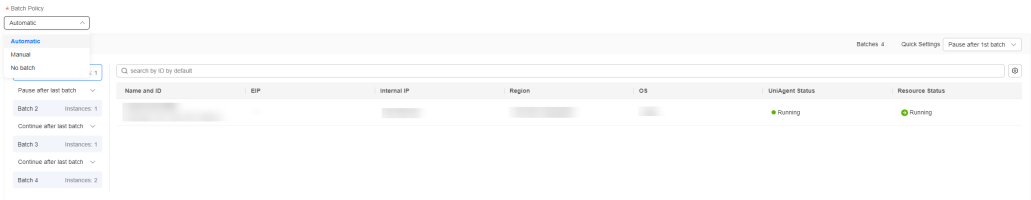
Figure 5-74 Selecting the target instance



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 5-75 Selecting a batch policy

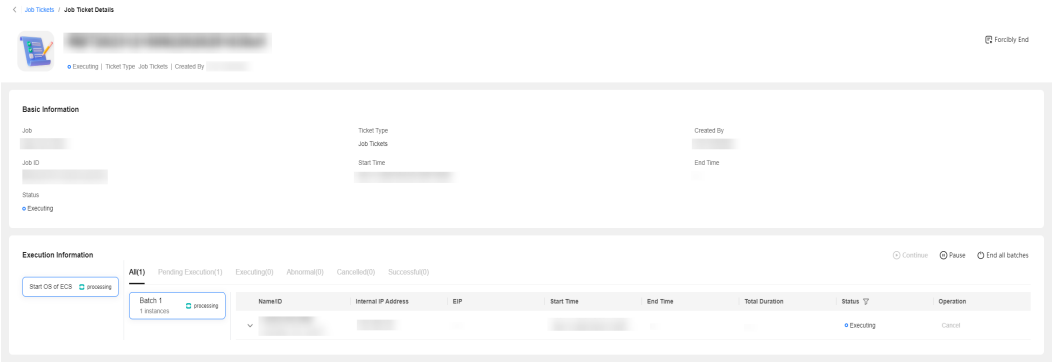


Step 9 Click **Submit** to execute the custom job. The **Job Ticket Details** page is displayed. View the execution status of jobs and each batch on the details page.

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 5-76 Job ticket details



----End

5.3.5 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.

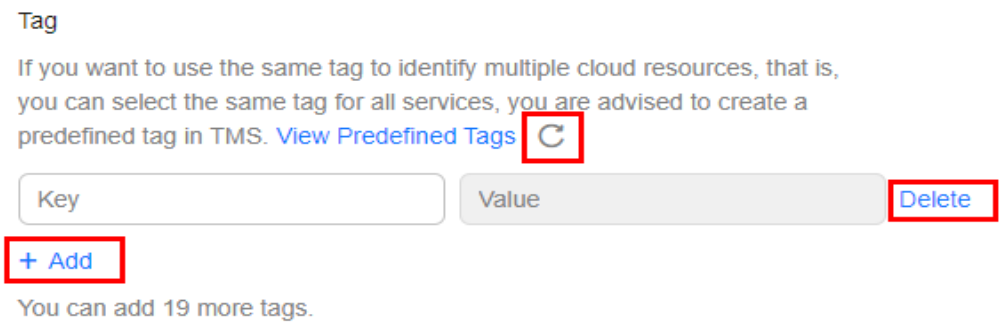
Adding a Tag

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 C to refresh predefined tag data.

Figure 5-77 Adding a tag



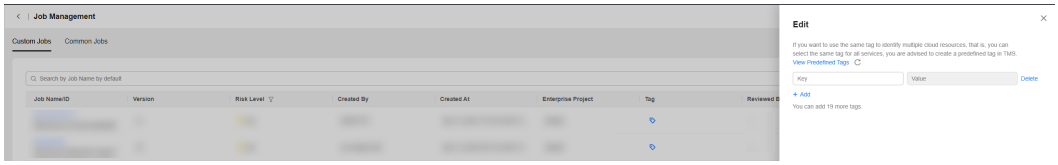
----End

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 5-78 Editing a tag



----End

5.3.6 Atomic Action

An atomic action defines a specific operation content and is the minimum unit of a job.

5.3.6.1 Execute API

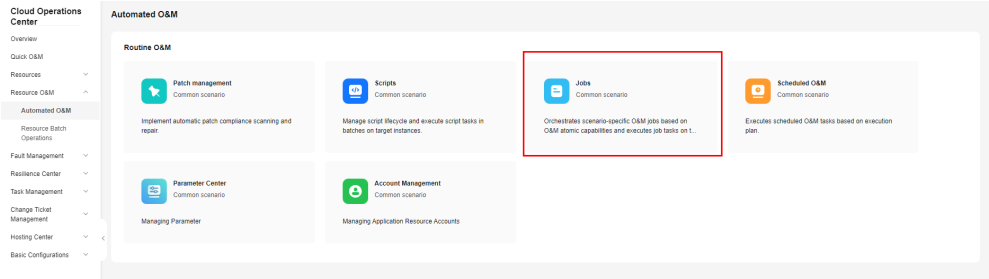
The atomic action can be used to invoke the OpenAPI of a cloud service registered with the API Explorer. If the OpenAPI is an asynchronous call, you can use the atomic action of Wait API to wait for the target object to reach the expected state.

Procedure

Step 1 Log in to **COC**.

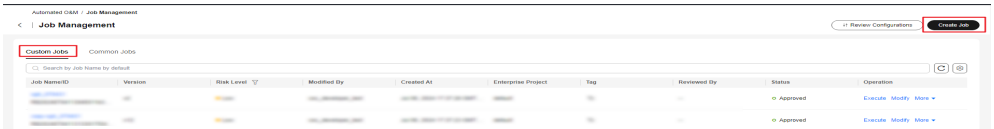
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Jobs**.

Figure 5-79 Jobs



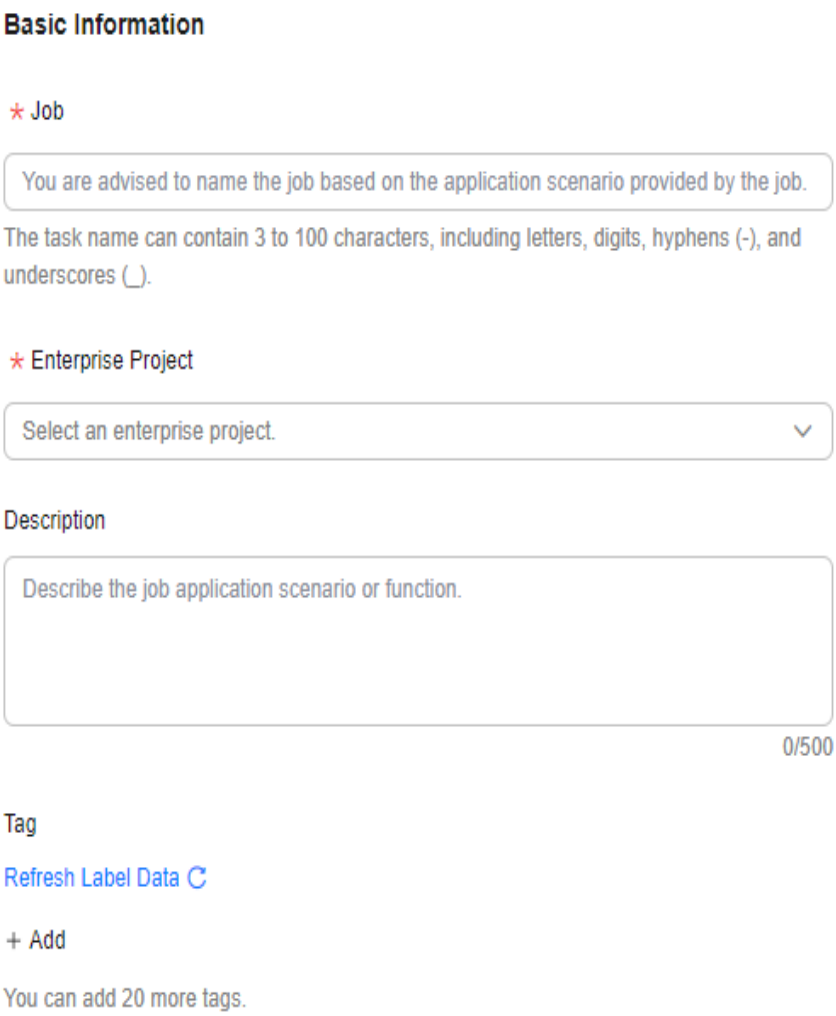
Step 3 Click the **Custom Jobs** tab and click **Create Job**.

Figure 5-80 Clicking **Create Job**



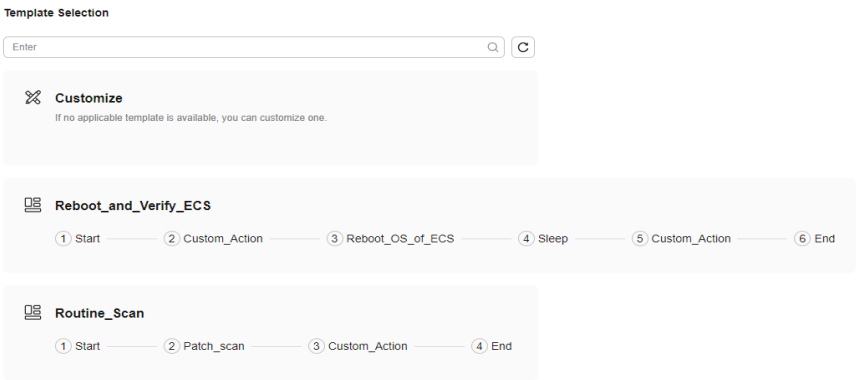
Step 4 Enter the basic job information. You can follow the steps in section **Managing Tags** to create a tag. After the required parameters are set, click **Next**.

Figure 5-81 Entering basic job information



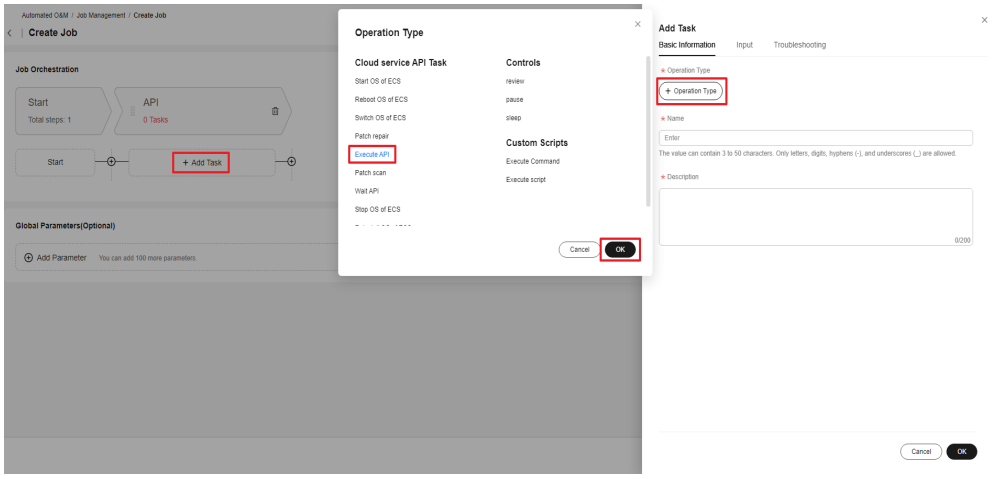
Step 5 Select a job template. If no proper template is available, click **Customize**, and click **Next**.

Figure 5-82 Selecting a job template



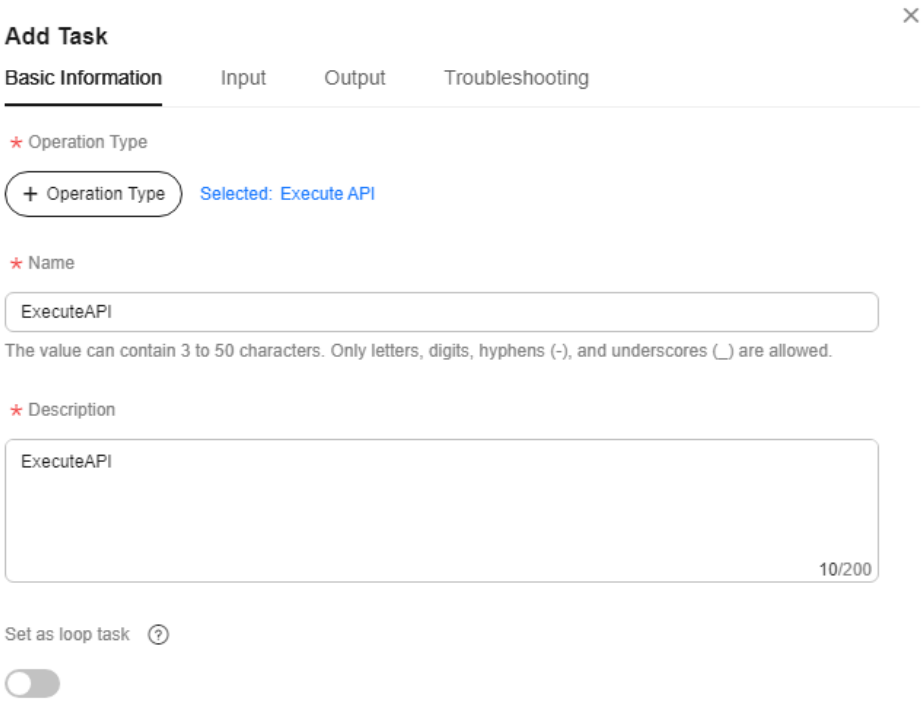
Step 6 Perform job orchestration. Click **+ Add Task**, and click **+ Operation Type**. On the displayed dialog box, click **Execute API**.

Figure 5-83 Adding tasks



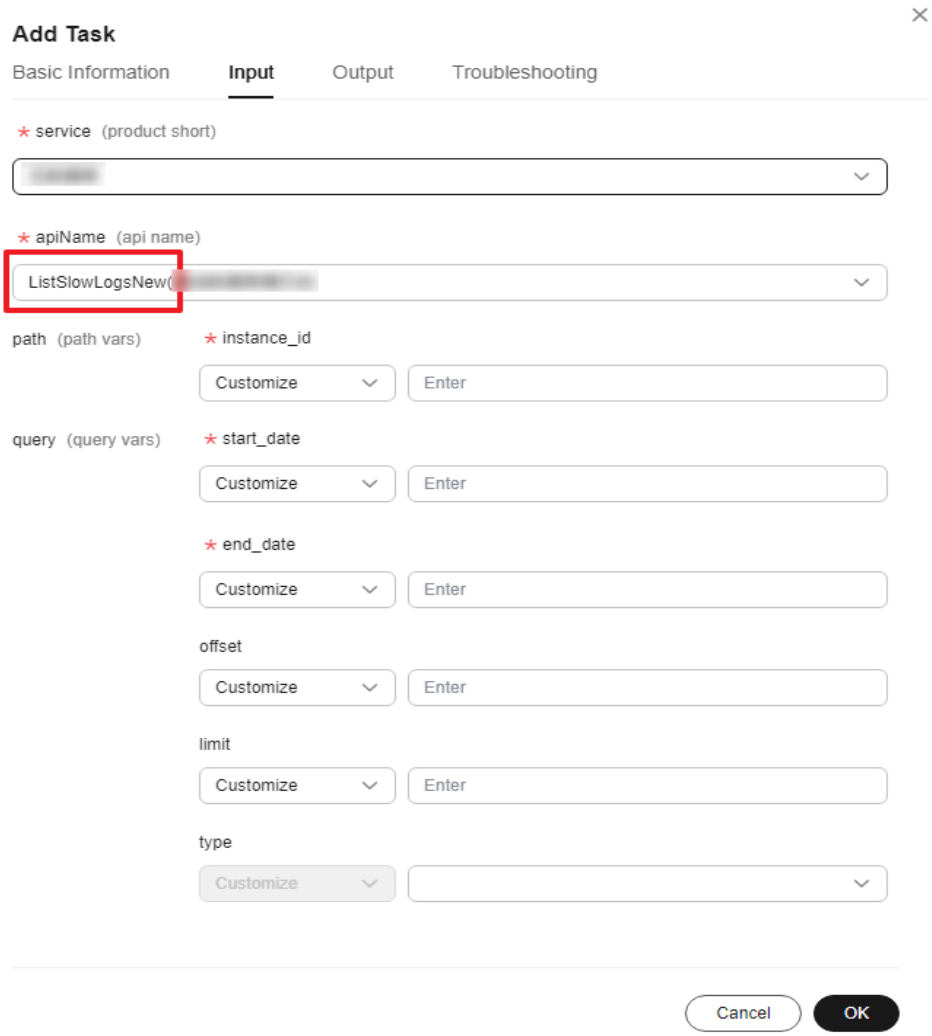
Step 7 Enter the task name and operation description.

Figure 5-84 Configuring basic information



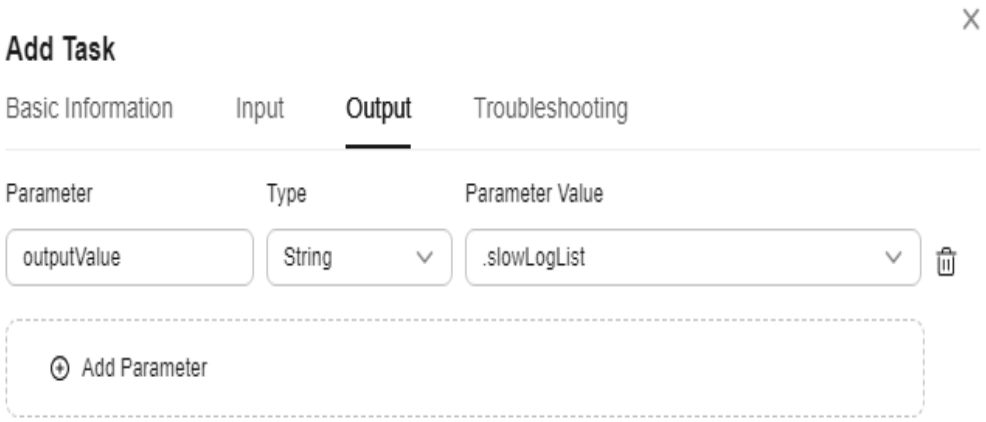
Step 8 Click **Input**, select **service** (product short name) and **apiName** (API name), and set the required OpenAPI parameters.

Figure 5-85 Adding input information



Step 9 Click **Output** and configure the output content as required. For example, you can add **slow_log_list** in the API response as the parameter of the string type, and name it **outputValue**. If output parameters are not required, you do not need to add output parameters.

Figure 5-86 Adding output information



Step 10 Click **Troubleshooting** and configure the policy for the action upon an execution error: **Terminate Job** or **Go to Next Step**.

Figure 5-87 Adding troubleshooting policy

Step 11 Click **OK**.

----End

5.3.6.2 Wait API

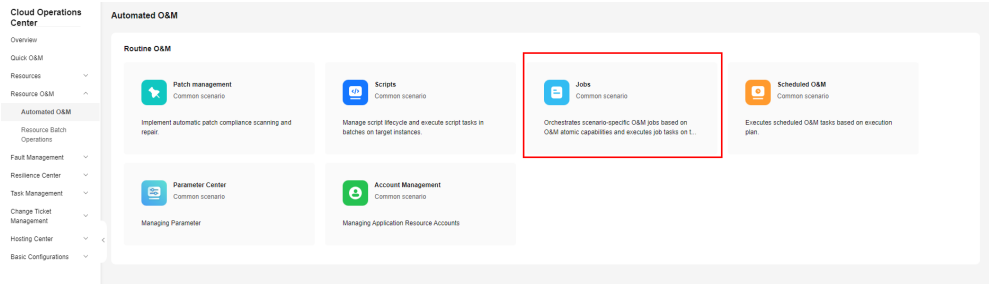
The atomic action can be used to wait for the target object to reach the expected state. For example, after calling the **StartServer** API of the ECS using the Execute API atomic action, call the **ShowServer** API of the ECS using the Wait API atomic action. Wait until the status in the API response becomes **ACTIVE**, that is, the status is running, then you can confirm that the ECS instance has been started.

Procedure

Step 1 Log in to **COC**.

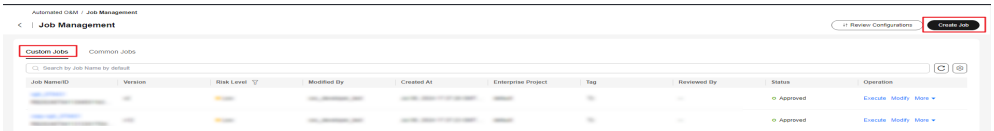
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Jobs**.

Figure 5-88 Jobs



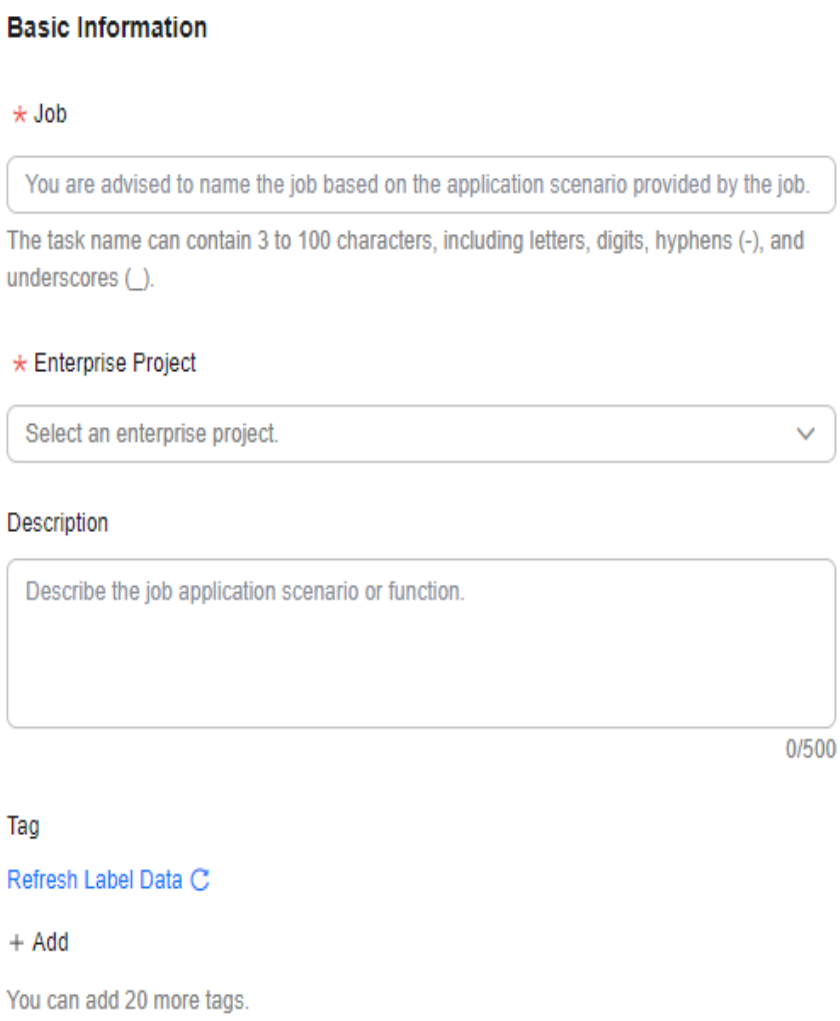
Step 3 Click the **Custom Jobs** tab and click **Create Job**.

Figure 5-89 Clicking **Create Job**



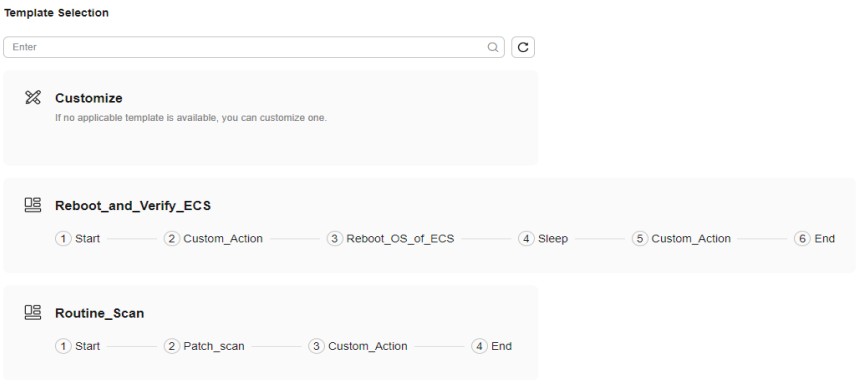
Step 4 Enter the basic job information. You can follow the steps in section **Managing Tags** to create a tag. After the required parameters are set, click **Next**.

Figure 5-90 Entering basic job information



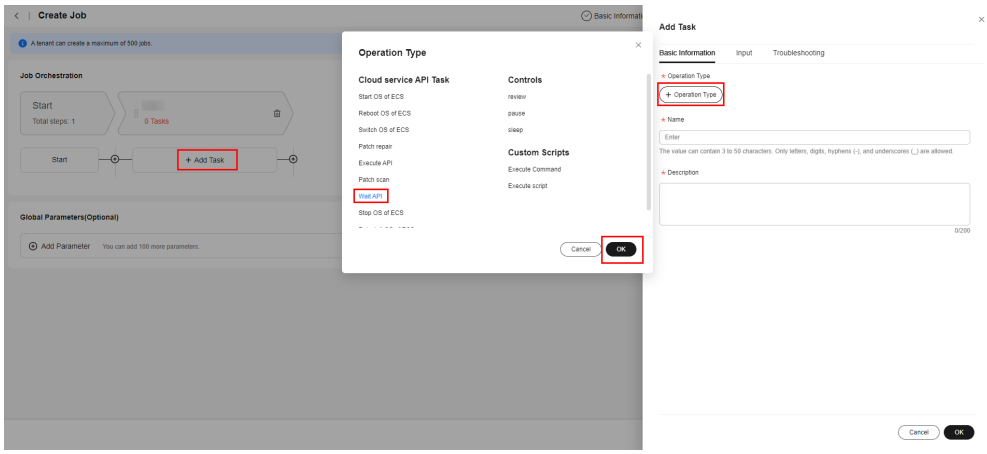
Step 5 Select a job template. If no proper template is available, click **Customize**, and click **Next**.

Figure 5-91 Selecting a job template



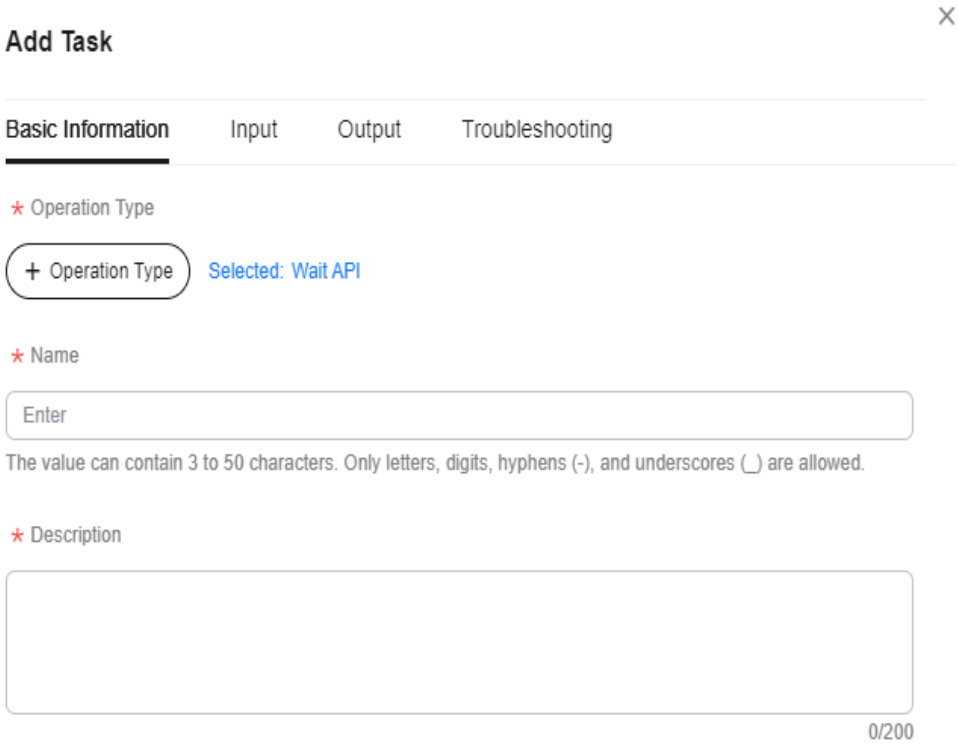
Step 6 Perform job orchestration. Click **+ Add Task**, and click **+ Operation Type**. On the displayed dialog box, click **Wait API**.

Figure 5-92 Adding tasks



Step 7 Enter the task name and operation description.

Figure 5-93 Setting the basic information



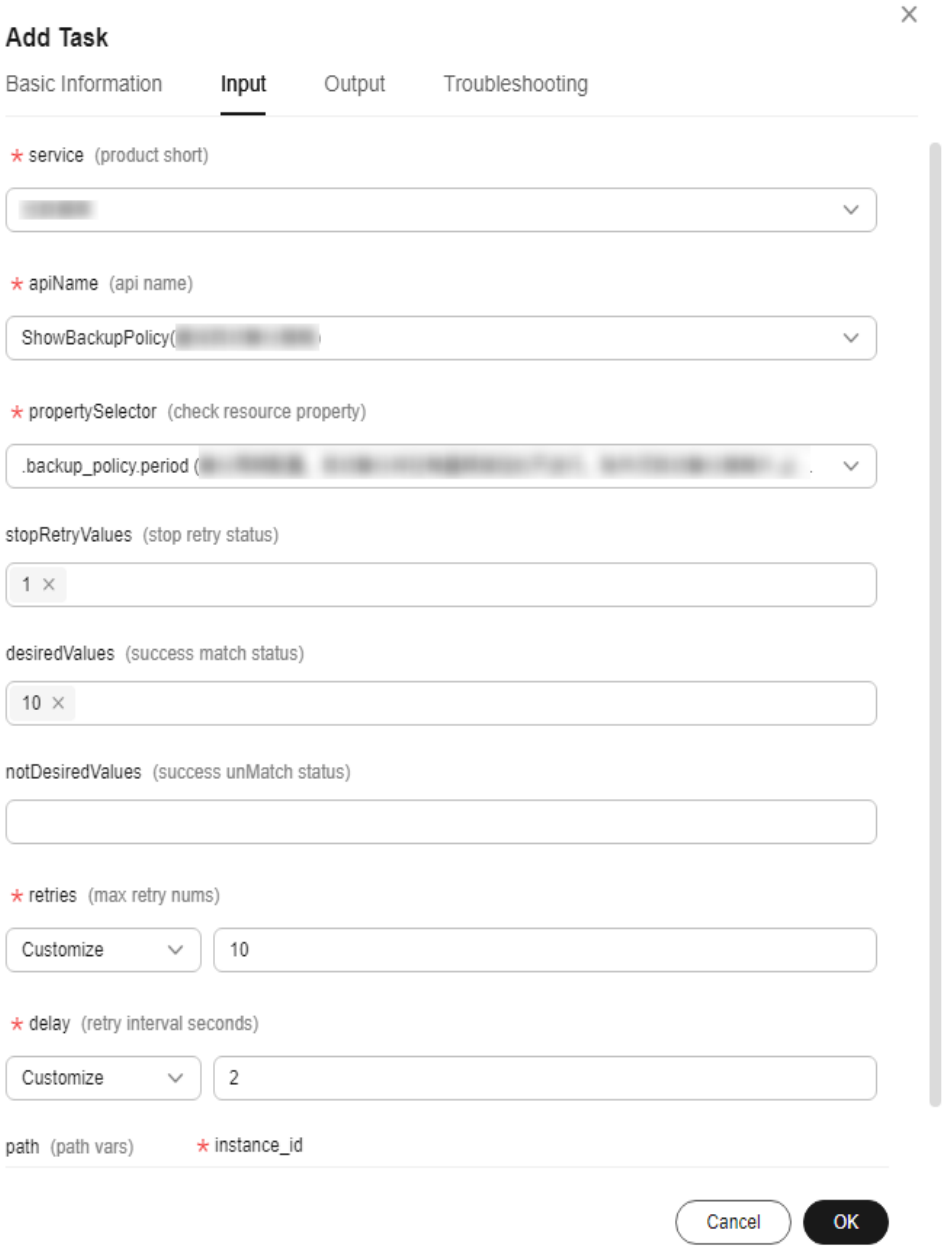
Step 8 Click **Input**, select **service** (product short name), **apiName** (API name),

and **propertySelector (check resource property)**, and specify the following parameters as response fields to be used as the judgment criteria as required:

- **stopRetryValues (stop retry status)**: Stop the current atomic action waiting.
- **desiredValues (success match status)**: Expected match value. When the value is the same as that of **propertySelector**, the current atomic action is successfully executed.

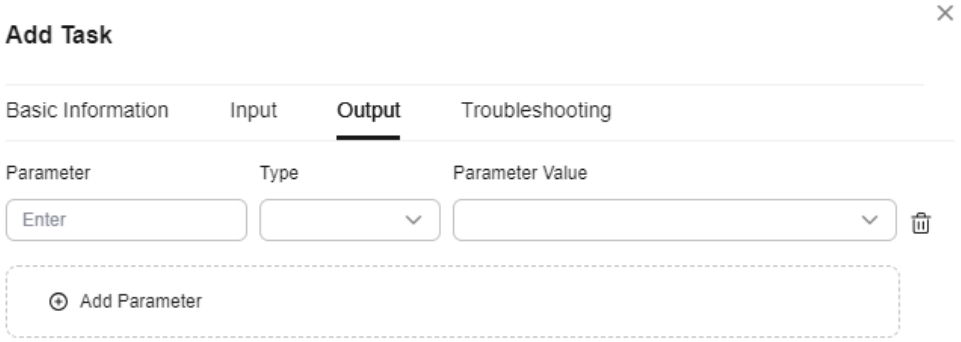
- **notDesiredValues (success unMatch status)**: Expected unmatch value. When the value is the same as that of **propertySelector**, the current atomic action fails to be executed.

Figure 5-94 Adding input information



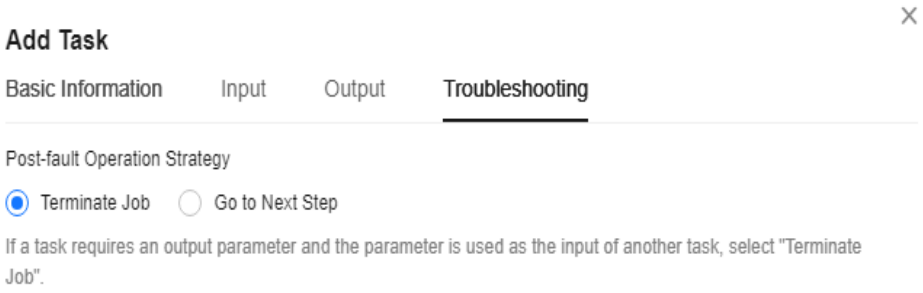
Step 9 Click **Output** and configure the output content as required. For example, you can add **backup_policy** in the API response as the parameter of the string type, and name it **outputValue**. If output parameters are not required, you do not need to add output parameters.

Figure 5-95 Adding output information



Step 10 Click **Troubleshooting** and configure the policy for the action upon an execution error: **Terminate Job** or **Go to Next Step**.

Figure 5-96 Adding troubleshooting policy



Step 11 Click **OK**.

----End

5.3.6.3 Execute Command

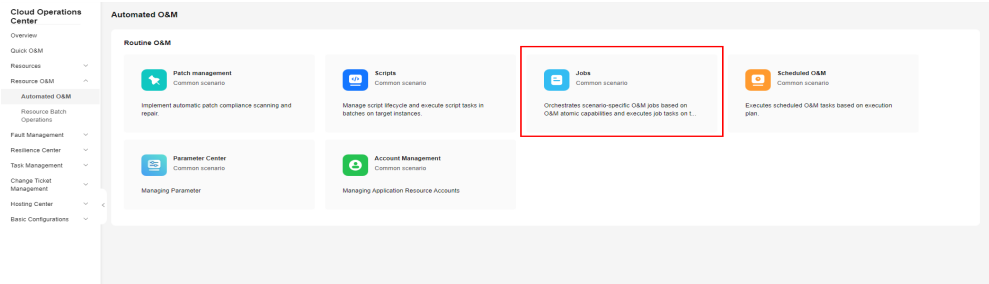
The atomic action can be used to execute a specific command.

Procedure

Step 1 Log in to **COC**.

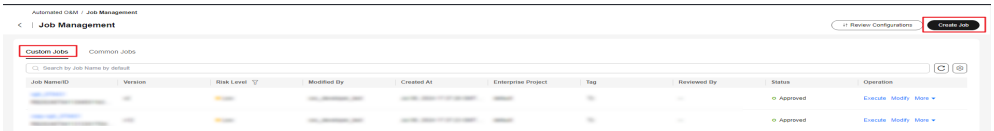
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Jobs**.

Figure 5-97 Jobs



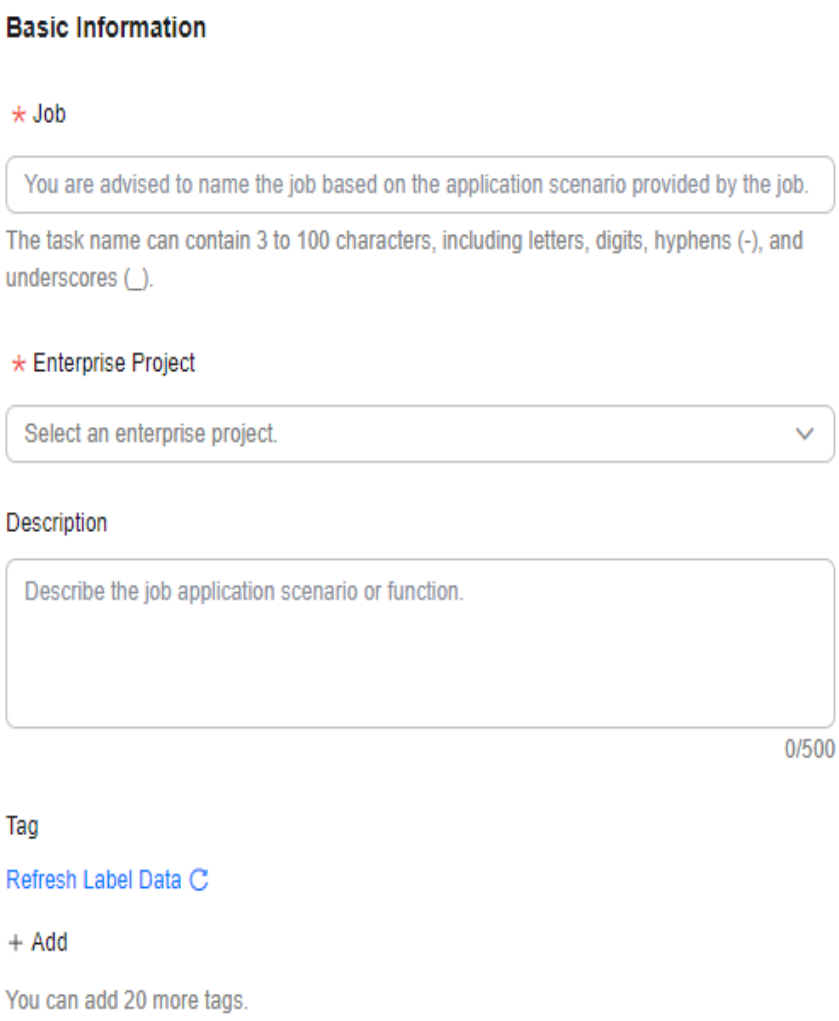
Step 3 Click the **Custom Jobs** tab and click **Create Job**.

Figure 5-98 Clicking **Create Job**



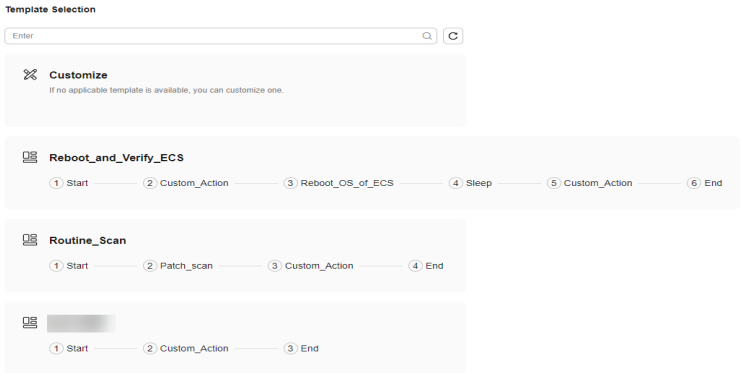
Step 4 Enter the basic job information. You can follow the steps in section **Managing Tags** to create a tag. After the required parameters are set, click **Next**.

Figure 5-99 Entering basic job information



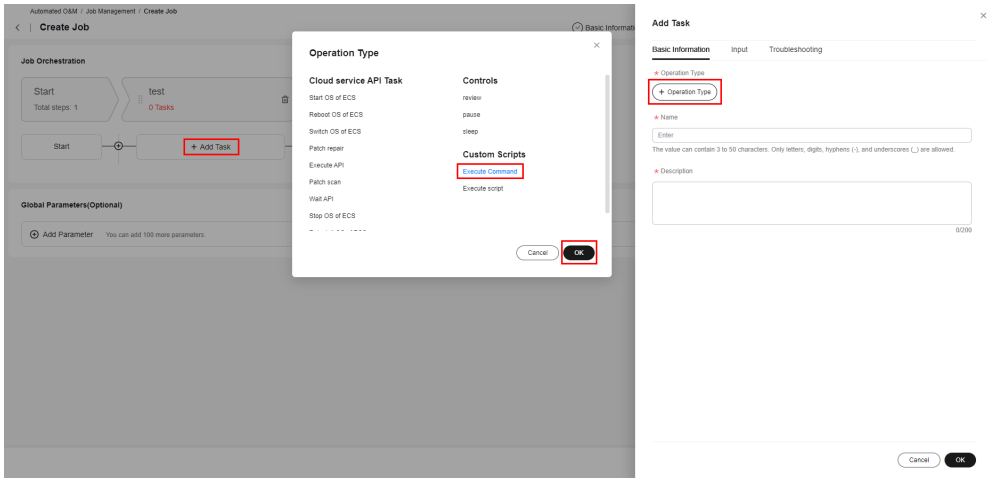
Step 5 Select a job template. If no proper template is available, click **Customize**, and click **Next**.

Figure 5-100 Selecting a job template



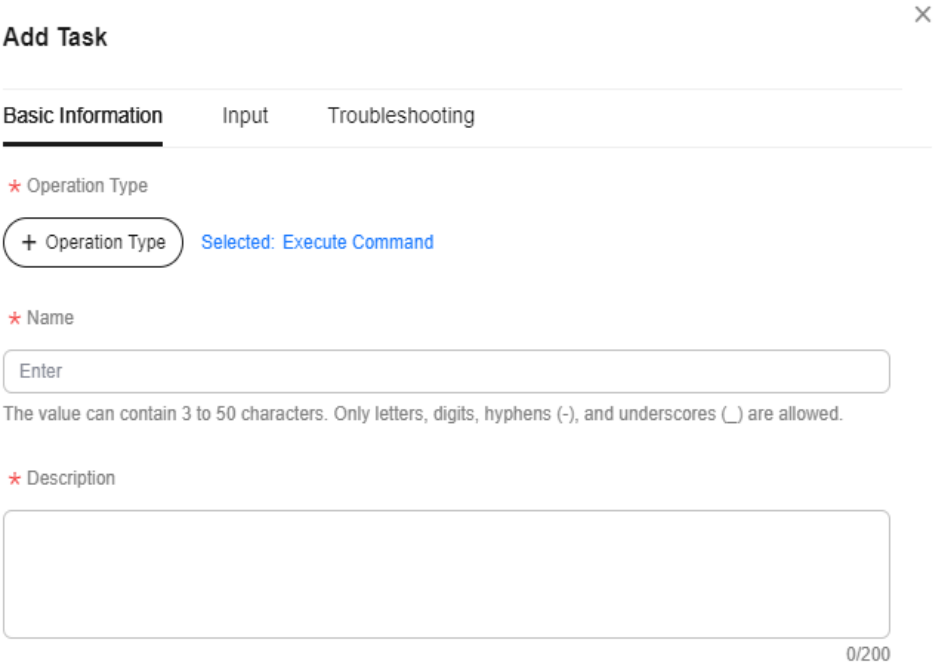
Step 6 Perform job orchestration. Click **+ Add Task**, and click **+ Operation Type**. On the displayed dialog box, click **Execute Command**.

Figure 5-101 Adding tasks



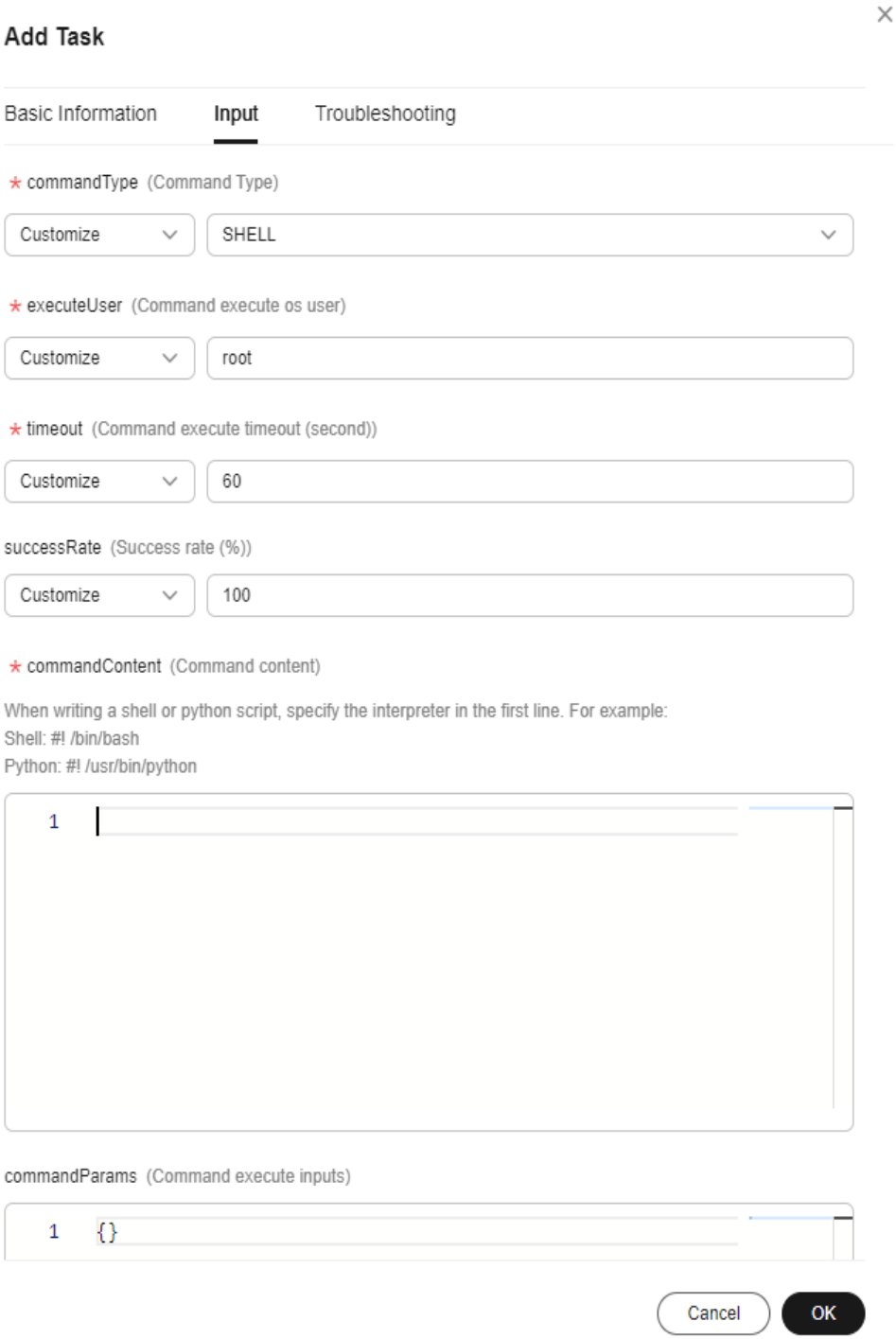
Step 7 Enter the task name and operation description.

Figure 5-102 Setting the basic information



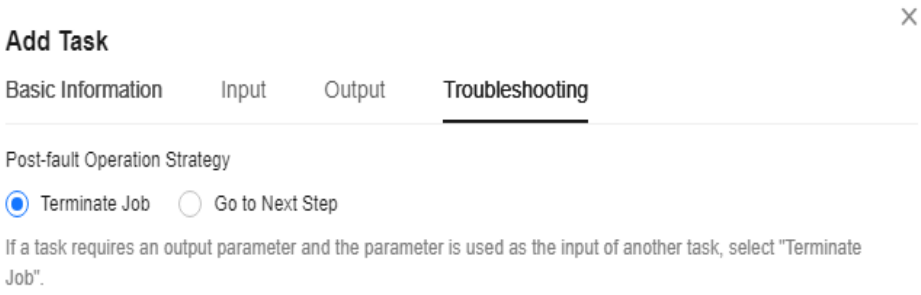
Step 8 Click **Input**, set **commandType (Command type)** to **SHELL**, **PYTHON**, or **BAT** as required. Set **executeUser (command execution os user)**, **timeout (Command execution timeout (second)**, **successRate (Success rate (%))**, **commandContent (Command content)**, and **commandParams (Command execute inputs)**.

Figure 5-103 Adding input information



Step 9 Click **Troubleshooting** and configure the policy for the action upon an execution error: **Terminate Job** or **Go to Next Step**.

Figure 5-104 Adding troubleshooting policy



Step 10 Click **OK**.

----End

5.4 Scheduled O&M

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

5.4.1 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 5-105 Scheduled O&M

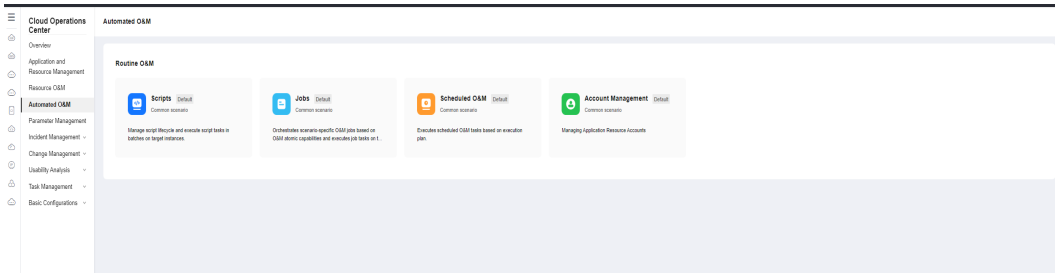
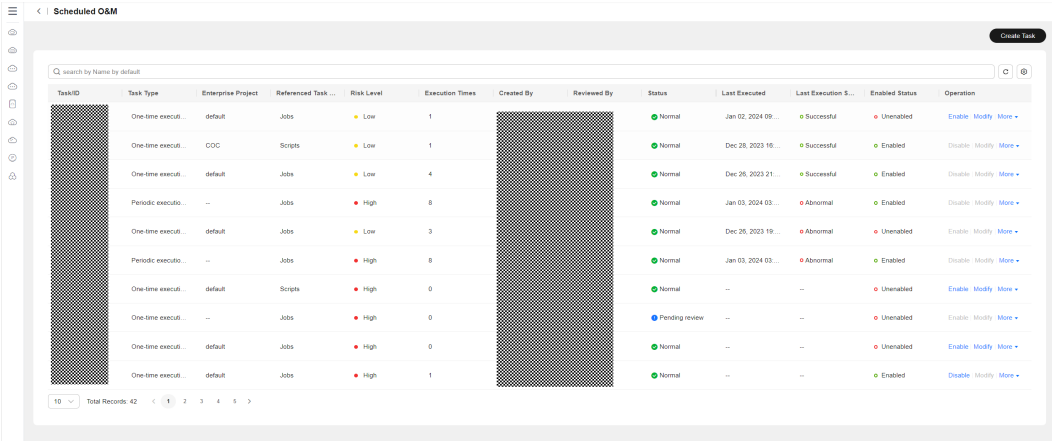
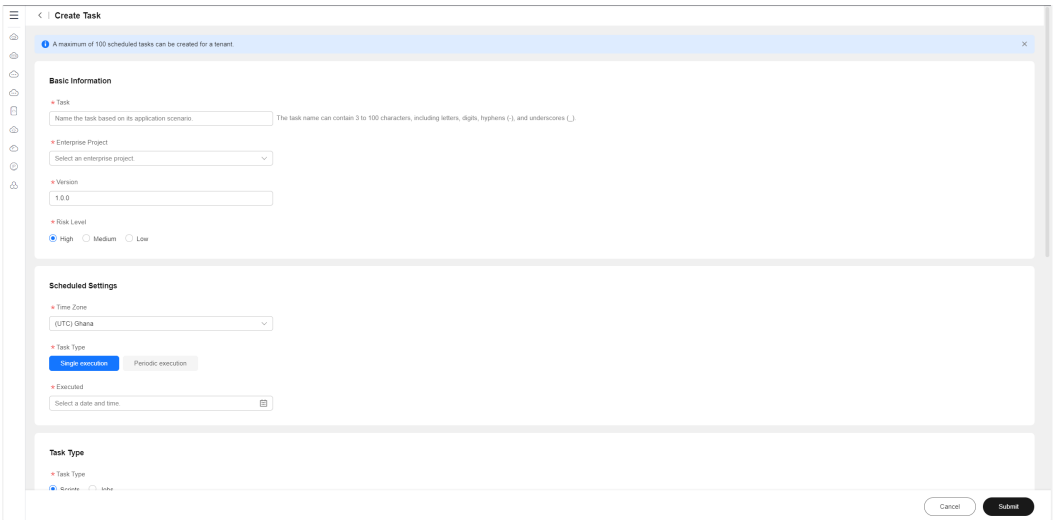


Figure 5-106 Scheduled task list



Step 3 Click **Create Task**.

Figure 5-107 Creating a scheduled task



Step 4 Enter the basic information about the scheduled task. **Table 5-10** describes the required parameters.

Figure 5-108 Entering basic information

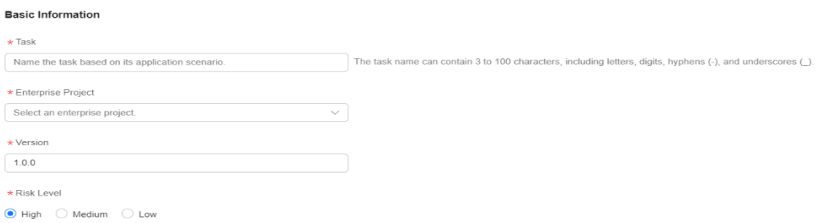


Table 5-10 Parameters

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.
Risk Level	Mandatory. There are three risk levels: ● High ● Medium ● Low **NOTE** If high risk is selected, manual review is enabled by default.

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 5-11** describes the required parameters.

Figure 5-109 Scheduled Settings

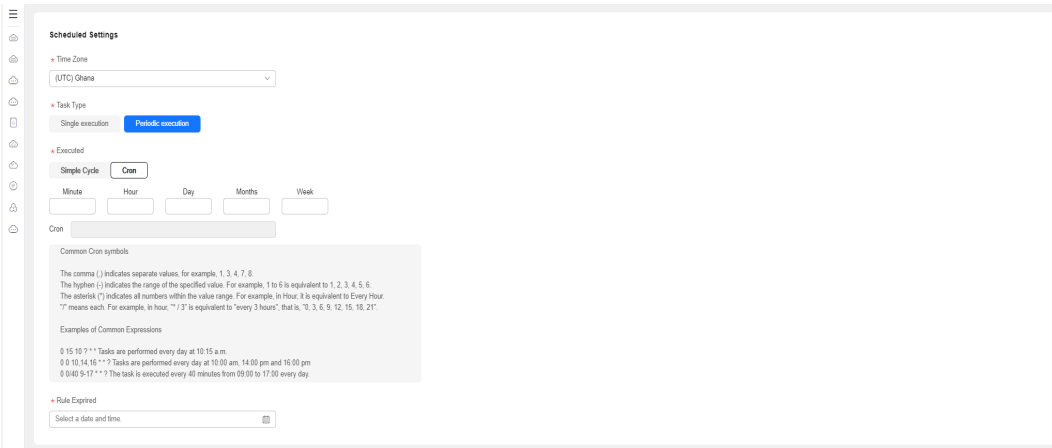
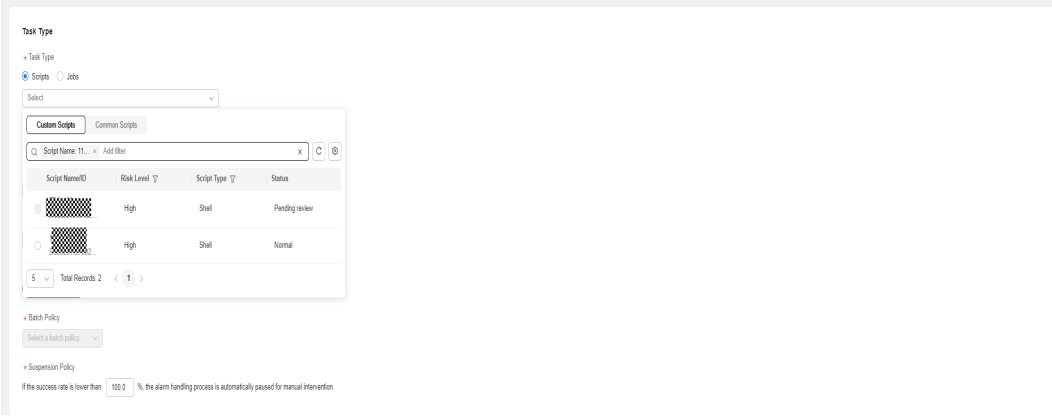


Table 5-11 Parameters

Parameter	Sub-parameter Name	Description
Time Zone	-	Mandatory. The scheduled task is executed based on the time zone.
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.
Executed	-	This parameter is used together with the task type. ● For a single execution, set this parameter to the execution time. ● For periodic execution, the following two modes are available: – Simple Cycle – Cron
Rule Expired	-	If you select **Periodic execution**, you need to configure the rule expiration time.

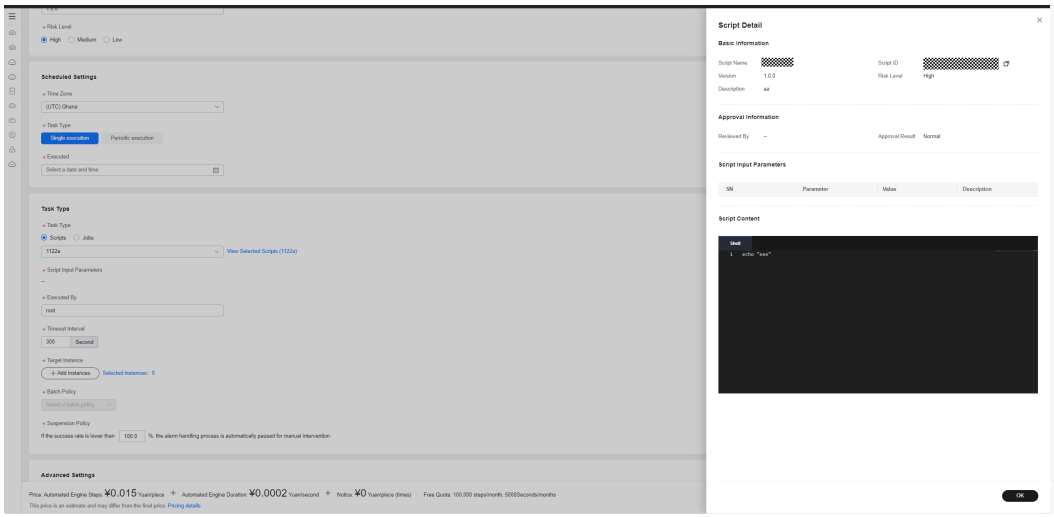
Step 6 a. Enter the task type. If you select **Scripts**, search for a desired script by keyword from the drop-down script lists. Select the desired script.

Figure 5-110 Task Type



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

Figure 5-111 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 5-112 Manually selecting instances (CloudCMDB Resource)

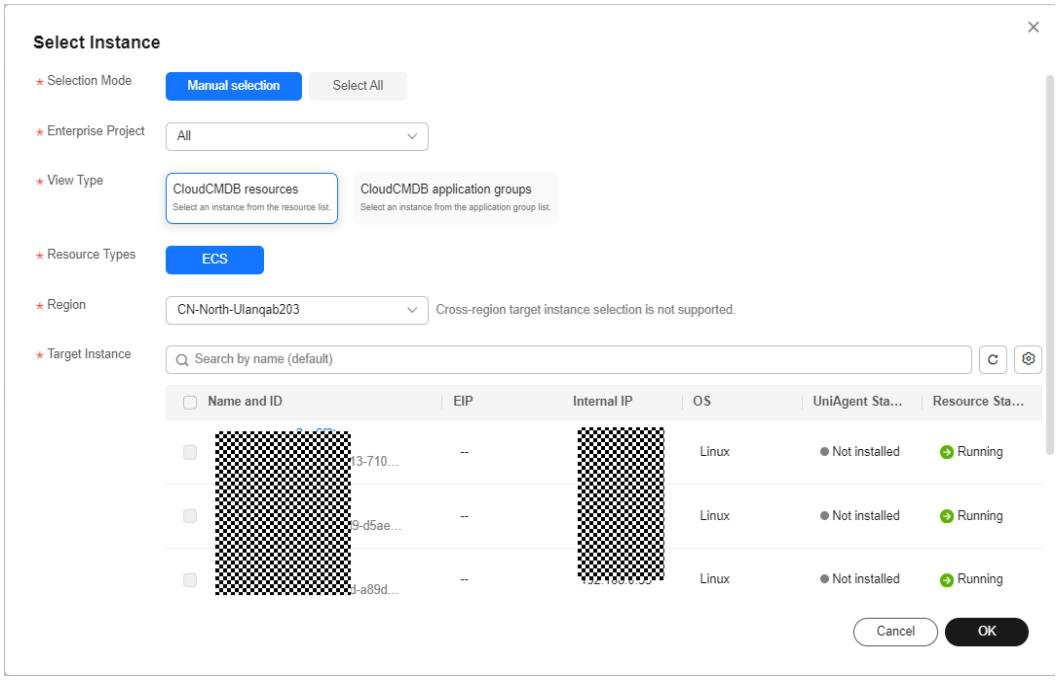
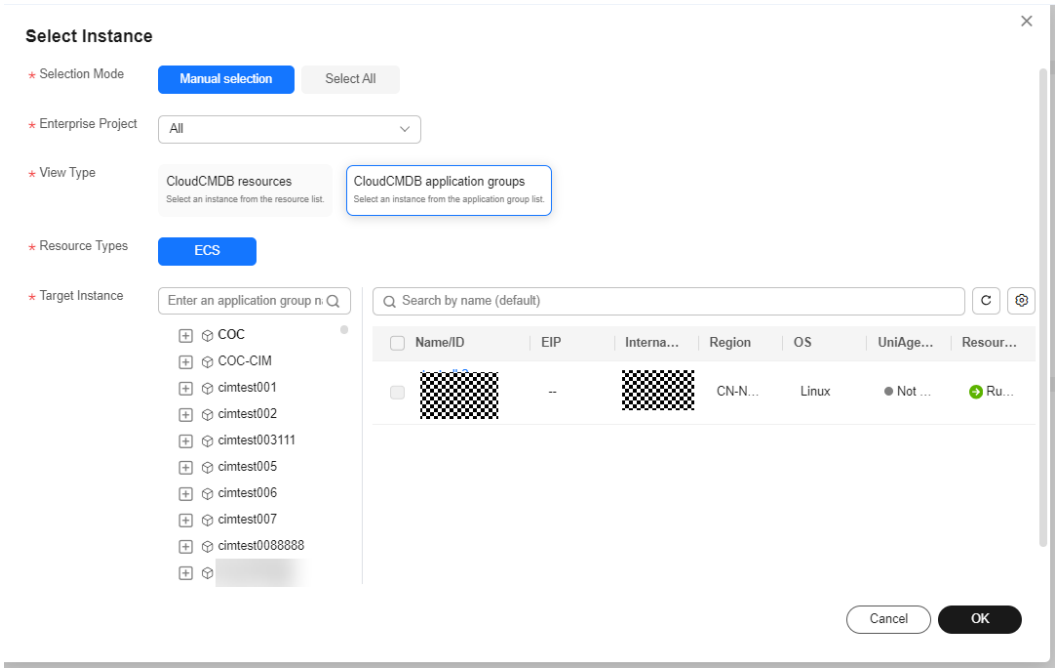


Figure 5-113 Manually selecting instances (CloudCMDB application groups)



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 5-114 Selecting All (CloudCMDB resources)

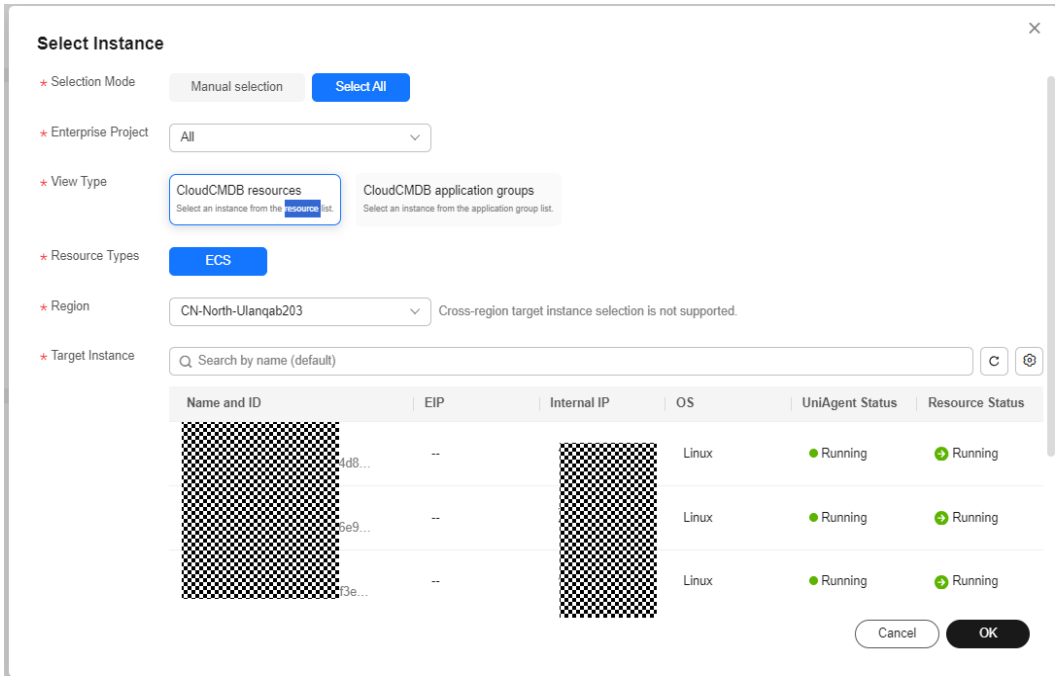
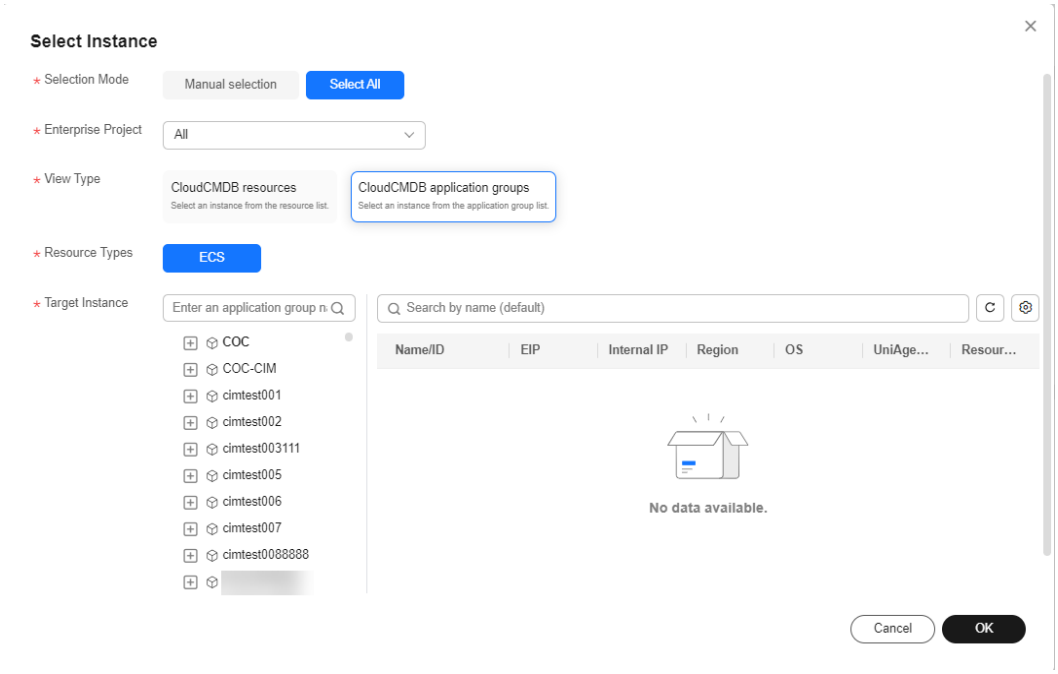


Figure 5-115 Selecting All (CloudCMDB Application groups)



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

Figure 5-116 No batch

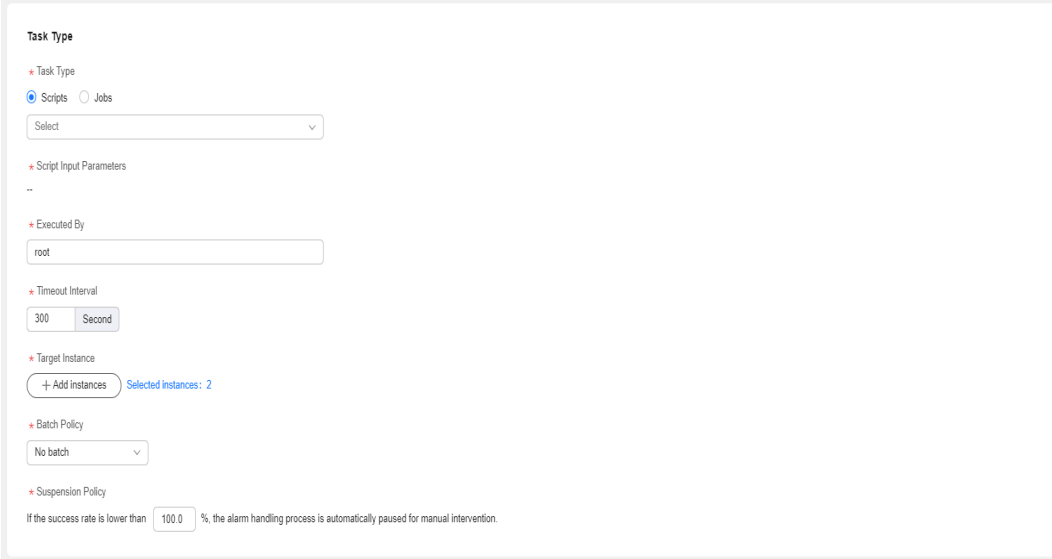
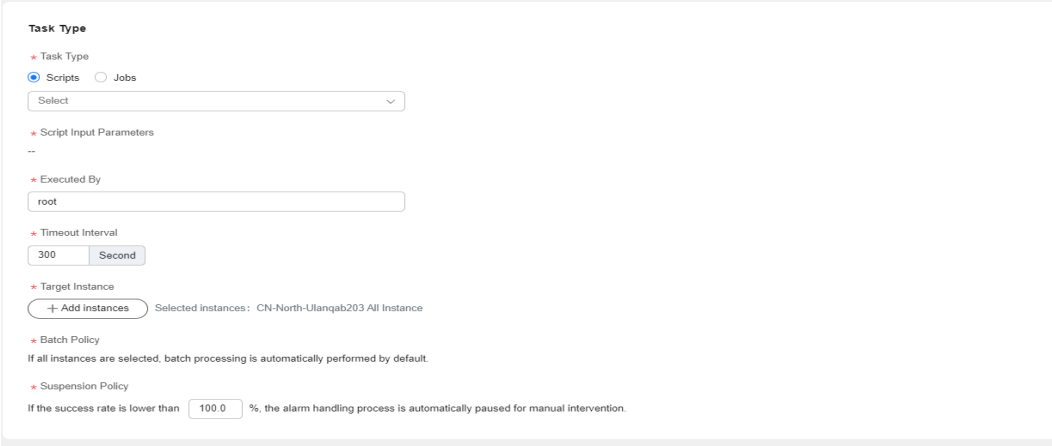
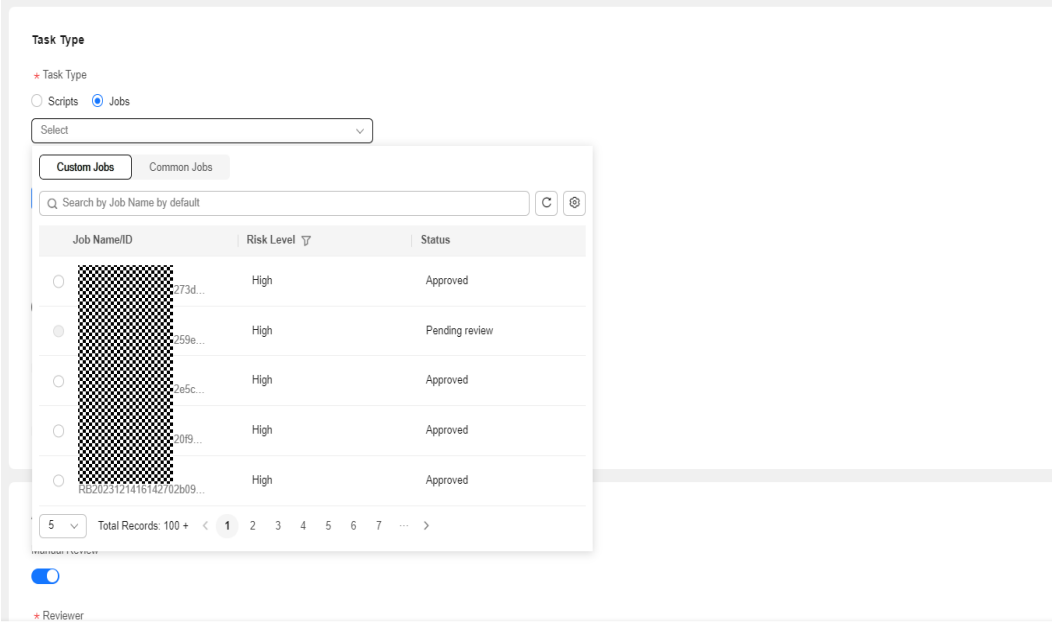


Figure 5-117 Automatic batch



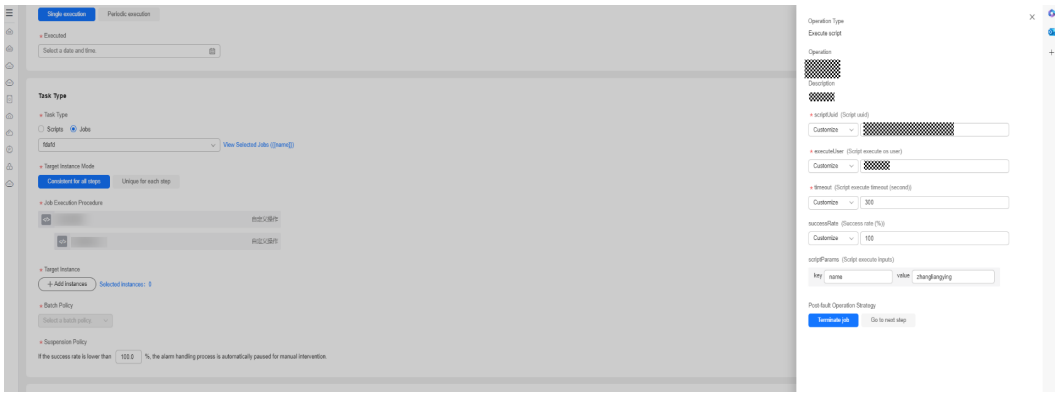
Step 7 a. Enter the task type. If you select **Jobs**, click the text box, and select custom jobs or common jobs by searching for the desired job name. Select the desired job.

Figure 5-118 Selecting **Jobs**



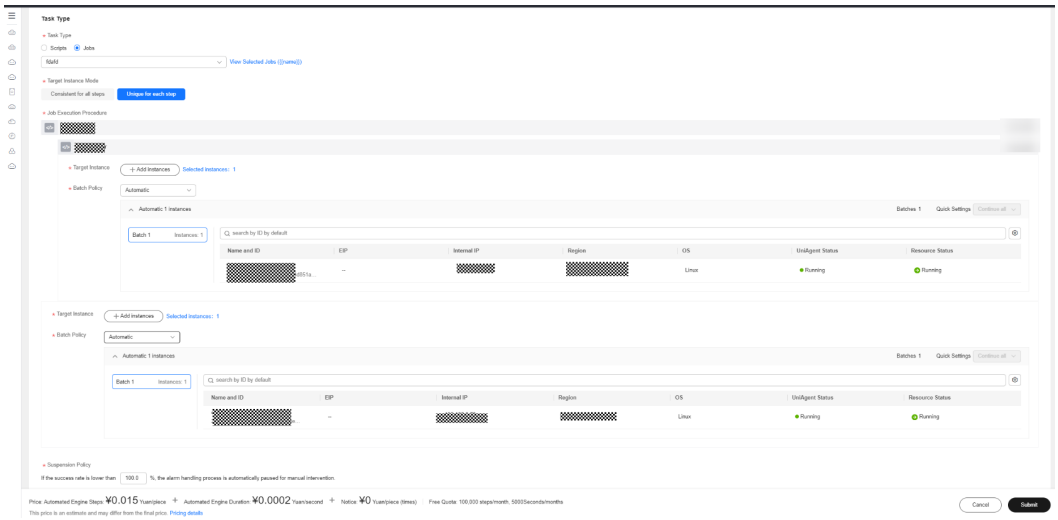
b. Click **View Selected Jobs**. The job details dialog box is displayed on the right.

Figure 5-119 Viewing job details



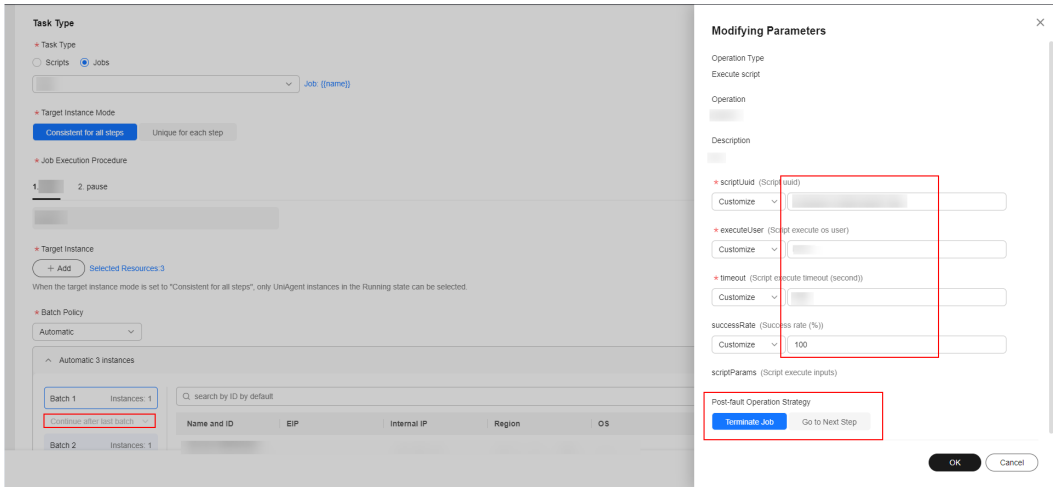
c. Select the target instance mode. If you select **Unique for each step**, you can set the target instance and batch policy for each job step.

Figure 5-120 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 5-121 Modifying job execution parameters

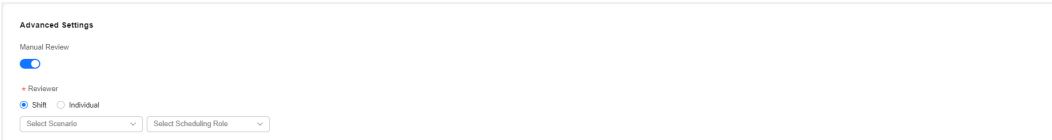


e. Select an instance. **Manual selection**: Manually select instances. **Select All**: Select all instances associated with a single region or application.

f. Select the batch policy and suspension policy.

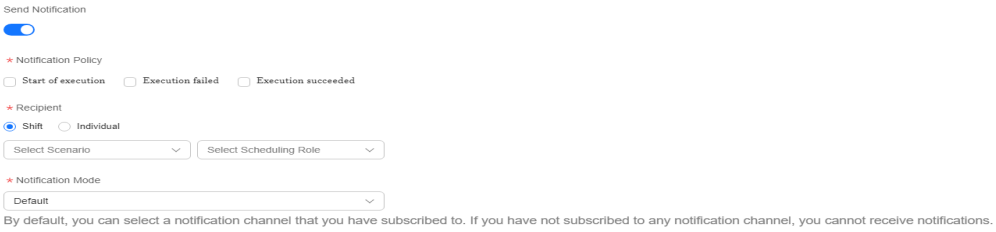
Step 8 You can select whether to manually review task.

Figure 5-122 Enabling manual review



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

Figure 5-123 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.

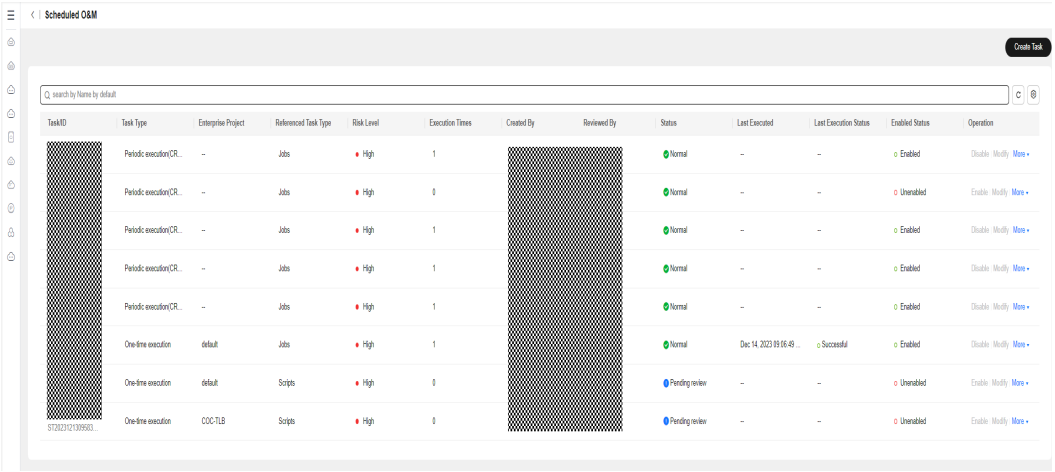
----End

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**.

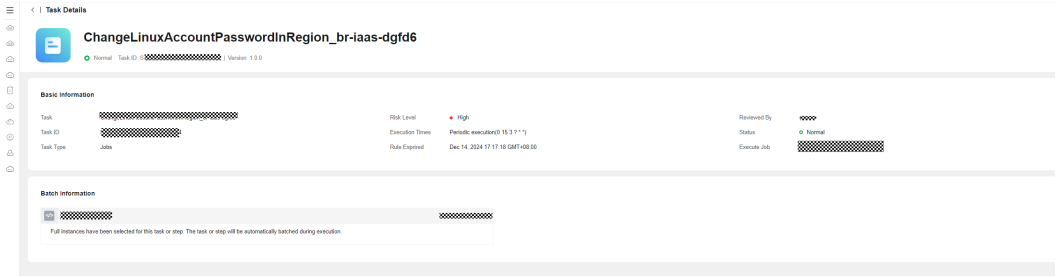
Figure 5-124 Scheduled tasks



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.

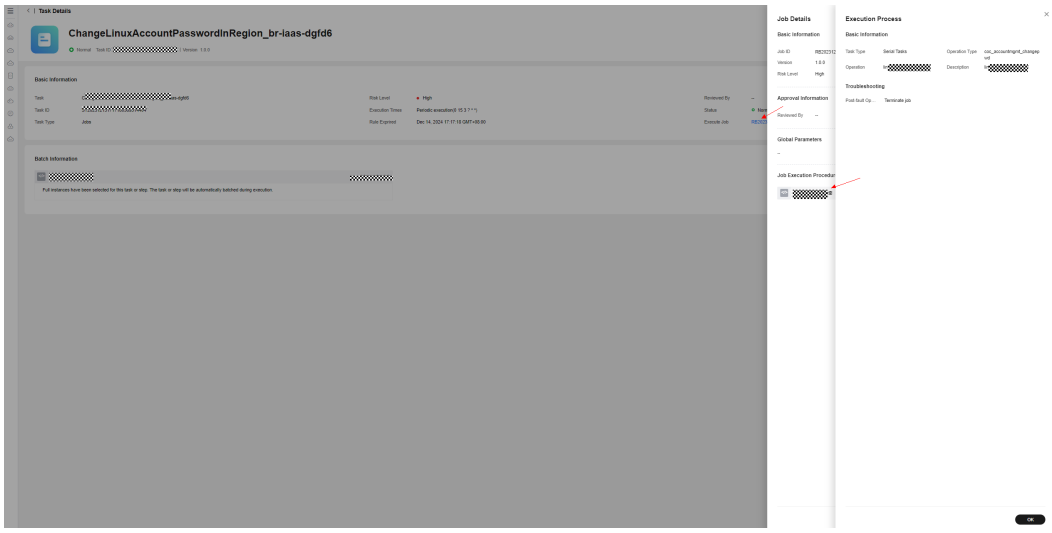
Step 4 Click a task name to view the scheduled task details.

Figure 5-125 Viewing task details



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 5-126 Script or job details



NOTE

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

----End

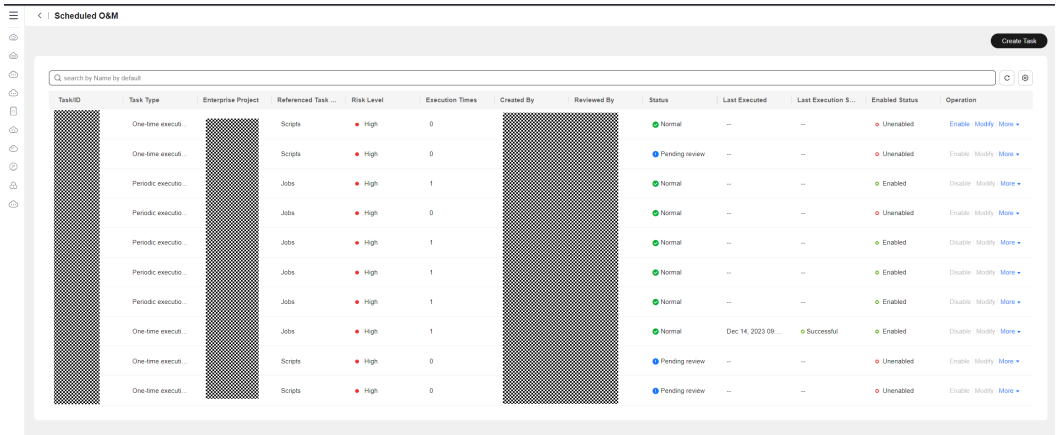
Enabling and Disabling a Scheduled Task

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 5-127 Viewing task list



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

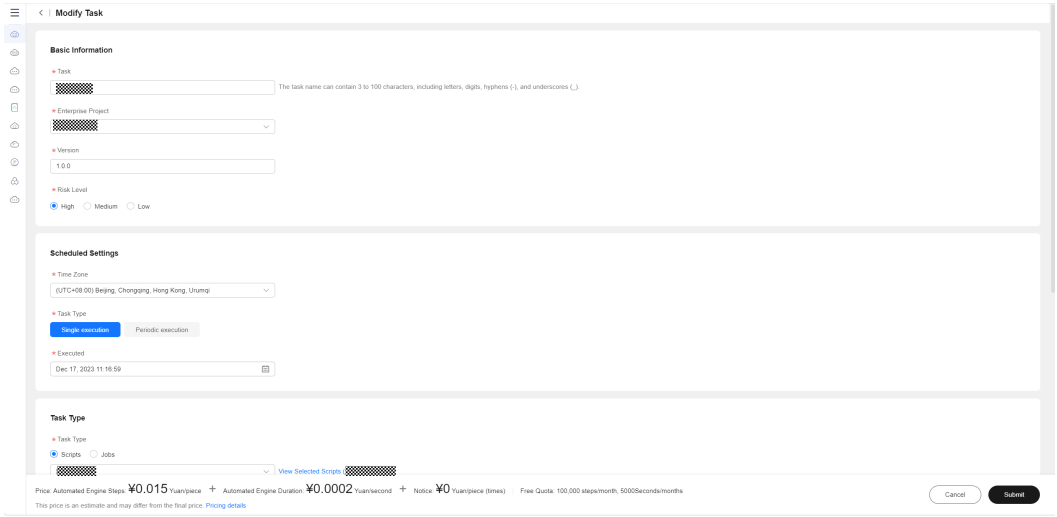
Editing a Scheduled Task

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 5-128 Modifying a scheduled task



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

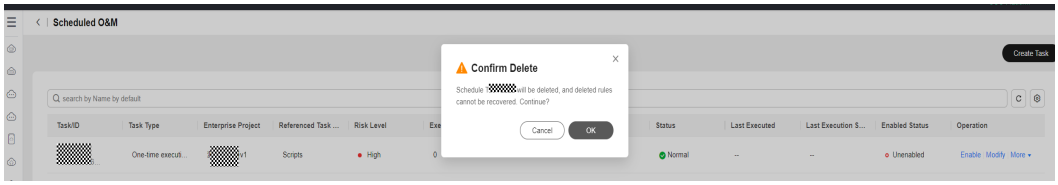
Deleting a Scheduled Task

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 5-129 Deleting a scheduled task



NOTE

Only disabled scheduled tasks can be deleted.

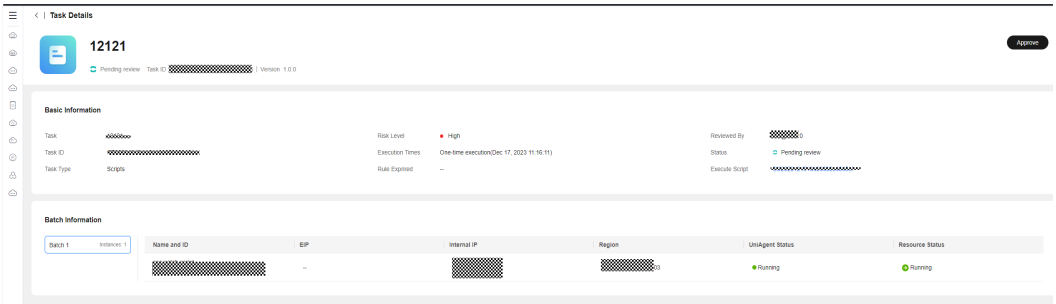
----End

Reviewing Scheduled O&M Tasks

Step 1 Log in to **COC**.

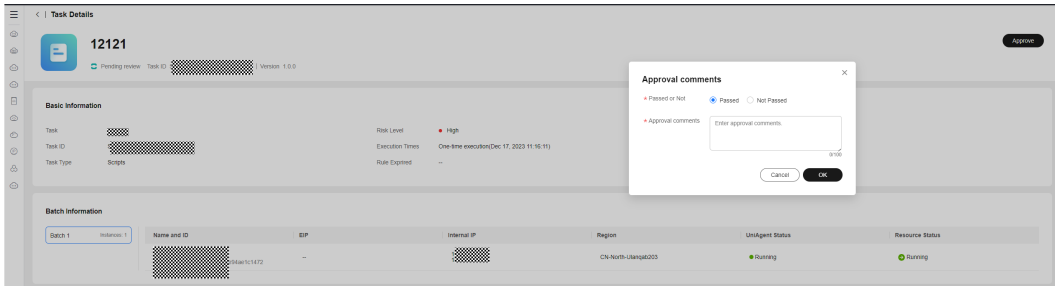
Step 2 In the navigation pane on the left, choose **Automated O&M** > **Scheduled O&M**. Select a record whose status is **Pending review** and click the task name.

Figure 5-130 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 5-131 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

5.4.2 Scheduled Task Execution Records

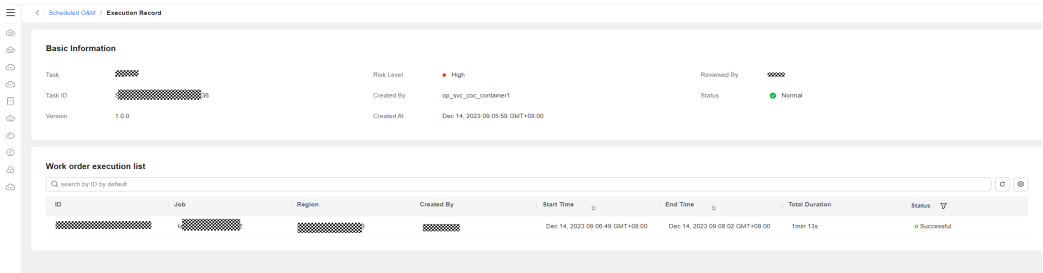
View the execution records of a scheduled task.

Step 1 Log in to **COC**.

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

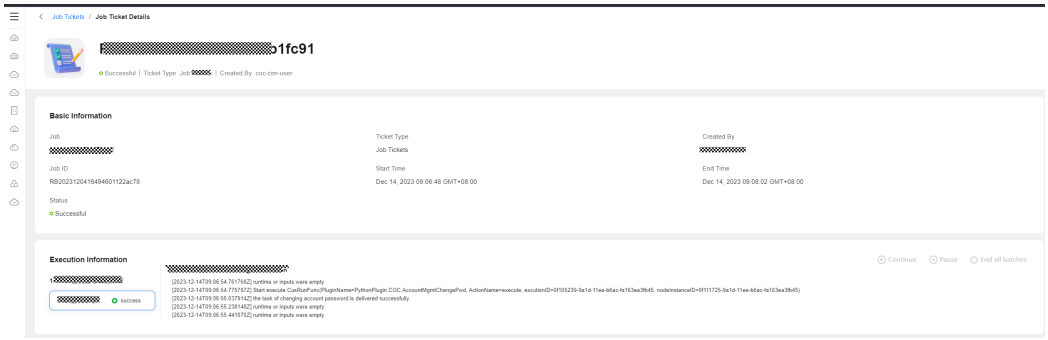
Step 3 On the **Scheduled O&M** page, locate a target task, choose **More** > **Execution Record** in the **Operation** column.

Figure 5-132 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 5-133 Job execution details



----End

5.5 Account Management

Account Management allows users to manage human-machine accounts of resource instances such as Linux OSs and databases, and to change account passwords automatically. Users can also obtain host passwords through account management.

Figure 5-134 Resource account management process

NOTE

You can obtain the host password from the **Accounts** tab page only after you complete the resource account management process.

5.5.1 Key Management

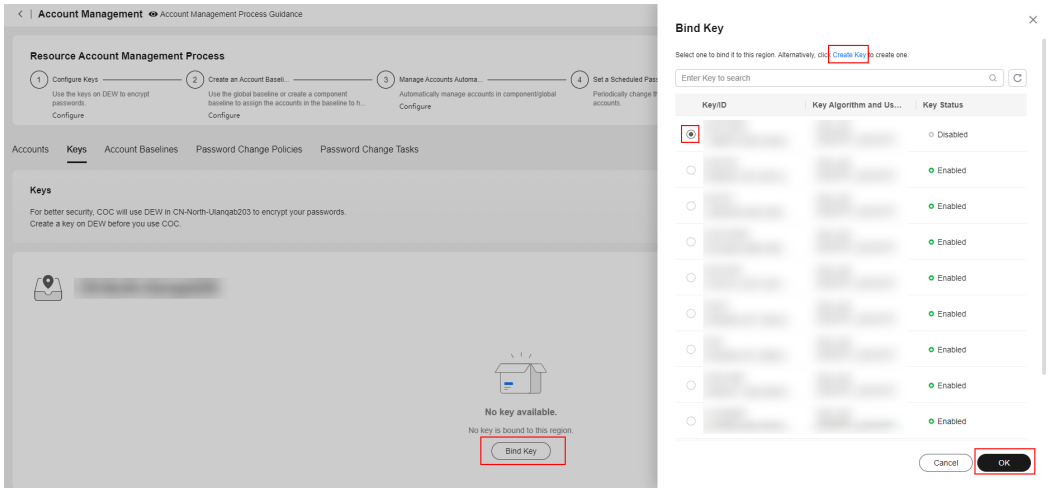
Configuring the Key

Step 1 Log in to **COC**.

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

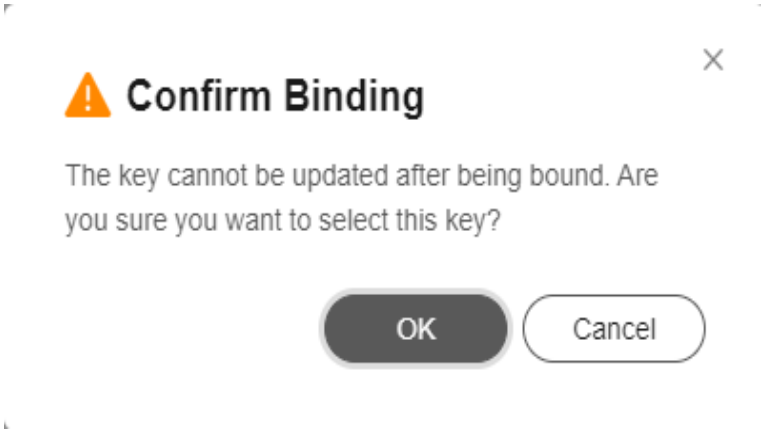
Step 3 On the displayed page, click the **Keys** tab, and click **Bind Key**. The **Bind Key** page is displayed. If no key is available, click **Create Key** to go to the DEW service page to create a key. After the key is created, refresh the key list to select the key.

Figure 5-135 Binding a key



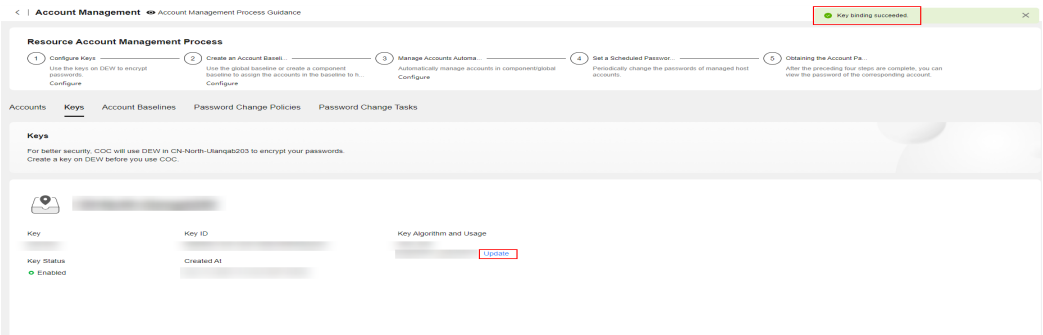
Step 4 Click **OK**. A dialog box is displayed, indicating that the bound key cannot be updated once it is used. Click **OK** again.

Figure 5-136 Confirming the binding



Step 5 Click **Update** to update the key as needed. (Only the keys that are not used to encrypt any host account password can be updated.)

Figure 5-137 Key binding succeeded



----End

5.5.2 Account Baseline

Creating an Account Baseline

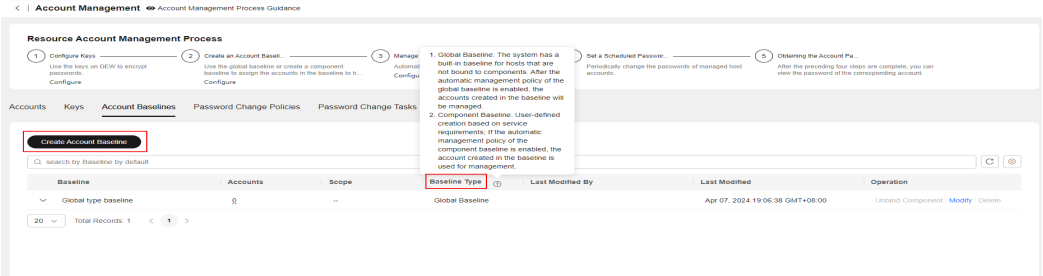
Step 1 Log in to **COC**.

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

Step 3 On the displayed page, click the **Account Baseline** tab.

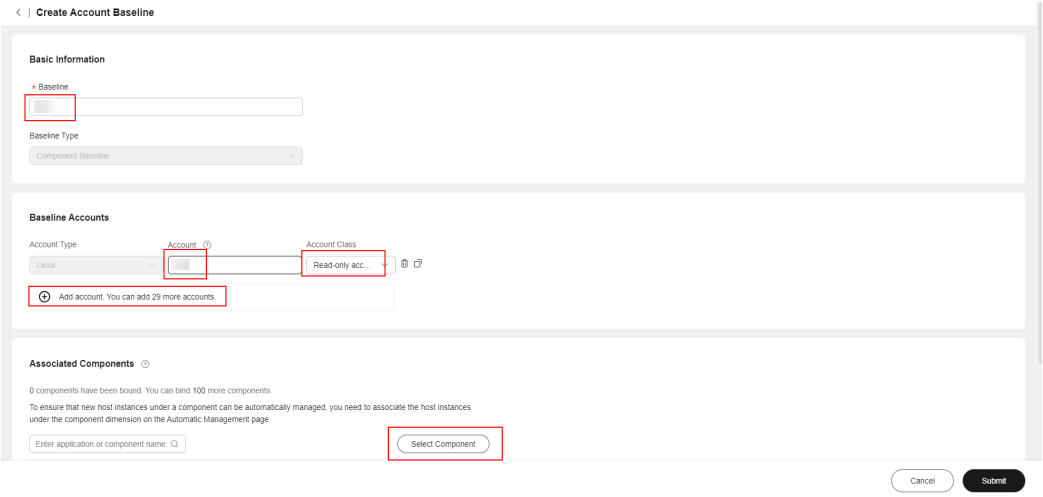
Step 4 Click **Create Account Baseline**. Only the accounts of the host that is bound to a component can be managed by the created baseline. For details about how to bind hosts to a component, see **Creating an Application** and **Creating a Component**. For hosts that are not bound to components, the system uses the built-in global baseline to manage host accounts by default.

Figure 5-138 Creating an account baseline



Step 5 Set the baseline name, and add baseline accounts based on service requirements. For example, set account name to root and account class to non-read-only account. Then associate the baseline with components. The associated components use the account baseline to manage hosts.

Figure 5-139 Baseline information

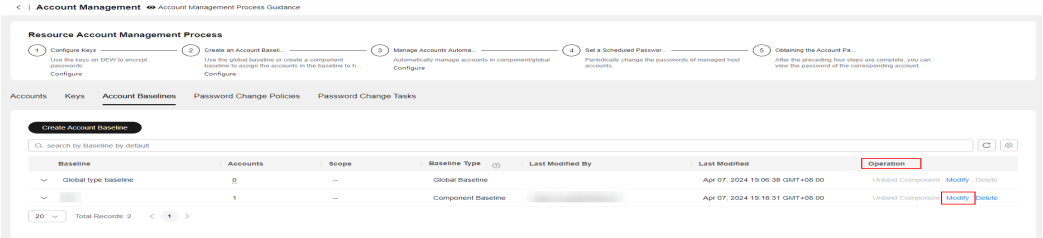


CAUTION

To ensure that new host instances of a component can be automatically managed, you need to perform association operations in the component dimension on the automatic management page.

Step 6 Delete or modify the account baseline in the **Operation** column as needed. Note: Before deleting a baseline, you need to unbind all associated components.

Figure 5-140 Deleting and modifying a baseline



----End

5.5.3 Password Change Policies

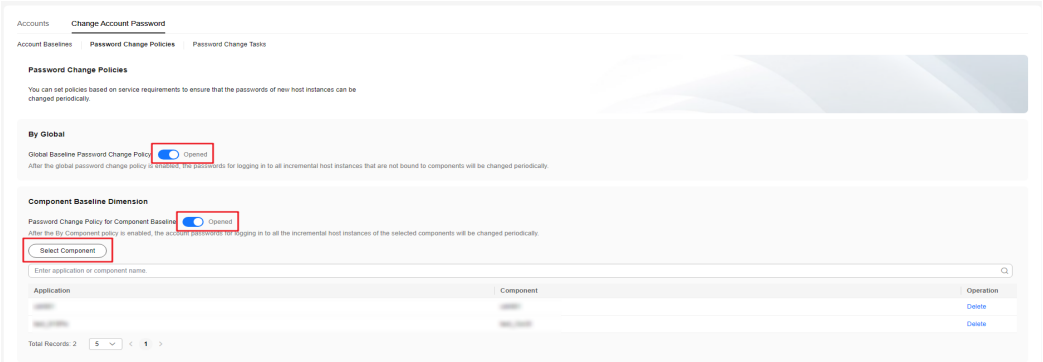
Enabling the Password Change Policy

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Account Management**.

Step 3 Click the **Change Account Password** tab and then the **Password Change Policies** tab, and set the management policy based on service requirements to ensure that incremental host instances can be automatically managed.

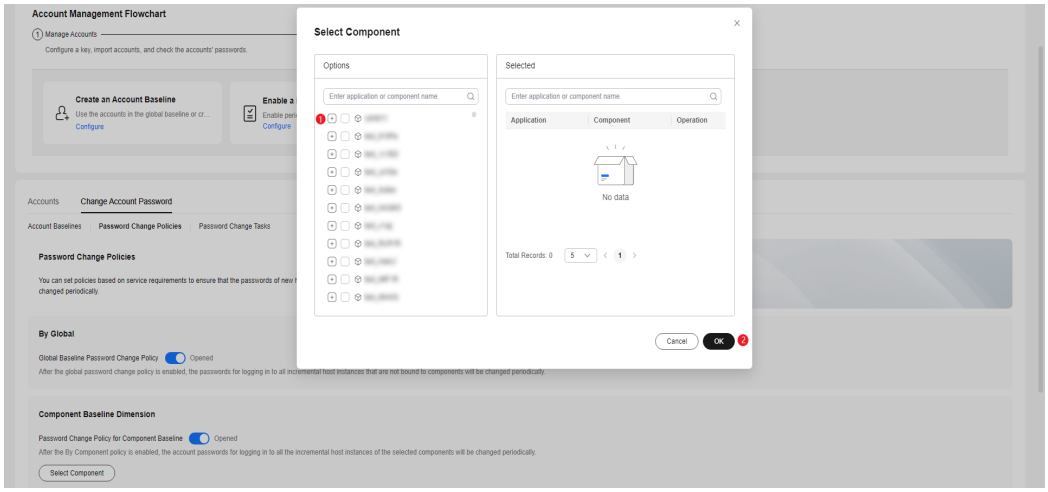
Figure 5-141 Enabling the password change policy



Step 4 To automatically manage incremental host instances that are not bound to components, enable **Global Baseline Password Change Policy** in **By Global**. To automatically manage the incremental host instances bound a component, enable **Password Change Policy for Component Baseline** in **Component Baseline**

Dimension, click **Select Component**, search for the application or component names, and click **OK**.

Figure 5-142 Selecting a desired component



----End

5.5.4 Password Change Tasks

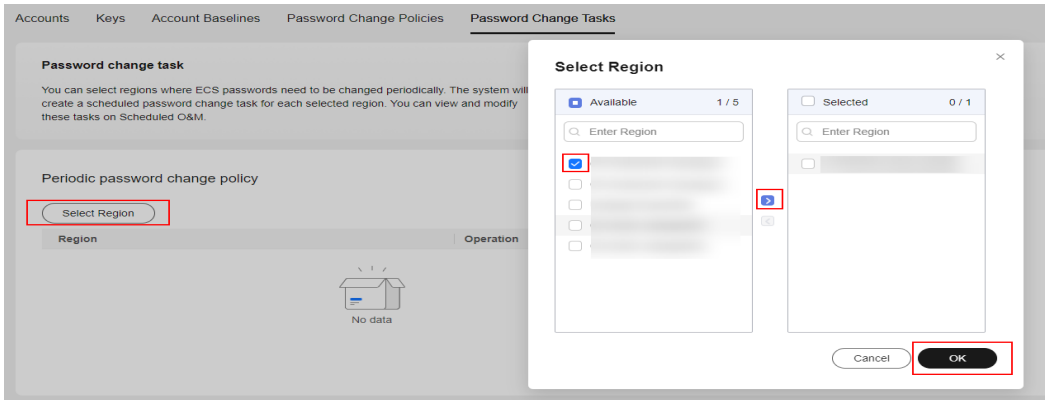
Configuring Password Change Regions

Step 1 Log in to **COC**.

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

Step 3 Click the **Password Change Tasks** tab and select the region where periodic password change needs to be enabled. Click **Select Region**, select the region to be configured, click the rightward arrow, and click **OK**. Then you can click View Task Details in the **Operation** column to view the password change task in the configured region. You can also delete the region based on service requirements.

Figure 5-143 Configuring regions



Step 4 Obtain host passwords on the **Accounts** tab page as needed.

----End

5.5.5 Querying a Host Password

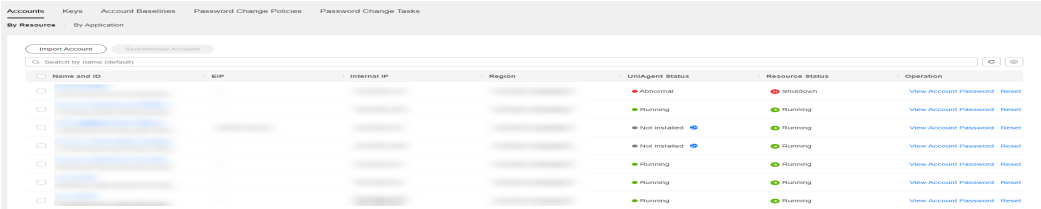
Obtaining a Host Password

Step 1 Log in to **COC**.

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

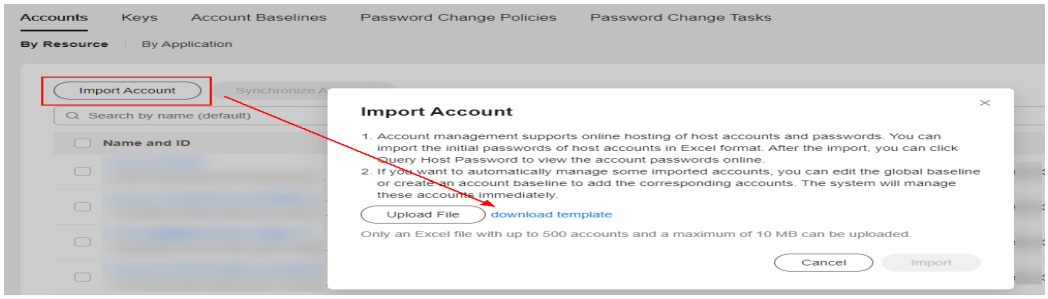
Step 3 Click the **Accounts** tab. **By Resource** is used to manage all purchased host instances, and **By Application** is used to manage purchased hosts that are bound to applications.

Figure 5-144 Account management



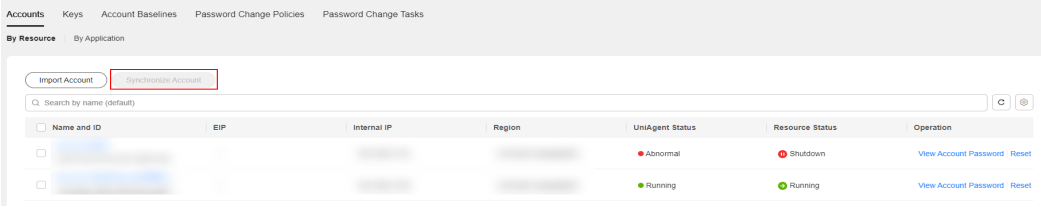
Step 4 To save accounts, click **Import Account**, download the Excel template, enter the host information, confirm the information, and upload the template. The imported host accounts are not managed. If you want to automatically manage the imported accounts, you can modify the global baseline or create an account baseline to add the accounts to be managed. Then, the system will immediately manage the host accounts.

Figure 5-145 Importing accounts



Step 5 To synchronize the accounts added to an OS, select the host corresponding to the OS on the **Accounts** tab page, and click **Synchronize Account**. If you want to automatically manage the added accounts, configure the accounts in the account baseline. For details, see **Account Baseline**.

Figure 5-146 Synchronizing OS accounts



Step 6 Locate the target host record, click **View Account Password** in the **Operation** column. The **Password Change Details** page is displayed on the right. You can view the password change status and the password change failure cause of the target account. Currently, only the account passwords of a single host can be queried once. Ensure that the password change status of the target host account is succeeded, or that the password change failure cause is that the target account is not managed. Otherwise, the password may fail to be obtained. If password change status is **Failed**, rectify the fault based on the failure cause.

Account passwords of hosts can be changed when the following conditions are met:

1. The resources status of the host is **Running**.

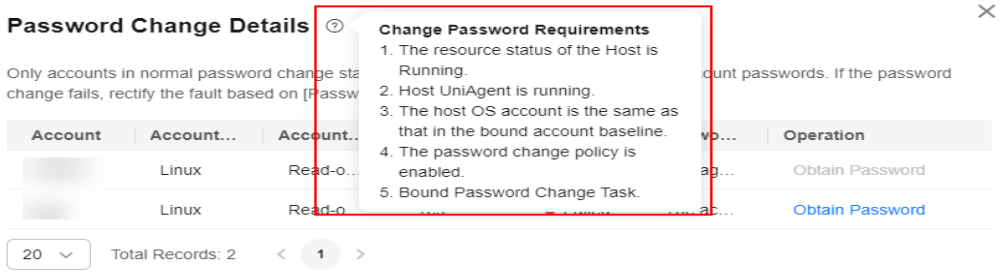
2. The UniAgent status of the host is **Running**.

3. The accounts on the host OS are the same as those in the bound account baseline.

4. The password change policy has been enabled.

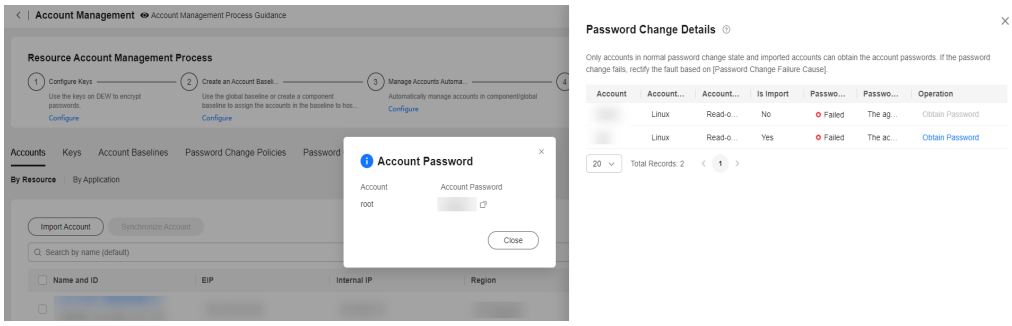
5. A password change task has been bound.

Figure 5-147 Password Change Details



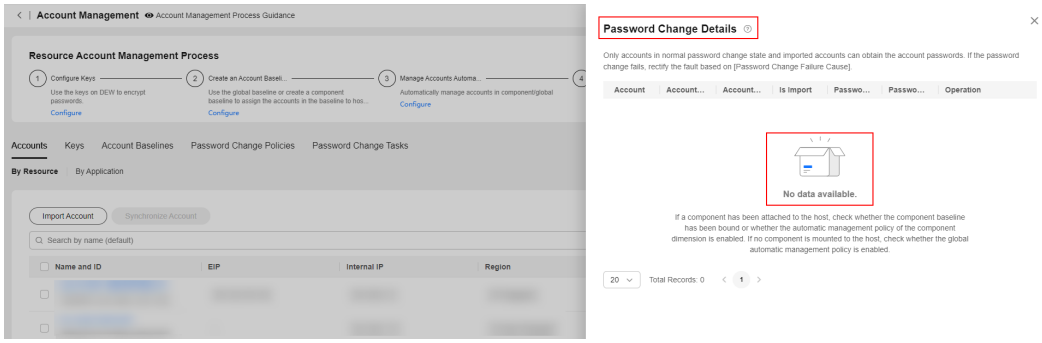
Step 7 Locate the target host account, and click **Obtain Password** in the **Operation** column to query the account password.

Figure 5-148 Obtaining account passwords



If no data is displayed on the **Password Change Details** page, check whether the host is bound to a component. If yes, check whether the automatic management policy of the bound component baseline or of the component dimension is enabled. If the host is not bound to a component, check whether the automatic management policy of the global dimension is enabled.

Figure 5-149 No data displayed



----End

5.6 Creating a Parameter

Scenarios

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

Precautions

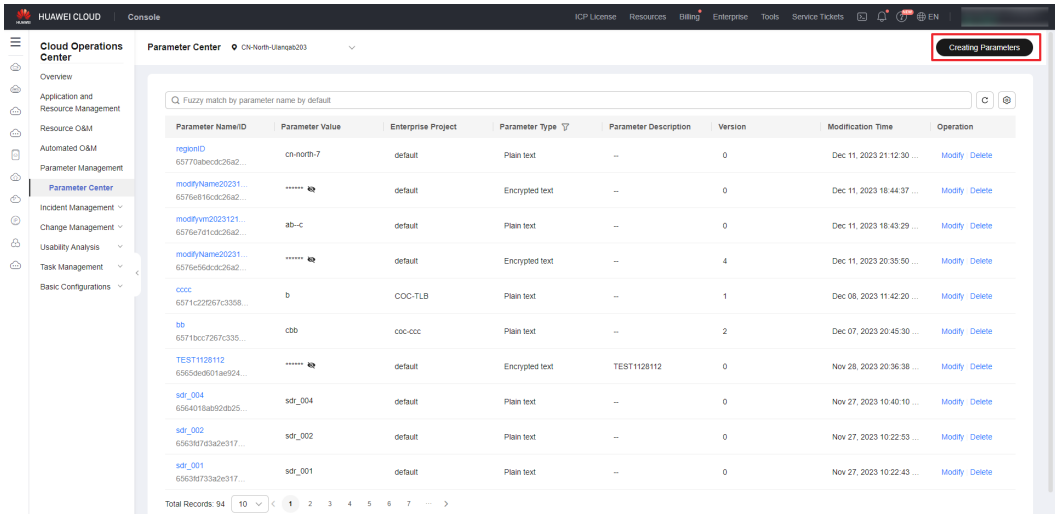
Parameter policies may delete parameters. Exercise caution when configuring parameter policies.

Procedure

Step 1 Log in to **COC**.

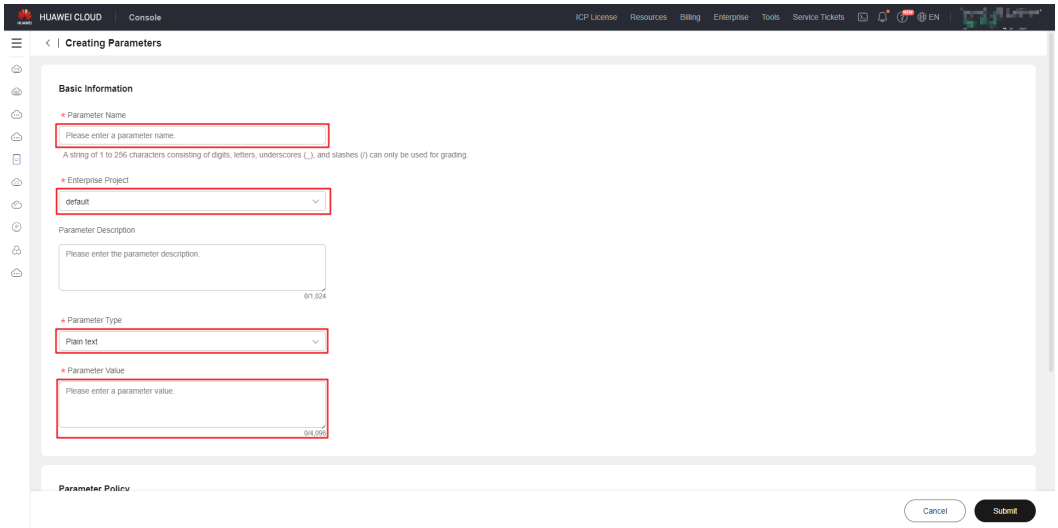
Step 2 In the left navigation pane, choose **Parameter Management** > **Parameter Center**. In the right pane, click **Creating Parameters**.

Figure 5-150 Creating a parameter



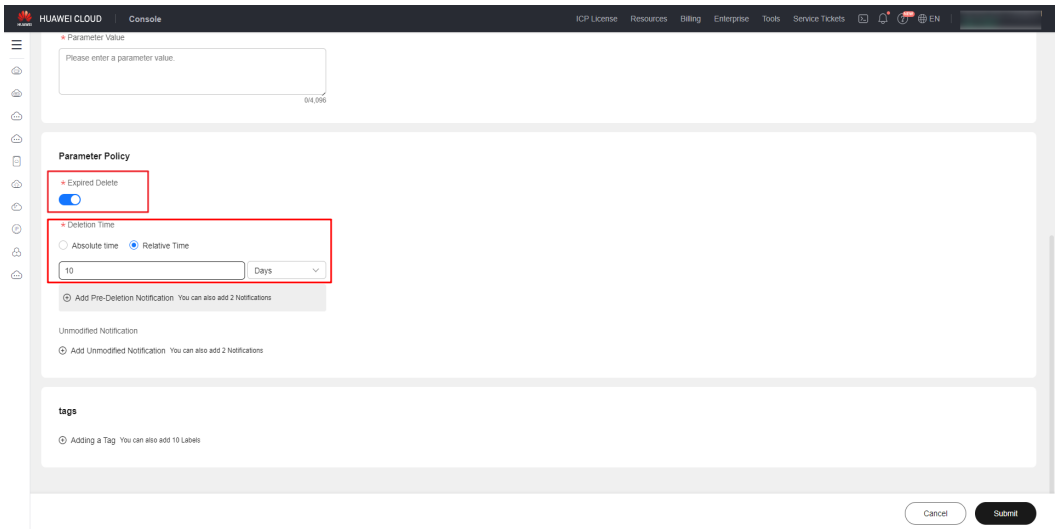
Step 3 Set the basic information, including **Parameter Type**. (**Parameter Name**, **Enterprise Project**, and **Parameter Type** cannot be changed after the parameter is created.)

Figure 5-151 Basic information



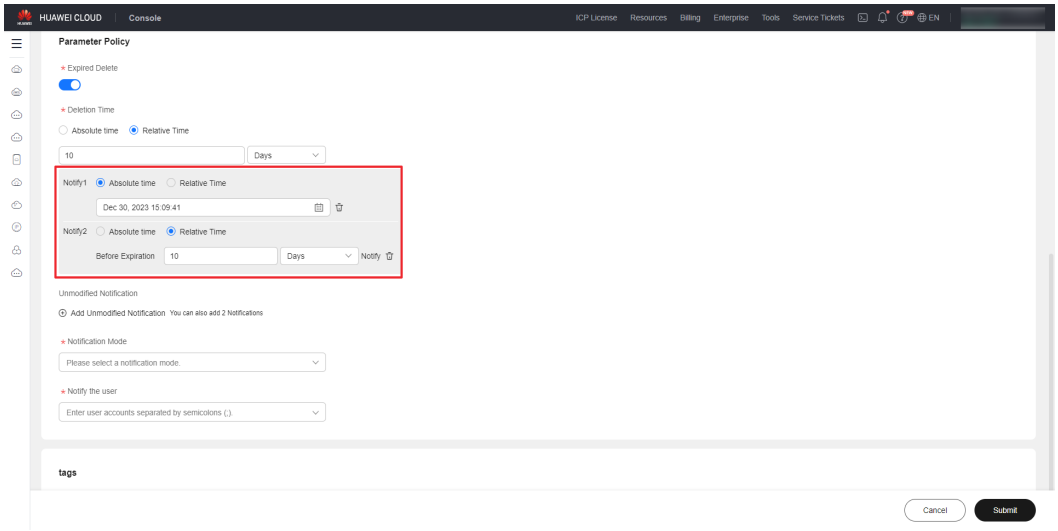
Step 4 Determine whether to set a policy for deleting the parameter upon expiration. If you do not want to set such a policy, skip steps 5 and 6.

Figure 5-152 Policy for deleting the parameter upon expiration



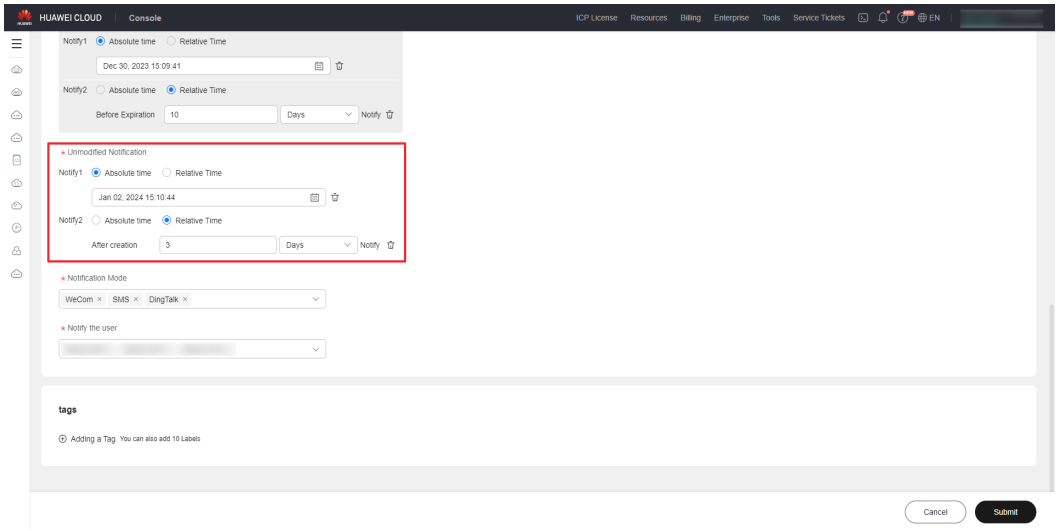
Step 5 Determine whether to set pre-deletion notifications. If you do not want to set such notifications, skip this step. If you want to set such notifications, click **Add Pre-Deletion Notification** and set the notification time.

Figure 5-153 Adding pre-deletion notifications



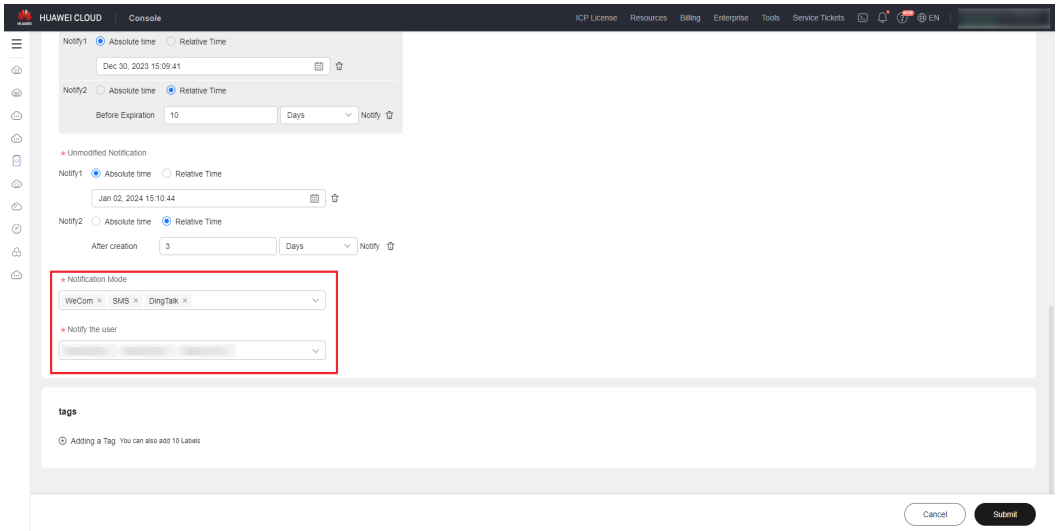
Step 6 Determine whether to set unmodified notifications. If you do not want to set such notifications, skip this step. If you want to set such notifications, click **Add Unmodified Notification** and set the notification time.

Figure 5-154 Adding unmodified notifications



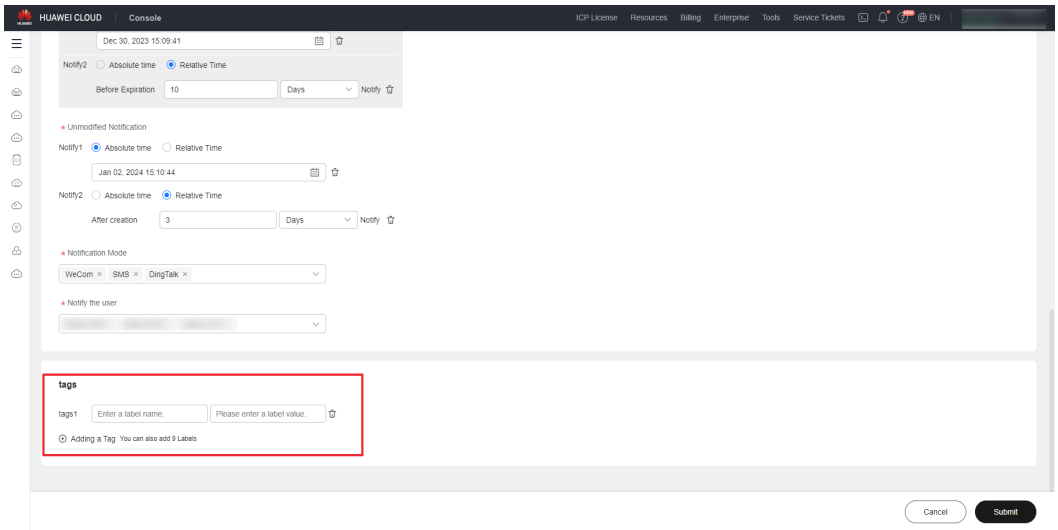
Step 7 If there are pre-deletion or unmodified notification policies, set **Notification Mode** and **Notify the user**.

Figure 5-155 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 5-156 Adding parameter tags



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

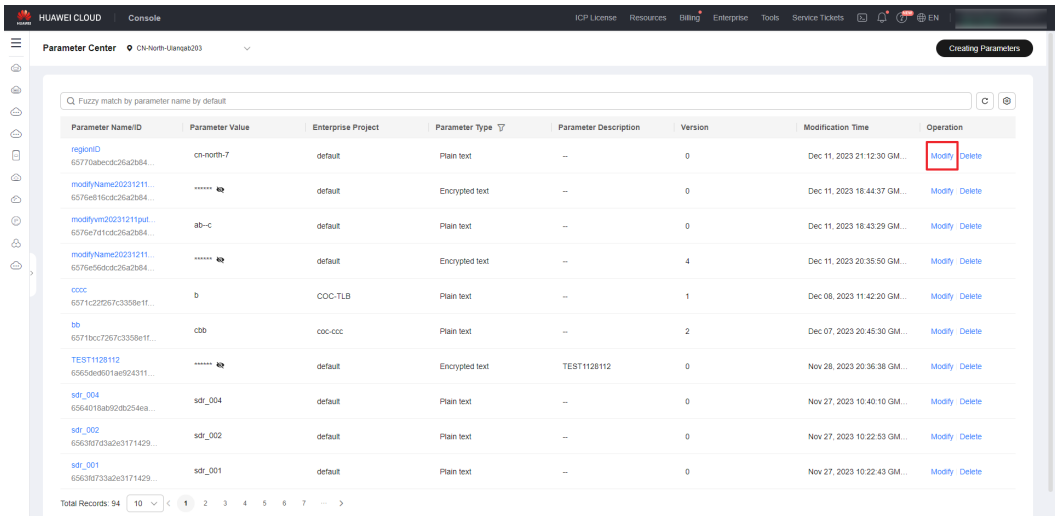
----End

5.7 Modifying a Parameter

Step 1 Log in to **COC**.

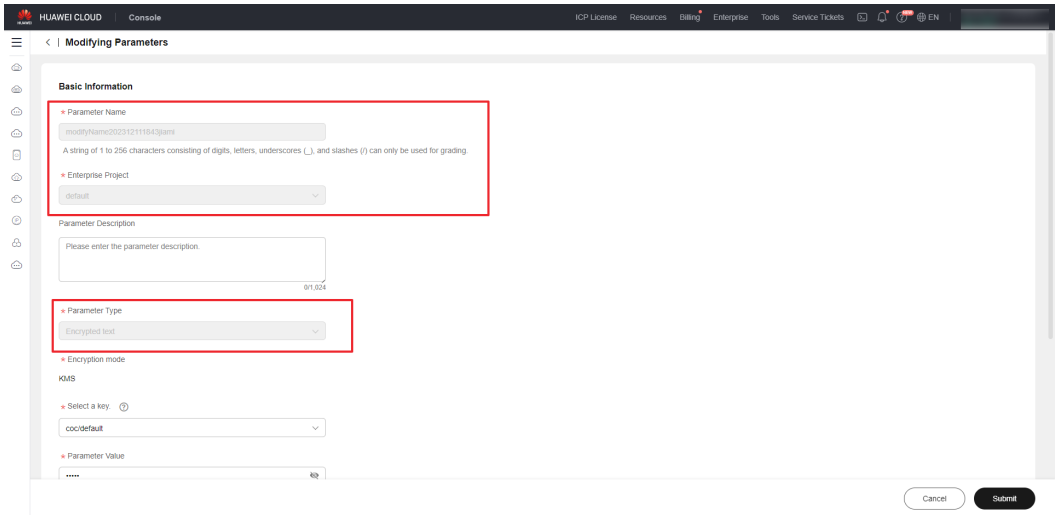
Step 2 In the left navigation pane, choose **Parameter Center**. Locate the target parameter and click **Modify** in the **Operation** column.

Figure 5-157 Parameter list



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

Figure 5-158 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.

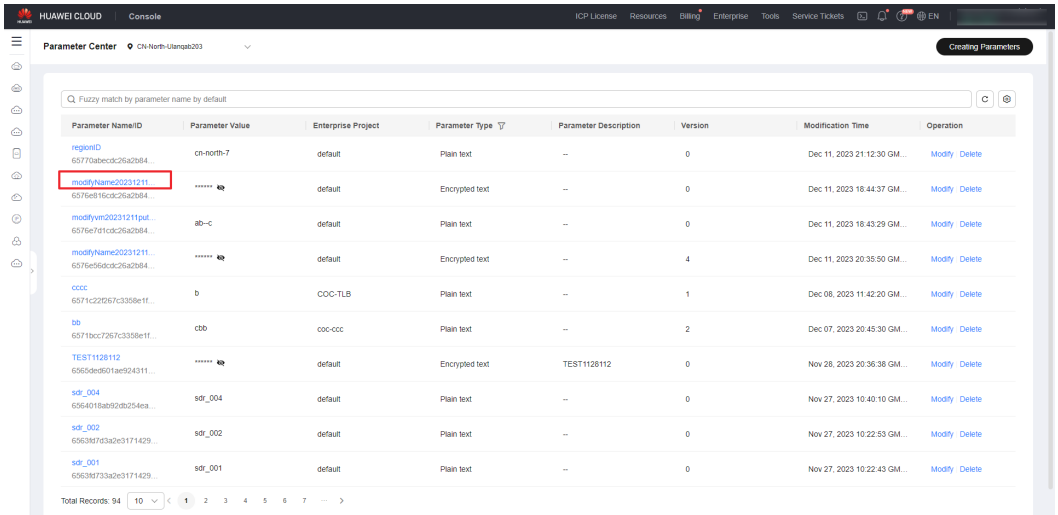
----End

5.8 Viewing Parameter Details

Step 1 Log in to **COC**.

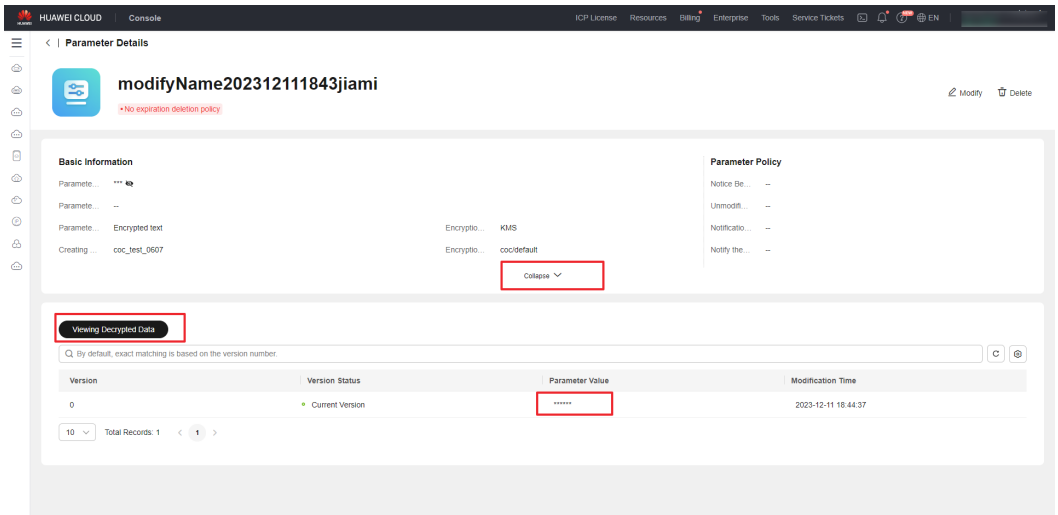
Step 2 In the navigation pane on the left, choose **Parameter Center**. Click the name of a parameter to go to the details page and view the parameter details and historical versions.

Figure 5-159 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 5-160 Parameter details

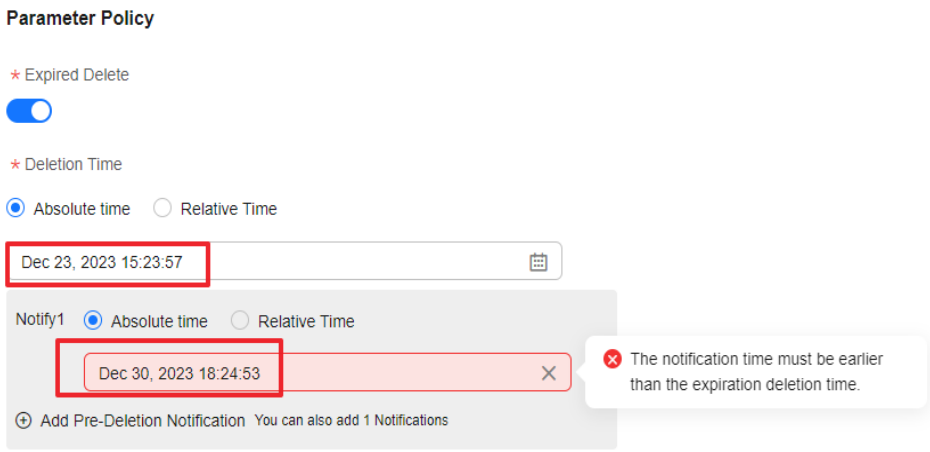


----End

5.9 Expiration Notification

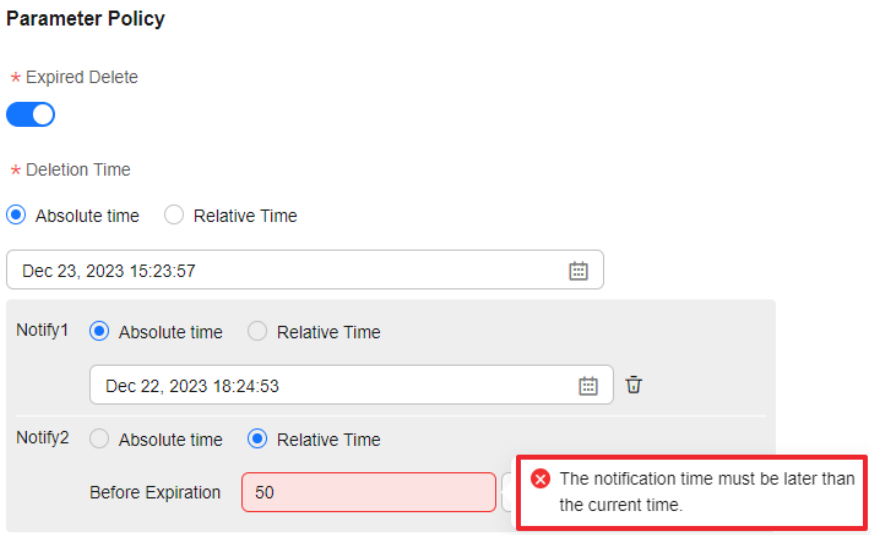
- The expiration notification time must be earlier than the time of deletion upon expiration.

Figure 5-161 If the expiration notification time is later than the time of deletion upon expiration



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

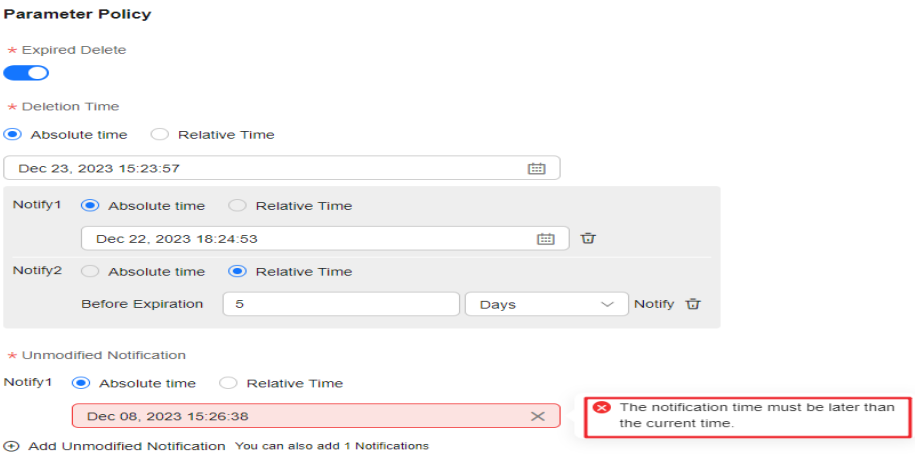
Figure 5-162 If the expiration notification time is earlier than the system time



5.10 Unmodified Notifications

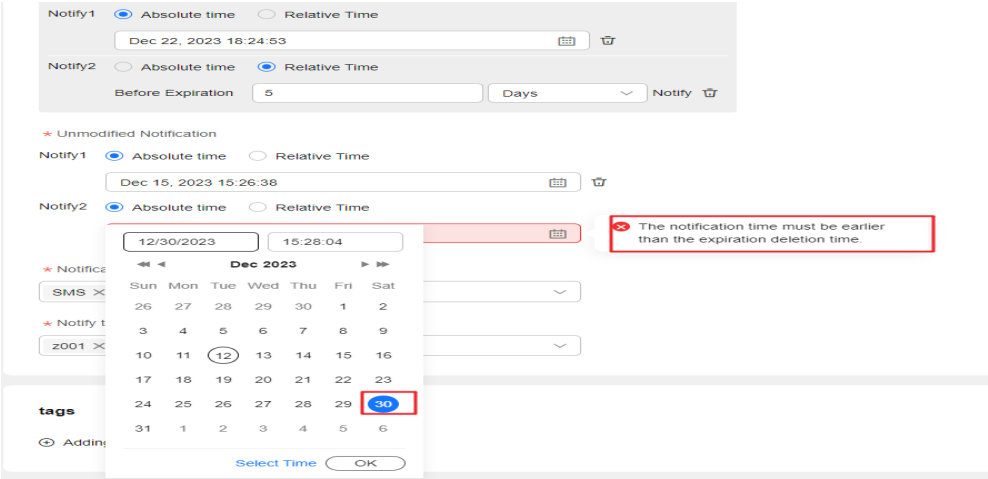
- The unmodified notification time cannot be earlier than the parameter creation or modification time.

Figure 5-163 If the notification time is 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 5-164 If the unmodified notification time is later than the time of deletion upon expiration



6 Incident Management

6.1 Alarms

6.1.1 Viewing Alarms

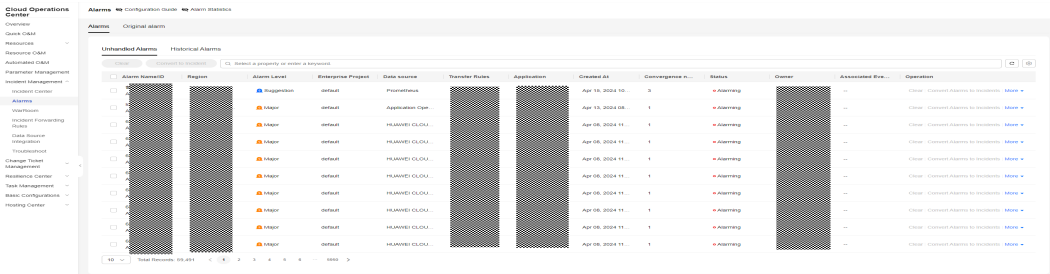
Step 1 Log in to **COC**.

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 6-1 Alarm list



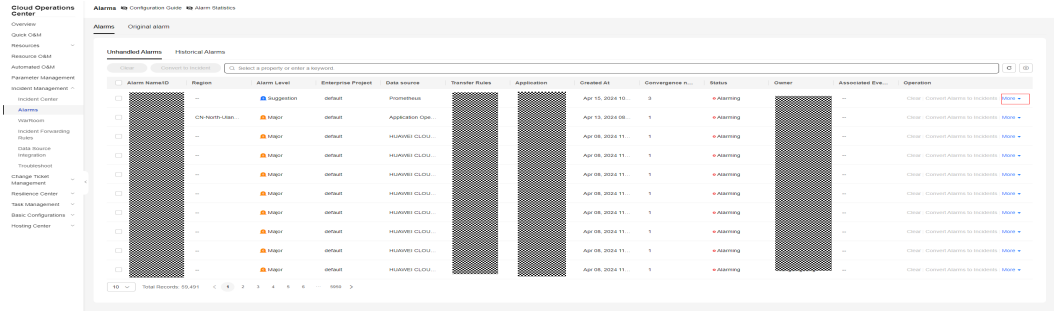
----End

6.1.1.1 Handling Alarms

Step 1 Log in to **COC**.

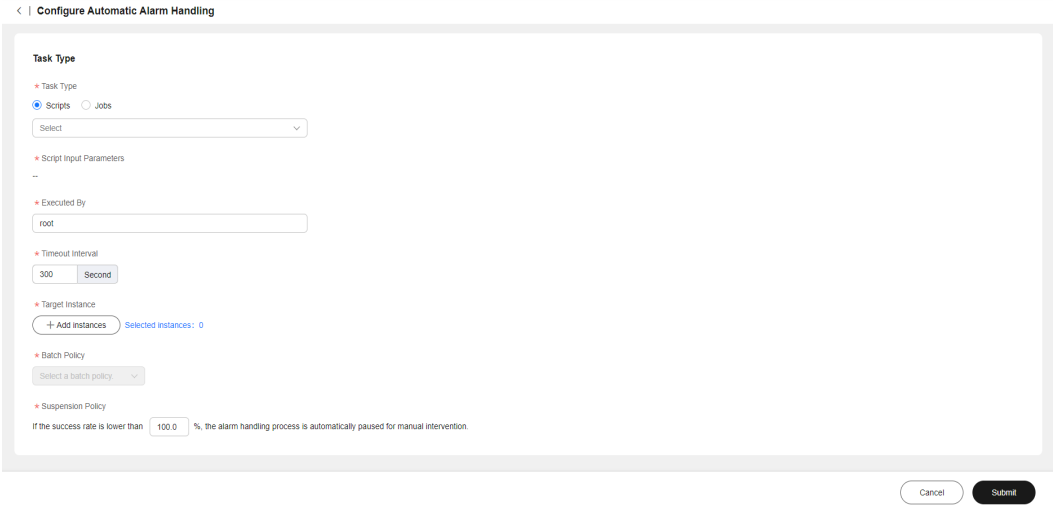
Step 2 In the navigation pane, choose **Incident Management** > **Alarms**. On the displayed **Alarms** tab page, click the **Unhandled Alarms** tab. In the displayed alarm list, locate the alarm you want to handle, click **More** in the **Operation** column and choose **Handle** to handle the alarms.

Figure 6-2 Handling alarms



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

Figure 6-3 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

6.1.1.2 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.

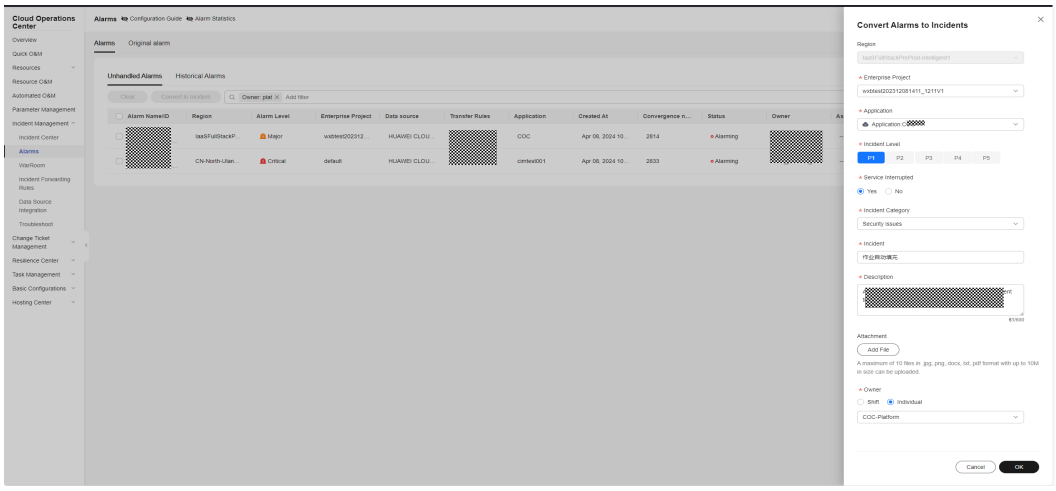
Step 3 Select the target alarms and click **Convert to Incident**.

NOTE

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

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

Figure 6-4 Converting an alarm to an incident



NOTE

For details about the incident parameters, see Creating an Incident.

----End

6.1.1.3 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.

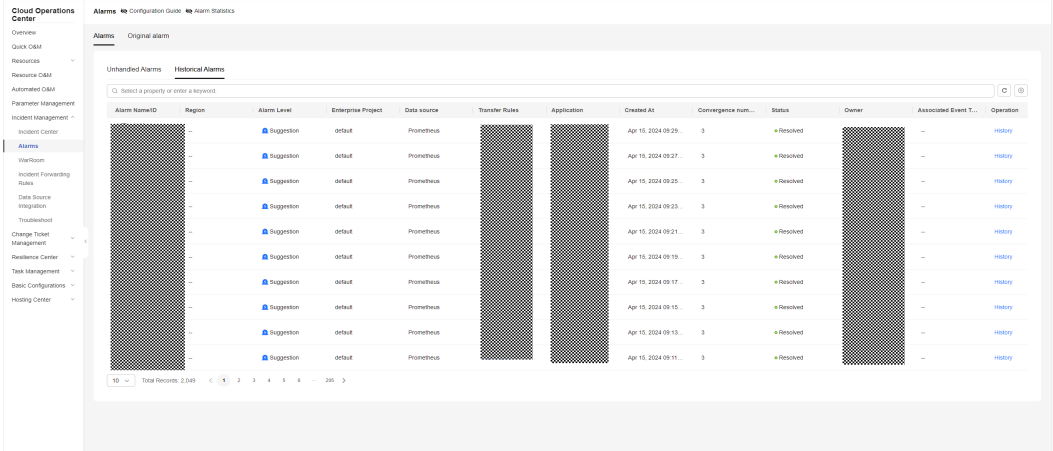
----End

6.1.1.4 Historical Alarms

Step 1 Log in to **COC**.

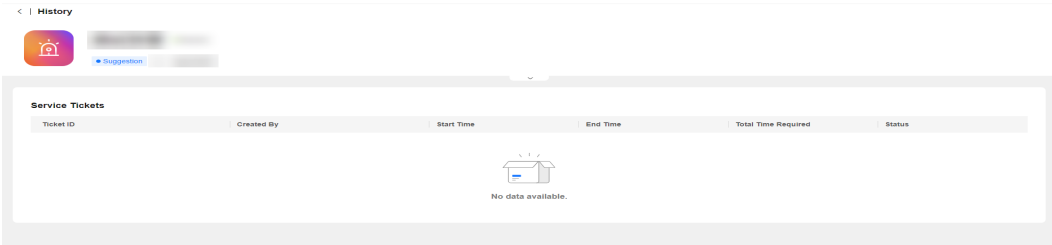
Step 2 In the navigation pane, choose **Incident Management** > **Alarms**. On the displayed **Alarms** tab page, click the **Historical Alarms** tab to view the historical alarms.

Figure 6-5 Historical alarm list



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

Figure 6-6 Historical records of an alarm



----End

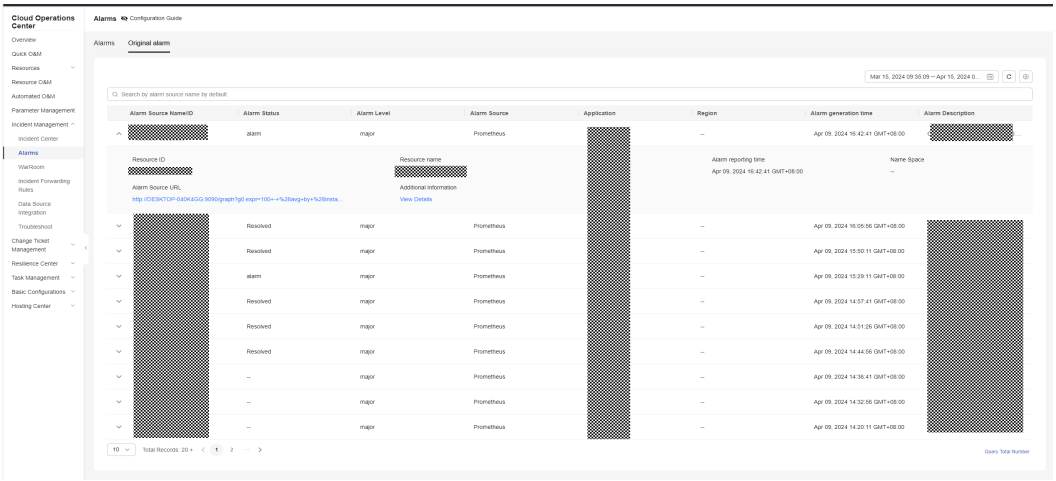
6.1.2 Original Alarms

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 6-7 Original alarms



----End

6.2 Incident Management

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.

6.2.1 Incidents

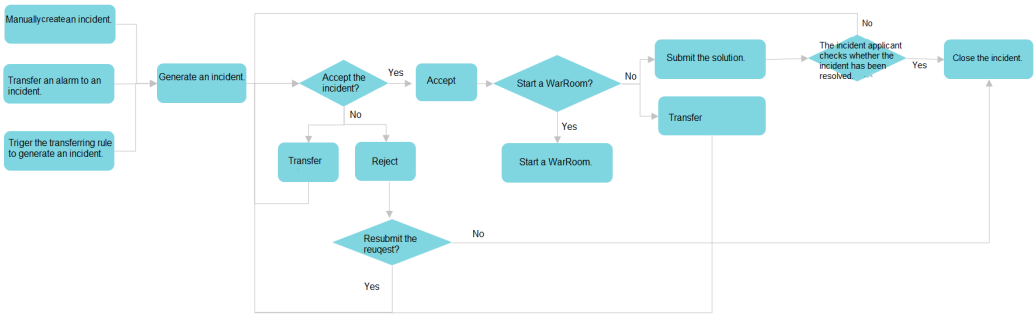
After an incident is created, it is in the unaccepted state. You can forward, reject, or accept the incident.

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 war room startup.

After an incident ticket is processed, it becomes the resolved and to be verified state. You can perform the verification operation. If the verification is successful, the incident ticket becomes the completed state. If the verification fails, the incident ticket becomes the accepted state again.

Figure 6-8 Incident flowchart



6.2.2 Creating an Incident

Scenarios

Create an incident ticket using Cloud Operations Center.

Prerequisites

You have created an application by referring to Application Management.

Precautions

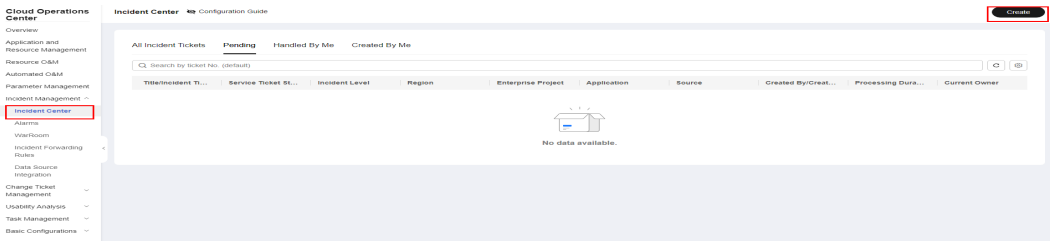
Create an incident service ticket.

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**.

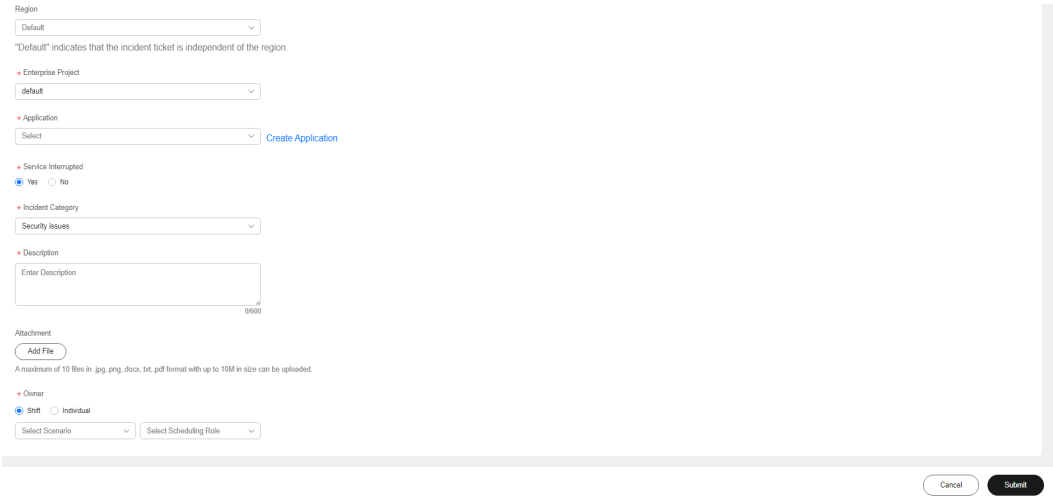
Figure 6-9 Incident ticket list



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 6-10 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

6.2.3 Handling an Incident

6.2.3.1 Rejecting an Incident

Scenarios

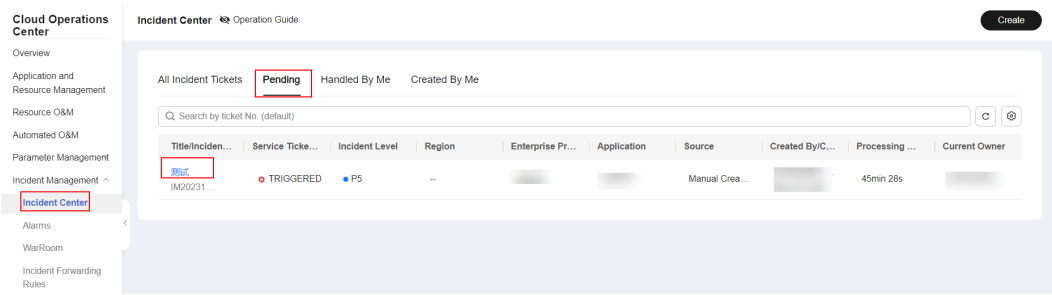
If an incident is unreasonable, the incident handler can reject the incident.

Procedure

Step 1 Log in to **COC**.

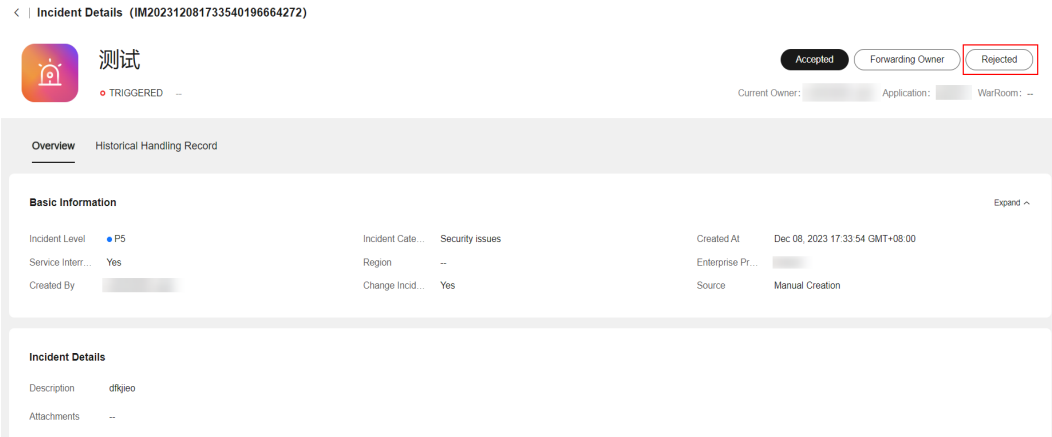
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-11 List of incidents to be handled



Step 3 Click **Rejected**.

Figure 6-12 Rejecting an incident



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

Figure 6-13 Entering a reason for rejection

----End

6.2.3.2 Resubmitting an Incident After Rejection

Scenarios

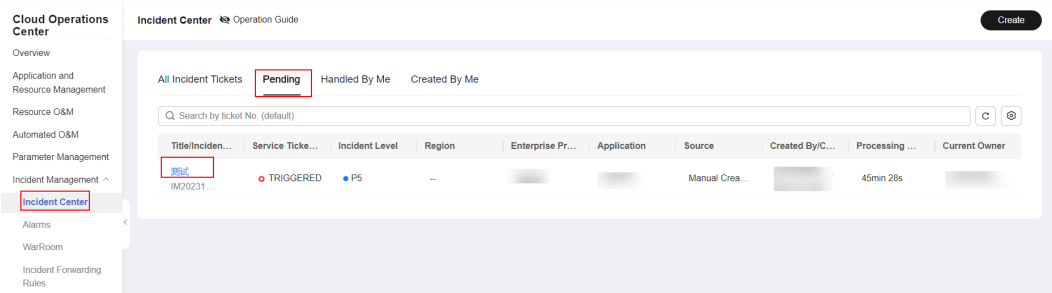
After an incident ticket is rejected, modify the incident ticket content.

Procedure

Step 1 Log in to **COC**.

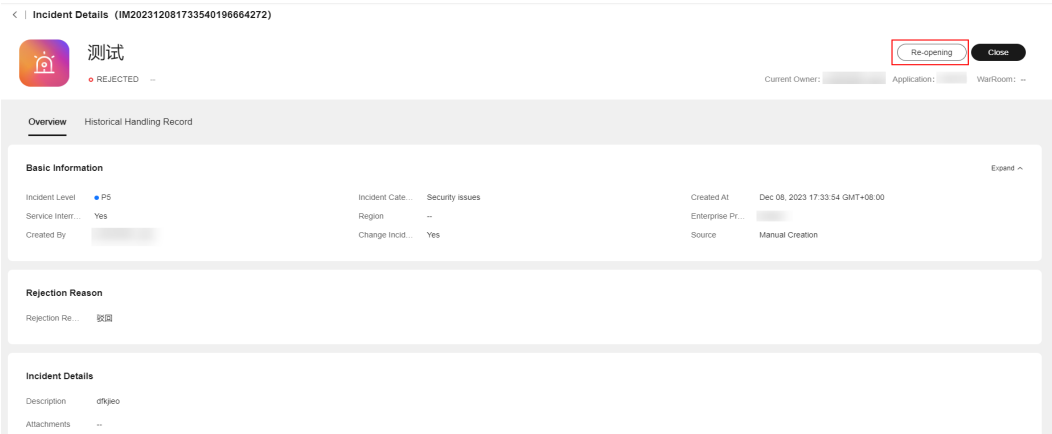
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-14 Incident details



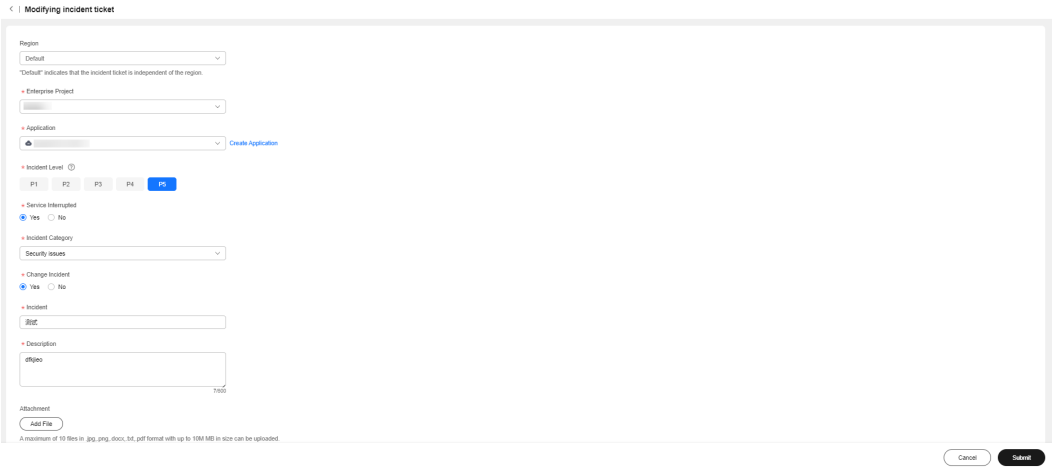
Step 3 Click **Re-opening**.

Figure 6-15 Restarting an incident



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

Figure 6-16 Modifying the content of an incident ticket



----End

6.2.3.3 Forwarding Incidents

Scenarios

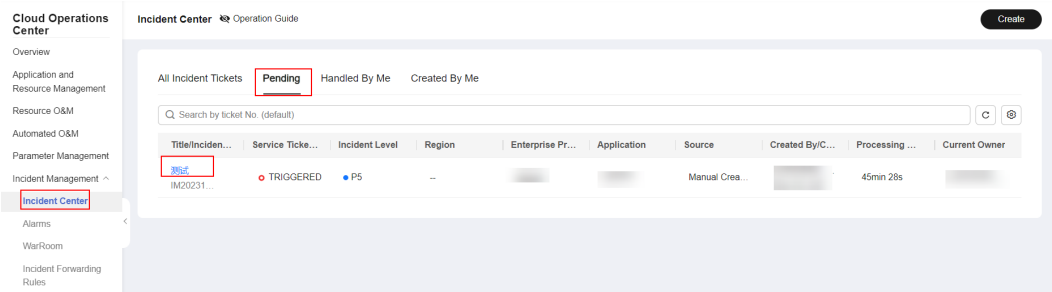
Forward the incident ticket to another person for processing.

Procedure

Step 1 Log in to **COC**.

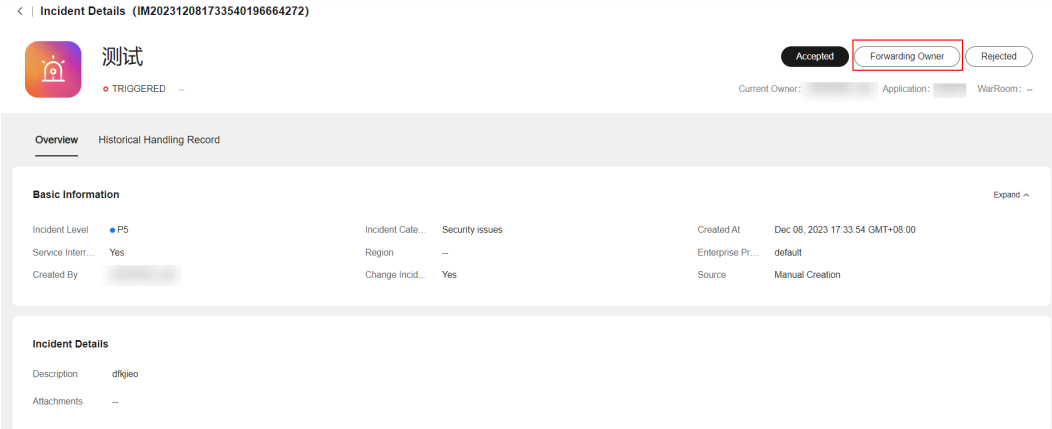
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-17 Incident details



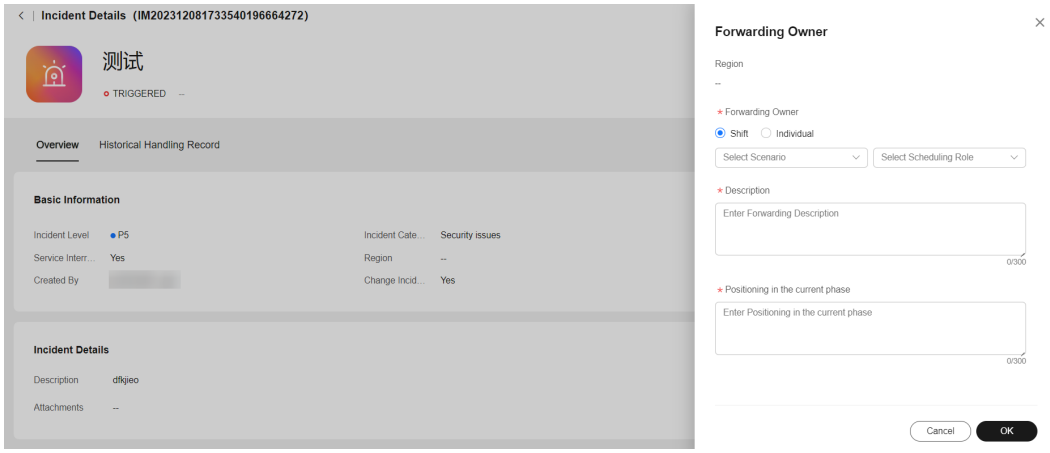
Step 3 Click **Forwarding Owner**.

Figure 6-18 Transferring the owner



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

Figure 6-19 Entering forwarding information



----End

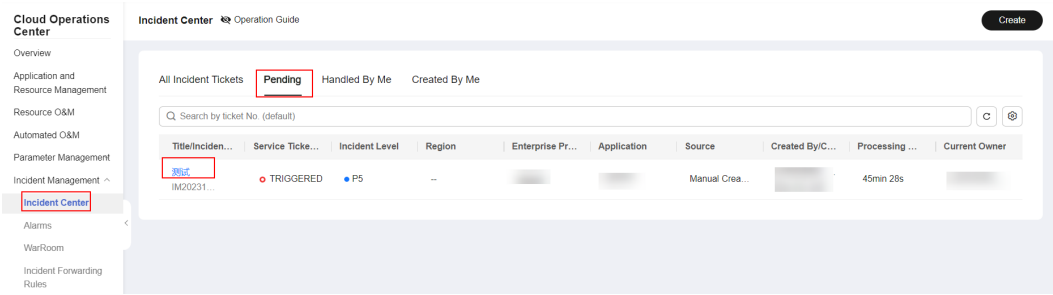
6.2.3.4 Handling Incidents

Procedure

Step 1 Log in to **COC**.

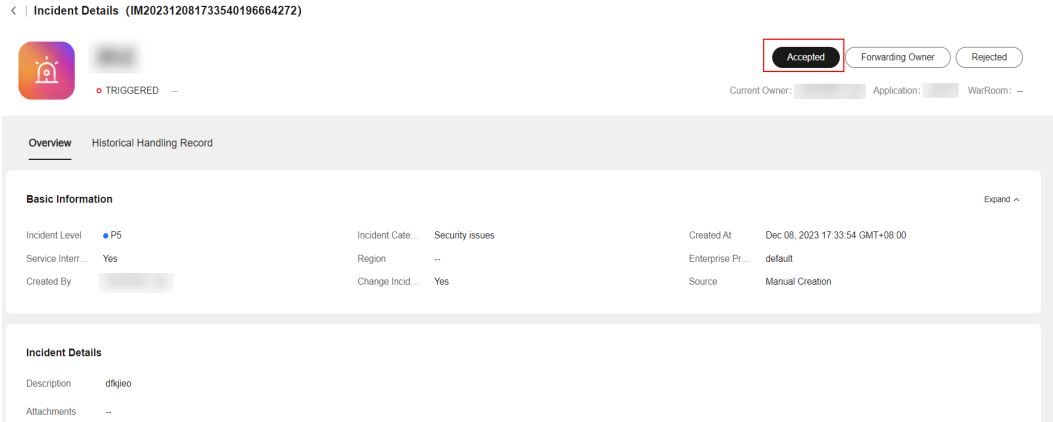
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-20 Incident details



Step 3 Click **Accepted**.

Figure 6-21 Handling an incident



----End

6.2.3.5 Upgrading/Downgrading an Incident

Scenarios

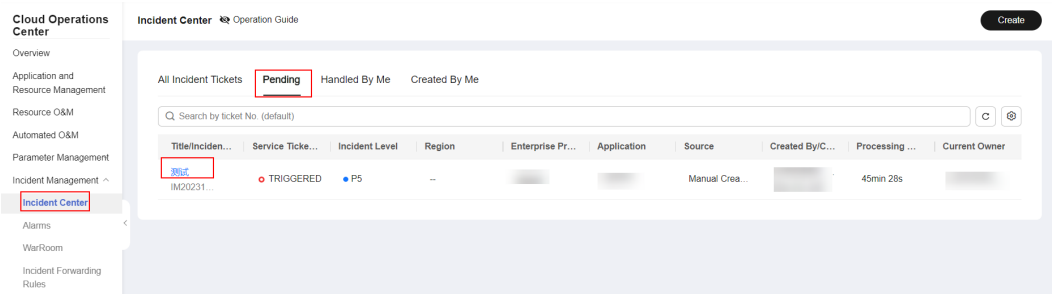
The incident ticket level is inconsistent with the actual situation. The incident level can be modified only after the incident is accepted.

Procedure

Step 1 Log in to **COC**.

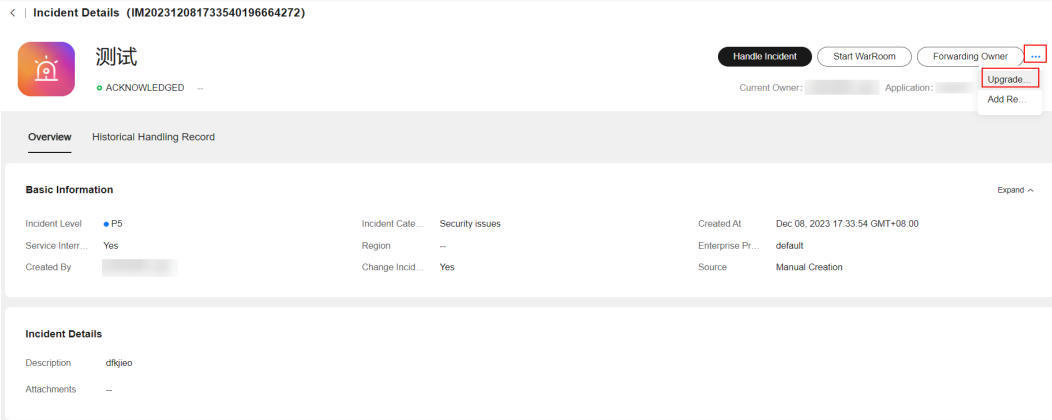
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident name to go to the incident details page.

Figure 6-22 Incident details



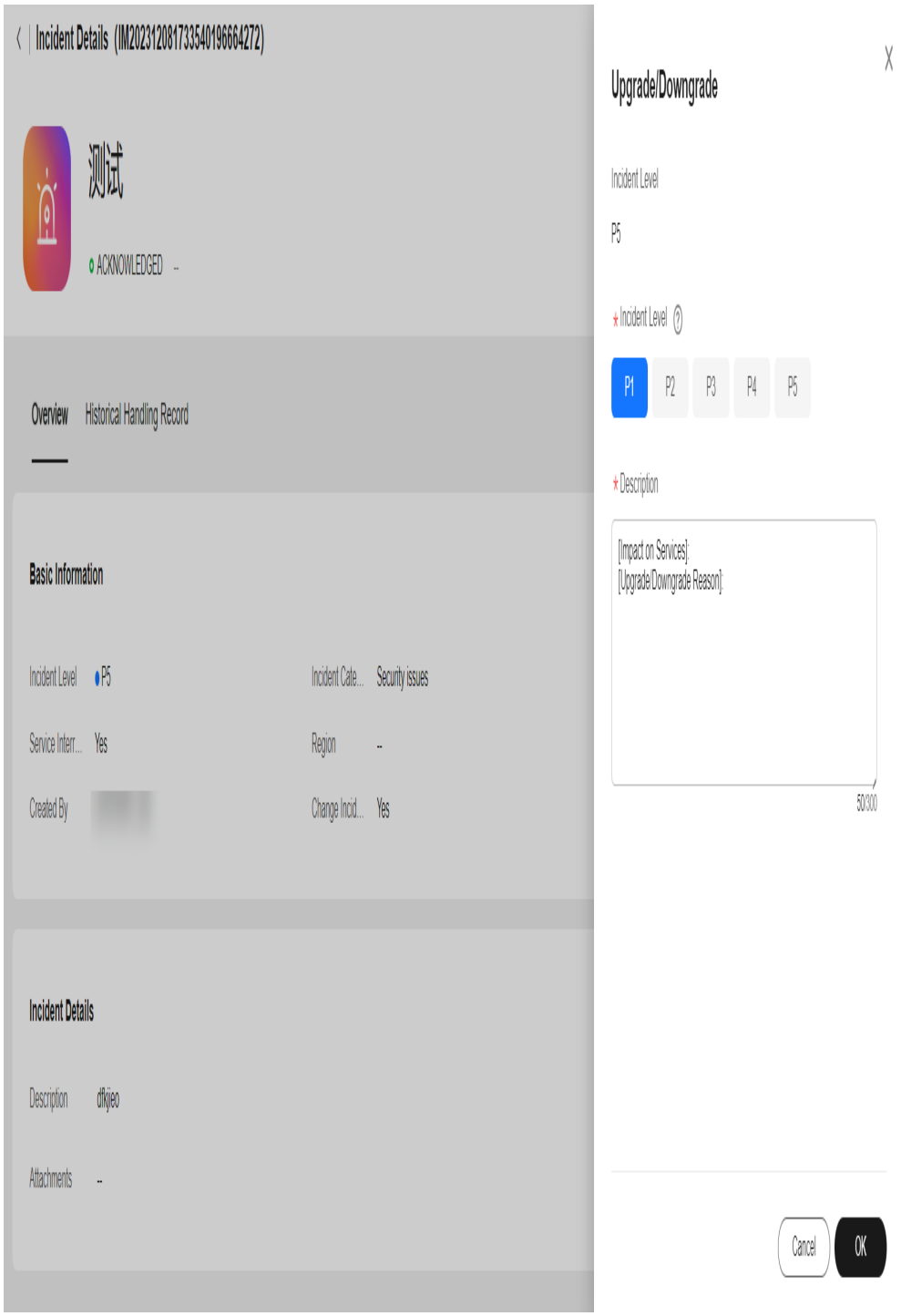
Step 3 Click the **...** icon and choose upgrade/degrade.

Figure 6-23 Upgrading/downgrading an incident



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

Figure 6-24 Entering upgrade and downgrade information



----End

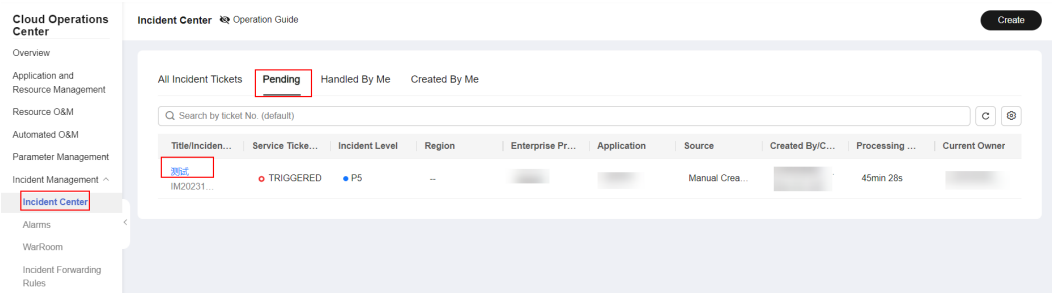
6.2.3.6 Adding Remarks

Procedure

Step 1 Log in to **COC**.

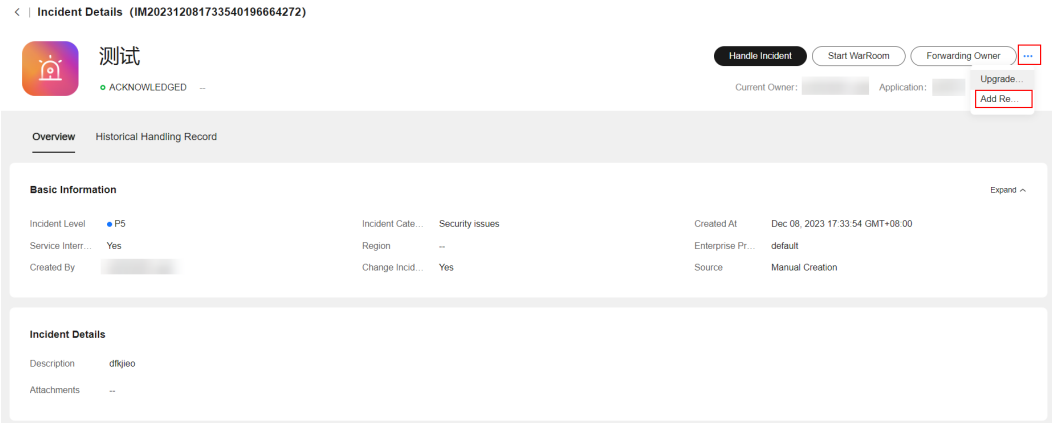
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-25 Incident details



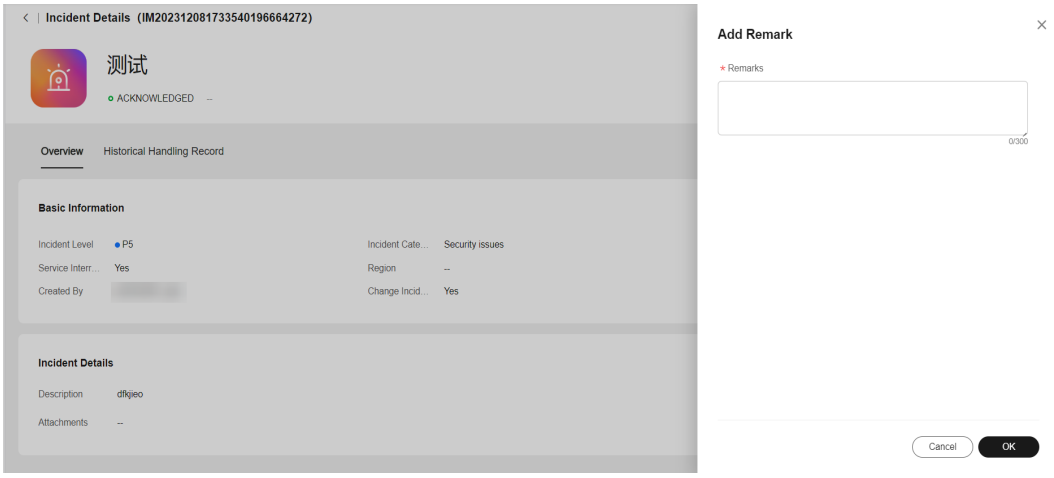
Step 3 Click the **...** icon and choose **Add Remarks**.

Figure 6-26 Adding remarks



Step 4 Enter the remarks and click **OK**.

Figure 6-27 Entering remarks information



----End

6.2.3.7 Starting a War Room

Scenarios

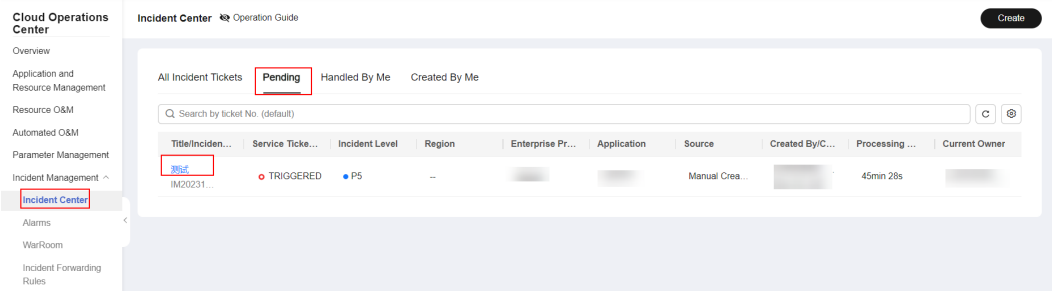
Start a war room for critical incident to recovery the incident quickly.

Procedure

Step 1 Log in to **COC**.

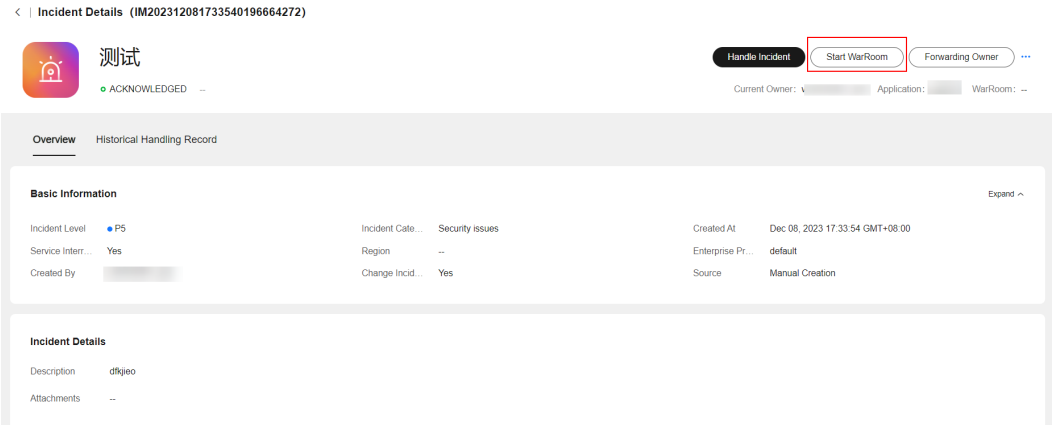
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-28 Incident ticket details



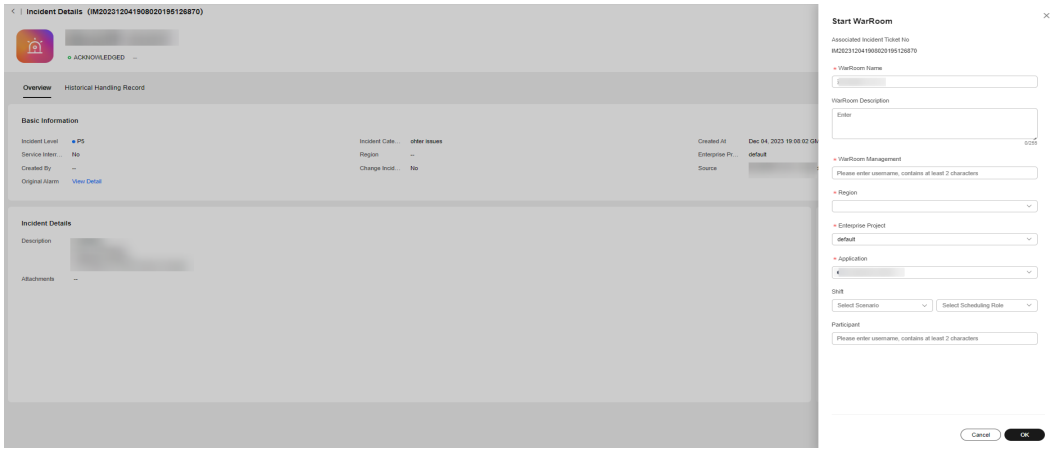
Step 3 Click **Start WarRoom**.

Figure 6-29 Starting a war room



Step 4 Enter war room information and click **OK**.

Figure 6-30 Entering war room information



CAUTION

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

(1) Configure applications in **Mobile Application Management** .

(2) Configure the enterprise WeChat email address on **O&M Engineer Management Overview**.

(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 war room starting rule is met.

----End

6.2.3.8 Handling an Incident

Scenarios

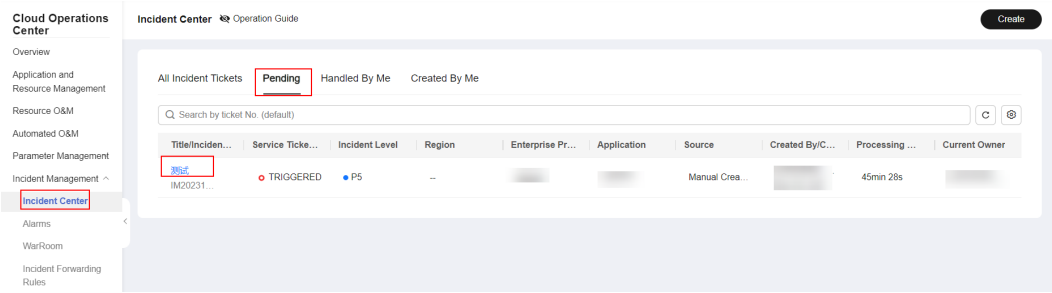
Handle the incident ticket after accepting the incident.

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.

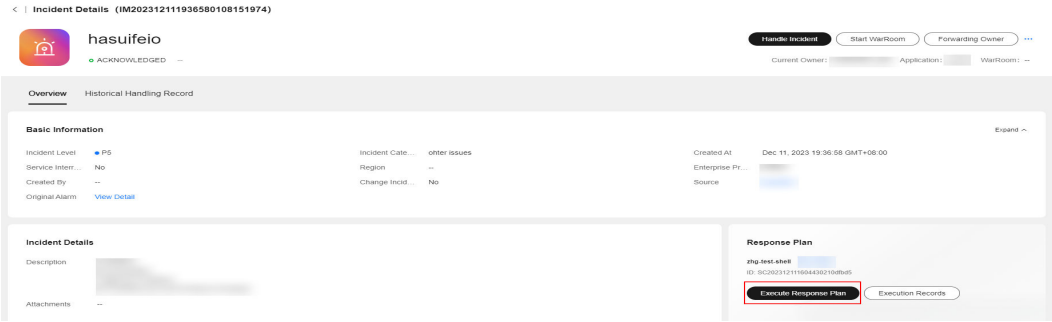
Figure 6-31 Incident details



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**.

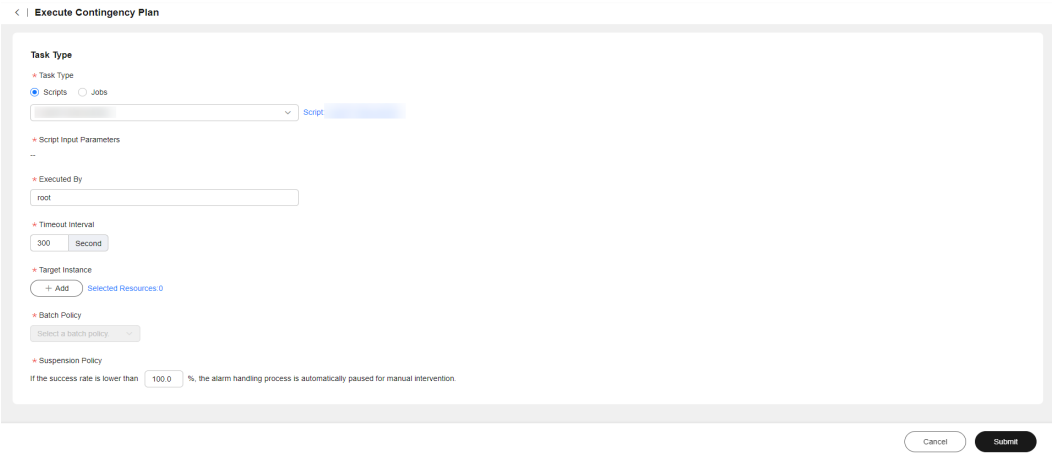
If the incident ticket that is generated through alarm transferring to incident, manual creation, and transferring rules does not associate with a response plan, you can create a contingency plan, script, or job.

Figure 6-32 Executing the response plan



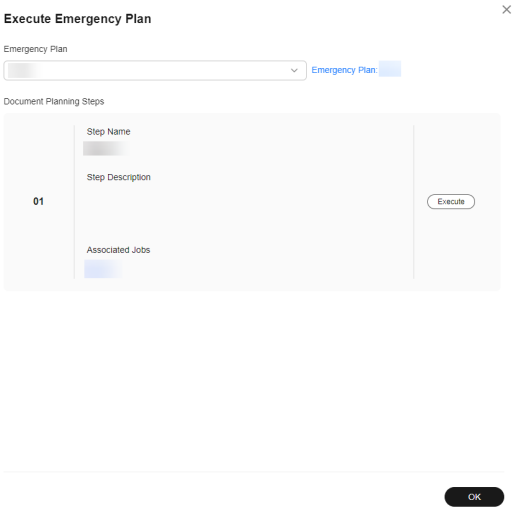
Step 4 If the response plan is a job and script, verify the job and script information and click **Submit**.

Figure 6-33 Page for executing a job or script



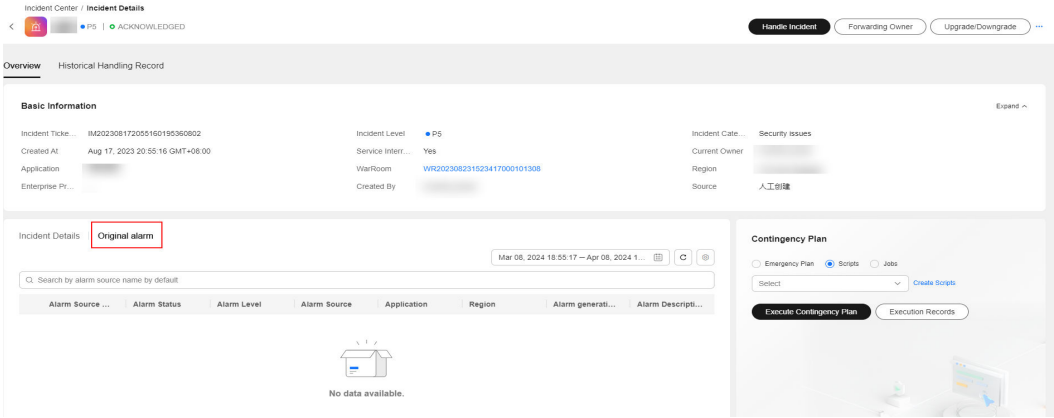
If Contingency Plan is selected for Response Plan, and the response plan is an automatic plan, click **Execute** to execute the script or job and then click **Submit**. If the contingency plan is a text plan, perform the corresponding steps and click **Submit**.

Figure 6-34 Executing a contingency plan



Step 5 View the original alarms associated with the incident.

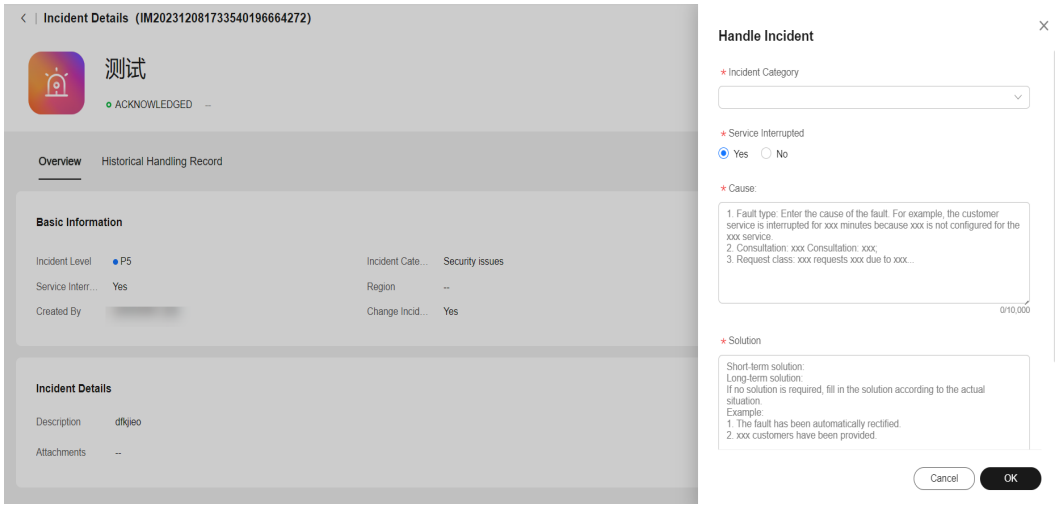
Figure 6-35 Viewing the alarm associated with an incident



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

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

Figure 6-36 Incident handling



----End

6.2.3.9 Verifying Incident

Scenarios

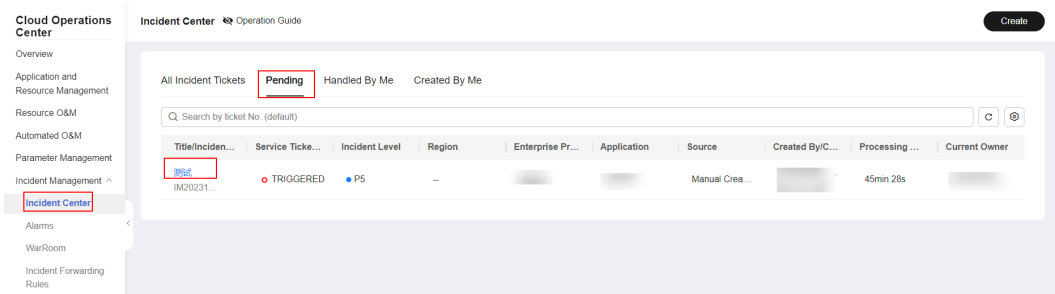
After the incident ticket is processed, verify whether the incident processing is completed.

Procedure

Step 1 Log in to **COC**.

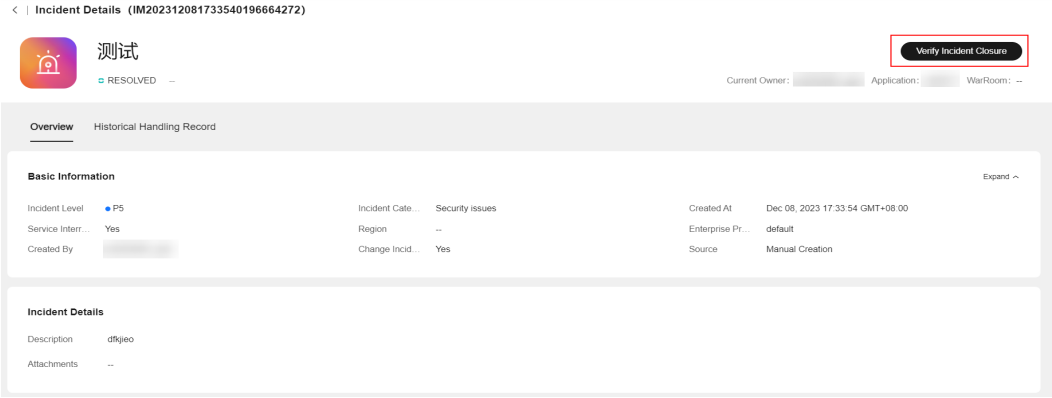
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-37 Incident details



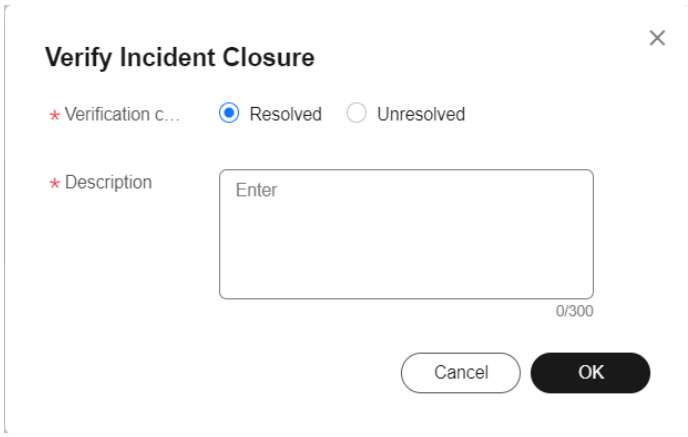
Step 3 Click **Verify Incident Closure**.

Figure 6-38 Verifying whether the incident is closed



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

Figure 6-39 Verifying close page



----End

6.2.4 Incident History

Scenarios

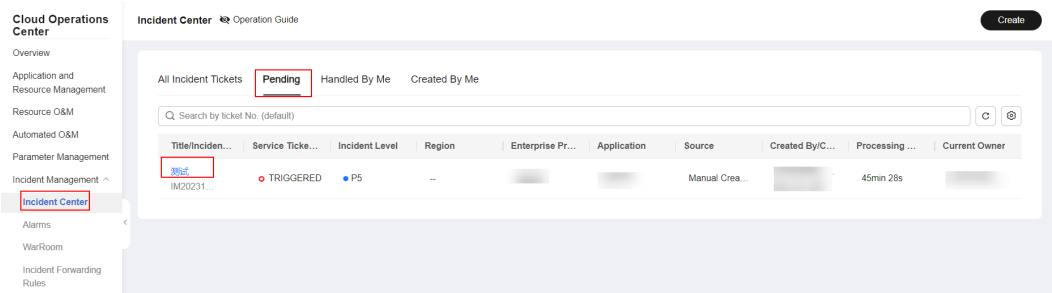
View the historical records of an incident, including the entire incident handling process.

Procedure

Step 1 Log in to **COC**.

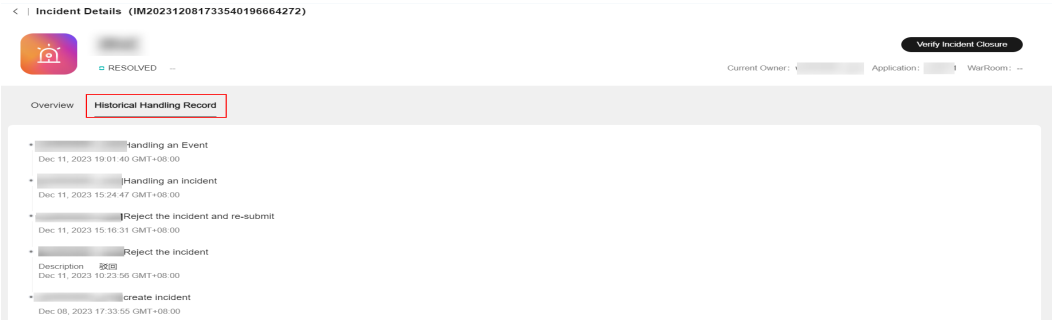
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-40 Incident details



Step 3 Click **Historical Handling Record**.

Figure 6-41 Viewing incident history



----End

6.3 WarRoom

A war room is a meeting that facilitates rapid service recovery through the joint efforts of O&M, R&D, and operations personnel. On the war room 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 war room is started** on the incident processing page.

6.3.1 War Room Status

Scenarios

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

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom** to view the war room list.

Step 3 Click a war room name in the war room list. The war room detail page is displayed. The war room status is displayed in the upper right corner of the page.

Step 4 Click **Update Status** on the right to update the war room status.

> **CAUTION**
>
> 1. Before changing to the **Fault Rectified** status, ensure that the status of the affected application is **Recovered**.
>
> 2. Before closing a war room, ensure that the fault information of the war room has been completed.

----End

6.3.2 Fault Information

Scenarios

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

Procedure

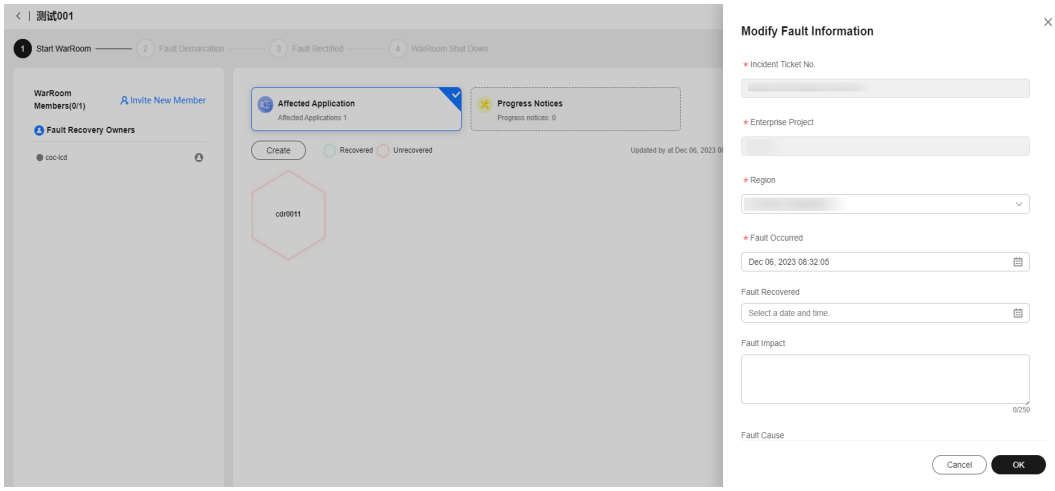
Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom** to view the war room list.

Step 3 Click a war room name in the war room list. The war room detail page is displayed.

Step 4 Click **Modify**, and modify fault information as prompted, and click **OK**.

Figure 6-42 Modifying fault information



----End

6.3.3 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.

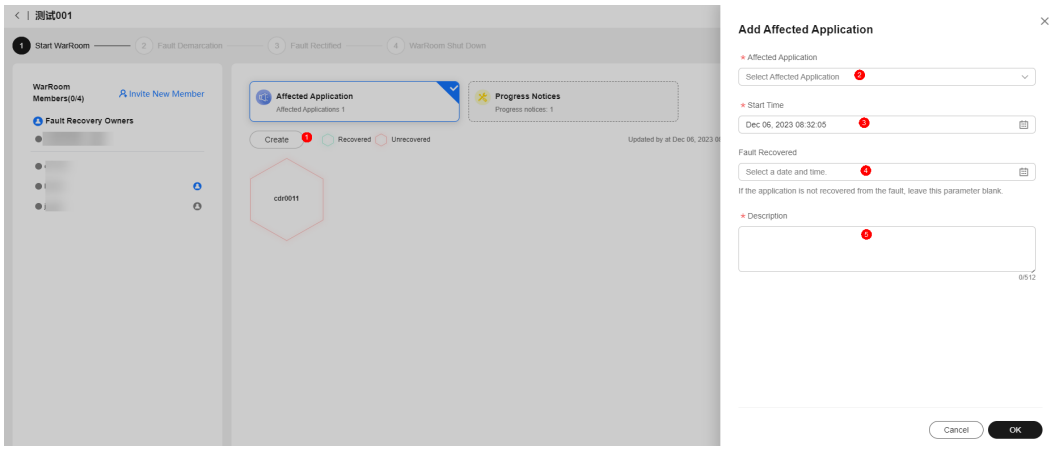
Step 4 Click **Create**.

The **Add Affected Application** page is displayed.

Step 5 Set the information about the new affected application as prompted.

Step 6 Click **OK**.

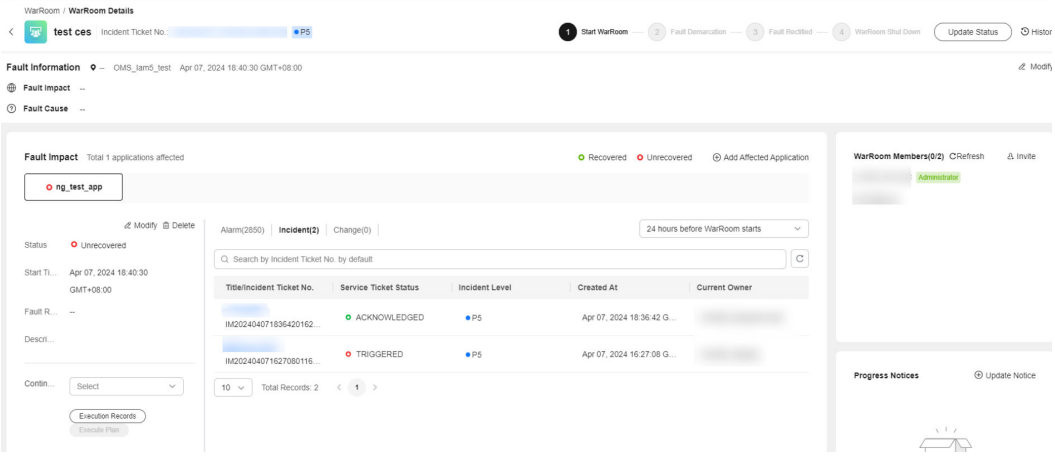
Figure 6-43 New affected applications



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 6-44 Affected application page



----End

6.3.4 War Room Members

Scenarios

After a war room 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 **Fault Management** > **WarRoom** to view the war room list.

Step 3 Click a war room name in the war room list. The war room detail page is displayed.

Step 4 In the **Member** area, click **Invite**, select the attendance mode and the members to be invited, and click **Add to WarRoom**.

----End

6.3.5 Progress Notification

Scenarios

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

Procedure

Step 1 Log in to **COC**.

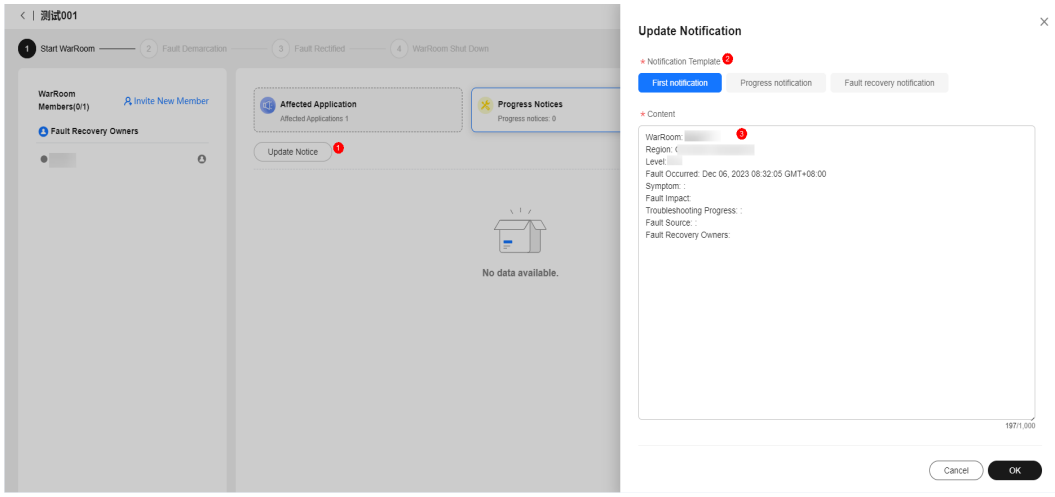
Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom** to view the war room list.

Step 3 Click a war room name in the war room list. The war room detail page is displayed.

Step 4 On the war room details page, you can view the current progress notification in the **Progress Notices** area.

Step 5 Click **Update Notice**, enter the notice content as prompted, and click **OK** to update the notice.

Figure 6-45 Updating notification



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

If the **Recipient** is set to **Shift**, create the shift by referring to **Overview**.

----End

6.3.6 Adding a War Room Initiation Rule

Scenarios

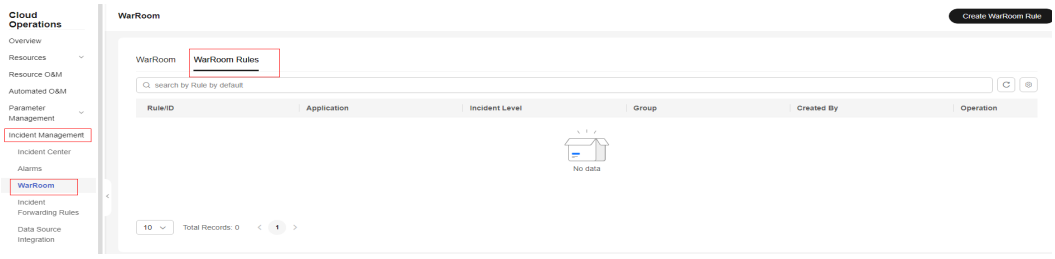
Create a war room initiation rule.

Procedure

Step 1 Log in to **COC**.

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

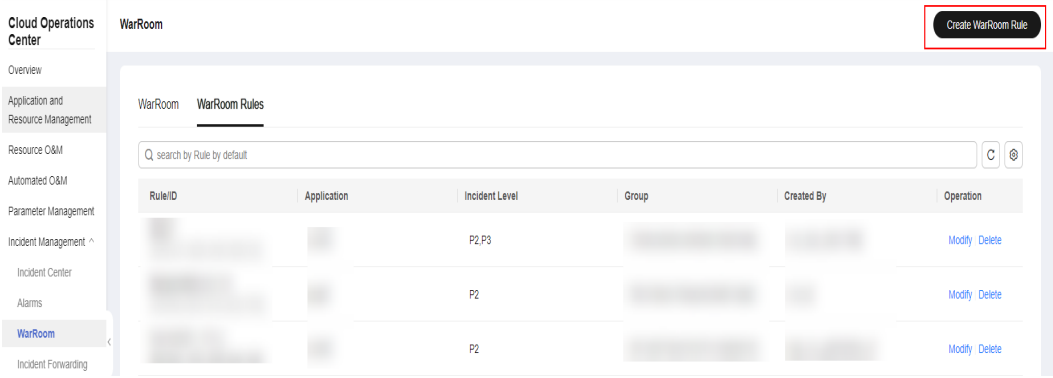
Figure 6-46 War room rules



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

Figure 6-47 Adding a war room rule



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

----End

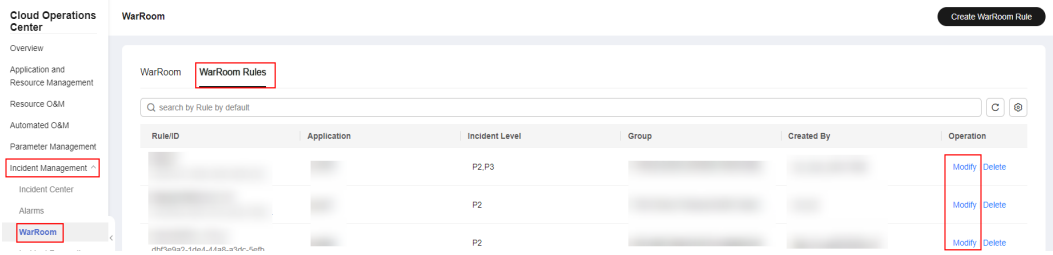
6.3.7 Modifying a War Room Rule

Procedure

Step 1 Log in to **COC**.

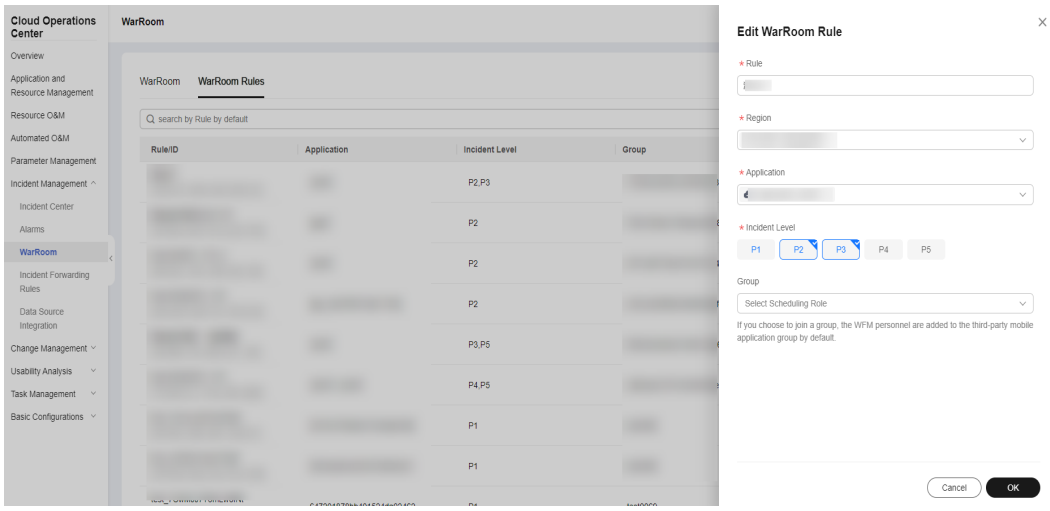
Step 2 In the navigation pane on the left, choose **Incident Management** > **WarRoom**. Click **WarRoom Rules**.

Figure 6-48 War room rules



Step 3 Locate the war room 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 6-49 Modifying a war room rule



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

----End

6.4 Improvement Management

6.4.1 Improvement Management

Prerequisites

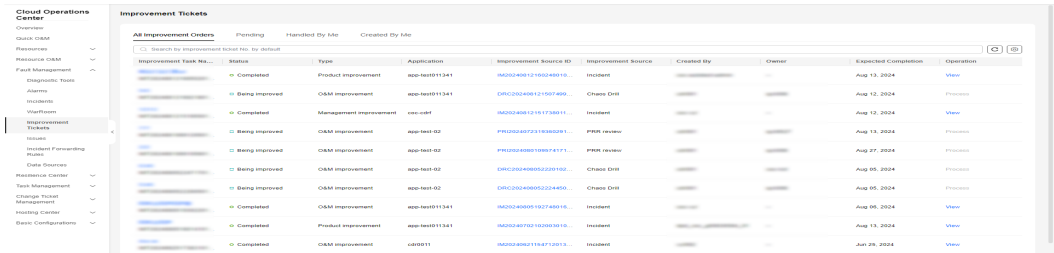
Create improvement tickets using incidents, war rooms, drills, and PRRs.

Handling Improvement Tickets

Step 1 Log in to **COC**.

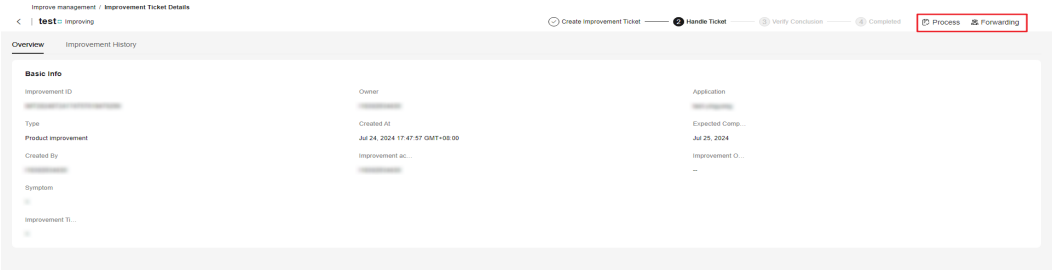
Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**. On the displayed page, click the **Pending** tab and click an improvement ticket name to go to the improvement ticket details page.

Figure 6-50 Improvement ticket list



Step 3 Click **Process** or **Forward** in the upper right corner.

Figure 6-51 Improvement ticket details



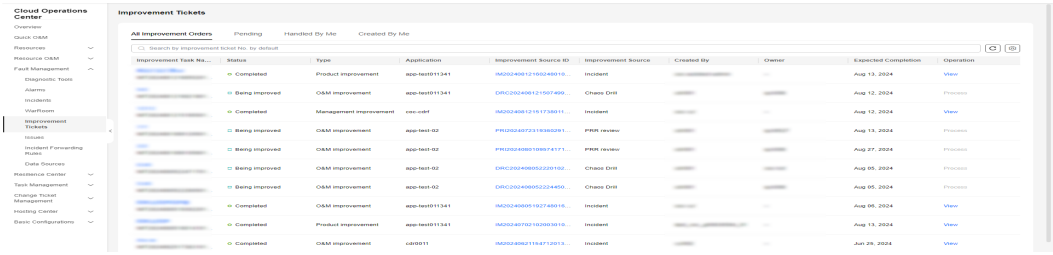
----End

Improvement Ticket Verification

Step 1 Log in to **COC**.

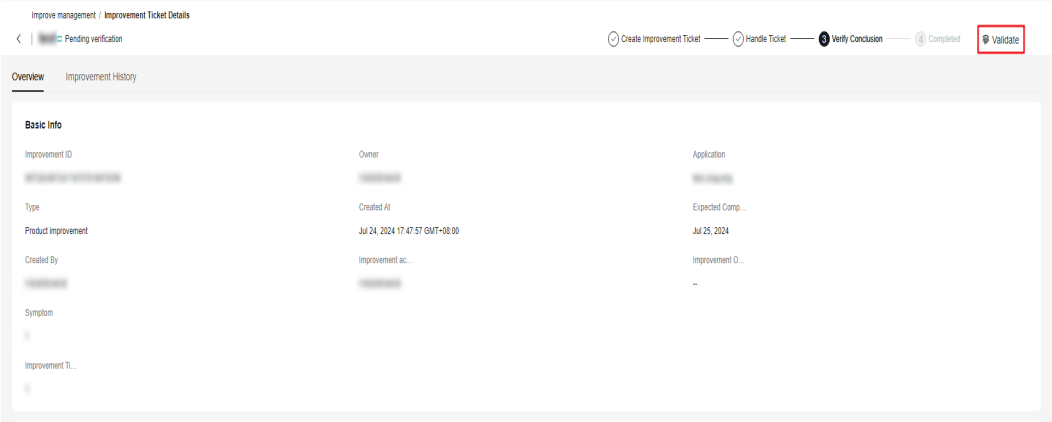
Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**. On the displayed page, click the **Pending** tab and click an improvement ticket that is in the state of waiting for validation to go to the improvement ticket details page.

Figure 6-52 Improvement ticket list



Step 3 Click **Validate** in the upper right corner and enter the validation conclusion.

Figure 6-53 Improvement ticket validation



----End

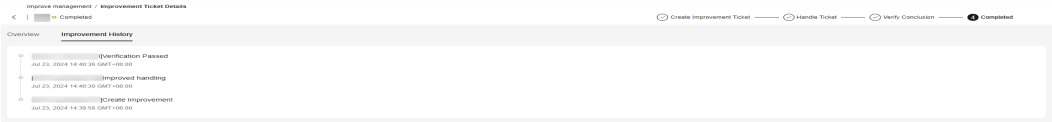
Improvement Ticket History

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Improvement Tickets**. On the displayed page, click the **Pending** tab and click an improvement ticket that is in the state of waiting for validation to go to the improvement ticket details page.

Step 3 On the improvement ticket details page, click the **Improvement History** tab to view the improvement history.

Figure 6-54 Improvement ticket history



----End

6.5 Forwarding Rules

6.5.1 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.

6.5.2 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 Data Sources.

Scenarios

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

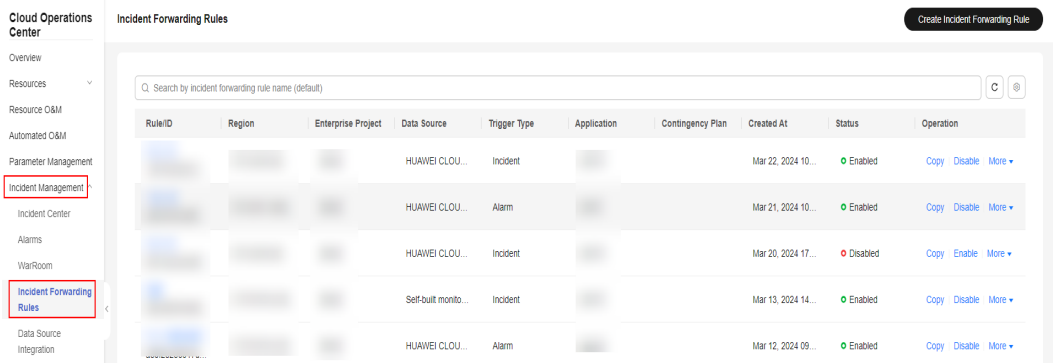
Procedure for Adding a Forwarding Rule

Step 1 Log in to **COC**.

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

Step 3 In the upper part of the list, click **Create Incident Forwarding Rule**.

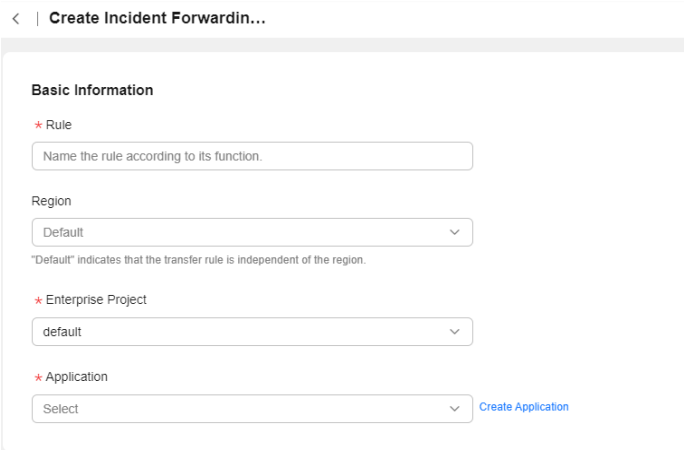
Figure 6-55 Creating an incident forwarding rule



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

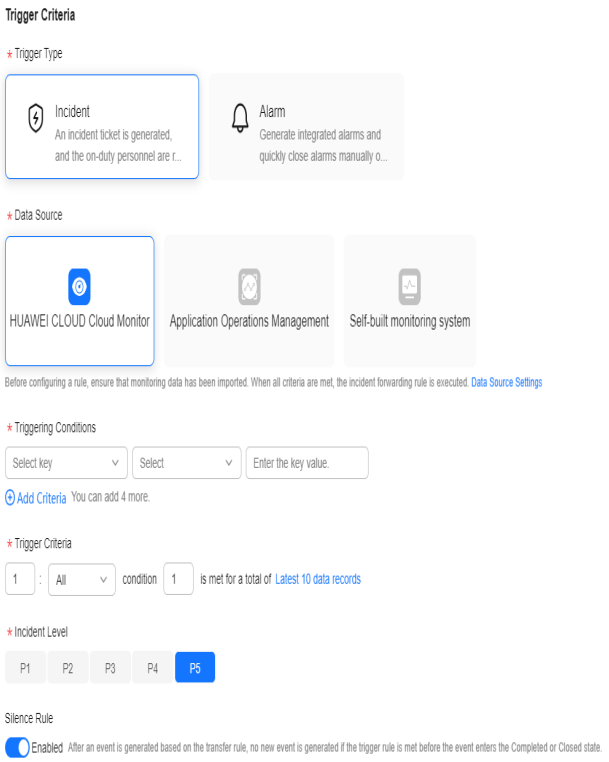
Step 4 Enter basic information such as the rule name and application name as prompted.

Figure 6-56 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 6-57 Entering a trigger criteria



The key in the trigger conditions is described as follows:

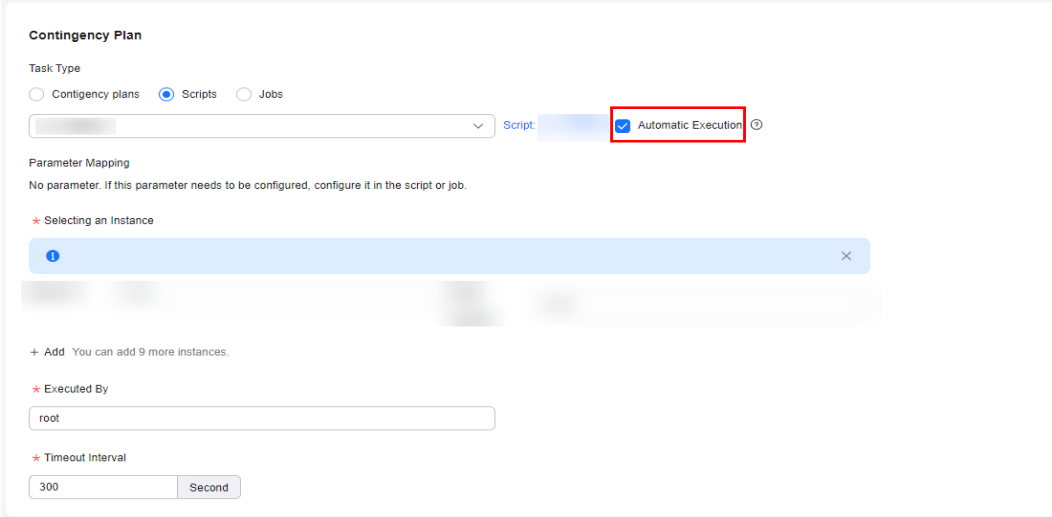
Parameter	Description	CES Alarm Field	AOM Alarm Field
alarmId	Alarm ID	alarm_id	id
alarmName	Alarm name	alarm_name	event_name in metadata
alarmLevel	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Suggestion**.	AlarmLevel	event_severity
time	Time when an alarm is generated	time	starts_at
nameSpace	Service namespace	namespace	namespace
region	Region	Region in template_variable	/
application	Application name	/	/
resourceName	Resource name	ResourceName in template_variable	resource_id in metadata

resourceId	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 Cloud Eye 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, jobs, and contingency plans associated with the forwarding rule. For details about how to add a script or job, see **Automated O&M**.

Scripts, jobs, and automated contingency plans support automatic fault recovery. After you select a script, job, or an automated contingency plan, the **Automatic Execution** check box is displayed. After you select the check box, the parameters corresponding to the script or job are displayed.

Figure 6-58 Specifying a contingency plan



NOTE

The parameter value, region ID, and target instance are in the format of ${}. You need to use this expression to parse the corresponding value. For details, see **Example of Automatic Parameter Execution**.

Step 7 In the **Assignment Details** area, configure required parameters and click **Submit**.

Figure 6-59 Filling the assignment rule

----End

Example of Automatic Parameter Execution

The parameter value, region ID, and target instance are in the format of ${}. You need to use this expression to parse the corresponding value. The example of automatic parameter execution is listed as follows.

Example:

Alarm information:

{

"alarmId": "al1696664837170EWbvx24kW",

"alarmName": "alarm-4z39coctest1007",

.....

"URL": "https://console.ulanqab.huawei.com/ces/?region=cn-north-7#/alarms/detail?alarmId=al16849986549022X5Vp4pxr",

"additional": {

"dimension": "instance_id:29d99a09-2d15-4ced-8723-6e94ae1c1472",

.....

},

.....

}

1. To obtain the value of alarmId in the current alarm information, use the following expression::

${currentAlarm.alarmId}

2. To obtain the UUID of instance_id from the additional.dimension string, use the following expression:

${string.substring(currentAlarm.additional.dimension, string.indexOf(currentAlarm.additional.dimension, 'instance_id:') + 12)}

Alternatively, use the following expression.

${string.substring(currentAlarm.additional.dimension, 12)}

3. To obtain the region ID of cn-north-7 from the URL string, use the following expression:

${string.substring(currentAlarm.URL, string.indexOf(currentAlarm.URL, 'region=') + 7, string.indexOf(currentAlarm.URL, '#/alarms'))}

In the expression, "currentAlarm." is a fixed prefix, which indicates that the data is obtained from the current alarm data.

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

Step 1 Log in to **COC**.

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

Step 3 To edit or delete a forwarding rule on the incident forwarding rule list page, locate a forwarding rule and click **More** and choose **Edit** or click **More** and choose **Delete** in the **Operation**. To enable or disable a forwarding rule, locate a desired forwarding rule and click **Enable** or **disable** in the **Operation** column. After a forwarding rule is disabled, no incidents or alarms will be triggered.

----End

6.6 Data Source Integration Management

You can quickly integrate with existing or external monitoring systems with ease for centralized alarm management. Each monitoring system employs distinct integration access keys for seamless interconnectivity.

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

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

6.6.1 Monitoring System Integration Management

This document describes how to integrate monitoring systems, which is also called monitoring data sources.

Scenarios

Each monitoring system is independent integrated into COC. For details, see the integration process description.

Procedure

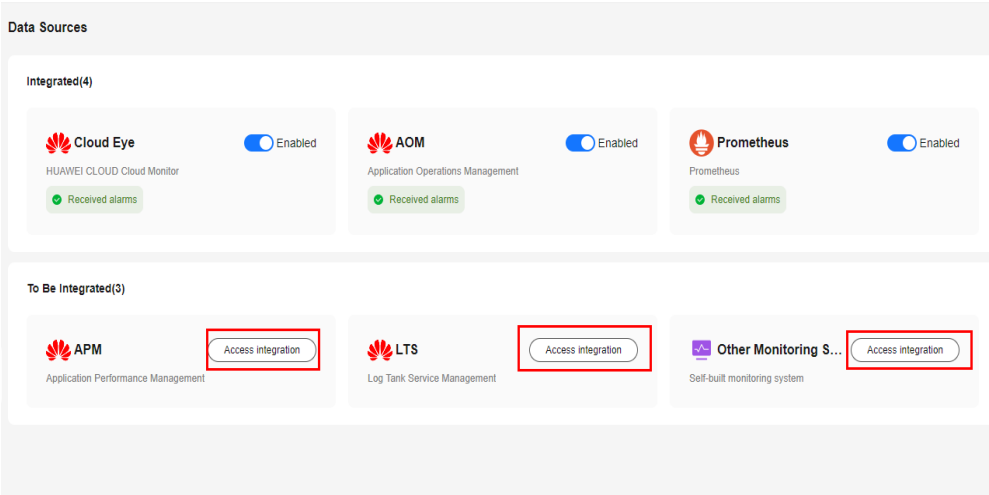
- **This part describes how to integrate Huawei Cloud and open-source monitoring systems to COC.**

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Data Sources**.

Step 3 On the displayed page, locate the monitoring system you want to integrate into COC based on service requirements and click **Access integration**.

Figure 6-60 Monitoring system integration



Step 4 On the integration page, you can view the data source integration introduction and integration procedure. After the integration is complete, click **Integrate**.

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

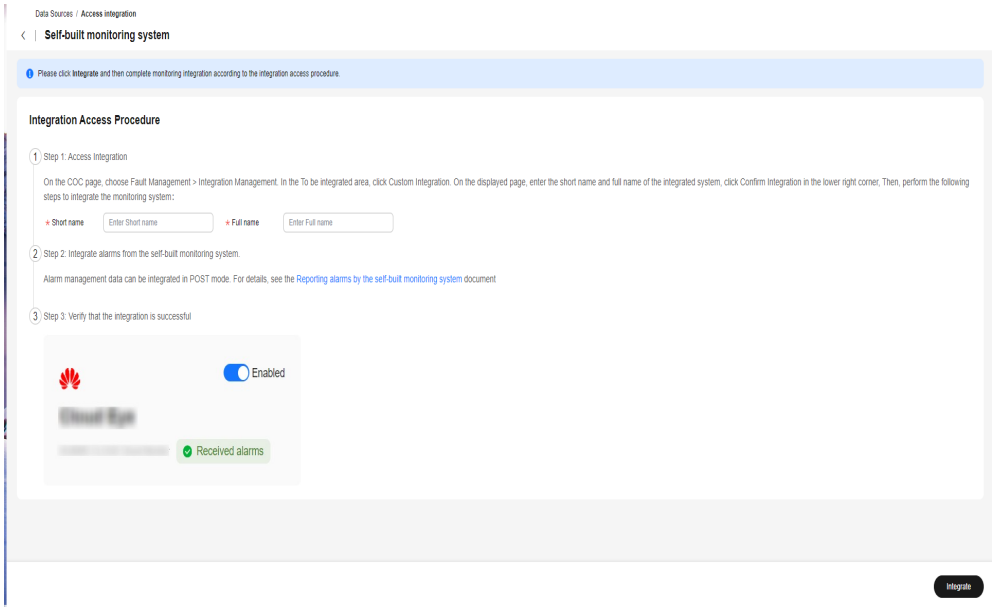
- **This part describes how to integrate monitoring systems except those mentioned in the above part into COC.**

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Data Sources**.

Step 3 On the **Data Sources** page, in the **To Be Integrated** area, locate the **Other Monitoring Systems** card and click **Access Integration**. On the displayed page, enter the short name and full name of the monitoring system you want to integrate into COC and access your monitoring system as prompted. The system can be renamed.

Figure 6-61 Procedure for integrating a monitoring system



NOTICE

A maximum of five monitoring systems can be integrated for customized integration. If the integration is incorrect, disable it and then delete it.

----End

Enabling and Disabling a Monitoring System

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Data Sources**.

Step 3 On the **Data Sources** page, locate the card of a monitoring system and click the **Enable** or **Disable** button to enable or disable the monitoring system. You can also click a monitoring system card to go to the details page and click **Enable** or **Disable** at the bottom.

----End

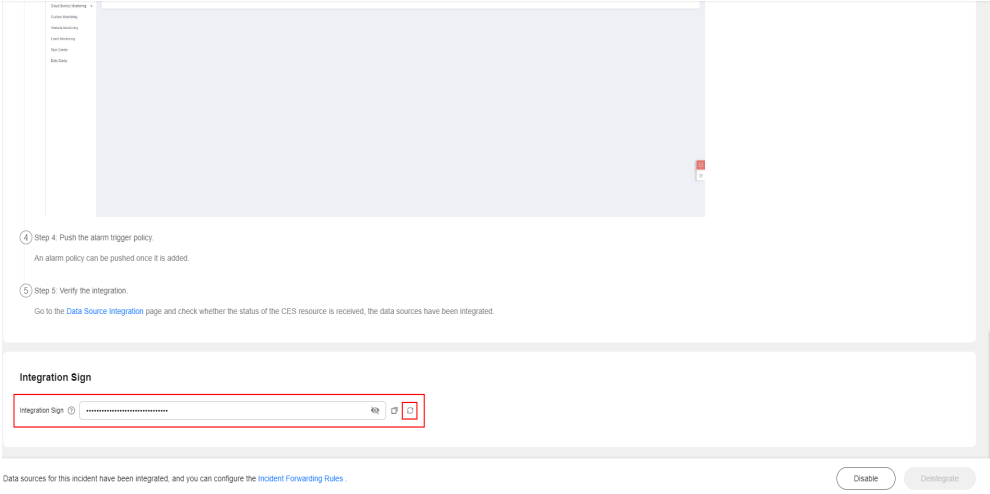
Updating an Integration Sign

Step 1 Log in to **COC**.

Step 2 In the navigation tree on the left, choose **Fault Management** > **Data Sources**.

Step 3 On the **Data Sources** page, click a monitoring system card. On the monitoring system details page that is displayed, in the Integration Sign area, click to update the integration sign.

Figure 6-62 Updating an integration sign



----End

7 Change Management

7.1 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.

7.1.1 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**.
2. You have created an approver shift by referring to **Overview**.

Precautions

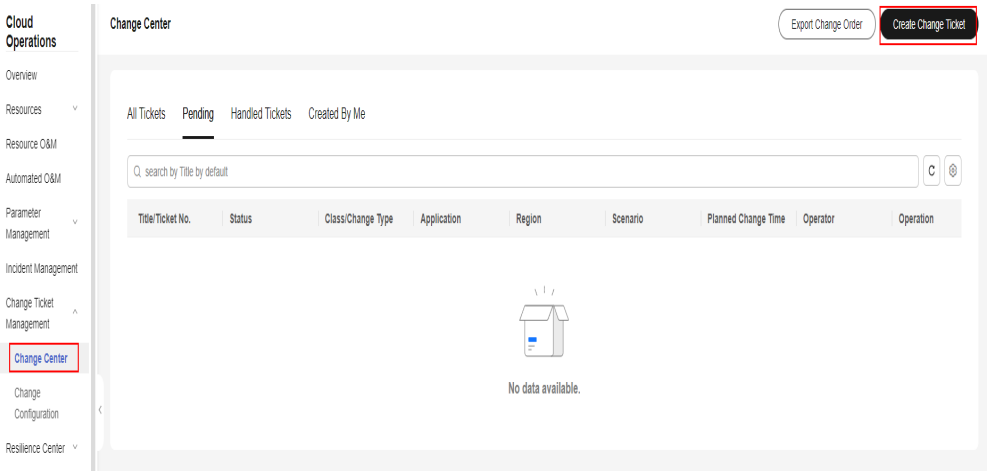
Confirm the content of change ticket and apply for the change based on the actual change requirement.

Procedure

Step 1 Log in to **COC**.

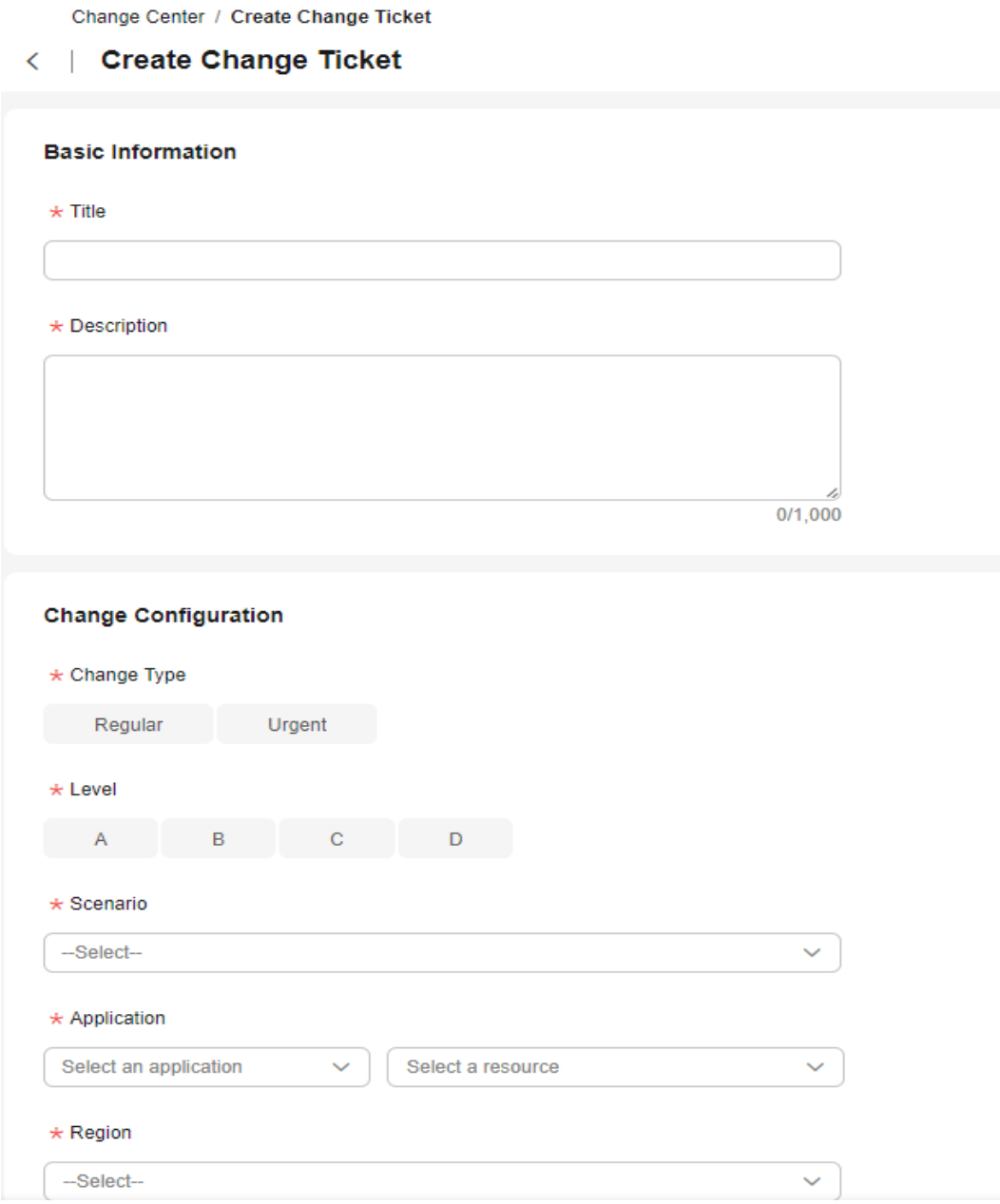
Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**. Click the **Pending** tab, and click **Create Change Ticket**.

Figure 7-1 Creating a change ticket



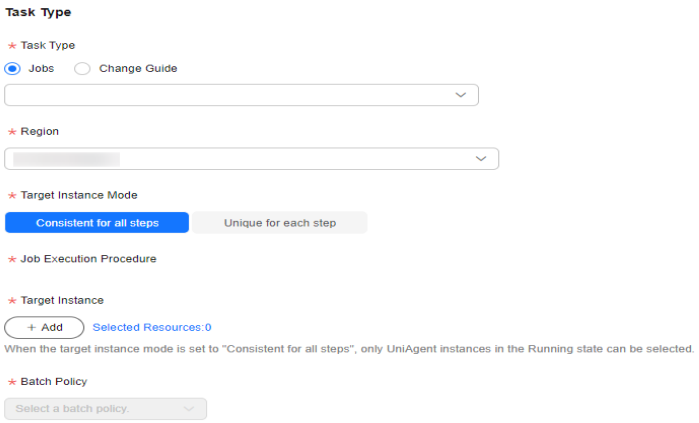
Step 3 Enter the basic information and change configuration of the change request.

Figure 7-2 Entering basic information about the change request



Step 4 Set the change task type. You can select **Jobs** and **Change Guide**. For details about job execution, see **Automated O&M**.

Figure 7-3 Setting the change task type



----End

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. **Task Type**: Select **Jobs** or **Change Guide**.

   After the configuration, click **Submit**.

7.2 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.

7.2.1 Configuring Approval Settings

Overview

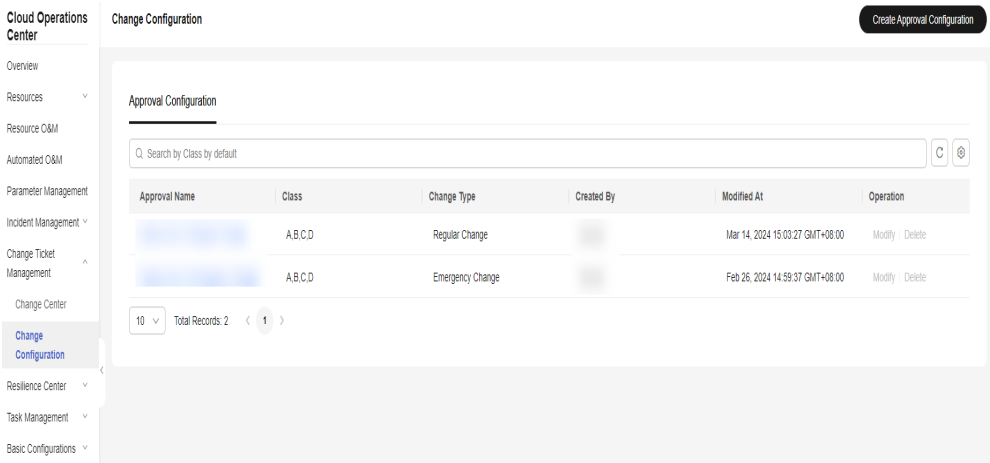
Users can configure the change type, change level, review process, and reviewer.

Creating an Approval Configuration

Step 1 Log in to **COC**.

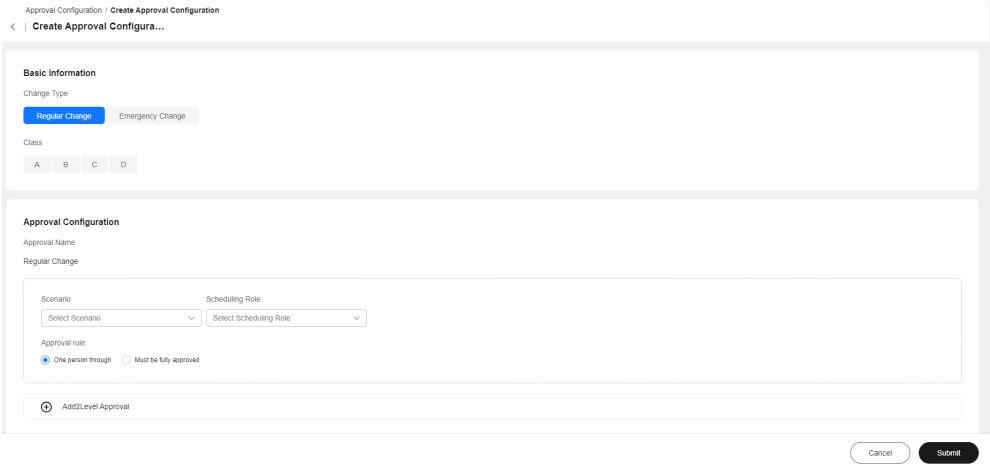
Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Configuration**. On the displayed page, click **Create Approval Configuration**.

Figure 7-4 Creating a review configuration



Step 3 Enter the approval configuration content and click **Submit**.

Figure 7-5 Setting the review configurations



----End

NOTE

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: A scheduling role takes effect only after the reviewer is configured. If the reviewer is not specified, the change request cannot be submitted.

8 Resilience Center

8.1 Chaos Drills

8.1.1 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.

8.1.2 Fault Type

Scenarios

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

Precautions

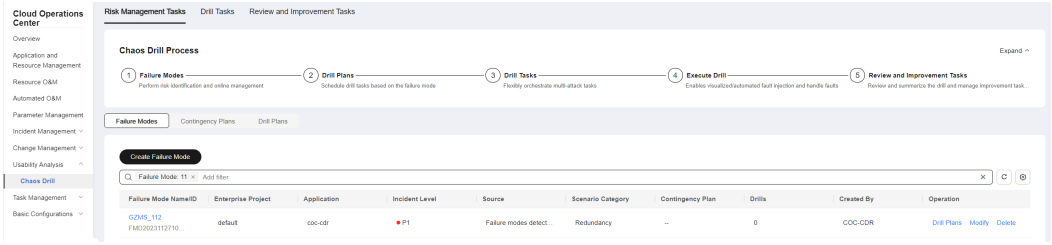
Check whether the application of the target host or container and the incident level is correct.

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 8-1 Failure Modes



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

Figure 8-2 Creating a failure mode

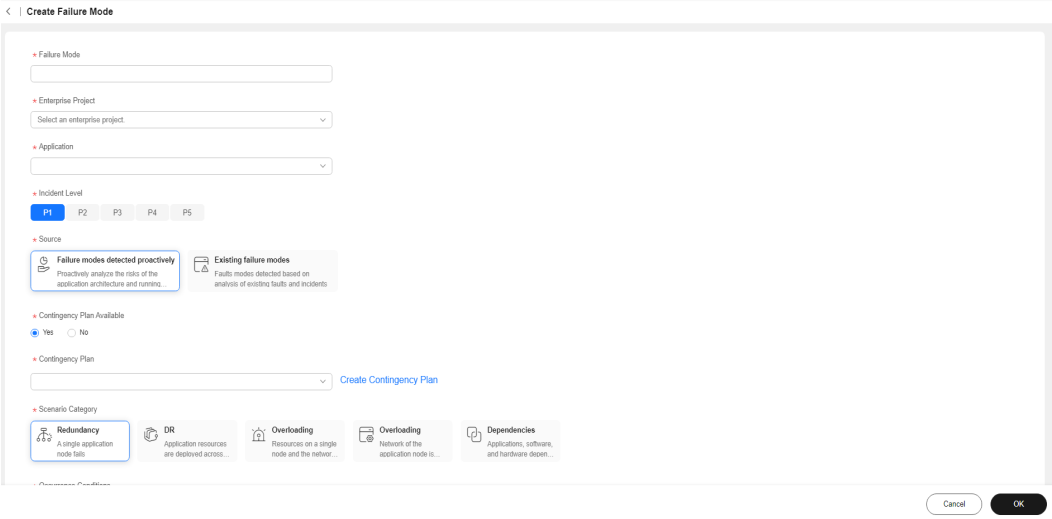


Table 8-1 Failure mode parameters

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 Management**.
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

8.1.3 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

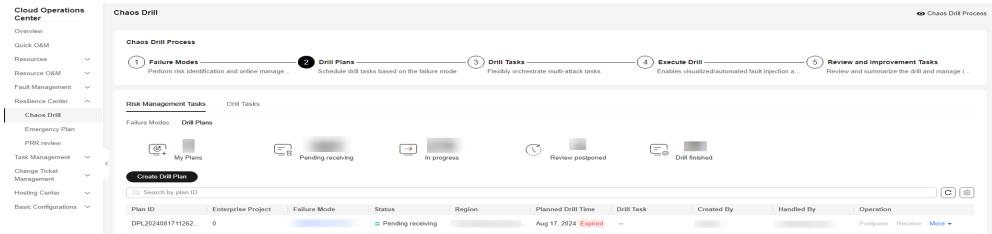
You do not need to specify the enterprise project to which the drill plan belongs. The enterprise project must be the same as that associated with the fault mode.

Procedure

Step 1 Log in to **COC**.

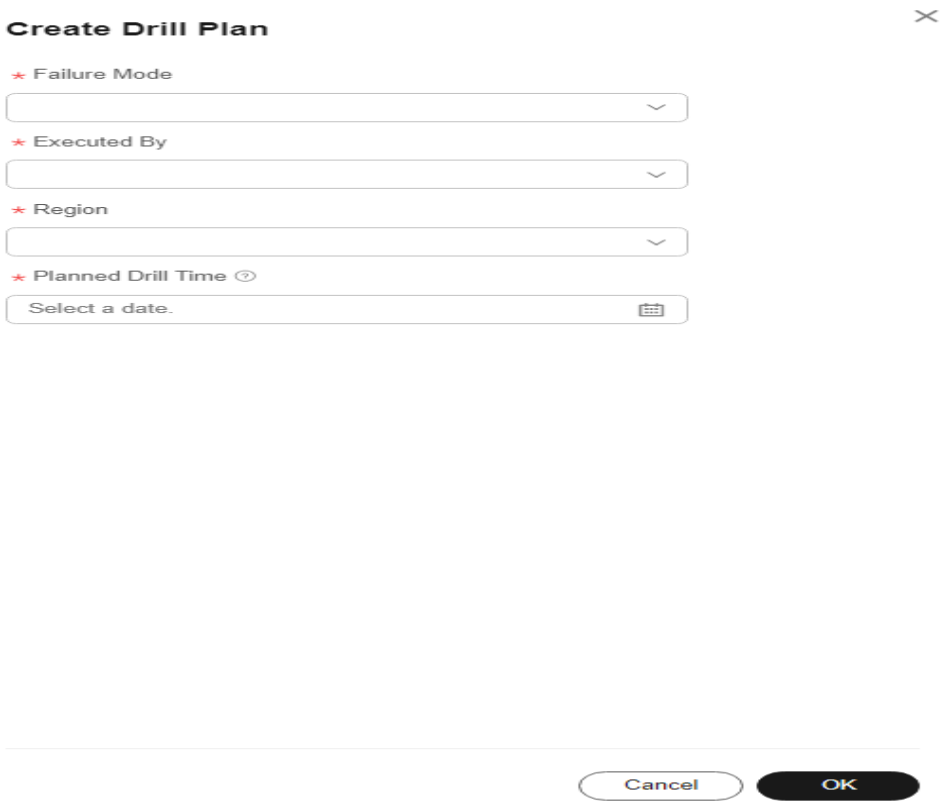
Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click **Risk Management Tasks**, and click **Drill Plans**.

Figure 8-3 Drill Plans



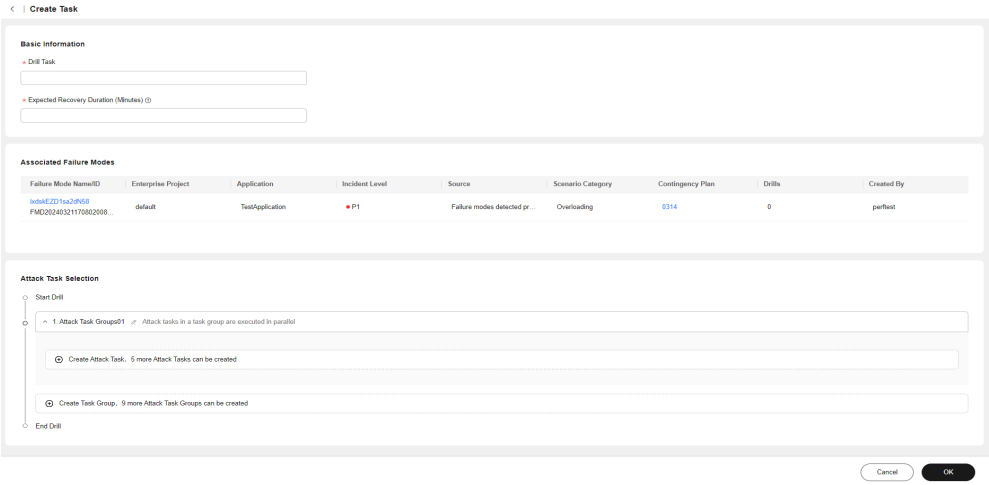
Step 3 Click **Create Drill Plan**. In the displayed dialog box, set **Failure Mode**, **Executed By**, **Region**, and **Planned Drill Time**, and click **OK**.

Figure 8-4 Creating a drill plan



Step 4 The executor clicks **Receive** 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 8-5 Creating a drill task



----End

8.1.4 Drill Tasks

Creating a Drill Task

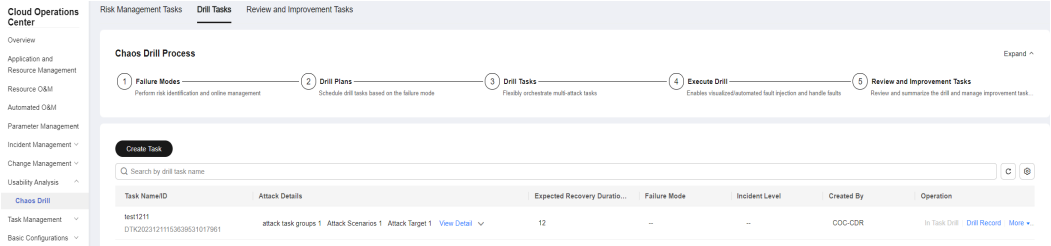
Create a drill task on COC.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab.

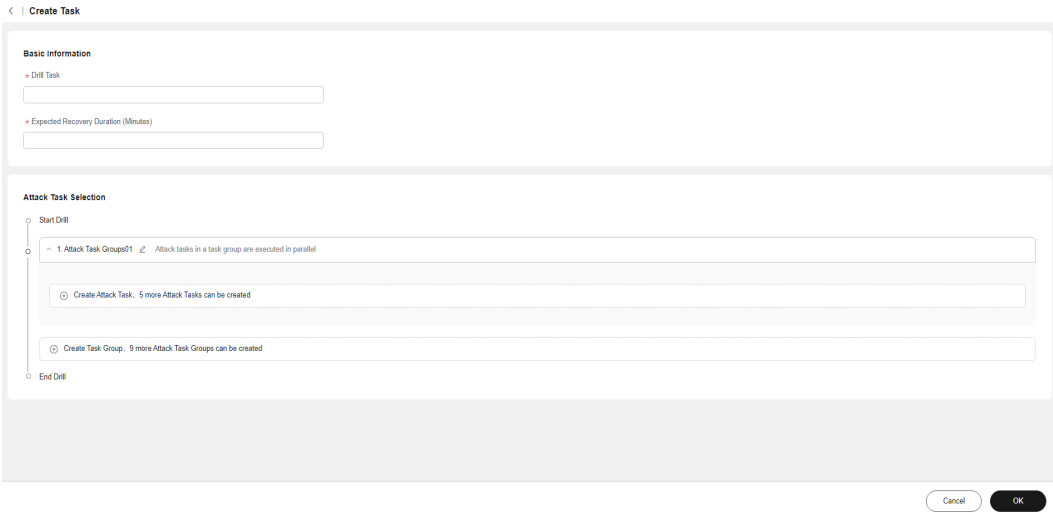
Step 3 Click **Create Task**. Or you can accept a drill plan to access the page for creating a drill task by following the instructions in **Drill Plan**.

Figure 8-6 Creating a drill task



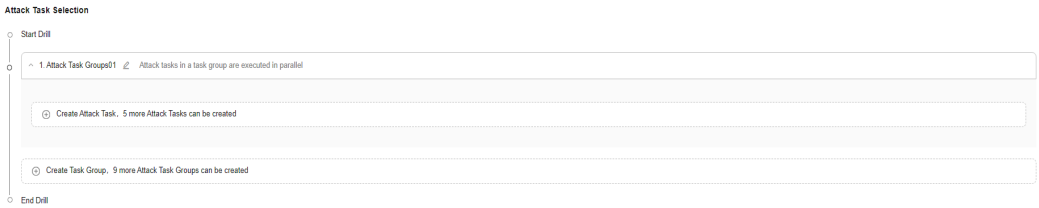
Step 4 Enter the basic information about the drill task, including the drill task name and expected recovery duration (in minutes).

Figure 8-7 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.

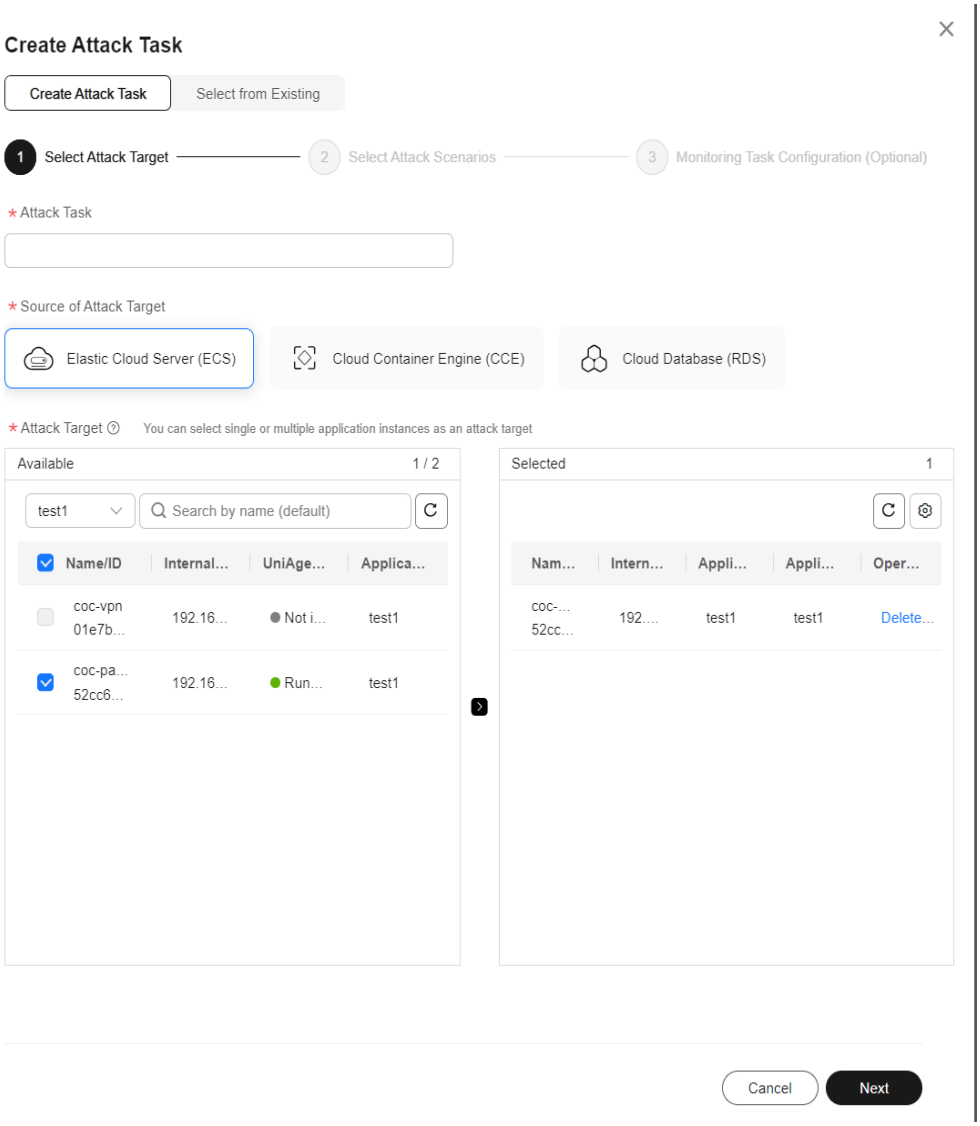
Figure 8-8 Selecting an attack task



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**.

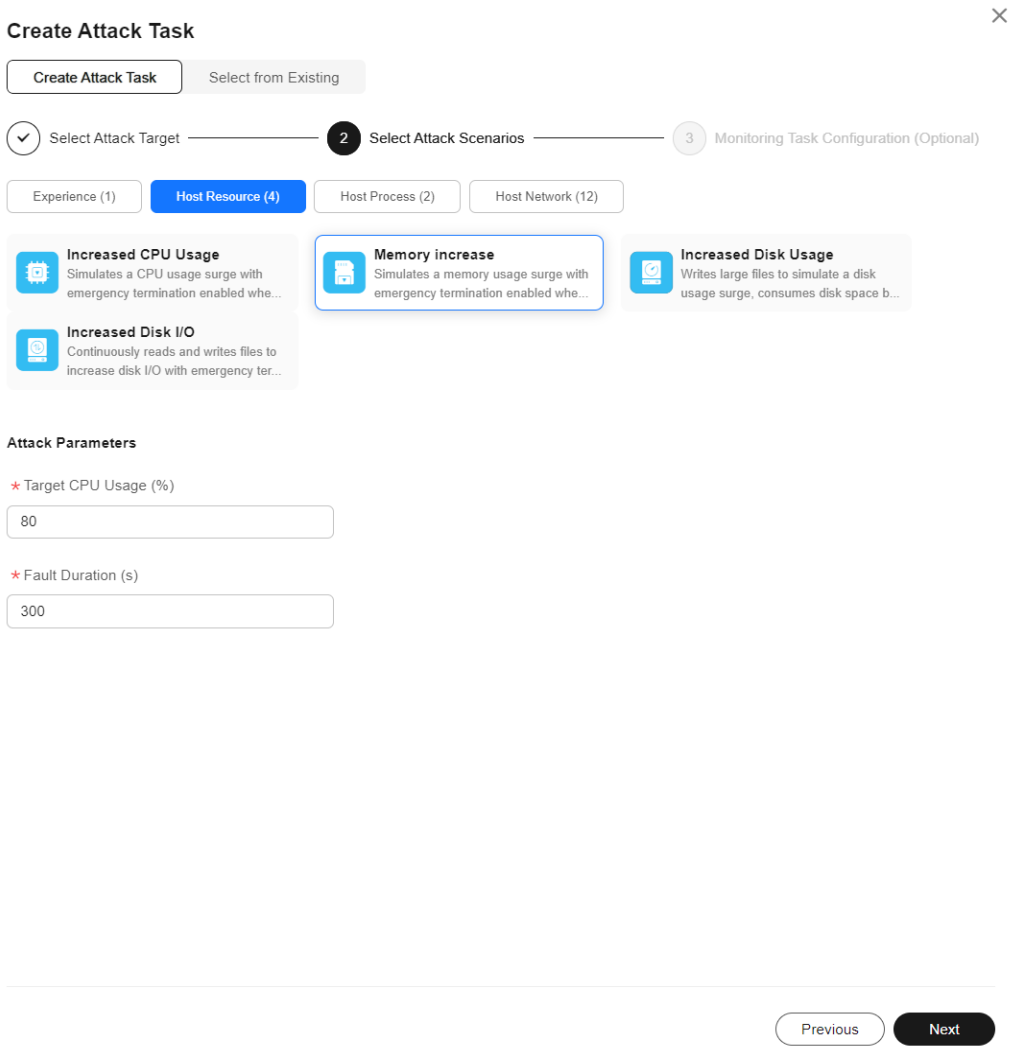
Step 7 Create an attack task. First, select an attack target, and then select an attack scenario. Different attack targets correspond to different attack scenarios. Enter the attack task name. The attack target sources include **Elastic Cloud Server (ECS)** or **Cloud Container Engine (CCE)**, **Cloud 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 8-9 Selecting ECS as the attack target source



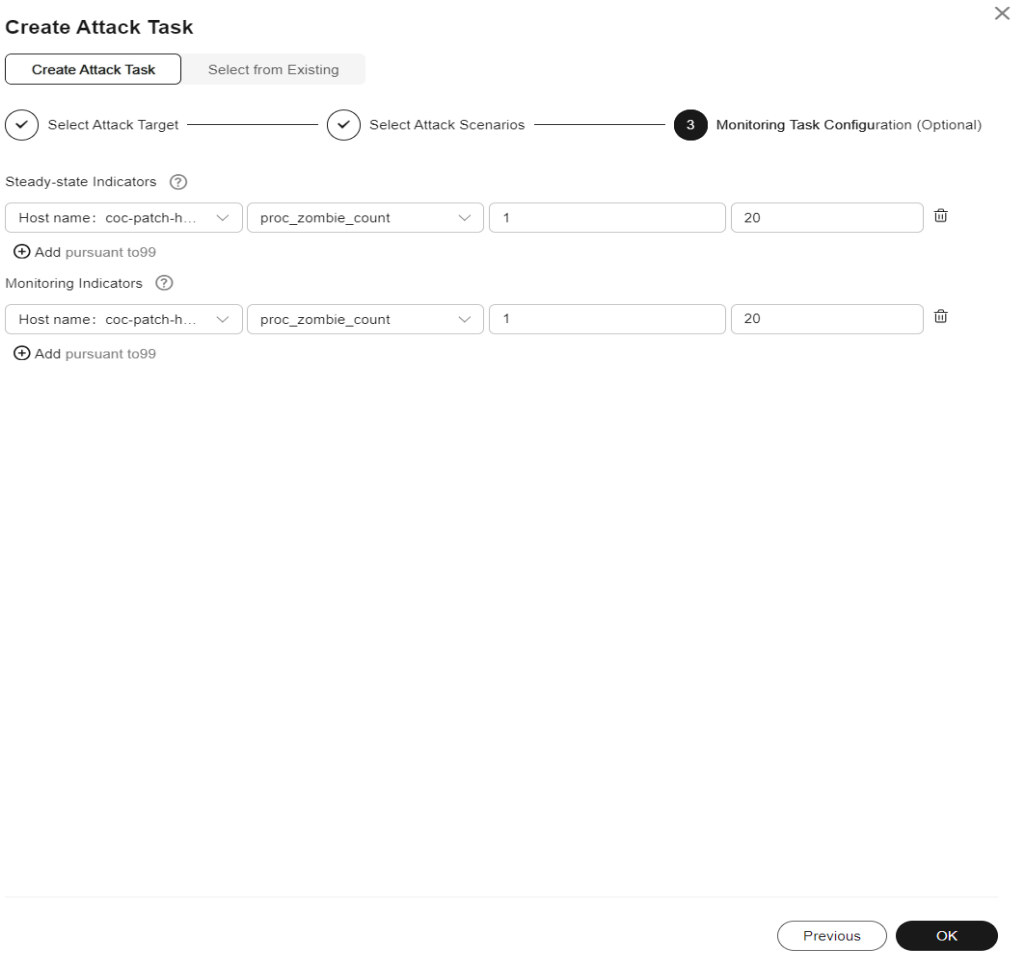
Step 8 Select an attack scenario, set attack parameters, and click **OK**. The scenarios include **Host Resource**, **Host Process**, and **Host Network**.

Figure 8-10 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 8-11 ECS attack scenario drill monitoring configuration



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 8-12 Selecting CCE as the attack target source and specifying a pod

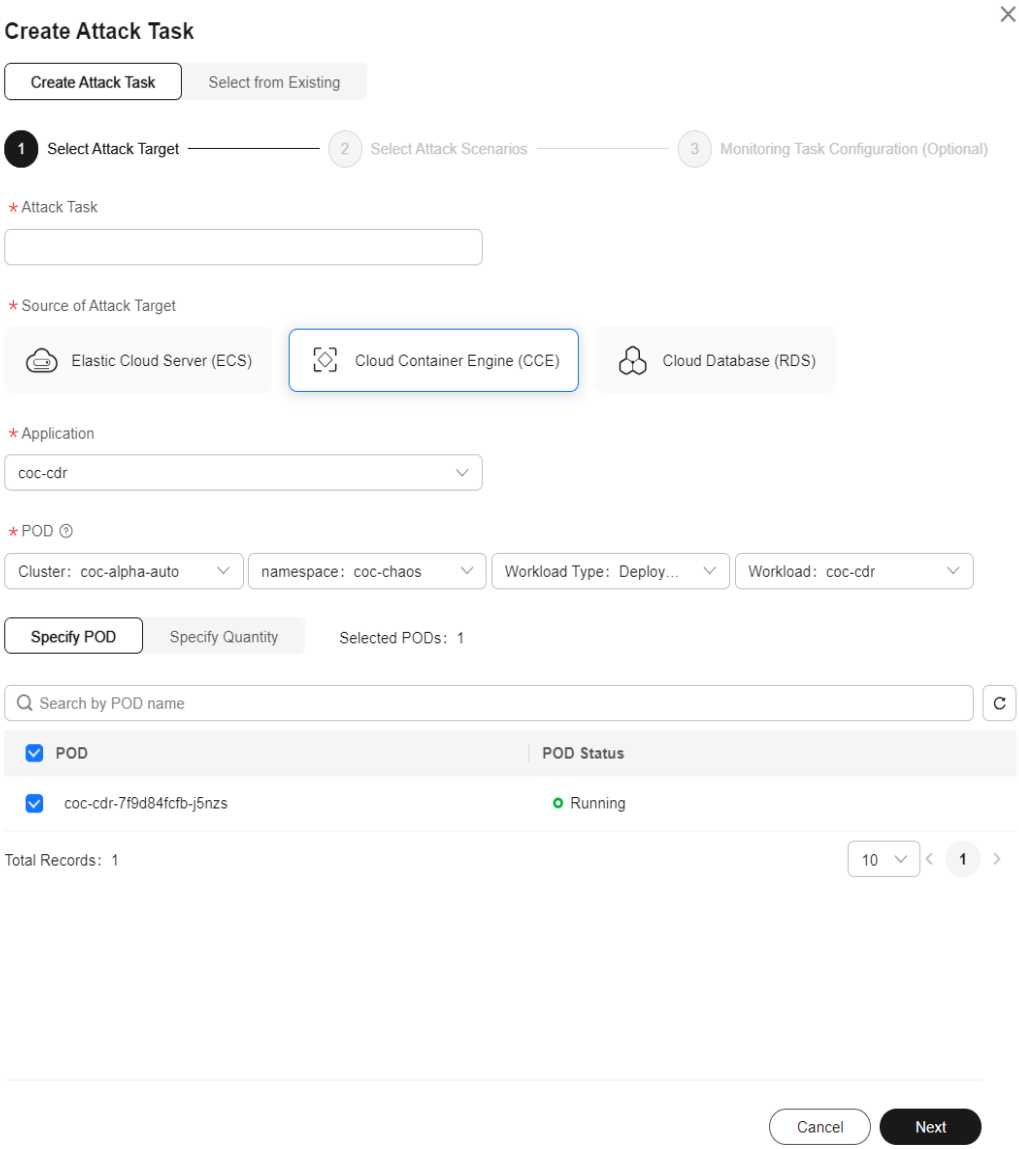
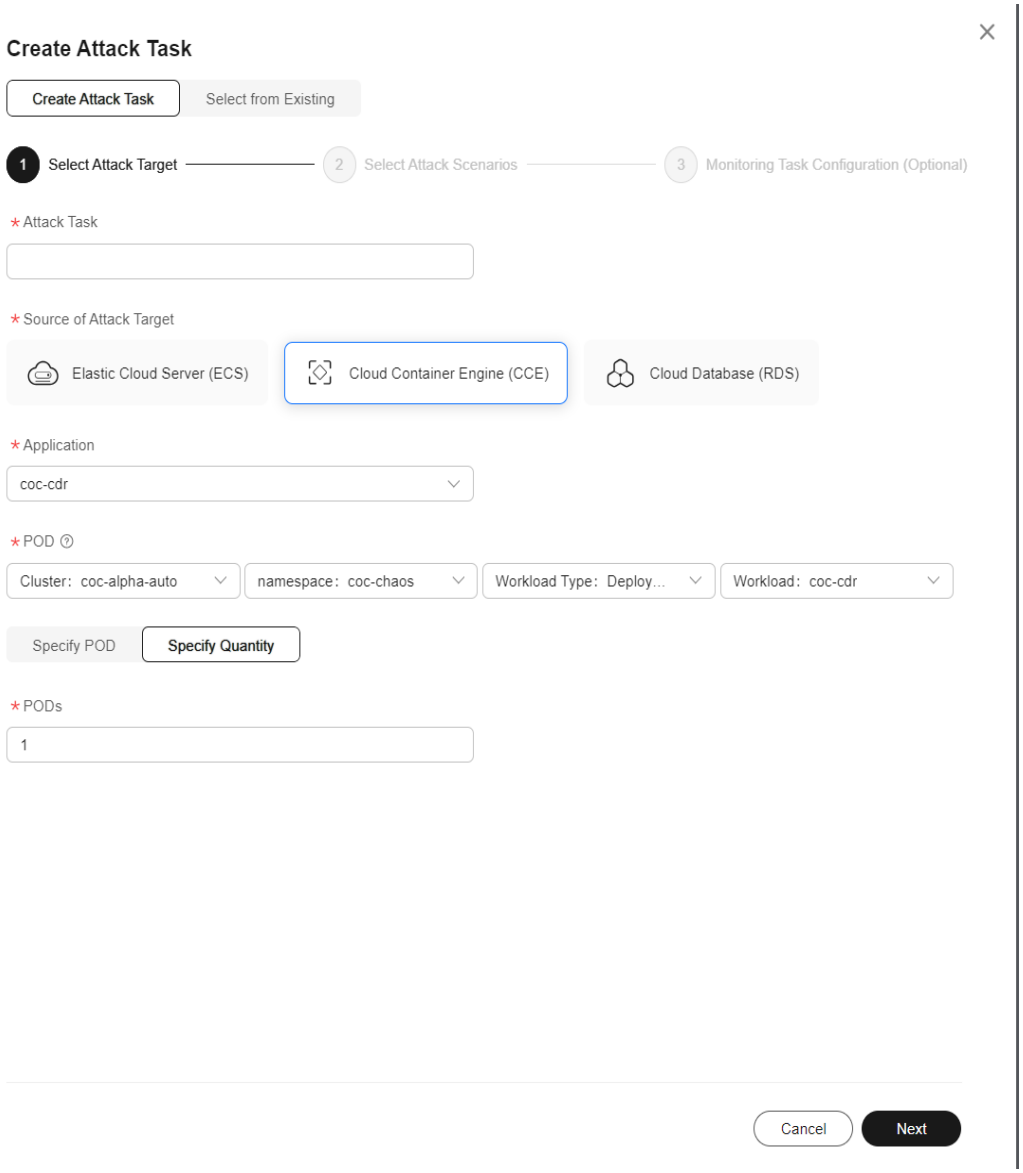
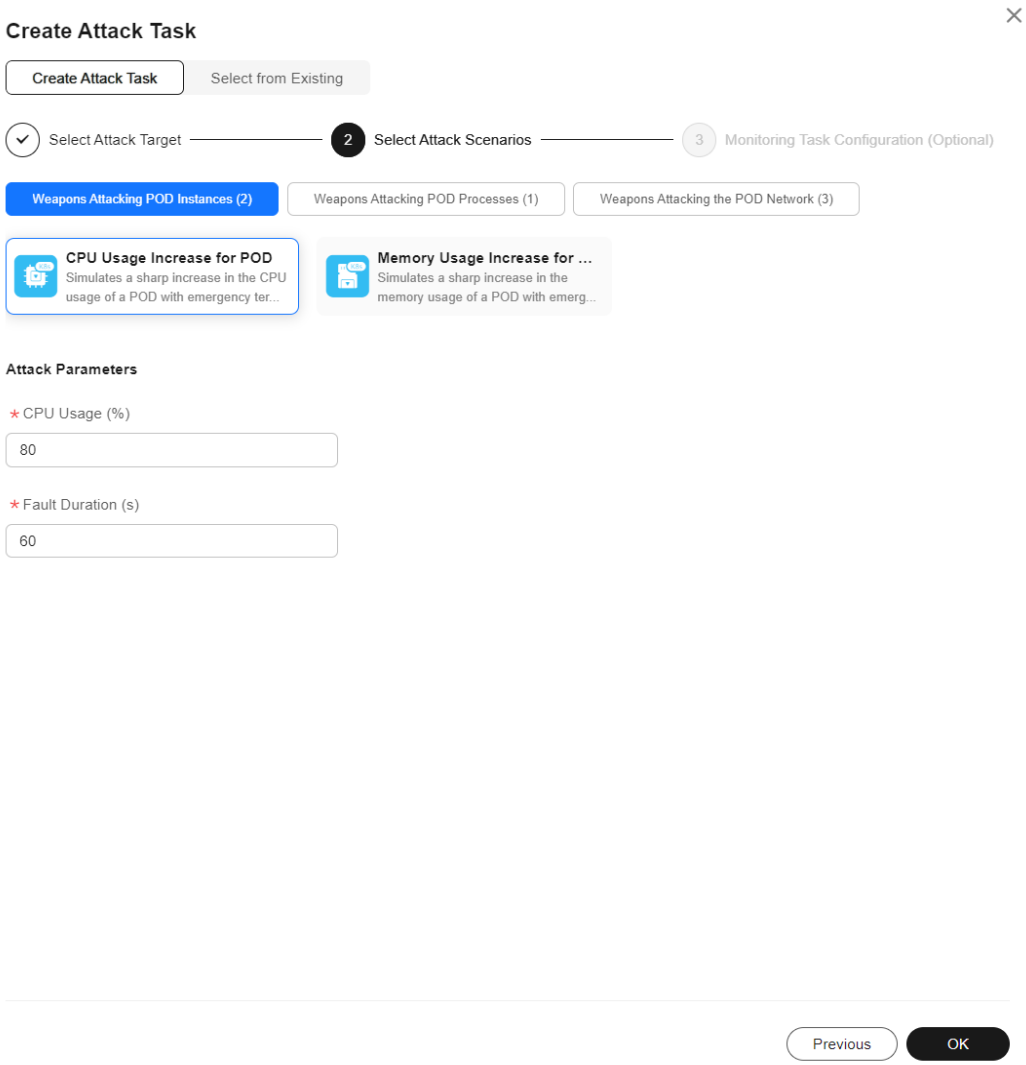


Figure 8-13 Selecting CCE as the attack target source and specifying the quantity



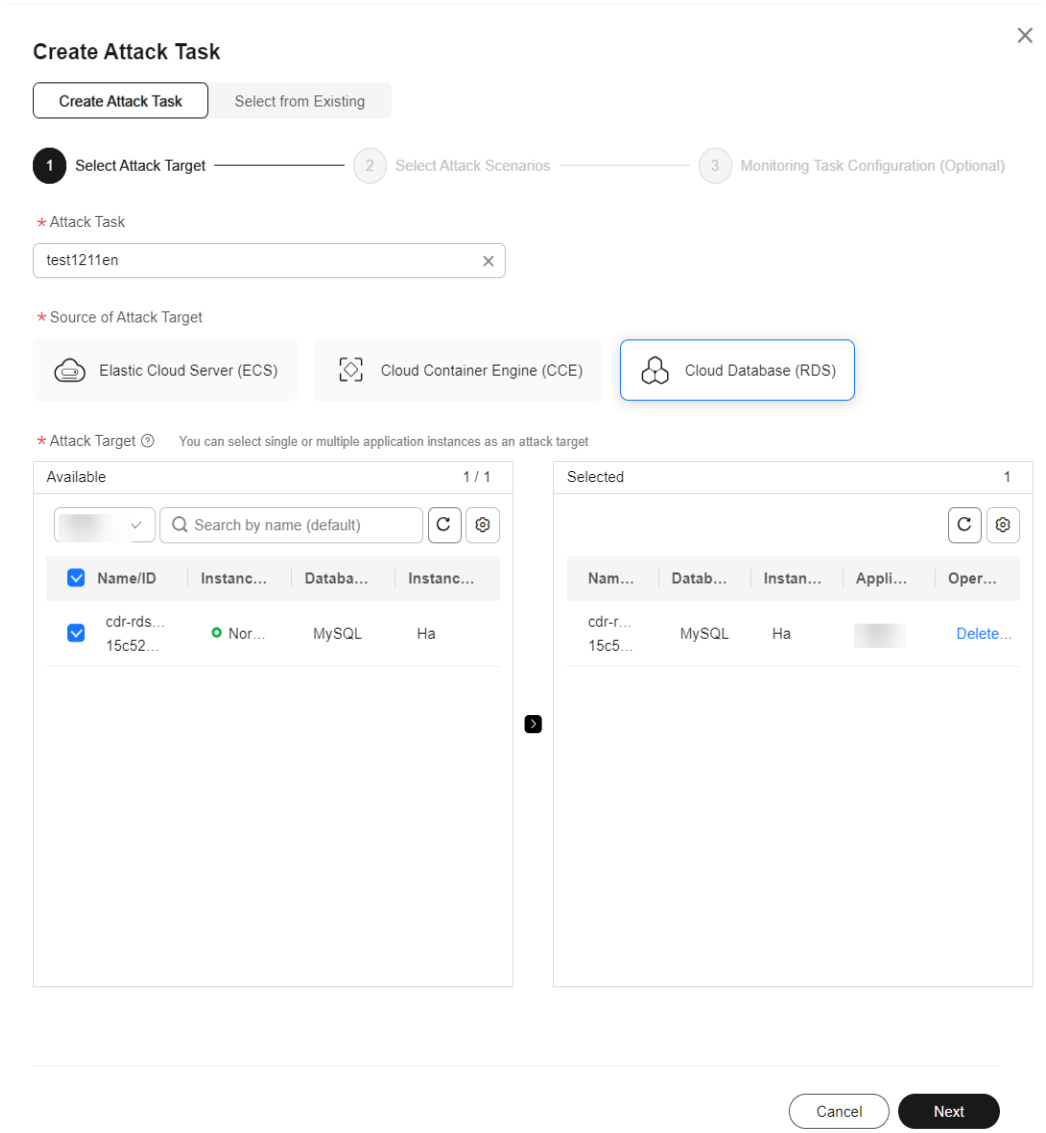
Step 11 Select a CCE attack scenario, set attack parameters, and click **OK**. The scenarios include **Weapons Attacking POD Instances**, **Weapons Attacking POD Processes**, and **Weapons Attacking the POD Network**.

Figure 8-14 CCE attack scenarios



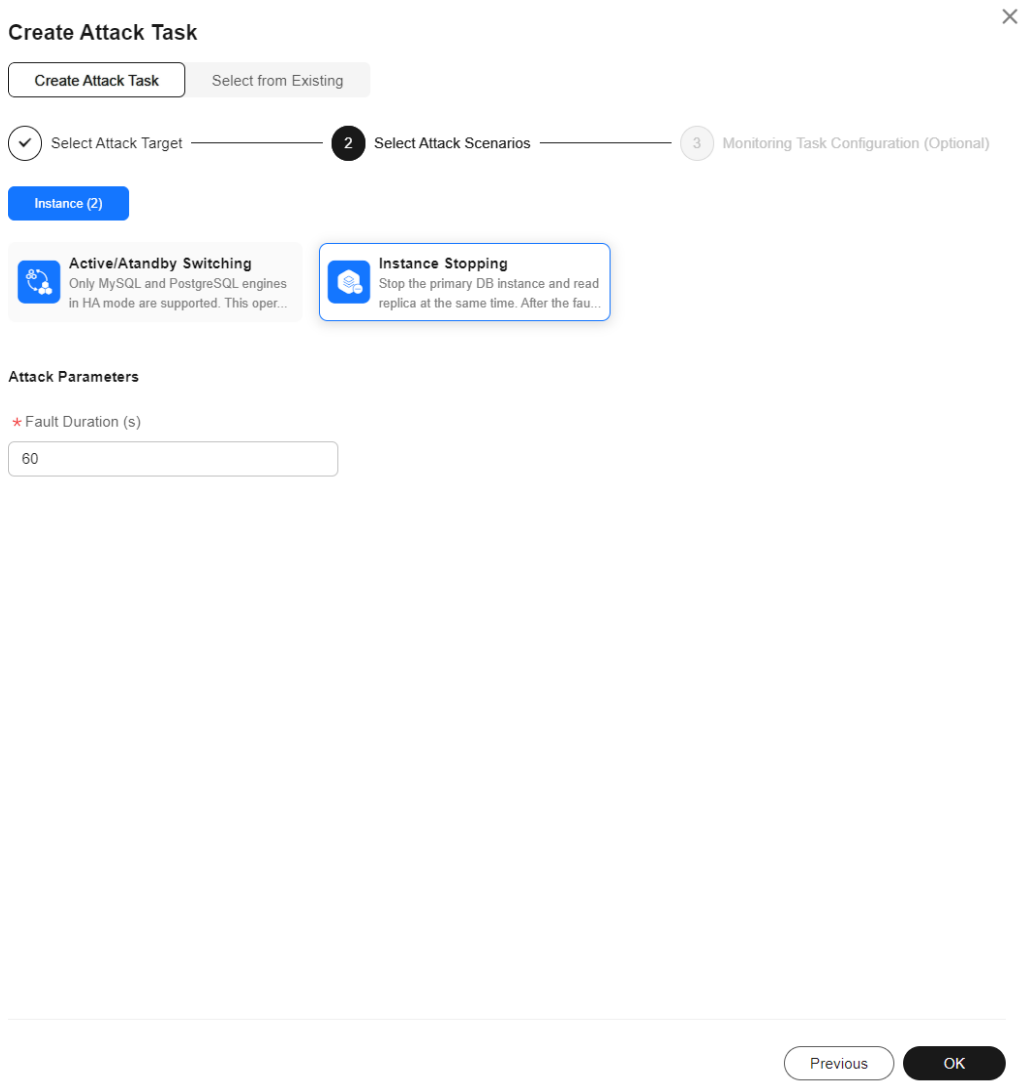
Step 12 If you select RDS as the attack source, select an RDS DB instance and click **Next**.

Figure 8-15 Selecting RDS as the attack target source



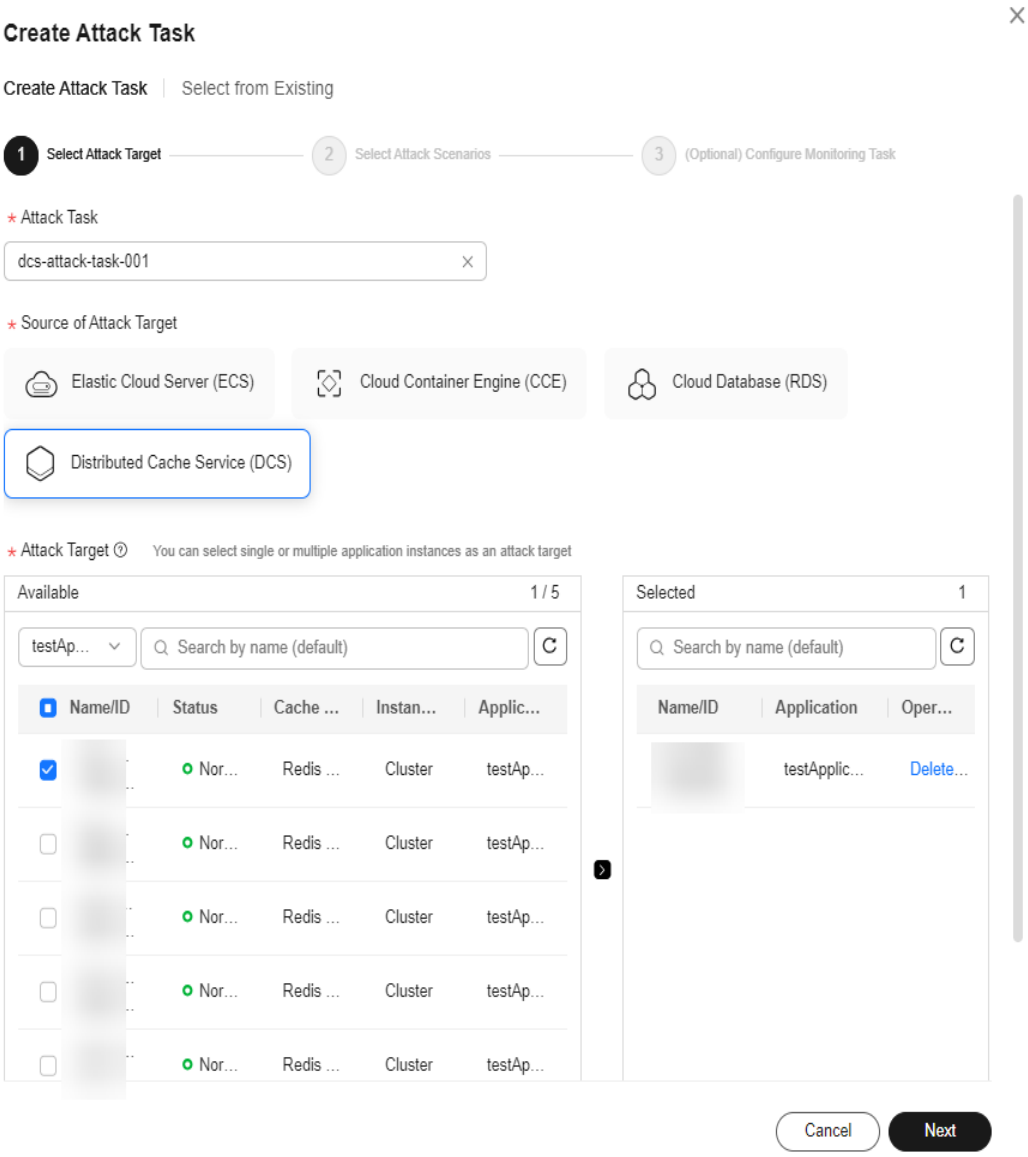
Step 13 Select an RDS attack scenario, set attack parameters, and click **OK**.

Figure 8-16 Cloud Database (RDS) attack scenarios



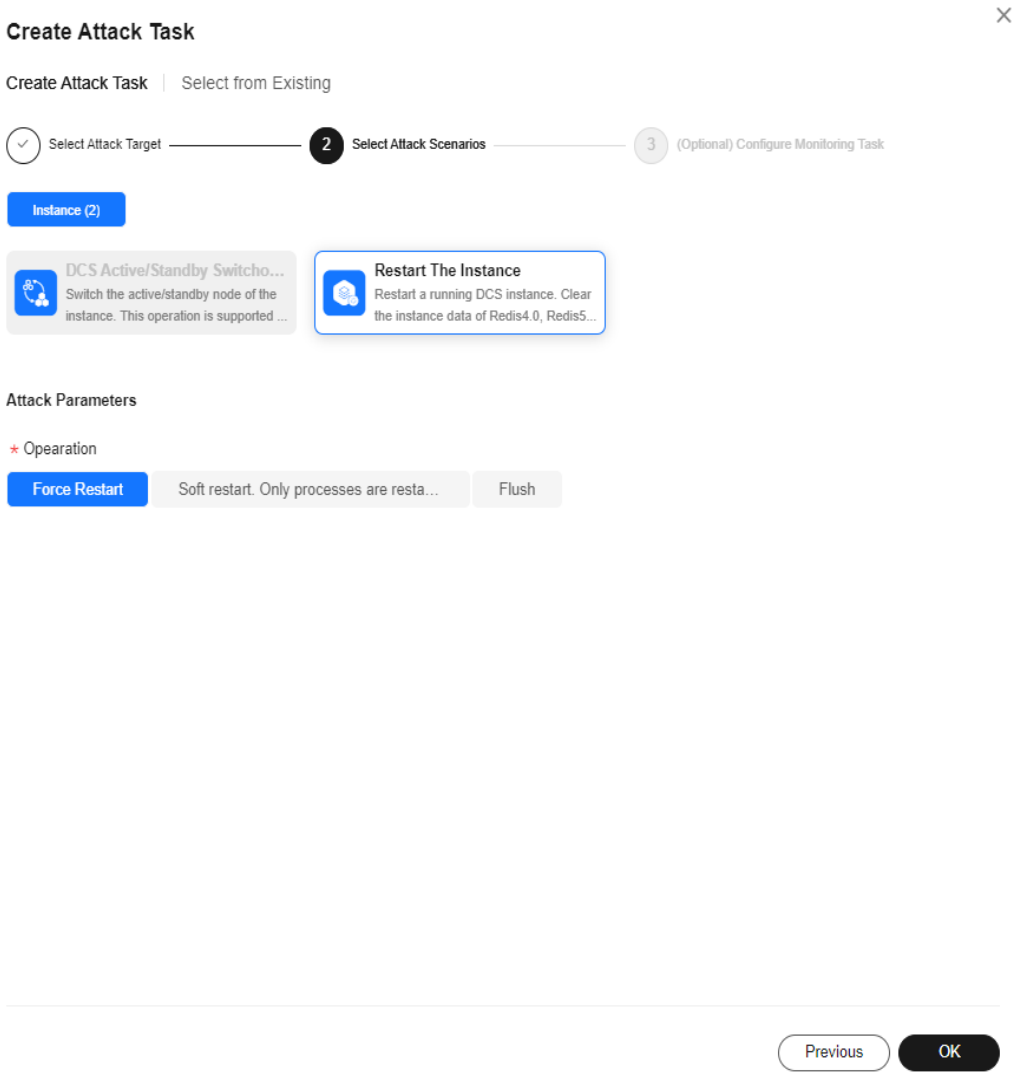
Step 14 If you select DCS as the attack source, select a DCS instance and click **Next**.

Figure 8-17 DCS attack scenarios



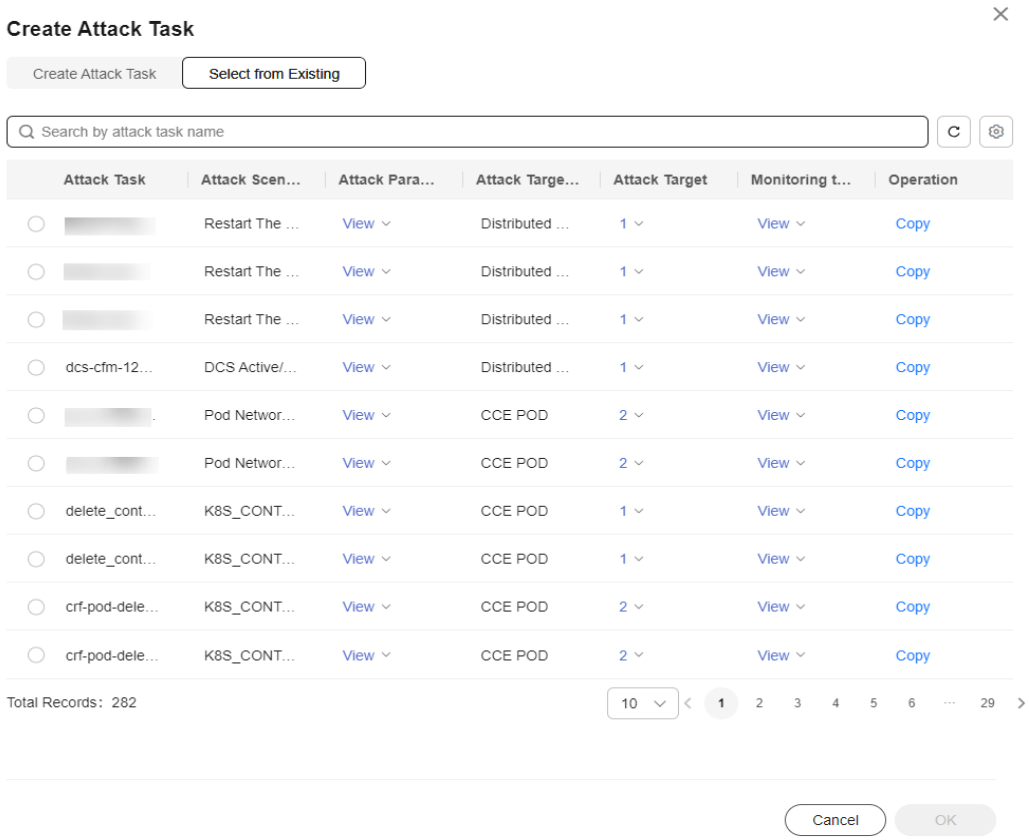
Step 15 Select the DCS attack scenario, set required parameters, and click **OK**.

Figure 8-18 DCS attack scenarios



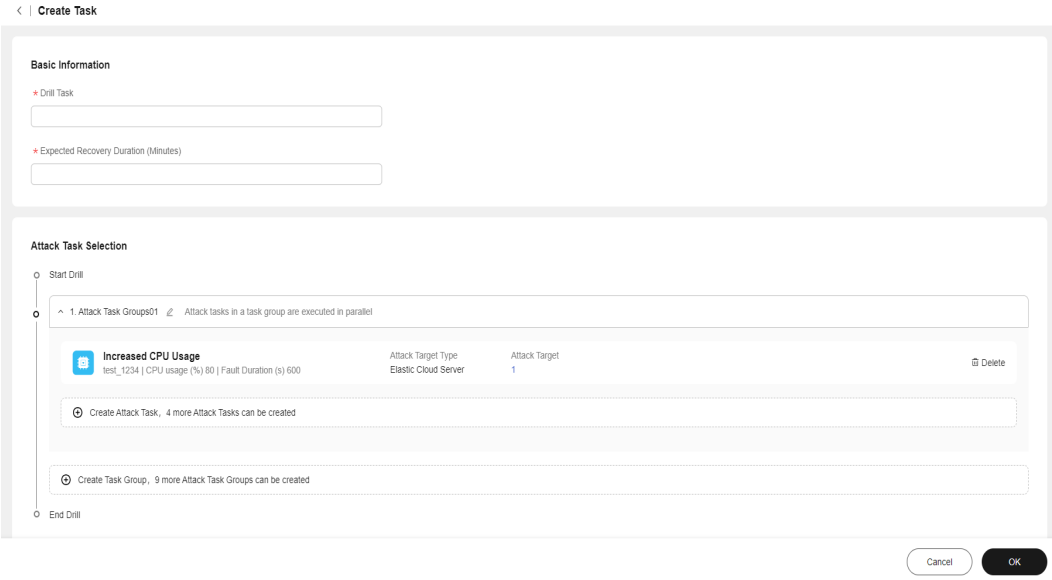
Step 16 If you select **Select from Existing**, select the created attack task from the task list below and click **OK**.

Figure 8-19 Selecting an existing attack task



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

Figure 8-20 Clicking OK



----End

Editing a Drill Task

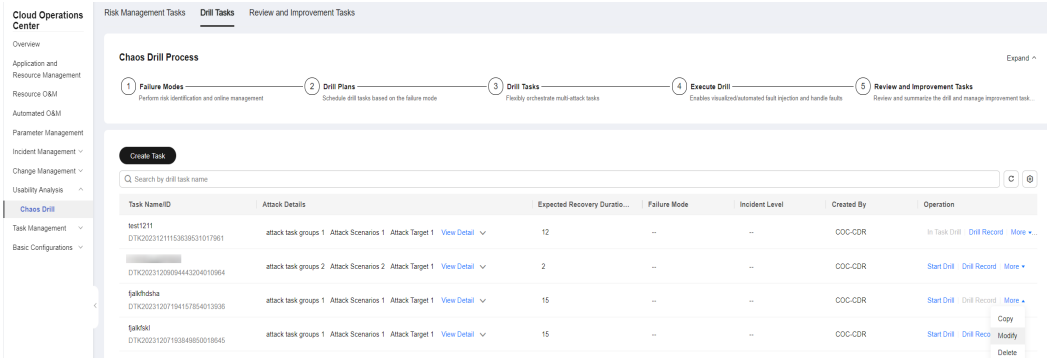
You can edit a drill task. However, if a drill record has been generated for the drill task, the task cannot be edited.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab.

Step 3 Locate the target task, choose **More** > **Modify** in the **Operation** column to modify the basic information about the drill task.

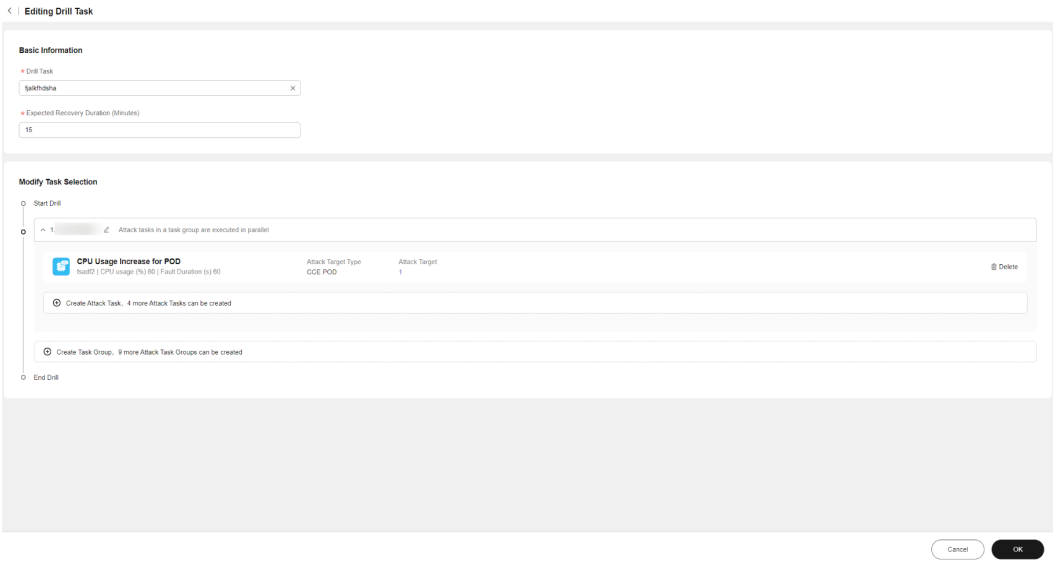
Figure 8-21 Clicking Modify



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 8-22 Modifying a drill task



----End

Deleting a Drill Task

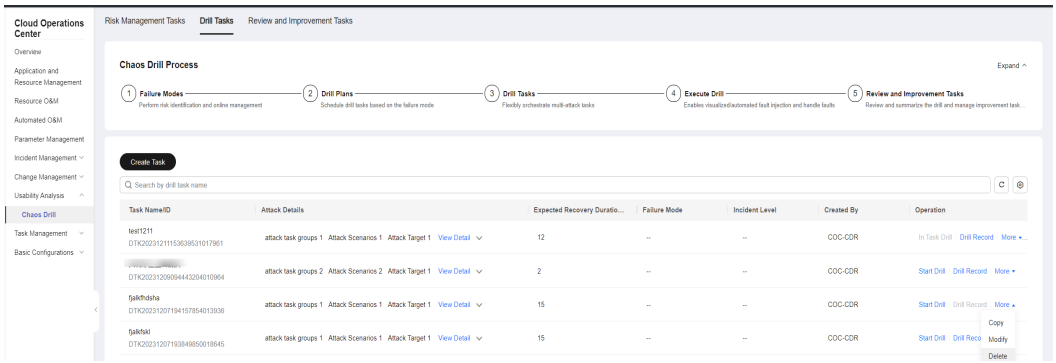
Delete a created drill task. A task that has generated drill records or has associated with drill plans cannot be deleted.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab.

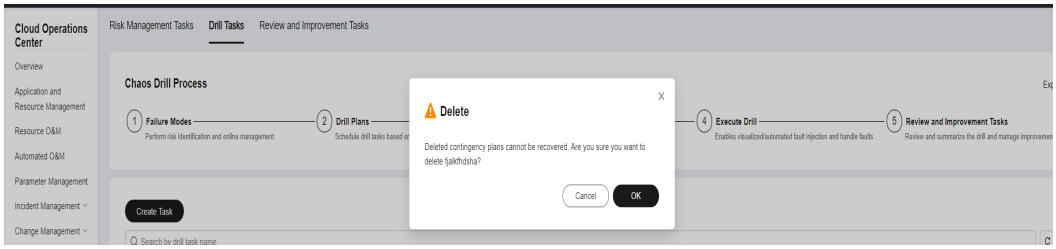
Step 3 Locate the target drill task, choose **More** > **Delete** in the **Operation** column.

Figure 8-23 Drill task list



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

Figure 8-24 Deleting a drill task



----End

Starting a Drill Task

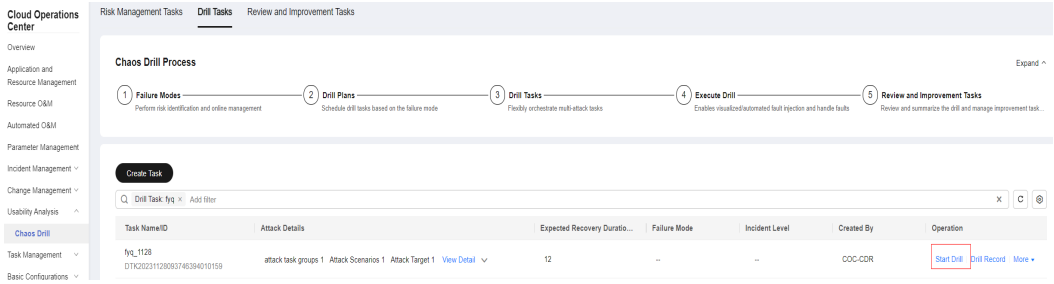
Start a drill task.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab.

Step 3 Locate the target drill task, click **Start Drill** in the **Operation** column.

Figure 8-25 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 8-26 Attack progress

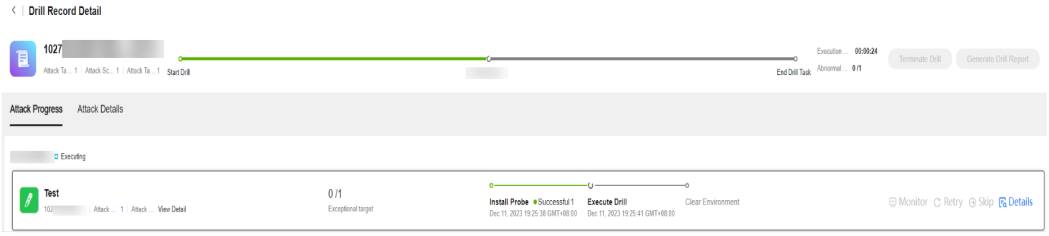
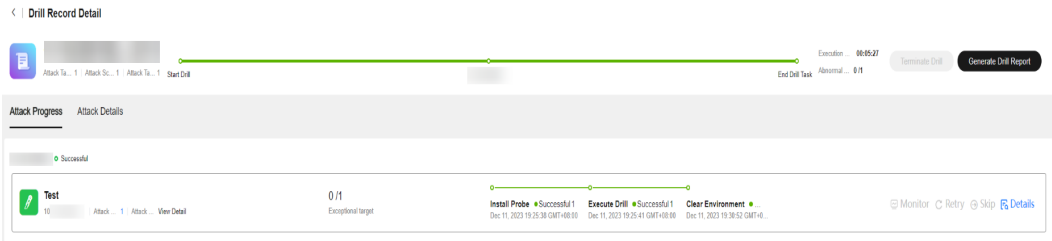
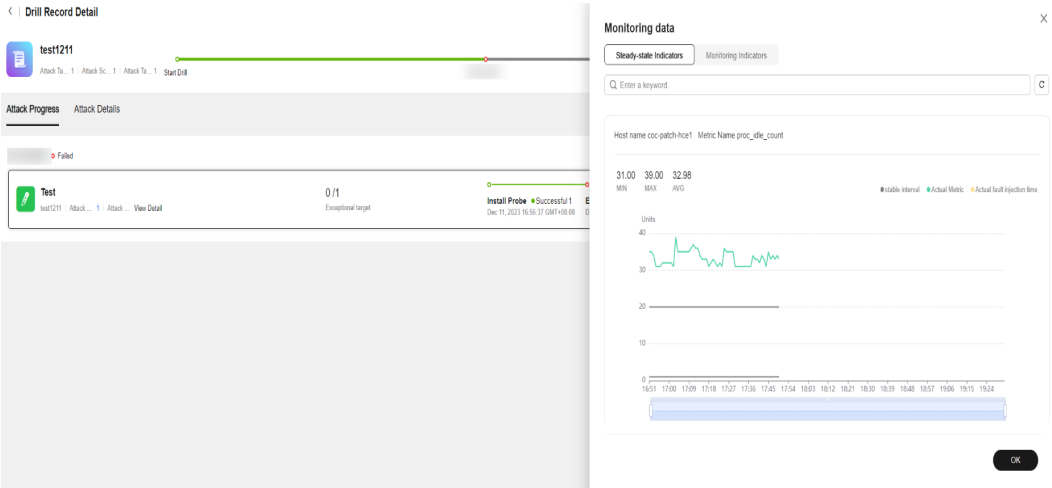


Figure 8-27 Attack completed



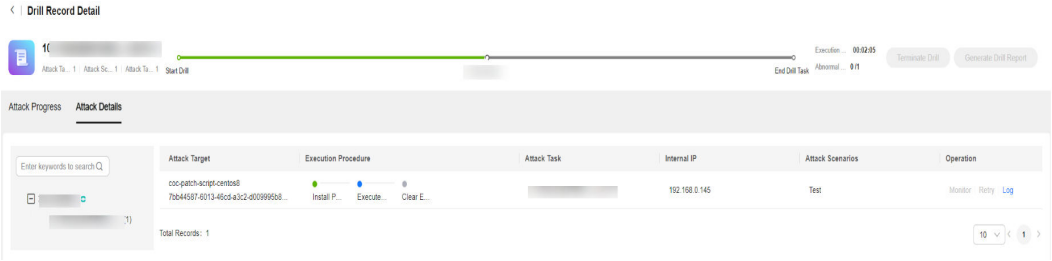
Step 5 During the drill task execution, you can click **Terminate Drill** to end the drill task, click **Retry** to retry the current step, or click **Skip** to skip the current step and go to the next step. If you have configured a drill monitoring task when creating the attack task, you can click **Monitor**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

Figure 8-28 Drill monitoring data



Step 6 Click **Details** to view attack details.

Figure 8-29 Attack details



----End

Viewing Drill Records

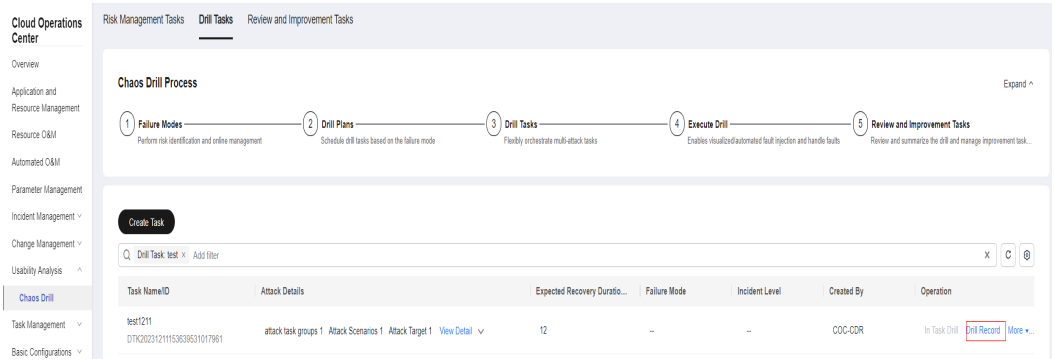
View the drill records of a drill task. A drill task that has not been drilled does not contain drill record.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab.

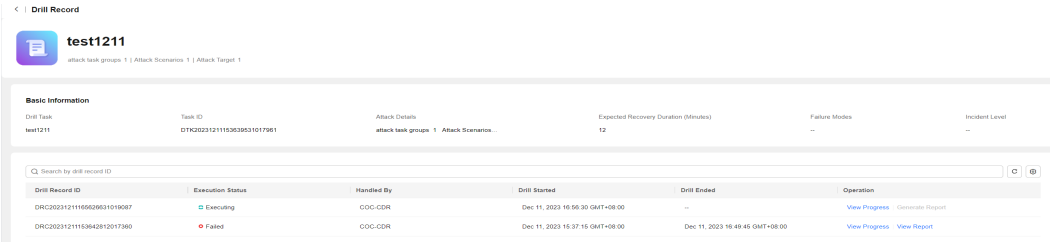
Step 3 Locate the target drill task, click **Drill Record** in the **Operation** column.

Figure 8-30 Drill task list



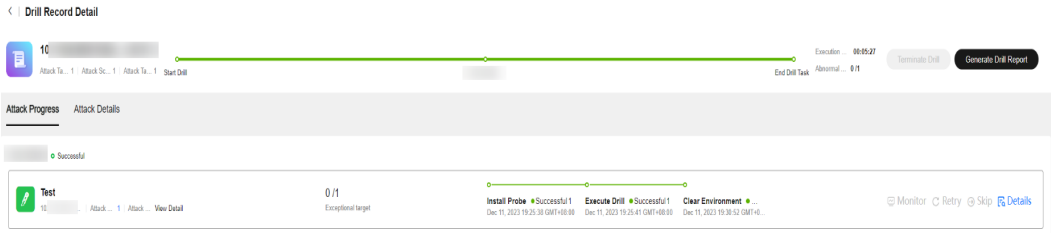
Step 4 The basic information about the drill task includes the drill task name, drill task ID, attack details, and failure mode. All drill records include the drill record ID, execution status, executor, drill start time, and drill end time.

Figure 8-31 Drill Records



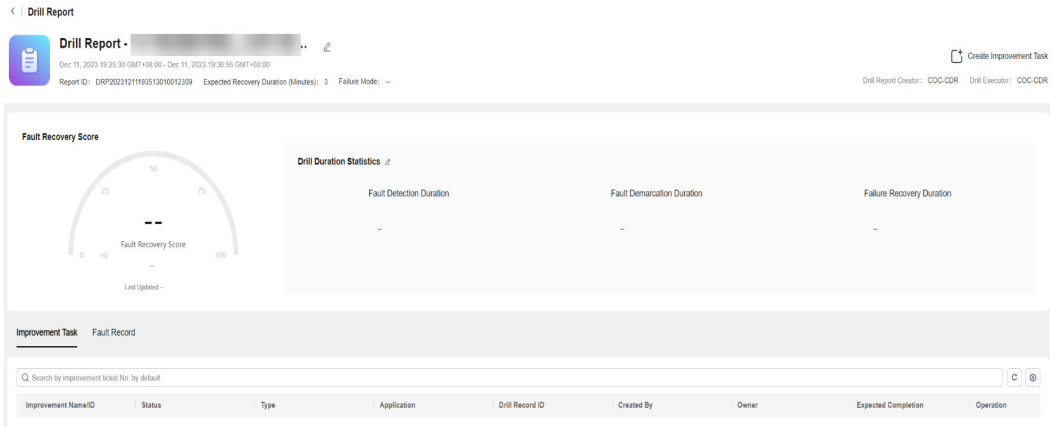
Step 5 Click **View Progress** to view the attack progress and attack details of the current drill task.

Figure 8-32 Attack progress



Step 6 Click **Generate Drill Report** to create or view a drill report. For details, see **Drill Report**.

Figure 8-33 Viewing a drill report



----End

8.1.5 Customizing a Fault

Scenarios

Create a drill task with a custom fault as the attack scenario on COC.

Precautions

A custom fault is determined by the script you compiled. Therefore, when scripts are used to attack ECSs, exceptions such as high resource usage and network faults may occur. As a result, the status of the UniAgent installed on the ECSs may change to offline or abnormal. Exercise caution when performing this operation.

Creating a Custom Fault

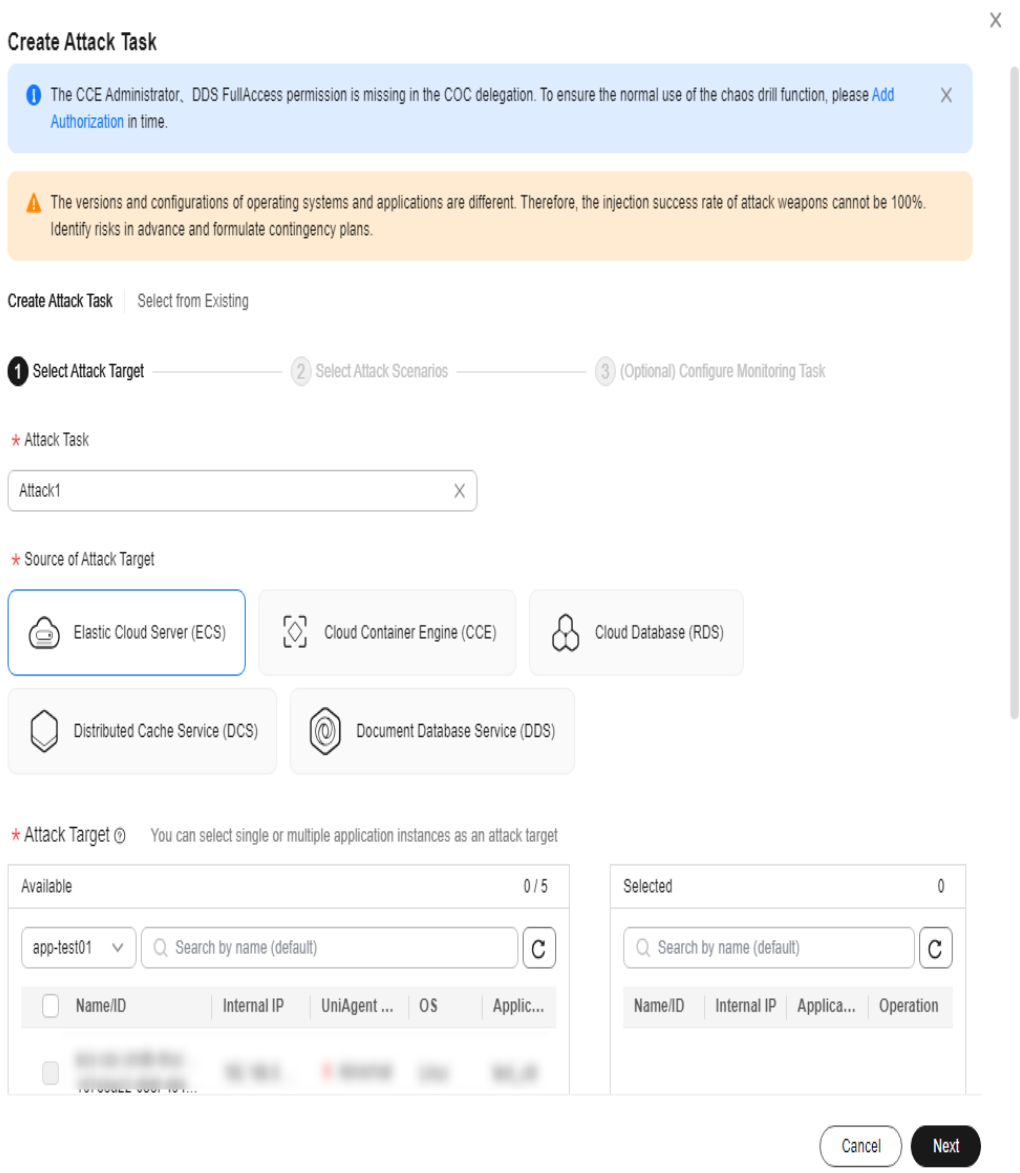
Create a drill task for a custom fault attack scenario on COC.

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Chaos Drill**. On the displayed page, click the **Drill Tasks** tab and create an attack task by referring to **Step 2** to **Step 6**.

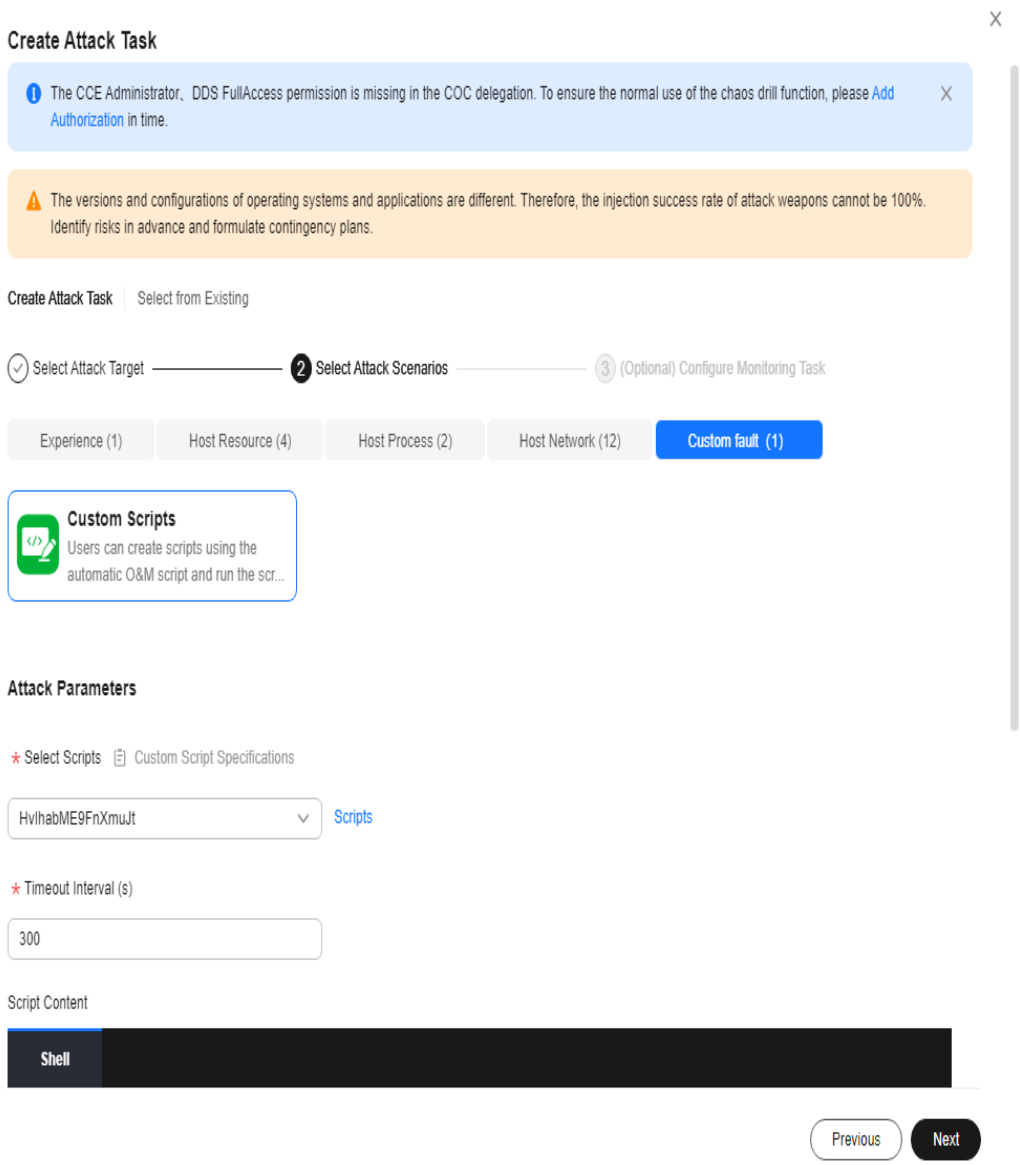
Step 3 Enter the attack task name, select Elastic Cloud Server (ECS) as **Source of Attack Target**, and click **Next**.

Figure 8-34 Selecting ECS as the attack target source



Step 4 On the **Select Attack Scenario** procedure, click **Custom fault**, and then **Custom Scripts**. If a custom fault script exists, you can select it. If no custom fault script available, you need to create a script.

Figure 8-35 Selecting the custom fault



Step 5 To create a custom fault script, click **Scripts**. The **Automated O&M** > **Scripts** page is displayed. Click **Create Script**. For details about how to create a script, see section **Creating a Custom Script**. For details about the script specifications, see the following code:

```
#!/bin/bash
set +x

function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}

function inject_fault()
{
    echo "inject fault"
}
```



```
function check_fault_status()
{
    echo "check fault status"
}

function rollback()
{
    echo "rollback"
}

function clean()
{
    echo "clean"
}

case "$ACTION" in
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
    *)
        usage
;;
esac
```

You are advised to define a custom fault script based on the preceding script specifications. In the preceding specifications, you can define the fault injection function, fault check function, fault rollback function, and environment clearing function by compiling customized content in the **inject_fault()**, **check_fault_status()**, **rollback()** and **clean()** functions.

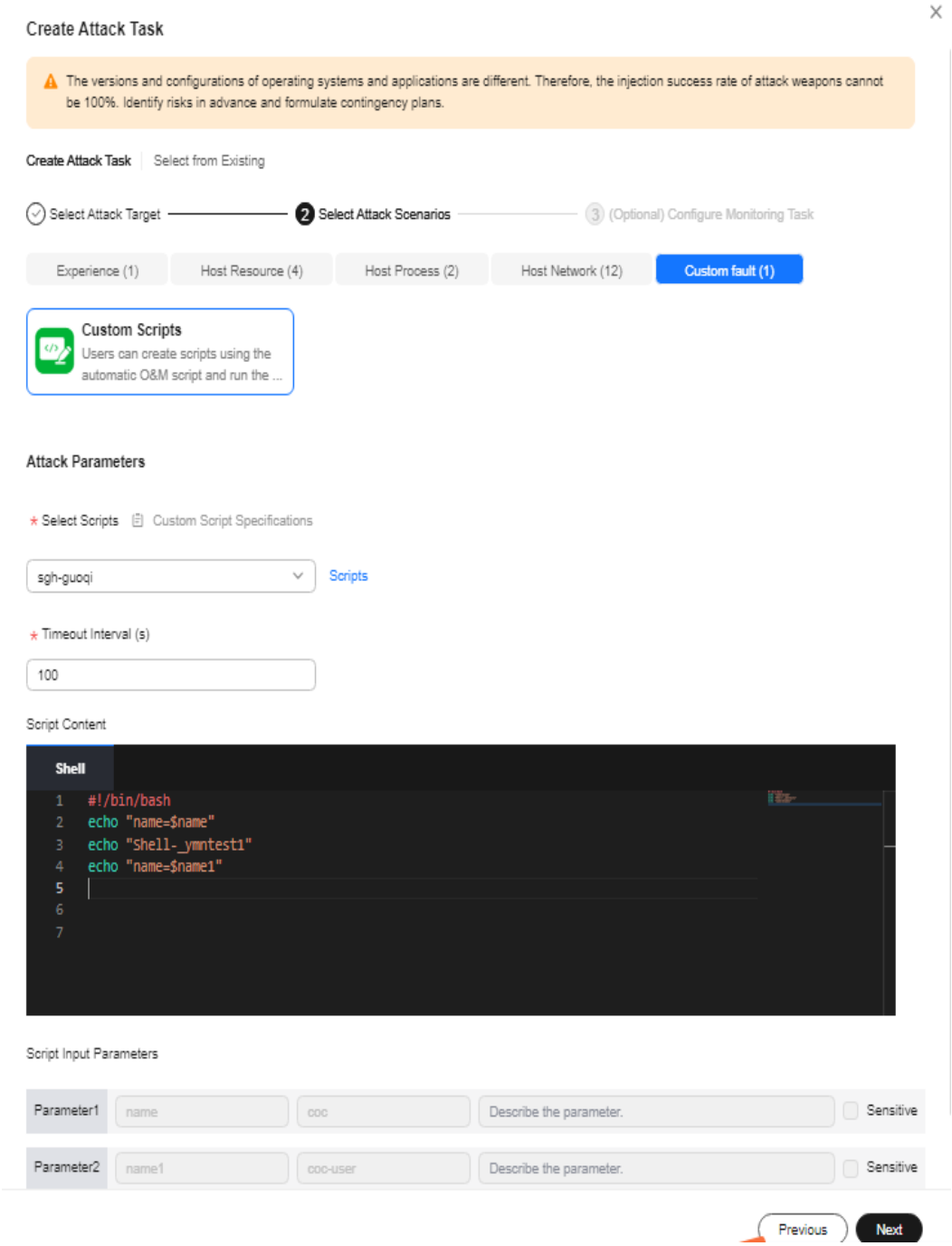
According to the preceding specifications, there are two mandatory script parameters: Whether other script parameters are included depends on your script content.

Table 8-2 Mandatory parameters for customizing a fault script

Parameter	Value	Description
ACTION	inject_fault	Drill operation action. The value is automatically changed by the system background in different drill phases. The value can be: ● **inject_fault**: The drill is in the fault injection phase. ● **check_fault_status**: The drill is in the fault query phase. ● **rollback**: The drill is in the phase of canceling the fault injection. ● **clean**: The drill is in the environment clearing phase.
CAN_ROLLBACK	false	Whether rollback is supported. The options are as follows: ● **true**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is executed. ● **false**: When the drill is in the phase of canceling the fault injection, the **rollback()** function is not executed.

Step 6 If you already have a custom script, you can select the script based on the script name. The script content and parameters are displayed. Enter a proper timeout interval and click **Next**.

Figure 8-36 Selecting a custom script



Step 7 Create a drill task with the custom fault by referring to **Step 9** to **Step 17**.

----End

Custom Script Example

The following is an example of a customized script.

The script content is as follows:

```
#!/bin/bash
set +x
```

```
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:~/bin
export PATH


function usage() {
    echo "Usage: {inject_fault|check_fault_status|rollback|clean}"
    exit 2
}

function inject_fault()
{
    echo "============start inject fault============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
        mkdir -p "${SCRIPT_PATH}/${DIR_NAME}"
        echo "mkdir ${SCRIPT_PATH}/${DIR_NAME} successfully"
    fi

    cd "${SCRIPT_PATH}/${DIR_NAME}"

    if [ ! -f ${FILE} ]; then
        touch "${FILE}"
        echo "create tmp file ${FILE}"
        touch inject.log
        chmod u+x "${FILE}"
        chmod u+x inject.log
    else
        echo "append content">${FILE}
    fi
    sleep ${DURATION}
    echo "successfully inject">${FILE}
    echo "============end inject fault============"
}

function check_fault_status()
{
    echo "============start check fault status============"
    if [ ! -d "${SCRIPT_PATH}/${DIR_NAME}" ]; then
        echo "inject has been finished"
        exit 0
    fi
    cd "${SCRIPT_PATH}/${DIR_NAME}"
    SUCCESS_FLAG="successfully inject"

    if [ -f ${FILE} ]; then
        if [[ "$(sed -n '1p' ${FILE})" = "${SUCCESS_FLAG}" ]]; then
            echo "fault inject successfully"
        else
            echo "The fault inject is in progress"
            check_fault_status
        fi
    else
        echo "inject finished"
    fi

    echo "============end check fault status============"
}

function rollback()
{
    echo "============start rollback============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end rollback============"
}

function clean()
{
```

```
    echo "============start clean============"
    cd "${SCRIPT_PATH}"
    if [ -d $DIR_NAME ]; then
        rm -rf "${SCRIPT_PATH}/${DIR_NAME}"
    fi
    echo "============end clean============"
}

case "$ACTION" in
    inject_fault)
        inject_fault
    ;;
    check_fault_status)
        check_fault_status
    ;;
    rollback)
        if [[ X"${CAN_ROLLBACK}" == X"true" ]]; then
            rollback
        else
            echo "not support to rollback"
        fi
    ;;
    clean)
        clean
    ;;
    *)
        usage
;;
esac
```

The input parameters of the script are as follows:

Table 8-3 Script input parameters of the customized script example

Parameter	Value	Description
ACTION	inject_fault	Drill operation action
CAN_ROLLBACK	false	Rollback is not supported.
SCRIPT_PATH	/tmp	Root directory of the custom fault log
DIR_NAME	test_script	Parent directory of the custom fault log
FILE	test.log	Custom fault log name
DURATION	10	Duration of a simulated custom fault, in seconds.

8.1.6 Drill Report

Creating a Drill Report

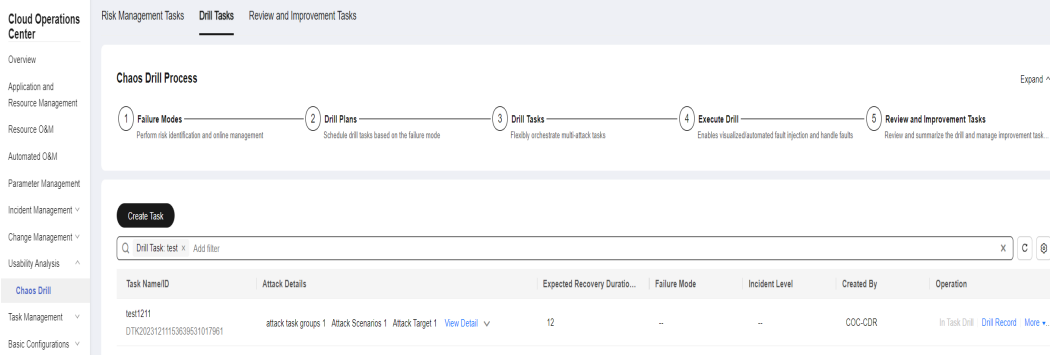
Once a drill is finished, you can create a drill report.

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 8-37 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 8-38 Drill record list

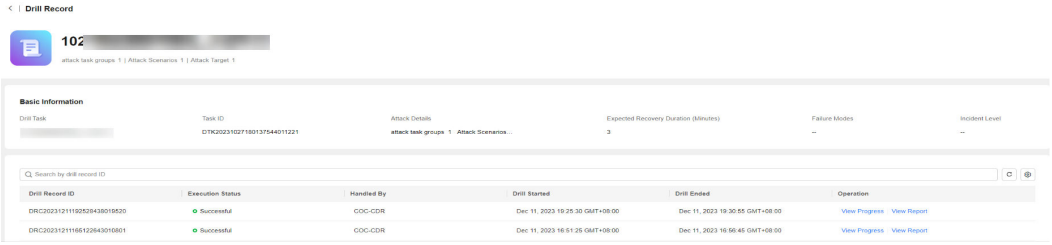
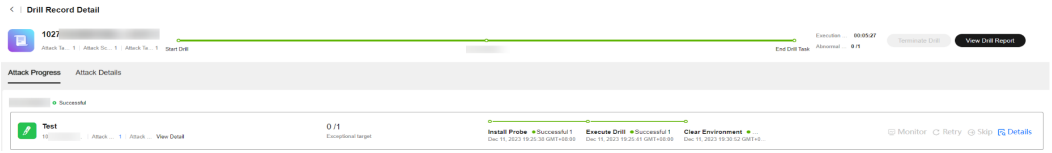
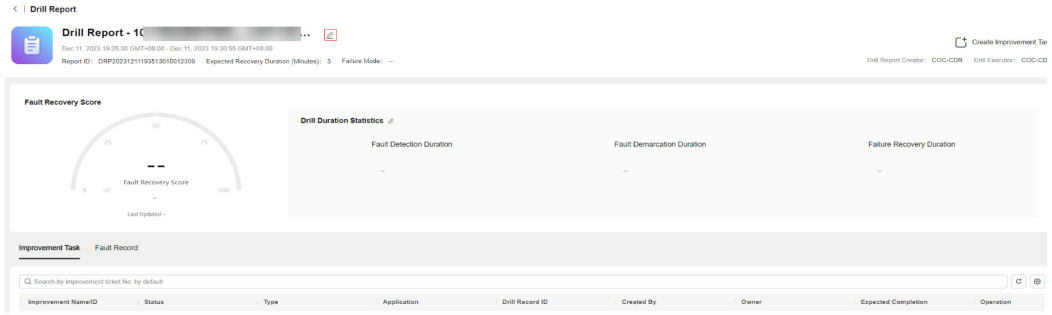


Figure 8-39 Drill Record Detail page



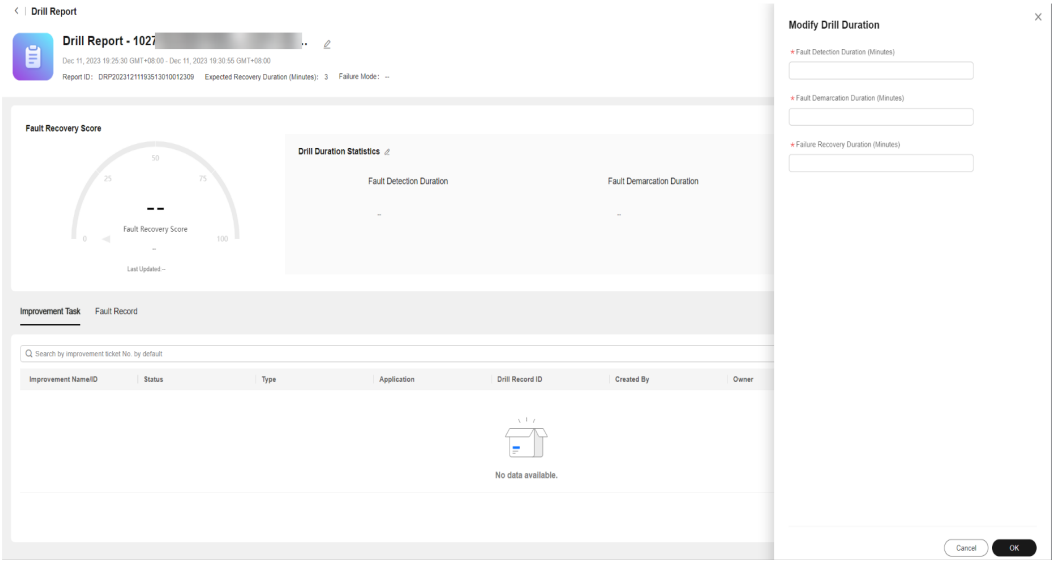
Step 4 Go to the drill report page and update the report name.

Figure 8-40 Drill report details



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

Figure 8-41 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 8-42 Creating Improvement Item

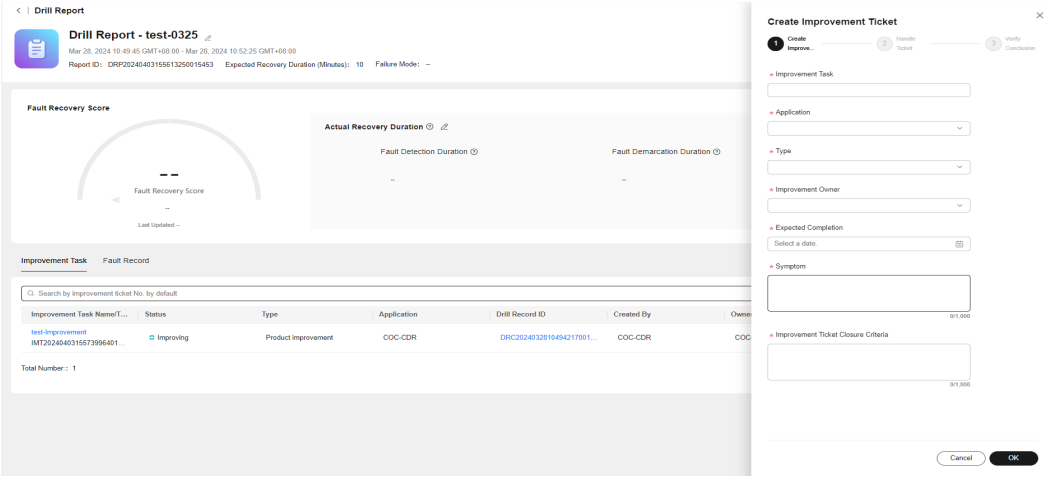


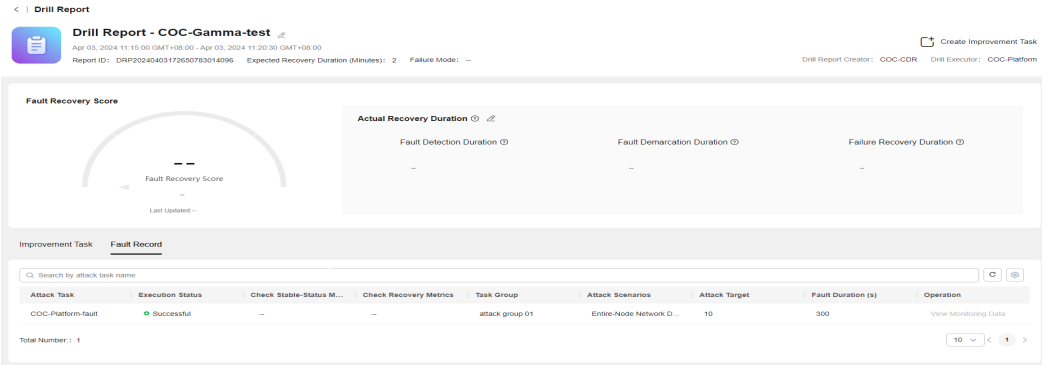
Table 8-4 Improvement ticket parameters

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

Parameter	Description
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 8-43 Fault record



----End

8.2 Emergency Plan

Overview

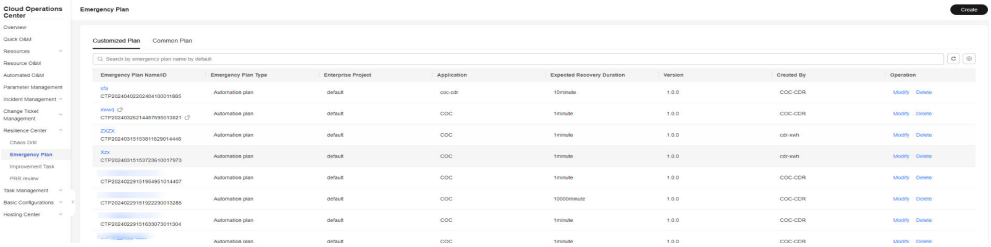
You can create an emergency plan for a system fault that may occur and use the plan if the fault occurs.

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 8-44 Customized Plan tab page



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

Figure 8-45 Creating an emergency plan

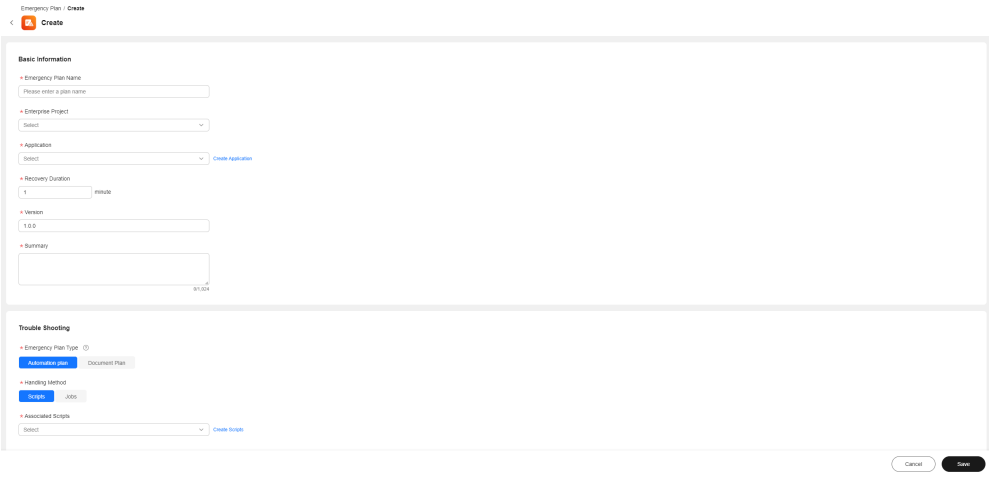


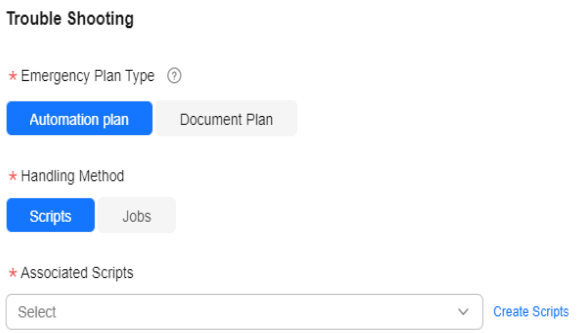
Table 8-5 Parameters for configuring basic information about an emergency plan

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 8-46 Troubleshooting



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

Figure 8-47 Associating a custom script

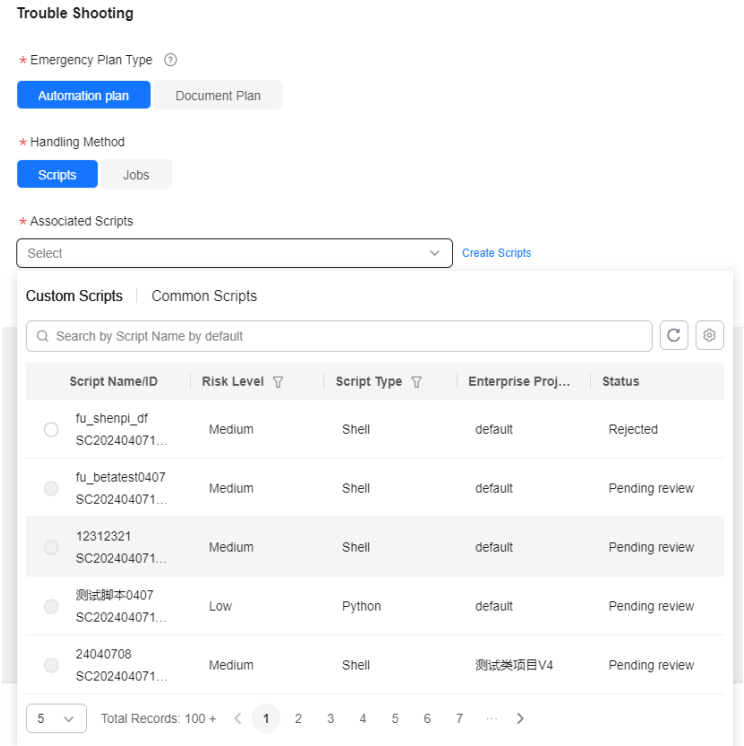
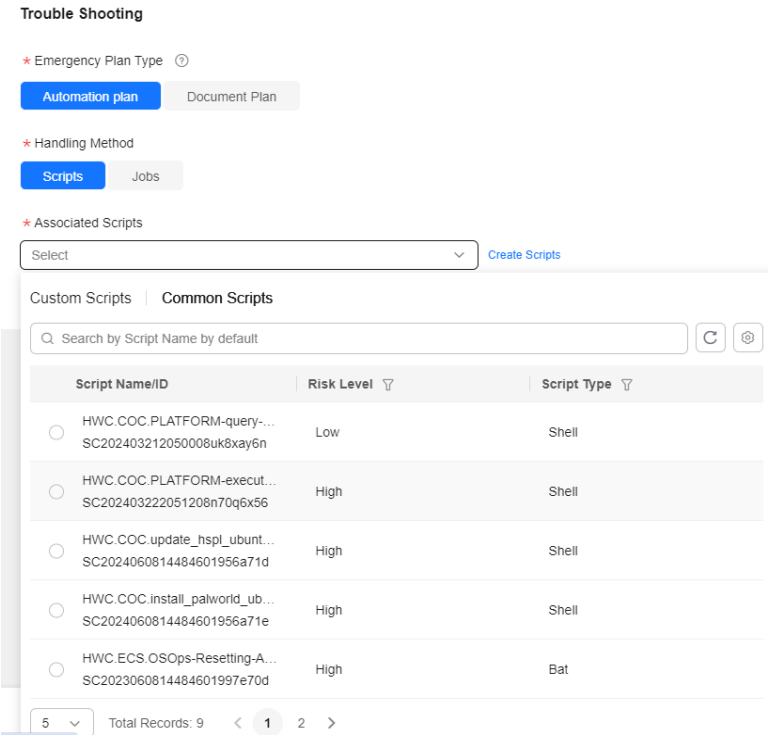


Figure 8-48 Associating a common script



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

Figure 8-49 Associating a custom job

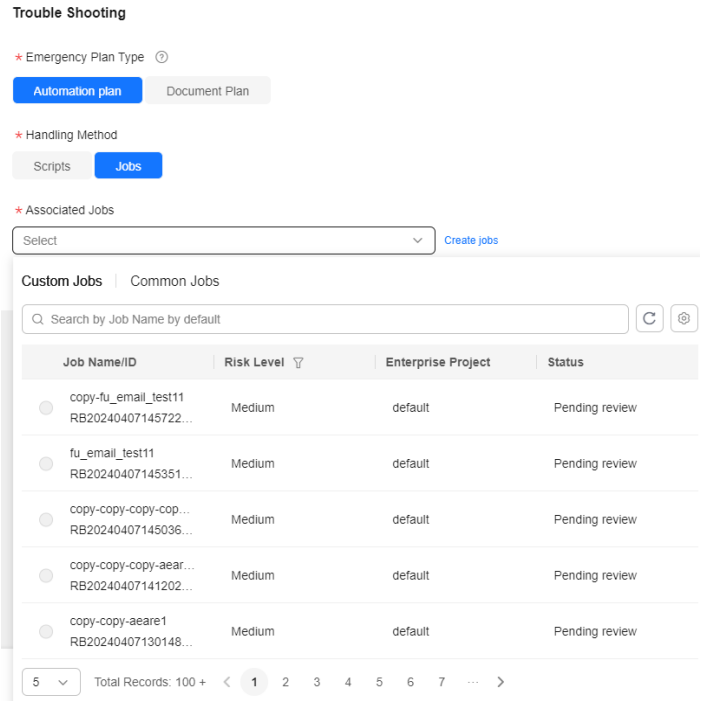
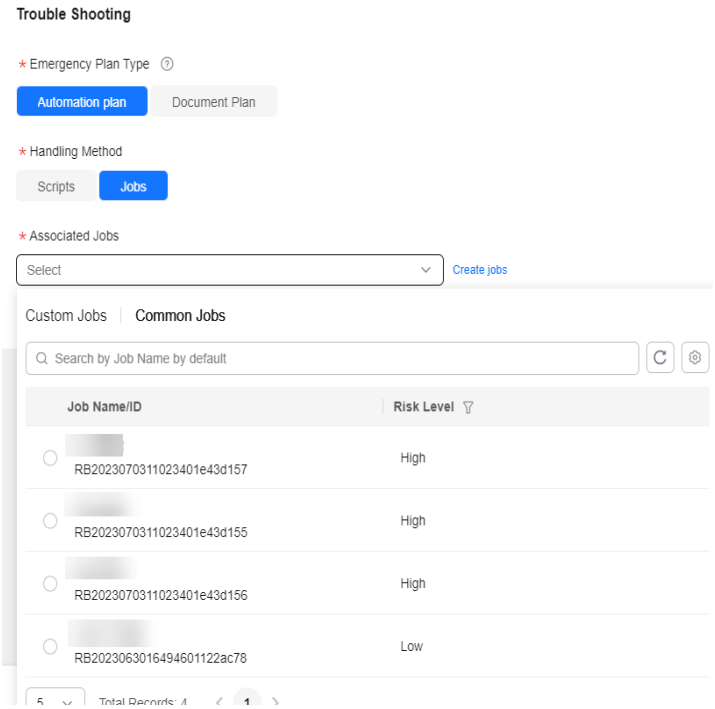
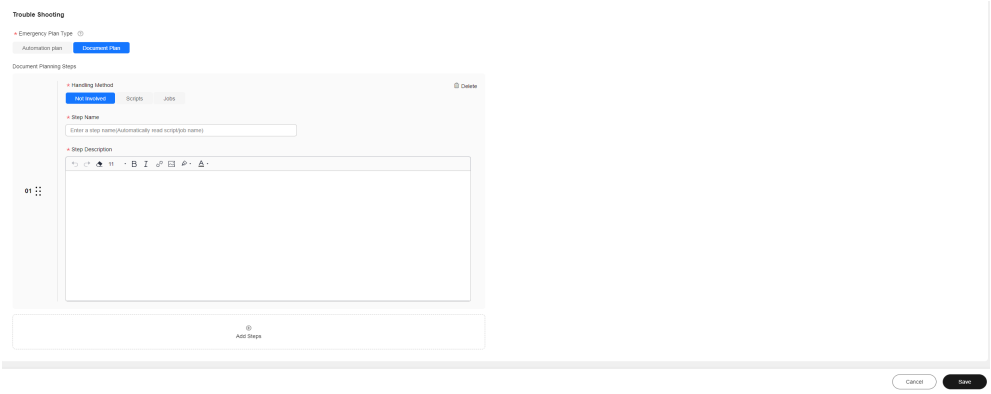


Figure 8-50 Associating a common job



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 8-51 Document plan steps



----End

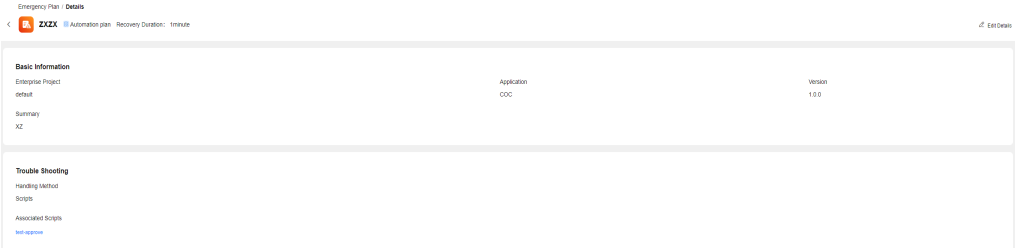
Viewing Emergency Plan Details

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 to view the emergency plan details.

Figure 8-52 Viewing emergency plan details



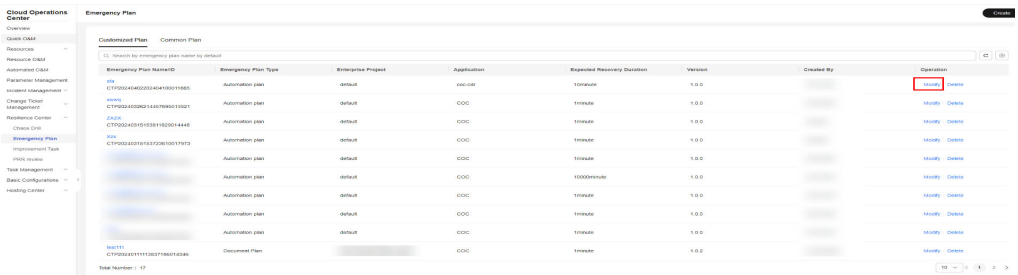
----End

Editing an Emergency Plan

Step 1 Log in to **COC**.

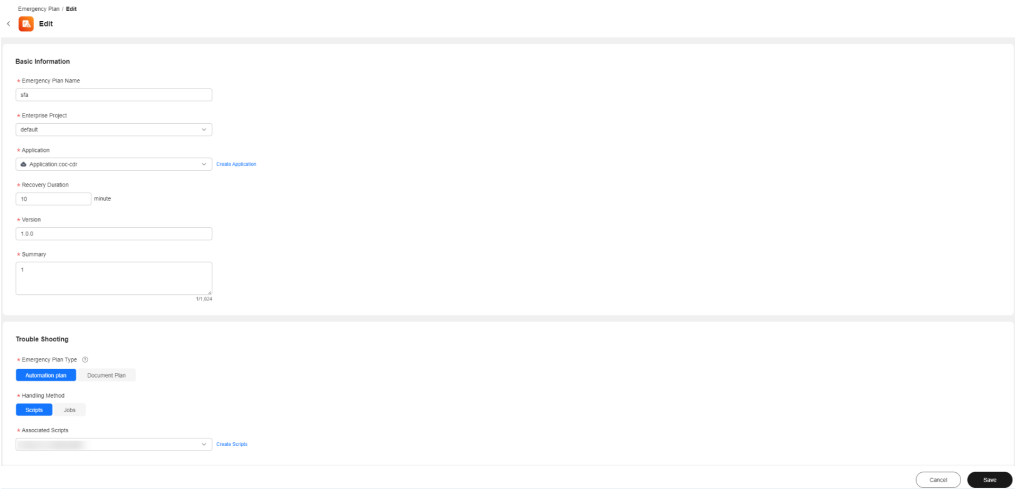
Step 2 In the navigation pane on the left, choose **Resilience Center** > **Emergency Plan**. Click the **Customized Plan** tab.

Figure 8-53 Customized Plan



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

Figure 8-54 Modifying an Emergency Plan



----End

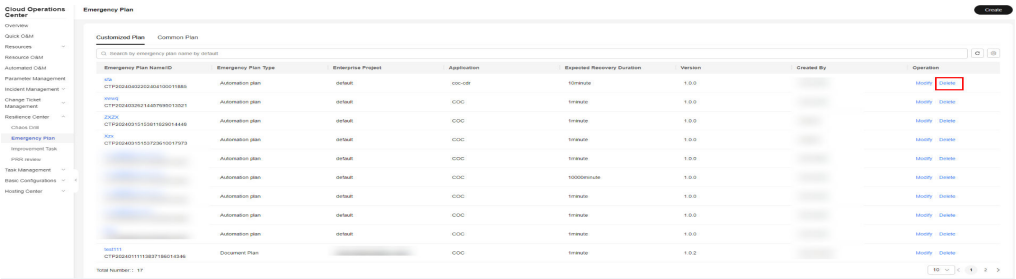
Deleting an Emergency Plan

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **Emergency Plan**. Click the **Customized Plan** tab.

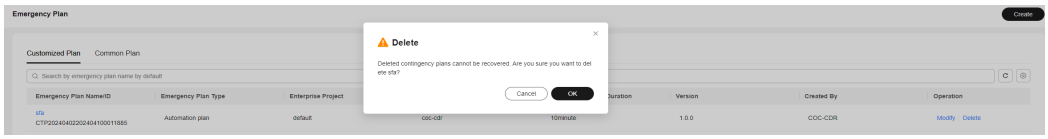
Step 3 Locate the target emergency plan and click **Delete** in the **Operation** column.

Figure 8-55 Emergency plans



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

Figure 8-56 Deleting an emergency plan



----End

8.3 Production Readiness Review

8.3.1 Overview

Production Readiness Review (PRR).

PRR provides the baselines for service availability and operations capabilities from dimensions such as SLI/SLO, redundancy, disaster recovery, overload control, fault management, change capability, operations, and secure production. It allows the frontend personnel to perform requirement planning, design, and development, as well as the production admission review before service rollout.

8.3.2 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 8-57 PRR template management

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

Figure 8-58 Creating a PRR template

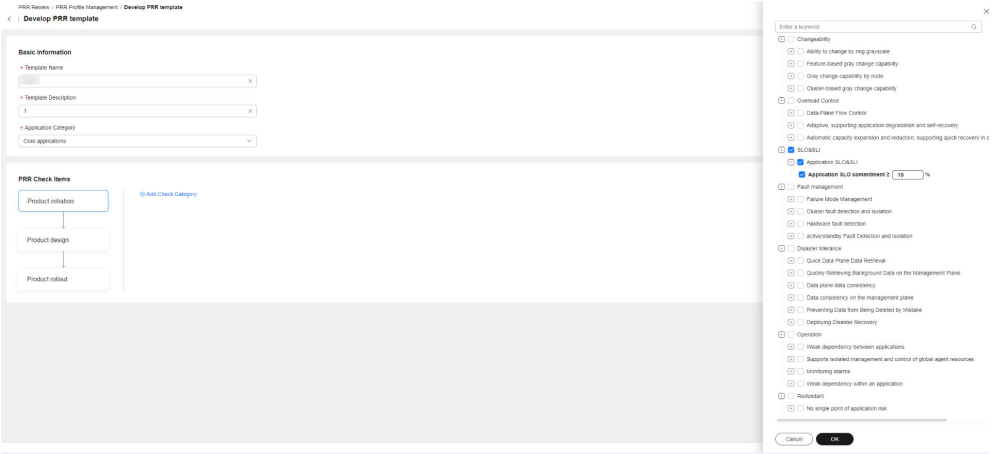
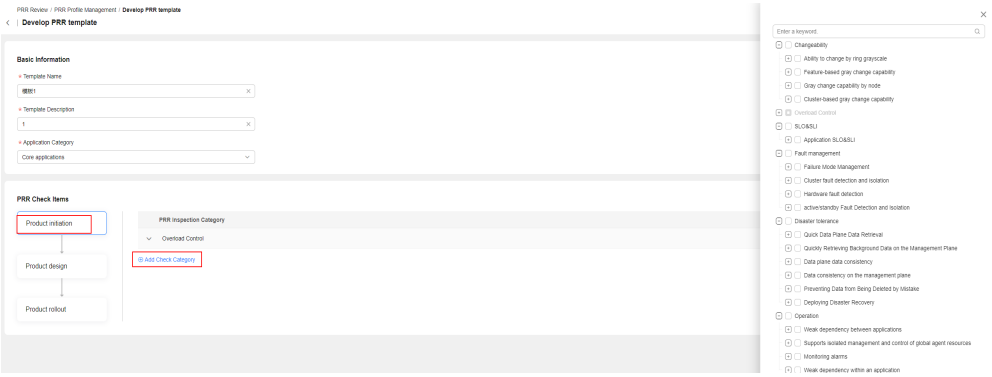


Table 8-6 Parameters for creating a PRR template

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

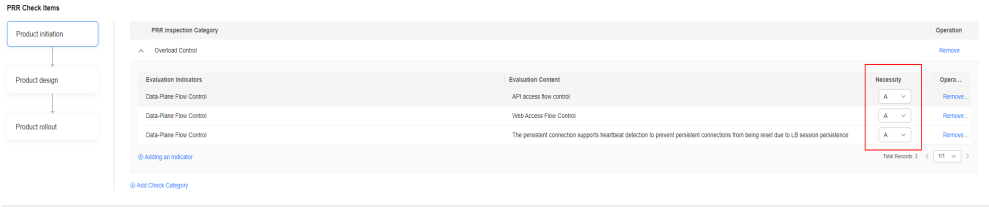
Step 4 Set check item information. Click **Product initiation**, **Product design**, or **Product rollout**, and click **Add Check Category**. The check items are displayed on the right. Select the check item as required.

Figure 8-59 Specifying check items



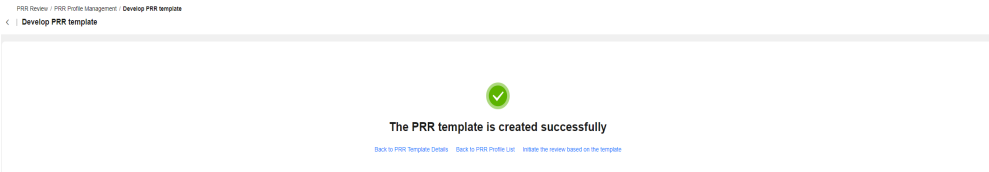
Step 5 Select the importance levels of check items. Note: If a check item whose importance level is A fails, the PRR review will fail.

Figure 8-60 Selecting the importance level of a check item



Step 6 Click **OK**.

Figure 8-61 PRR template created



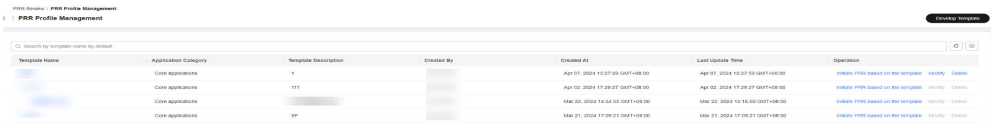
----End

Viewing PRR Template Details

Step 1 Log in to **COC**.

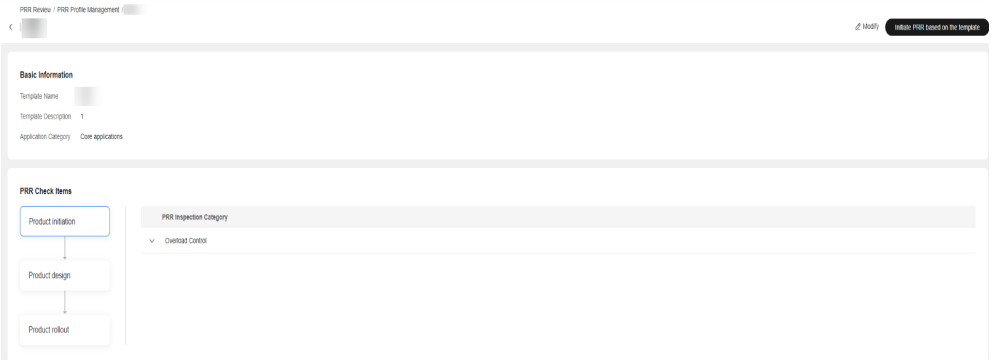
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 8-62 PRR template list



Step 3 Click the name of the target template.

Figure 8-63 PRR template details



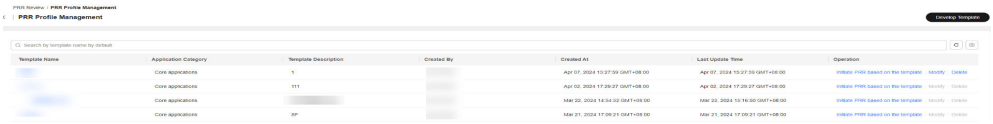
----End

Modifying a PRR Template

Step 1 Log in to **COC**.

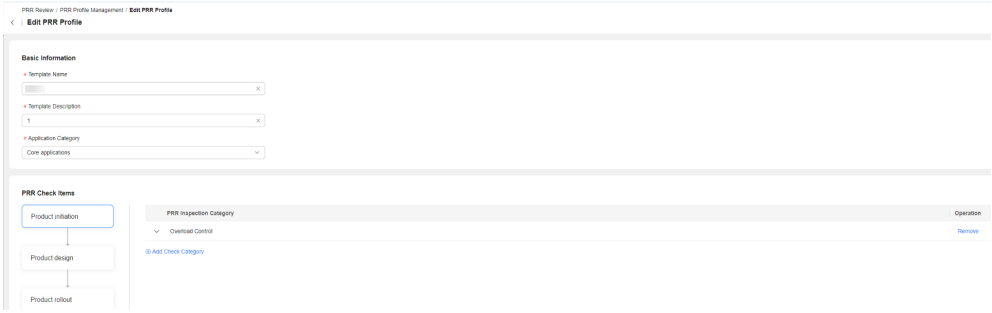
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 8-64 PRR template list



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

Figure 8-65 Modifying a PRR template



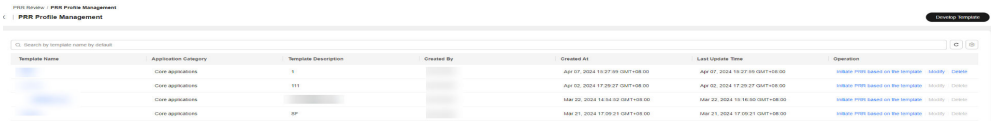
----End

Deleting a PRR Template

Step 1 Log in to **COC**.

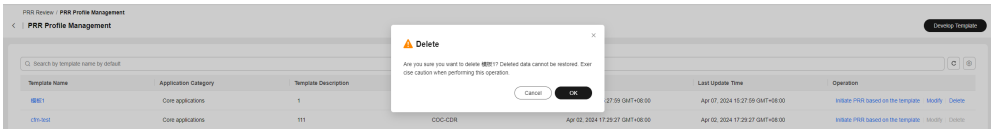
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 8-66 PRR template list



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

Figure 8-67 Deleting a PRR template



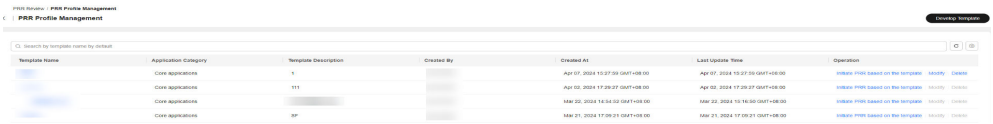
----End

Initiating PRR Based on a Template

Step 1 Log in to **COC**.

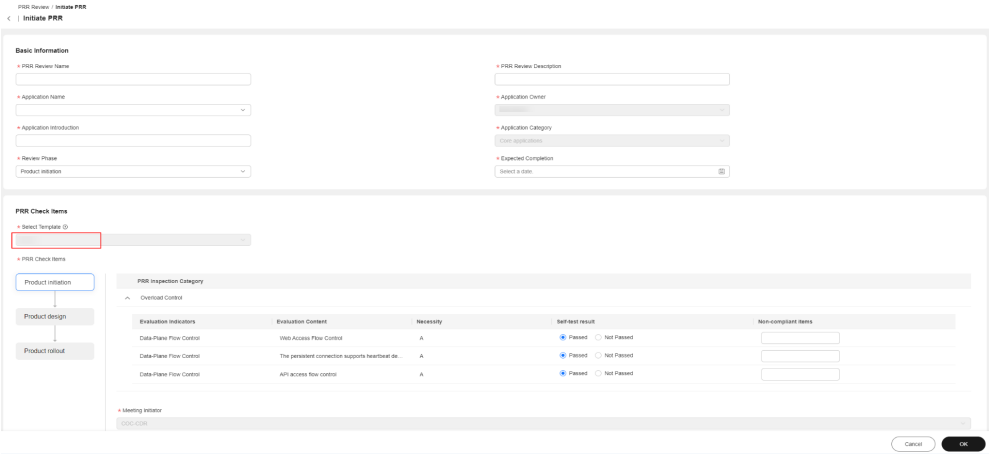
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. In the upper right corner, click **PRR Profile Management**.

Figure 8-68 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 8-69 Initiating PRR based on a template



----End

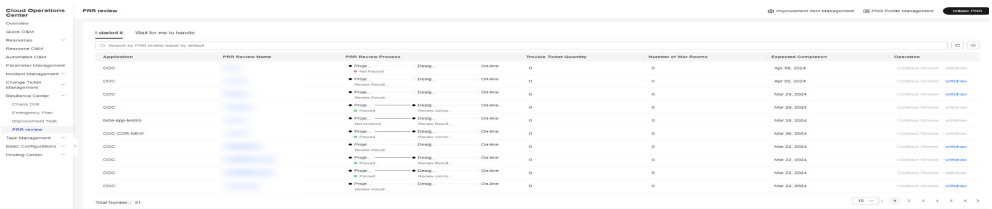
8.3.3 PRR Management

Initiating PRR

Step 1 Log in to **COC**.

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

Figure 8-70 PRR list



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

Figure 8-71 Initiating PRR- Specifying PRR basic information

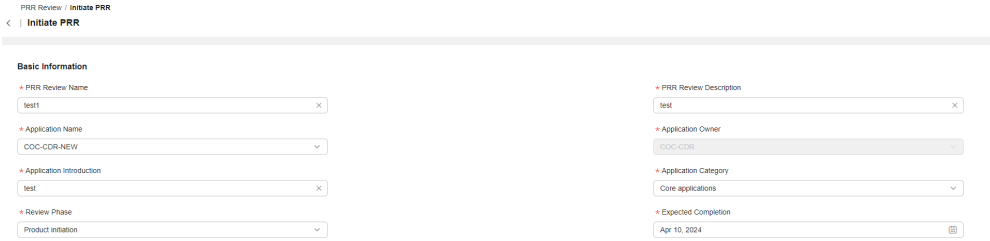


Table 8-7 Basic parameters for initiating PRR

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 8-72 Initiating PRR - Specifying PRR check items

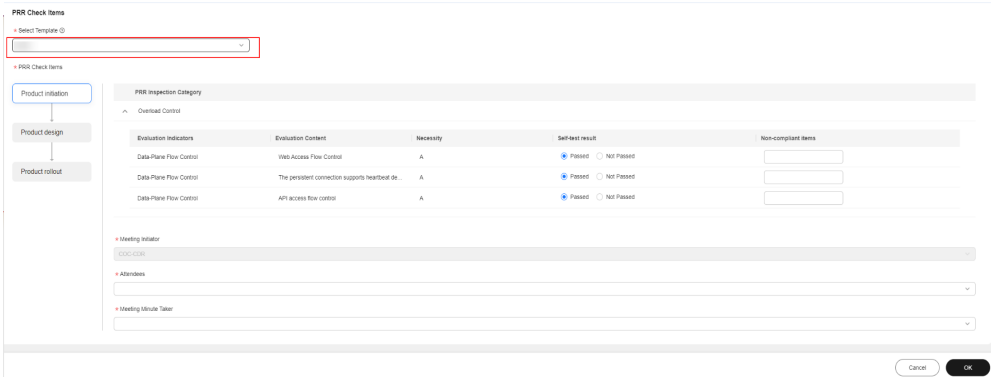
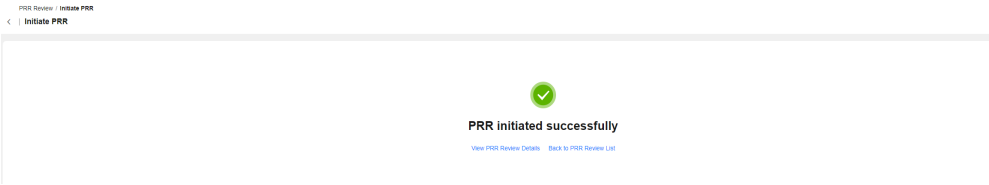


Table 8-8 Parameters of check items

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 8-73 PRR initiated



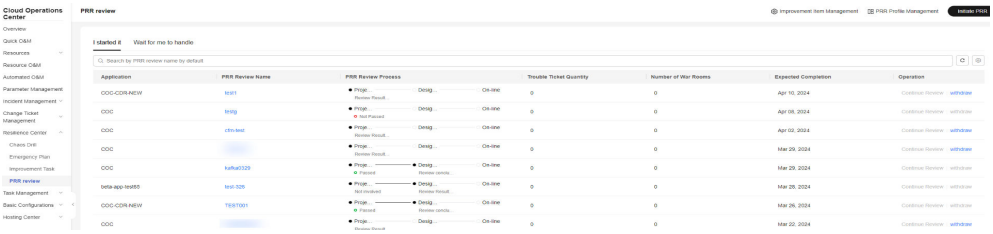
----End

Viewing PRR Details

Step 1 Log in to **COC**.

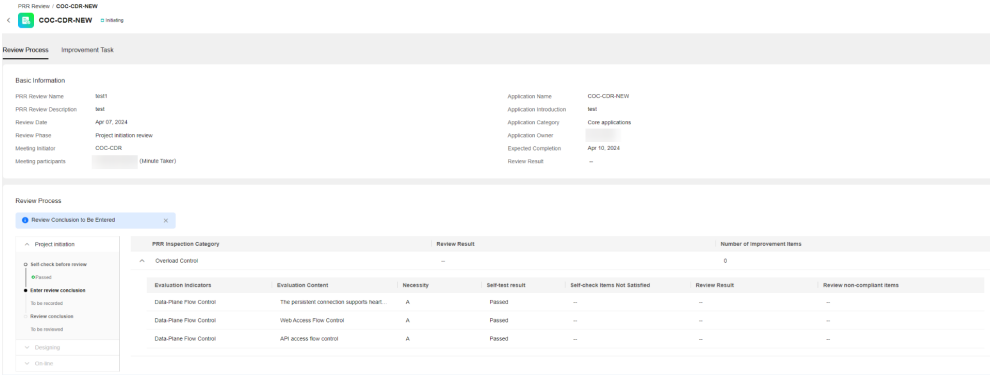
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**.

Figure 8-74 PRR list



Step 3 Click the name of the target PRR.

Figure 8-75 PRR details



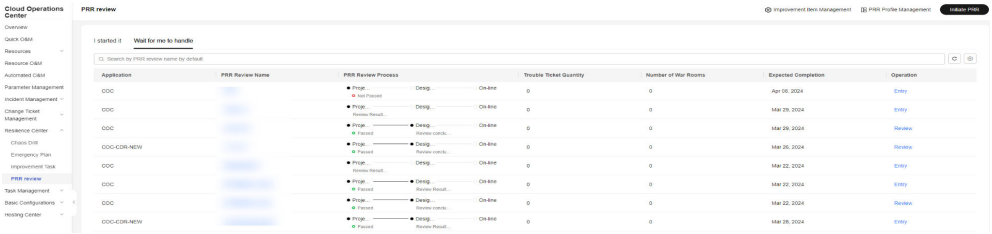
----End

Recording Review Minutes

Step 1 Log in to **COC**.

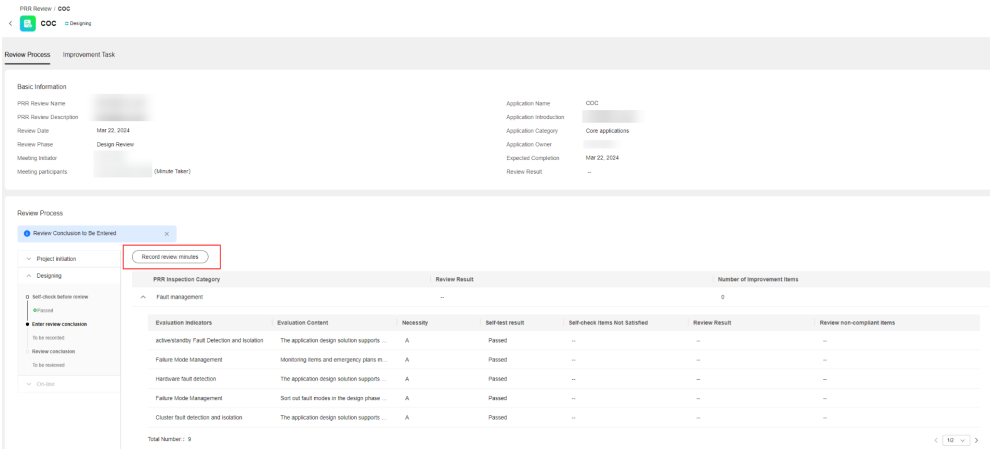
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click the **Wait for me to handle** tab.

Figure 8-76 PRR to be processed



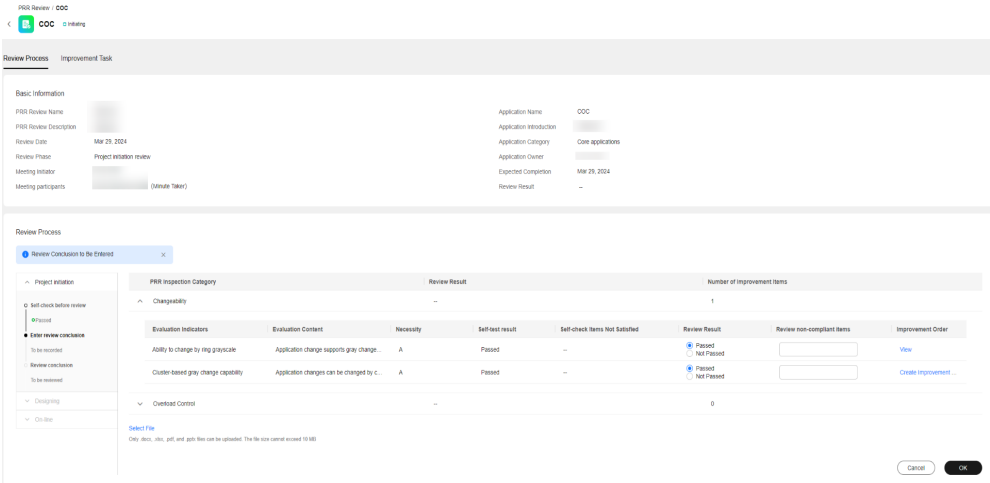
Step 3 Locate the target PRR record, and click **Entry**. On the displayed PRR details page, click **Record review minutes** to enter the review minutes.

Figure 8-77 PRR details - entering review minutes



Step 4 Enter review minutes.

Figure 8-78 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 8-79 Entering review minutes - creating an improvement ticket

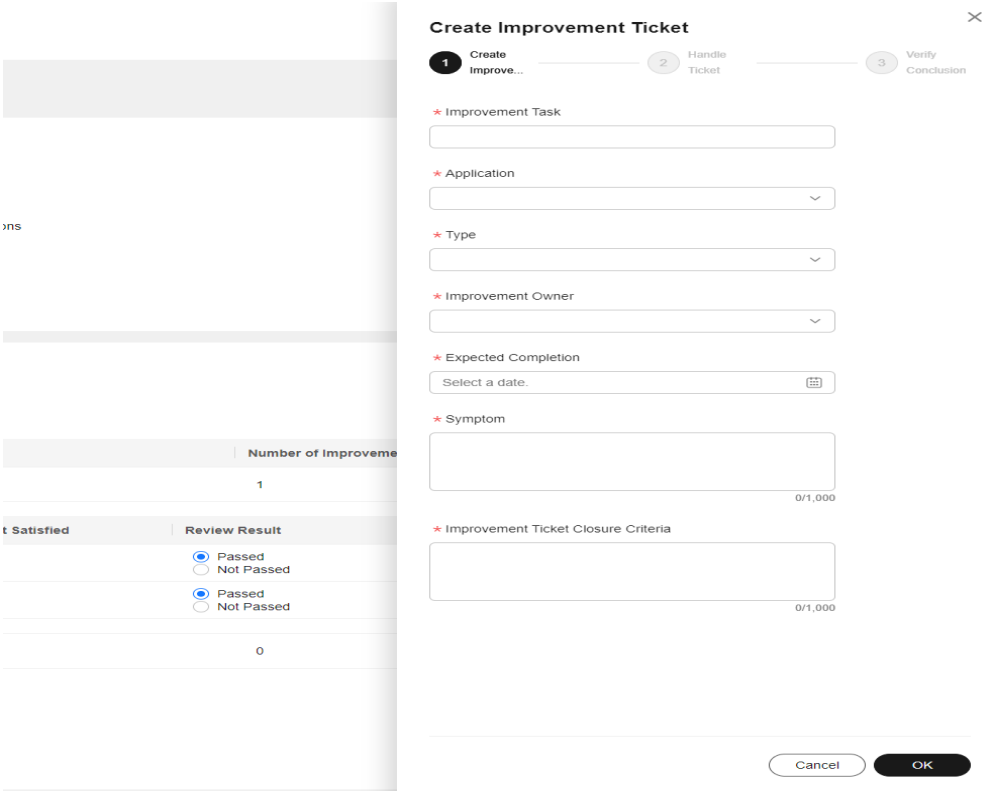


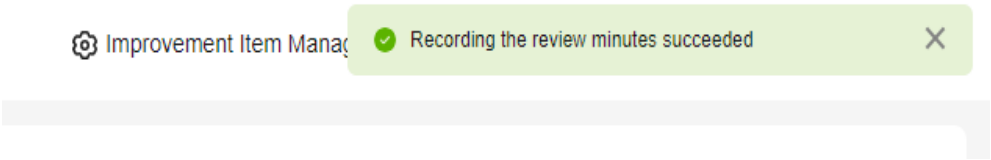
Table 8-9 Improvement ticket parameters

Parameter	Description
Improvement Task	Improvement ticket name

Parameter	Description
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 8-80 Review minutes recorded



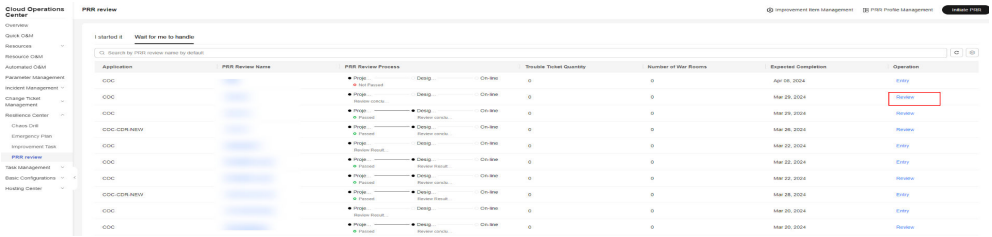
----End

Recording the Review Conclusion

Step 1 Log in to **COC**.

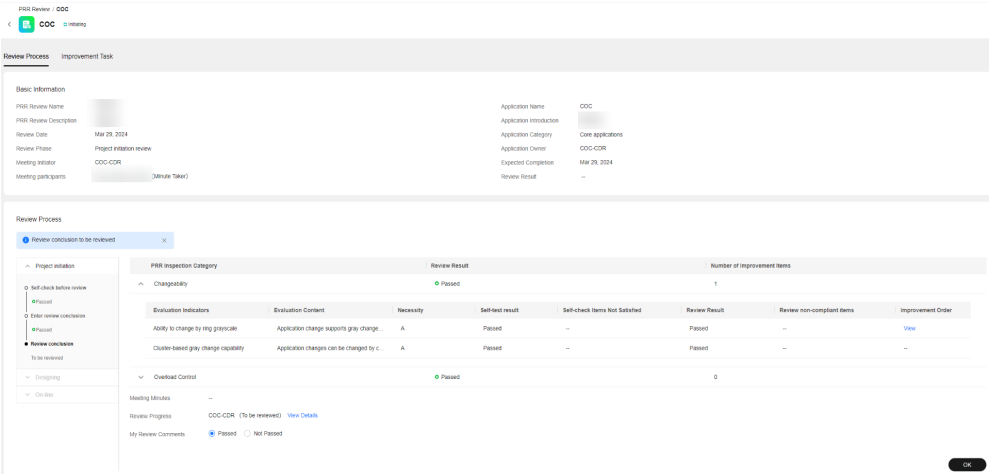
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click the **Wait for me to handle** tab.

Figure 8-81 PRR to be processed



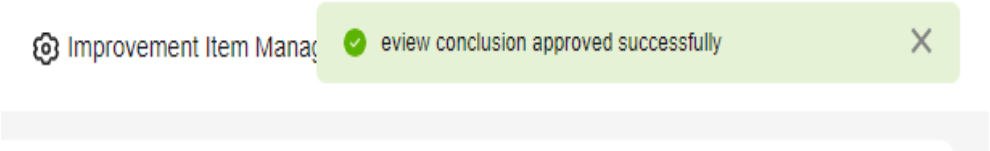
Step 3 Locate the target PRR record, and click **Review** in the **Operation** column. On the displayed page, enter the review conclusion.

Figure 8-82 Recording the review conclusion



Step 4 Click **OK**.

Figure 8-83 Review conclusion recorded



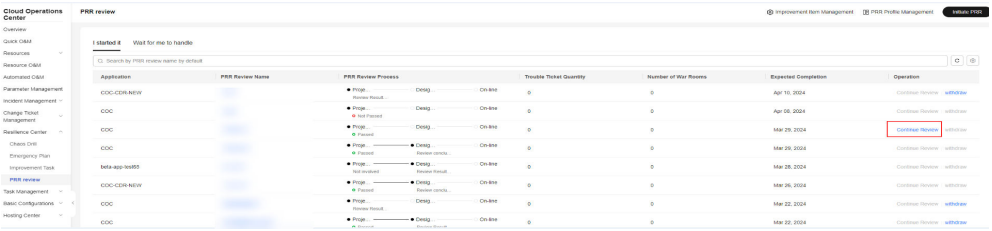
----End

Continuing to Initiate PRR

Step 1 Log in to **COC**.

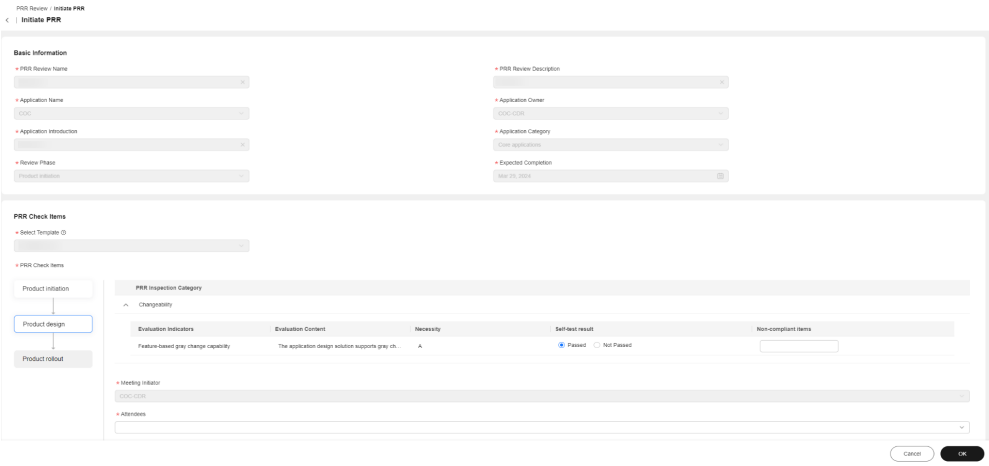
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**.

Figure 8-84 PRR list



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 8-85 Continuing to initiate PRR



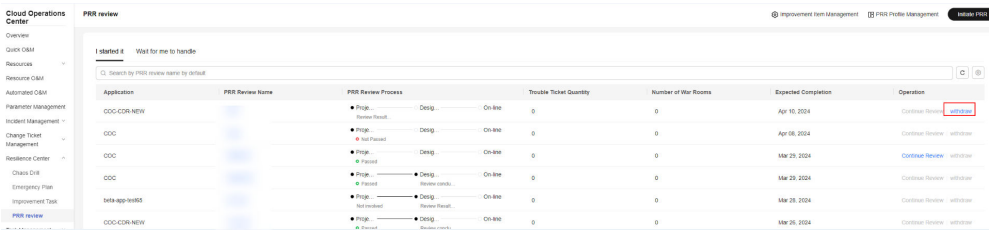
----End

Canceling the PRR

Step 1 Log in to **COC**.

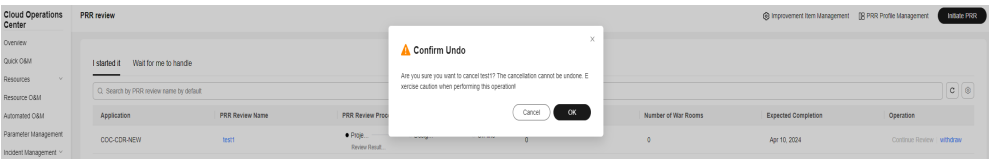
Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**.

Figure 8-86 PRR list



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

Figure 8-87 Canceling the PRR



----End

9 Task Management

9.1 Execution Records

9.1.1 Script Tickets

You can view and manage script tickets.

Prerequisites

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

Scenarios

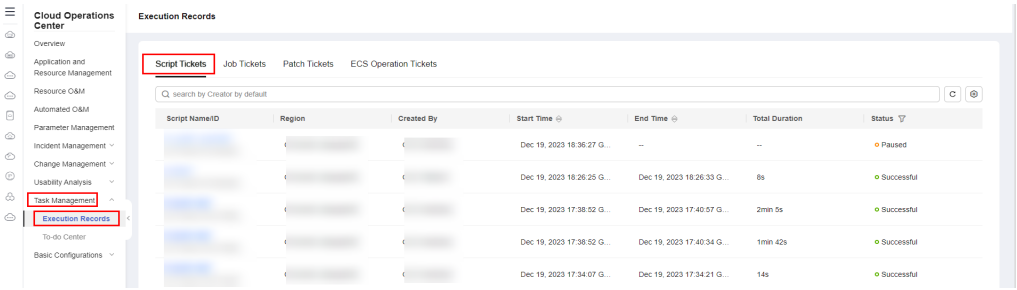
View script tickets on the **Cloud Operations Center** page.

Procedure

Step 1 Log in to **COC**.

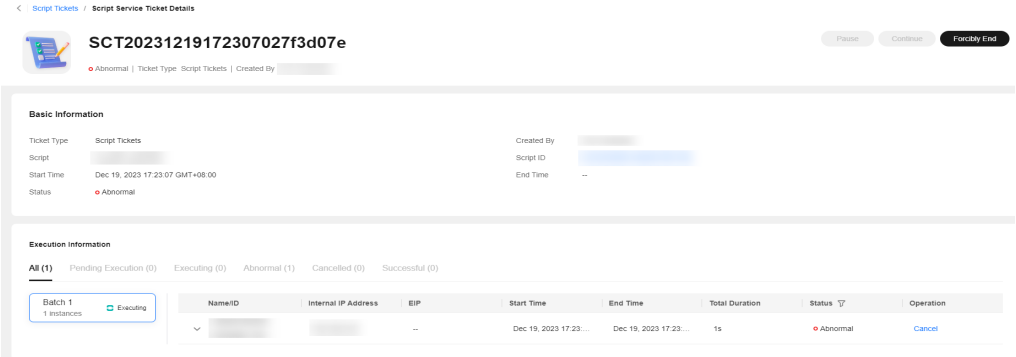
Step 2 In the navigation pane on the left, choose **Task Management** > **Execution Records** and click the **Script Tickets** tab.

Figure 9-1 Script Tickets



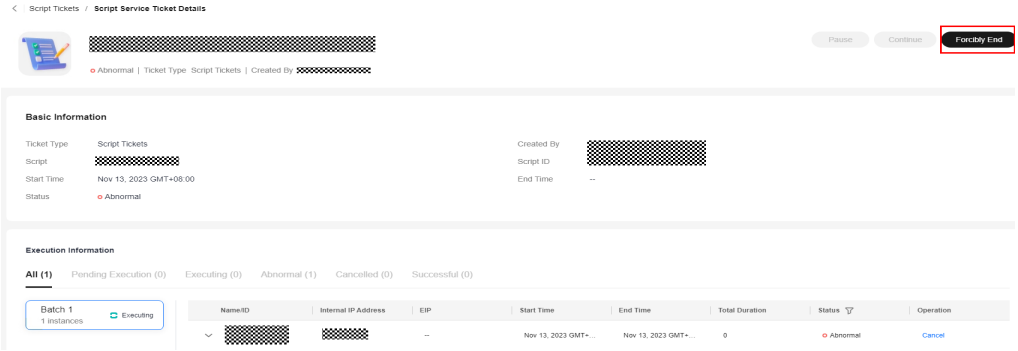
Step 3 Select a script ticket in the **Abnormal** state.

Figure 9-2 Selecting a script ticket in the **Abnormal** state



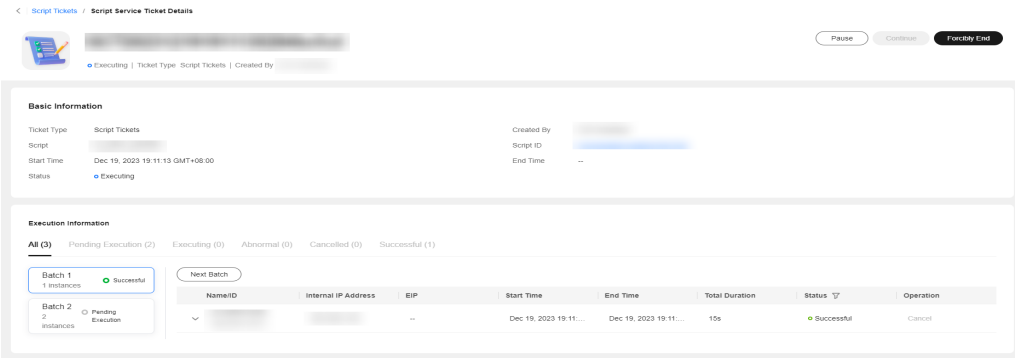
Step 4 Click **Forcibly End** to end the abnormal script ticket.

Figure 9-3 Closing an abnormal script ticket



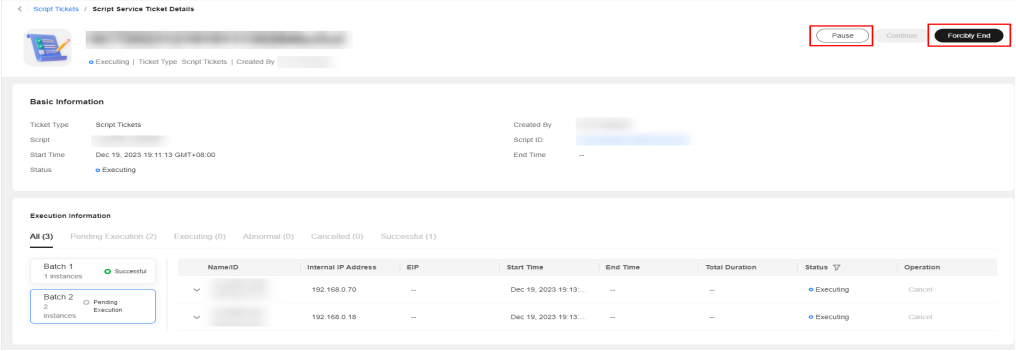
Step 5 Select a script ticket in the **Executing** state.

Figure 9-4 Selecting a script ticket in the **Executing** state



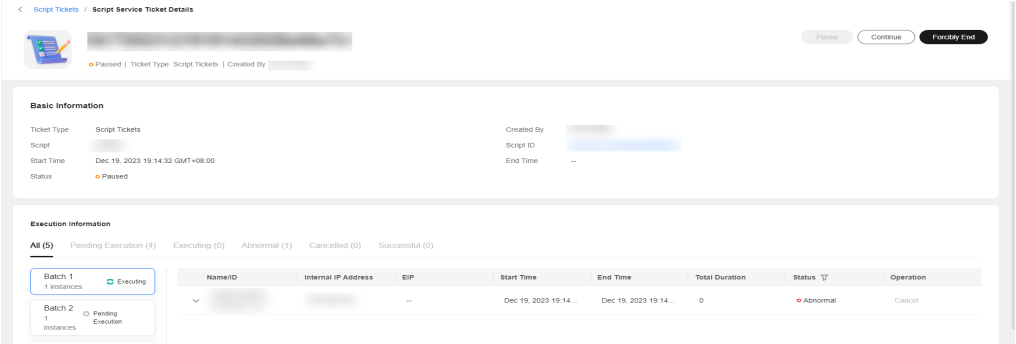
Step 6 Click **Pause** or **Forcibly End** to pause or end the script ticket.

Figure 9-5 Pausing or closing a script ticket



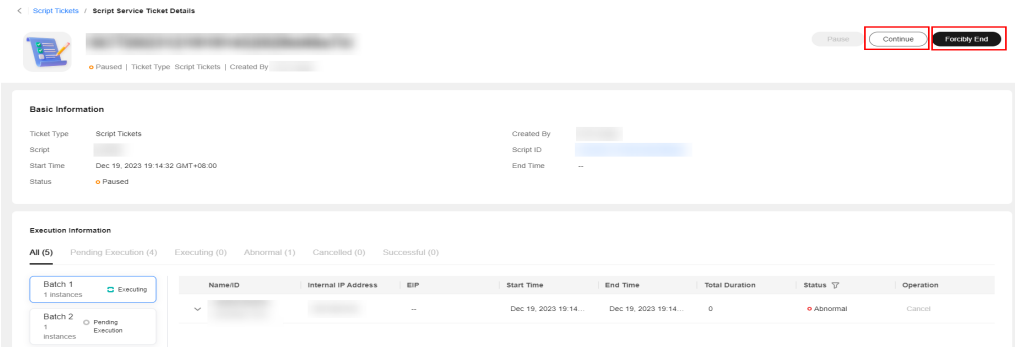
Step 7 Select a script ticket in the **Paused** state.

Figure 9-6 Selecting a script ticket in the **Paused** state



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

Figure 9-7 Continuing or pausing a paused script ticket



----End

9.1.2 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.

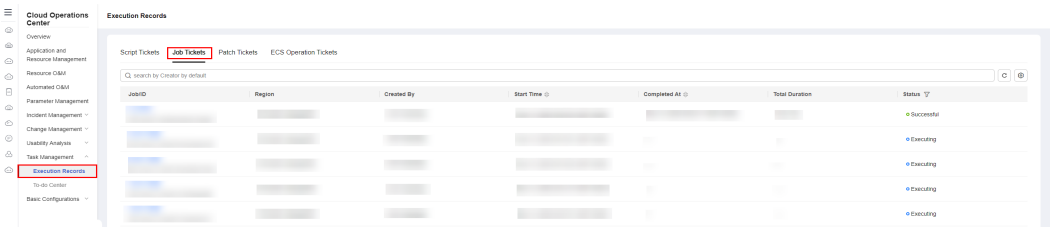
Procedure

Step 1 Log in to **COC**.

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

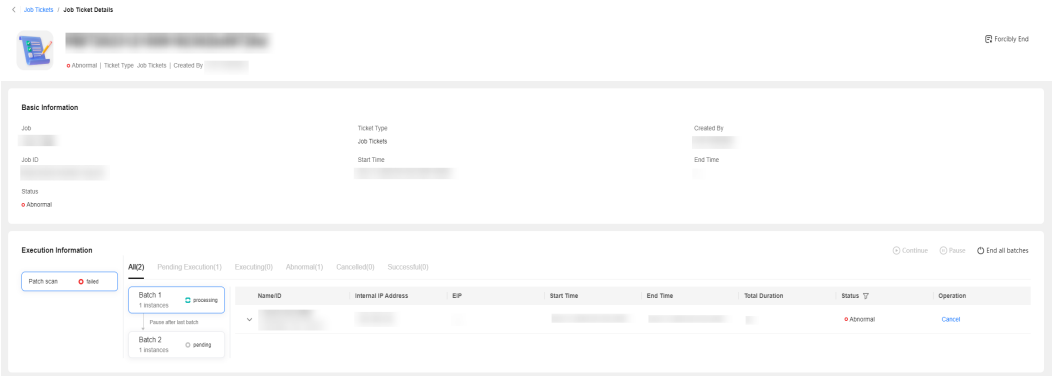
- Cloning a ticket: Click **Clone** of a job ticket to go to the **Execute Job** page. You can execute the job again by following the instructions provided in **Executing a Custom Job**.
- Editing a tag: Modify job tags by following the instructions provided in **Managing Tags**.

Figure 9-8 Job tickets



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

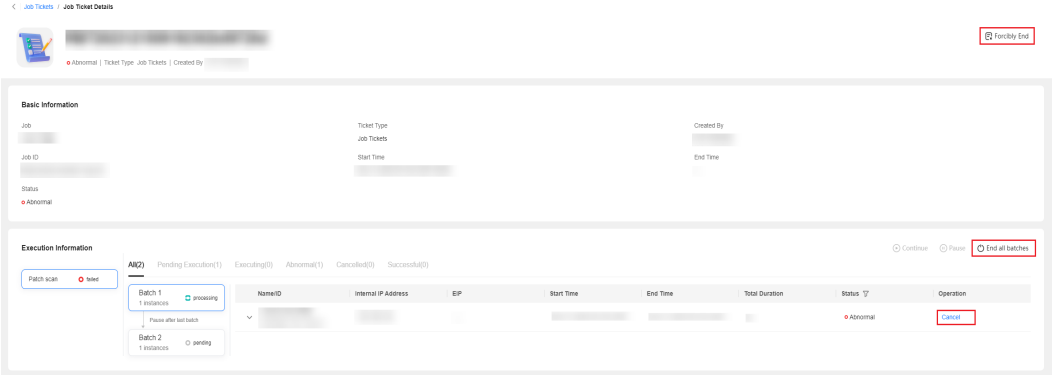
Figure 9-9 Job ticket details



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

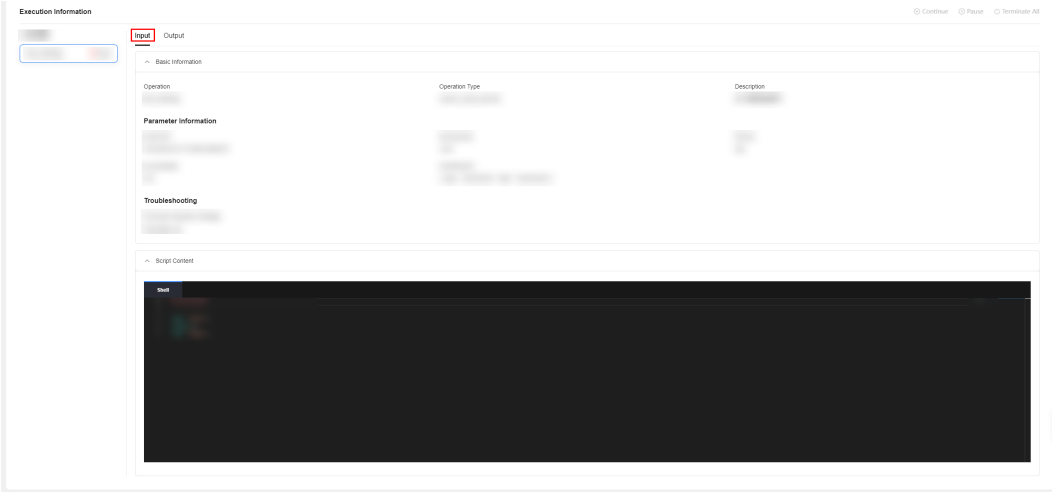
- **Forcibly End**: Forcibly end all tasks of the current job.
- **Terminate All**: End all batches in the current step.
- **Cancel**: Stop the execution jobs of a single instance.
- Editing a tag: Modify job tags by following the instructions provided in **Managing Tags**.

Figure 9-10 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 9-11 Viewing the job details



----End

9.1.3 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.

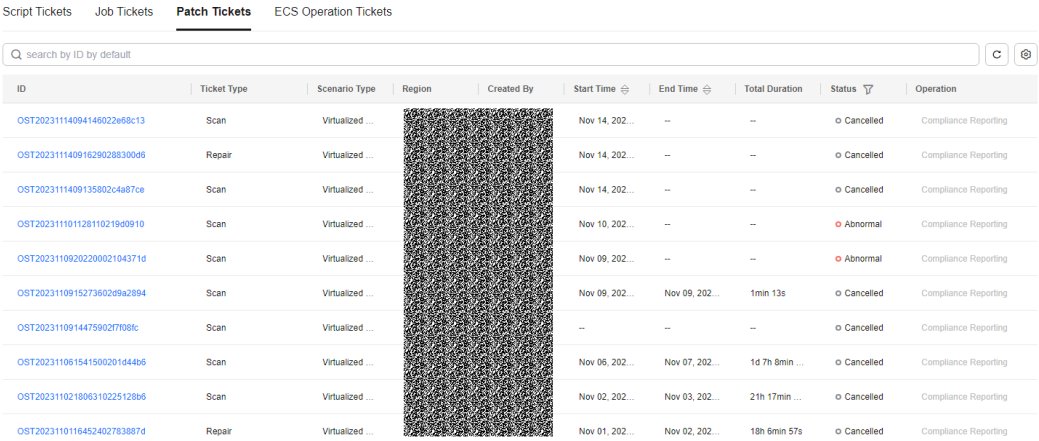
Procedure

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 9-12 Patch ticket list



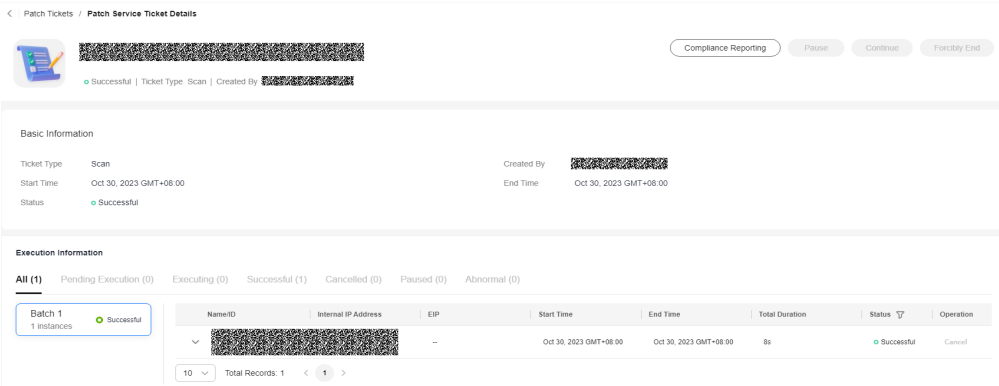
NOTE

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 9-13 Service ticket details



----End

9.1.4 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.

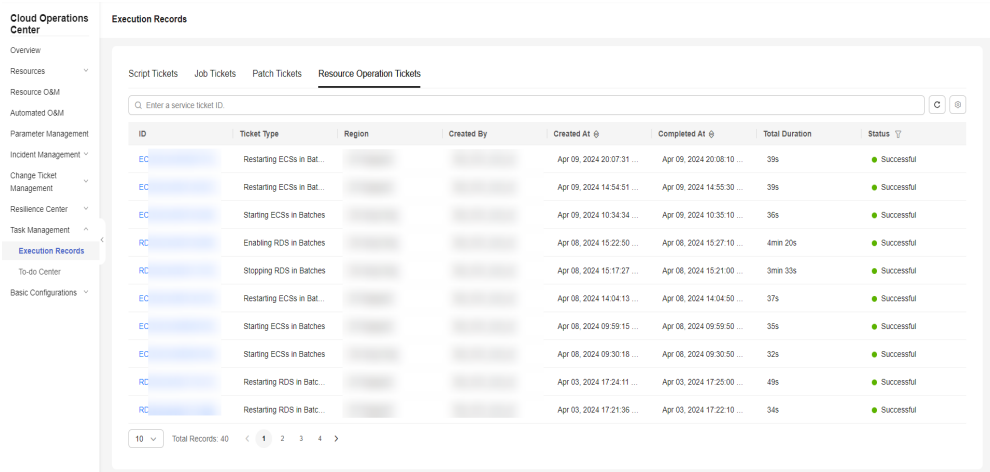
Procedure

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 9-14 Resource operation Tickets



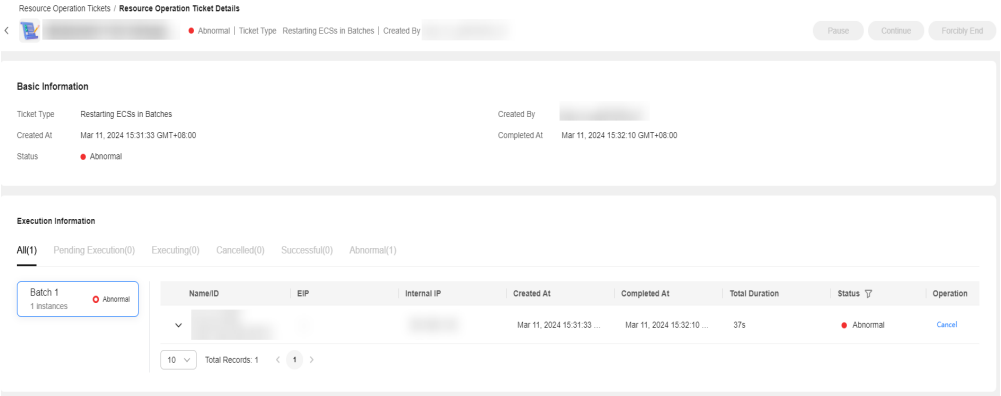
NOTE

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 9-15 Details about a resource operation ticket



----End

9.2 To-do Center

Overview

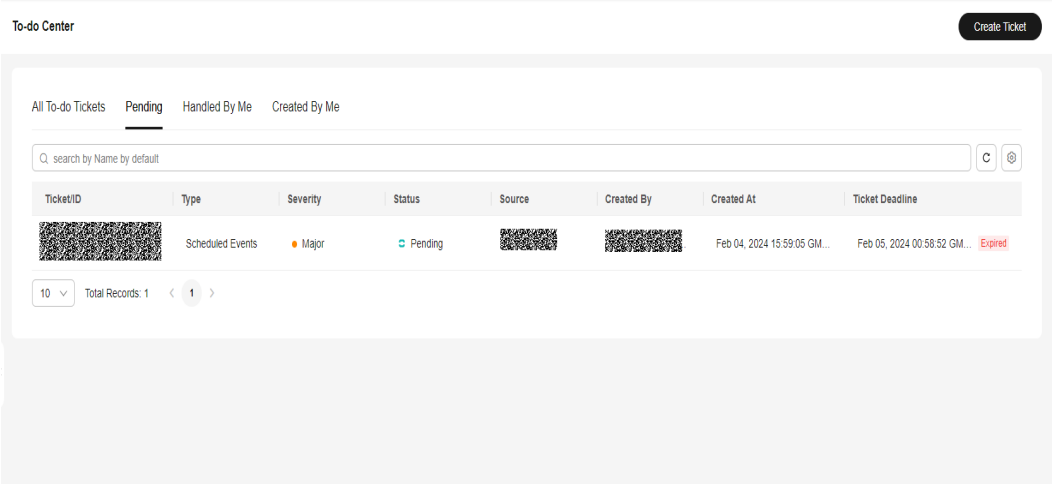
Main function of To-do Center: You can use a HUAWEI ID (primary SRE of the tenant) to create tasks for IAM users (sub-SREs of the tenant). For example, a company can create IAM accounts for different departments.

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 9-16 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 9-1**.

Figure 9-17 Creating a to-do ticket

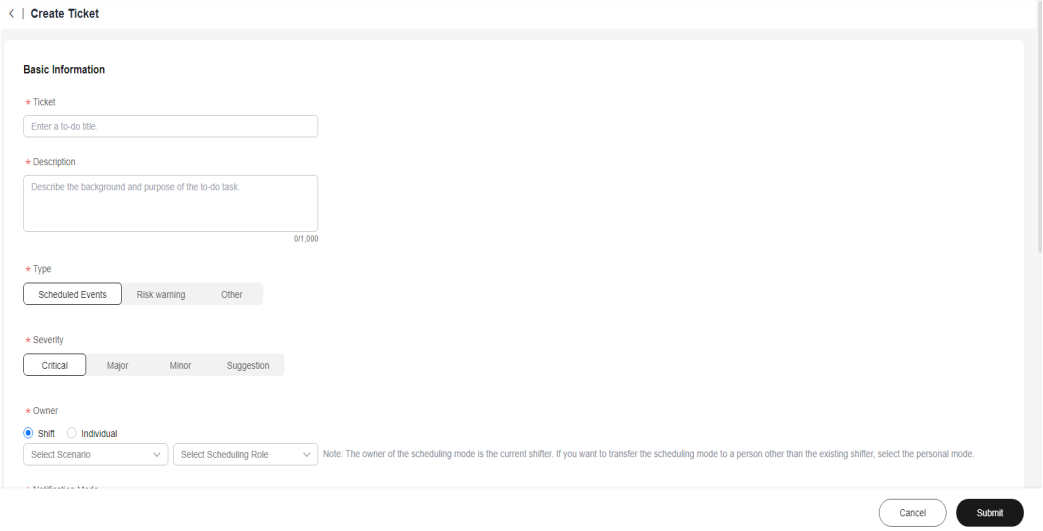


Table 9-1 Parameters

Parameter	Description
Ticket	Mandatory. ● 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	Mandatory. The description can contain a maximum of 1,000 characters, including letters, numbers, and special characters.
Type	Mandatory. To-do ticket type. The options are as follows: ● **Scheduled incidents** ● **Risk warning** ● **Other**

Parameter	Description
Severity	Mandatory. Severity of a to-do ticket. The options are as follows: ● **Critical** ● **Major** ● **Minor** ● **Suggestion**
Owner	Mandatory. The owner of a to-do ticket can be: ● **Shift** ● **Individual**
Notification Mode	Mandatory. Notification mode. The options are as follows: ● **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.

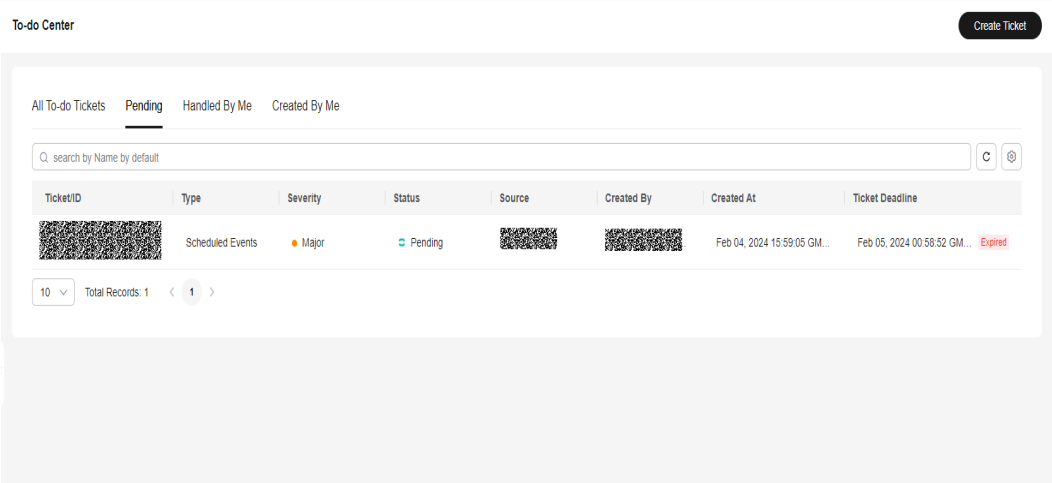
----End

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.

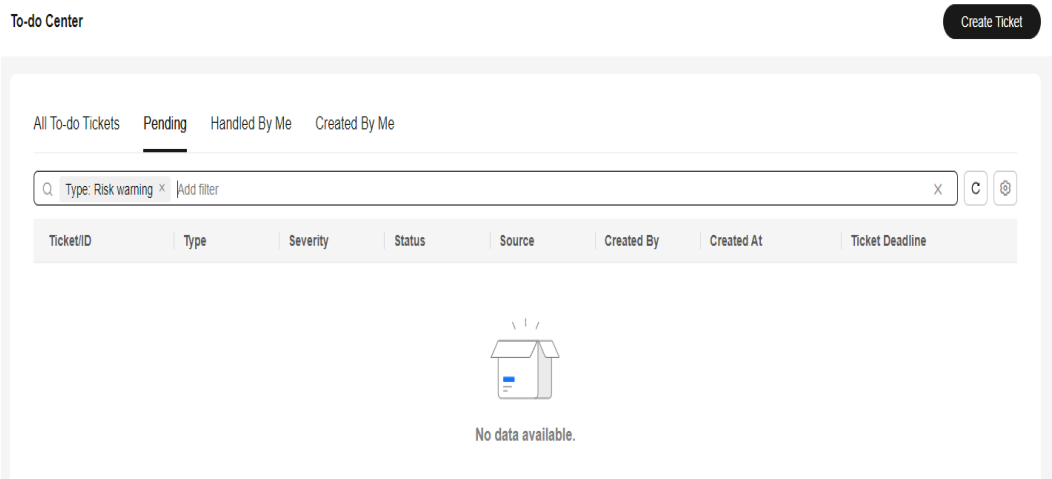
Figure 9-18 Viewing the to-do center list



Step 3 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data.

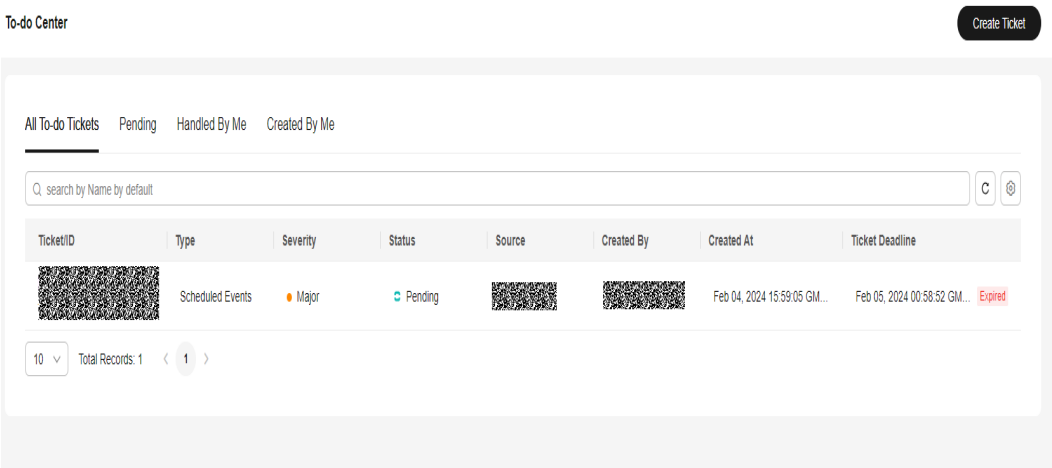
Step 4 You can click the icons next to the search box to refresh the list data and set the fields to be displayed in the list.

Figure 9-19 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 9-20 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

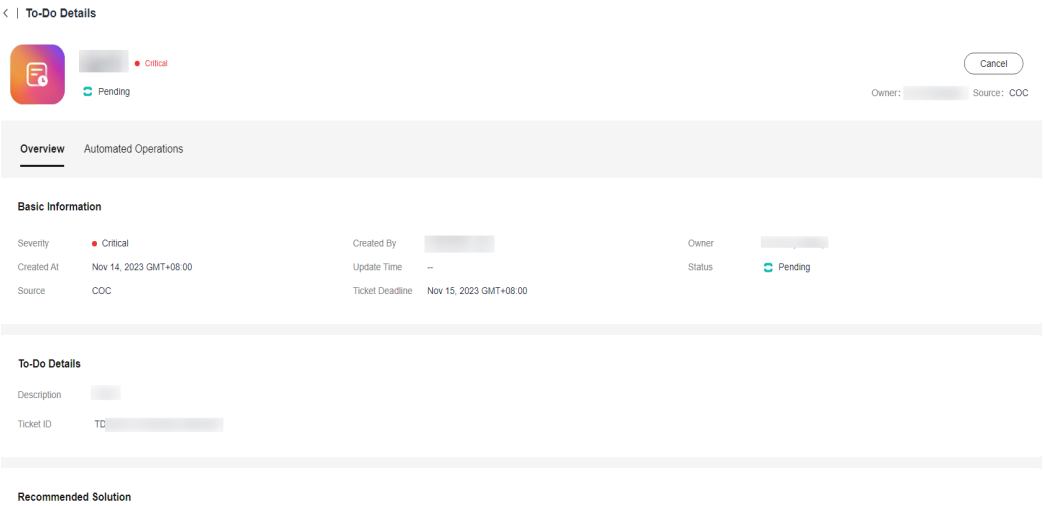
Viewing Pending Tickets

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.

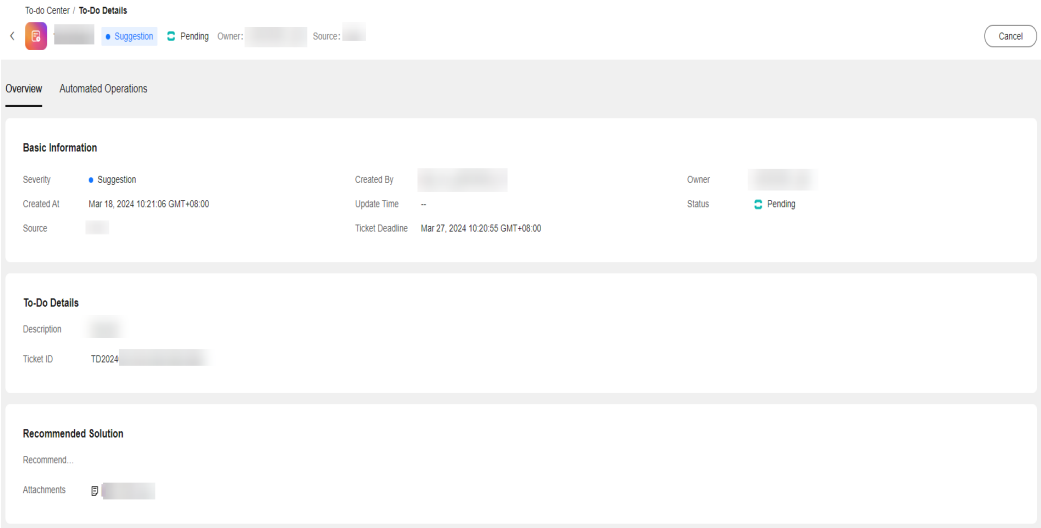
Step 3 Click a to-do ticket name in the list. The to-do ticket details are displayed.

Figure 9-21 To-do ticket details



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

Figure 9-22 Downloading an attachment



NOTE

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

----End

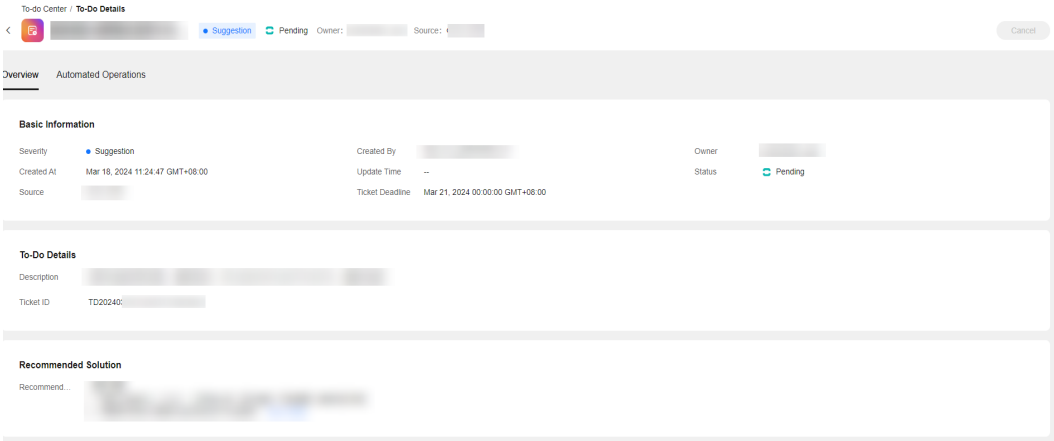
Handling To-do Tickets

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 9-23 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

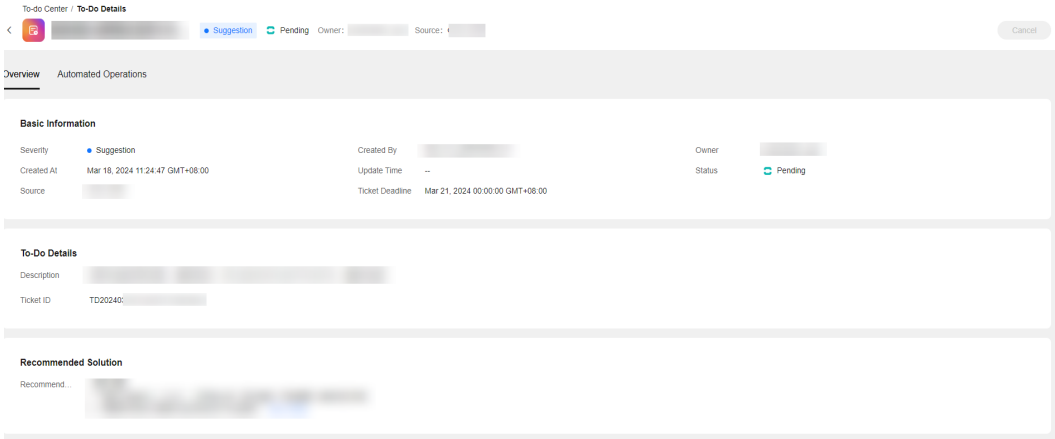
Step 1 Log in to **COC**.

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 9-24 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

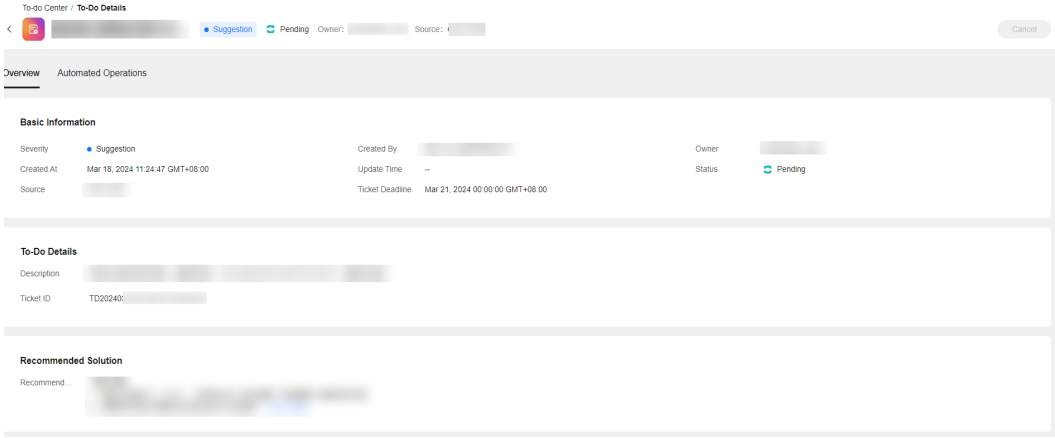
Closing a To-do Ticket

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 9-25 Closing a to-do ticket



NOTE

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

----End

10 Basic Configurations

10.1 O&M Engineer Management

10.1.1 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.

10.1.2 O&M Engineer Management Usage

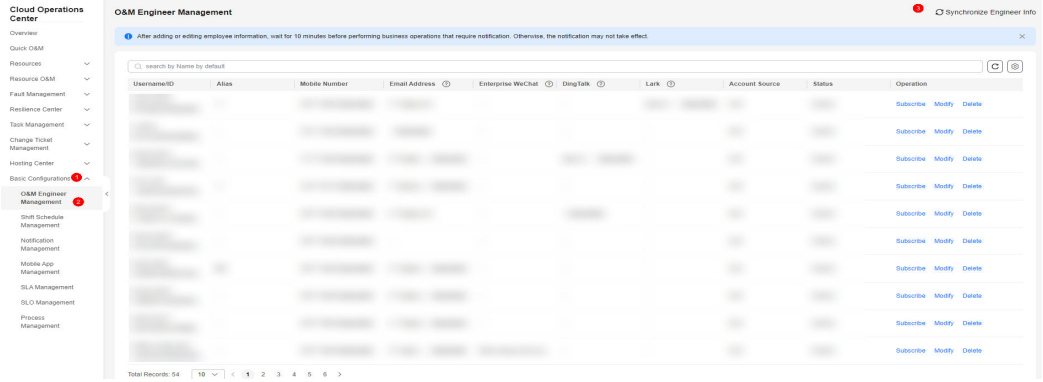
This section describes how to use the **O&M Engineer Management** module.

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 **Synchronize Engineer Info** in the upper right corner.

Figure 10-1 Synchronizing information about engineers



----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**. Locate the row that contains the O&M engineer you want to edit and click **Edit** in the **Operation** column.

Figure 10-2 Modifying personal information

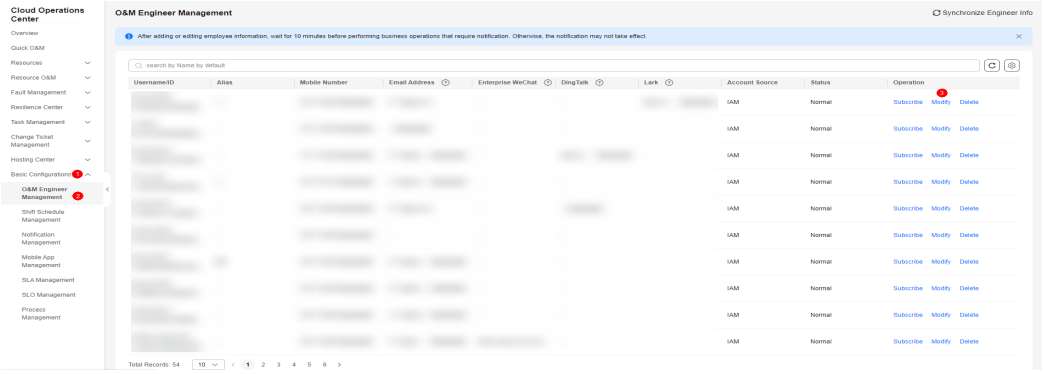
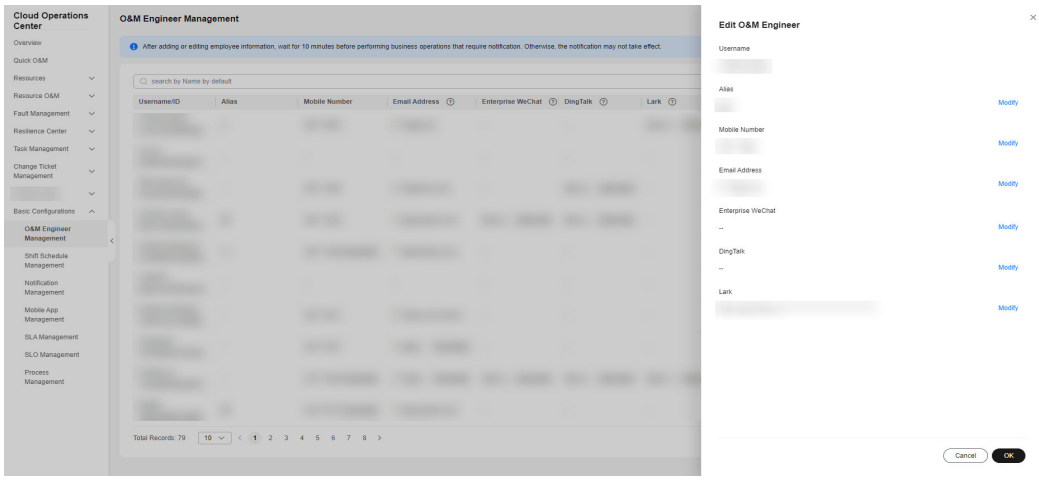


Figure 10-3 Modifying details



- **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 WeCom group chatbot.
- **DingTalk**: The webhook address of the DingTalk group chatbot.
- **Lark**: The webhook address of the robot customized for the Lark group chat.

NOTE

The usage of the communication methods in the personnel information:

After the communication methods are 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.
- **Lark**: After you fill in and save the configuration, you can use Lark without creating a subscription.

Notes:

- The current version supports the following notification methods: SMS messages, WeCom, voice calls, DingTalk, Lark, and emails. WeCom, DingTalk, Lark, 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 **O&M Engineer Management** page.
- After the DingTalk, WeCom, and Lark notification method configurations are 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.

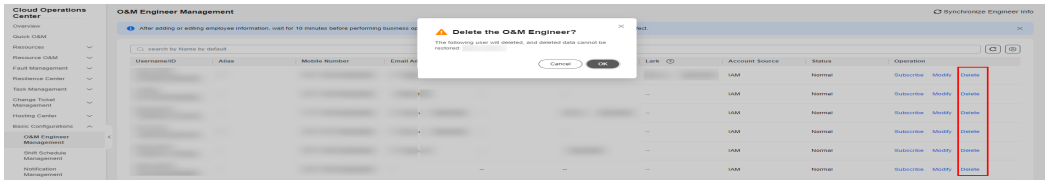
----End

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**. Locate the row that contains the O&M engineer you want to edit and click **Delete** in the **Operation** column.

Figure 10-4 Deleting a member



----End

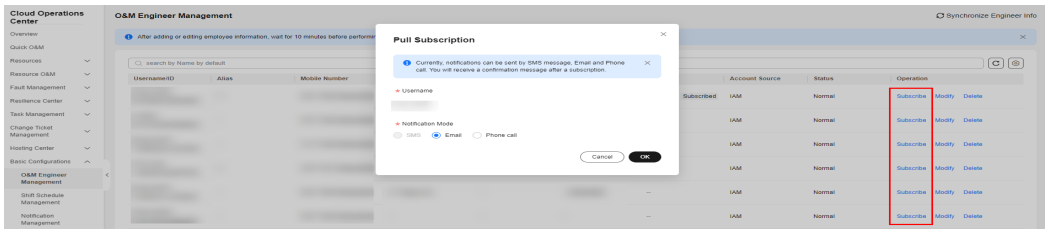
Subscribing to a User

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**. Locate the row that contains the O&M engineer you want to edit and click **Subscribe** in the **Operation** column.

Figure 10-5 Subscription



NOTE

The usage of subscription in personnel management is as follows:

- After you click **Subscribe**, you can select a notification method in the displayed dialog box.
- If the subscription of a notification method has been confirmed, its option will be unavailable in the **Pull Subscription** dialog box.
- If a user has confirmed the subscription of all notification methods, the **Subscribe** button in the **Operation** column on the page is unavailable.

----End

10.2 Shift Schedule Management

10.2.1 Overview

Schedule management allows you to centrally manage O&M engineers and customize shifts. You can manage **scheduling scenarios** on the shift schedule management page and add personnel on the **O&M Personnel Management** page to shift schedules.

- When you need to configure or obtain O&M engineers in a schedule, go to the **Shift Schedule Management** page to configure or query a shift schedule.
- Created shift schedules can be directly used to configure 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

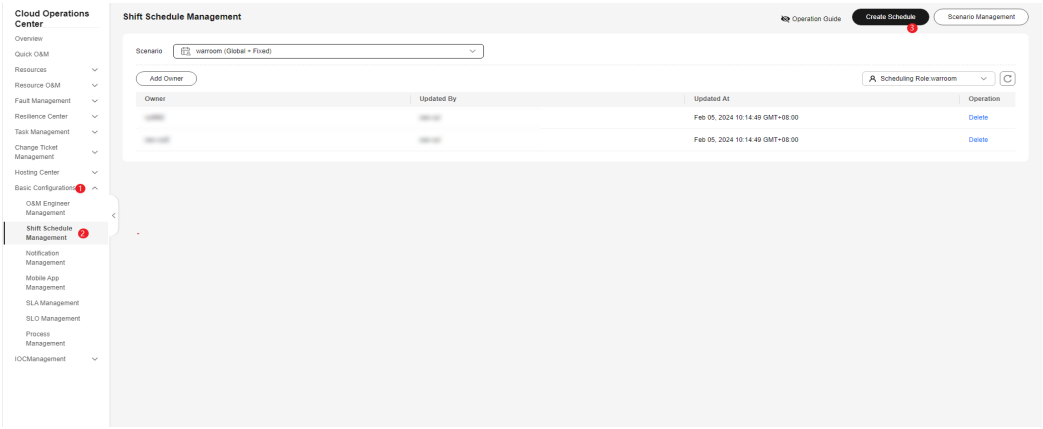
A scheduling scenario role is the minimum unit for setting a schedule. Multiple roles can be created in a scheduling scenario, and each role can be attached to multiple O&M engineers.

10.2.1.1 Creating a Schedule

Step 1 Log in to **COC**.

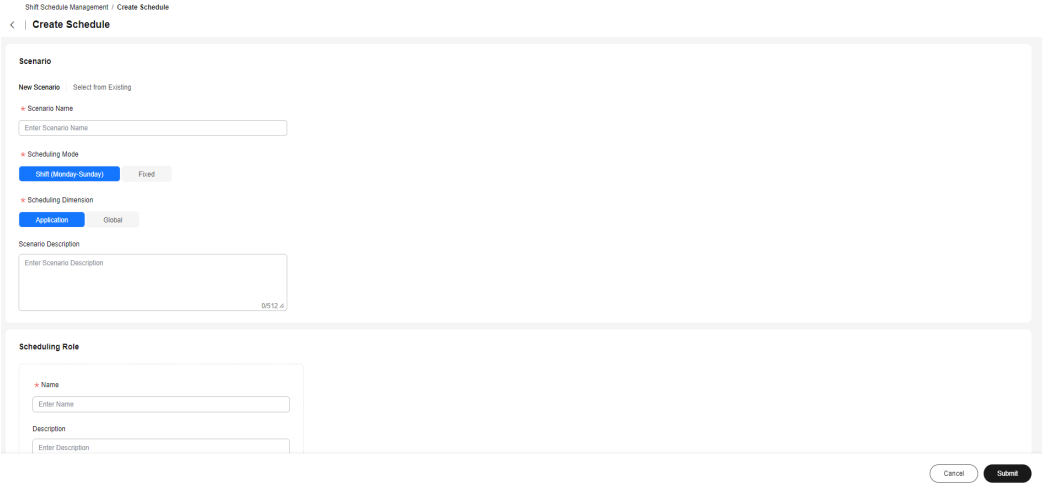
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Shift Schedule Management**. On the displayed page, click **Schedule**.

Figure 10-6 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 are scheduling scenarios and scheduling roles, you can select an existing scenario on the page for creating a schedule and view the roles in the scenario.

Figure 10-7 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

10.2.1.2 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**

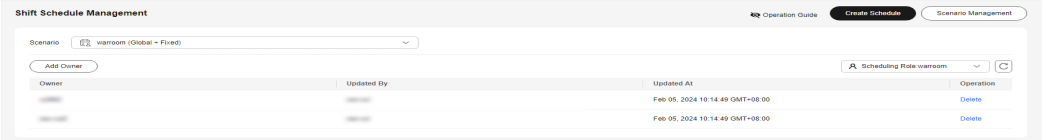
Global Schedule of Fixed Shifts

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

Step 1 Log in to **COC**.

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 10-8 Adding the owner of a **Global + Fixed** scenario



----End

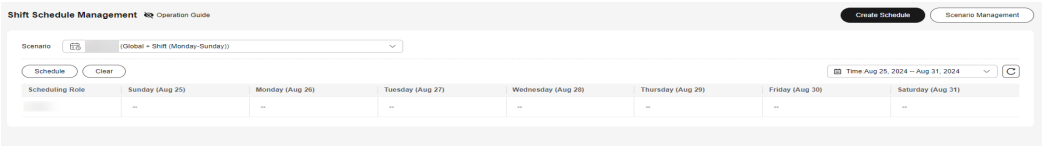
Global Schedule of Rotating Shifts

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

Step 1 Log in to **COC**.

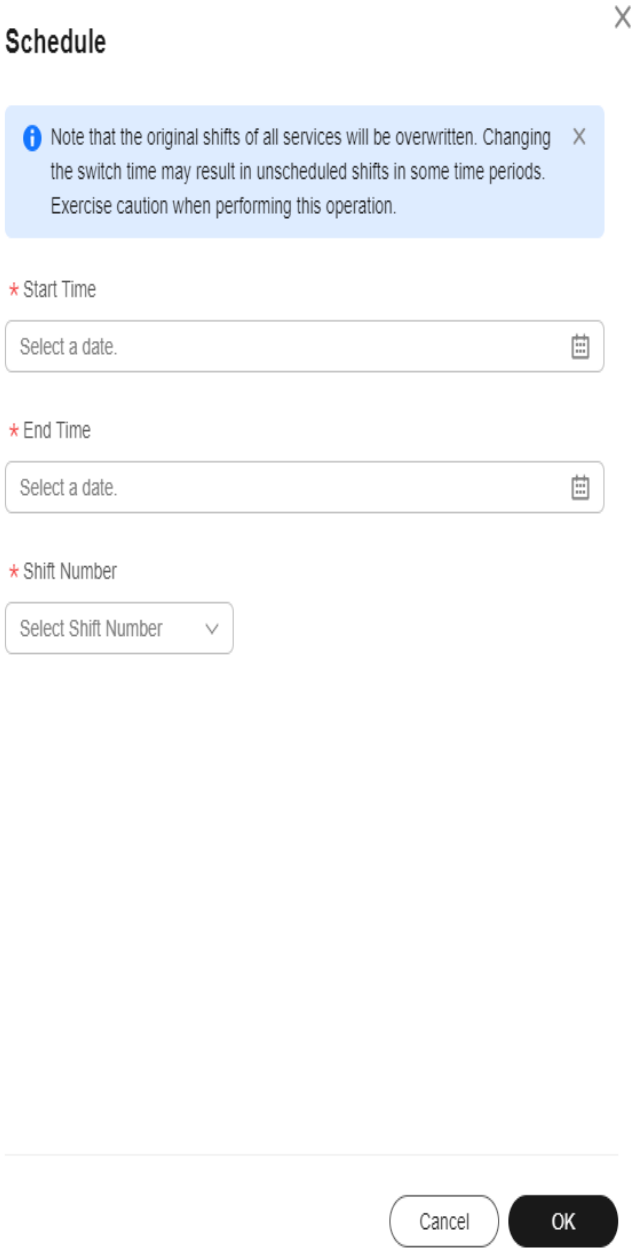
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Shift Schedule Management**. On the displayed page, select a created schedule scenario (**Global + Shift (Monday–Sunday)** is displayed next to the scenario name), and click **Schedule**.

Figure 10-9 Adding a schedule



Step 3 Enter the information about the O&M engineers to be added and click **OK**.

Figure 10-10 Adding O&M engineers



- **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

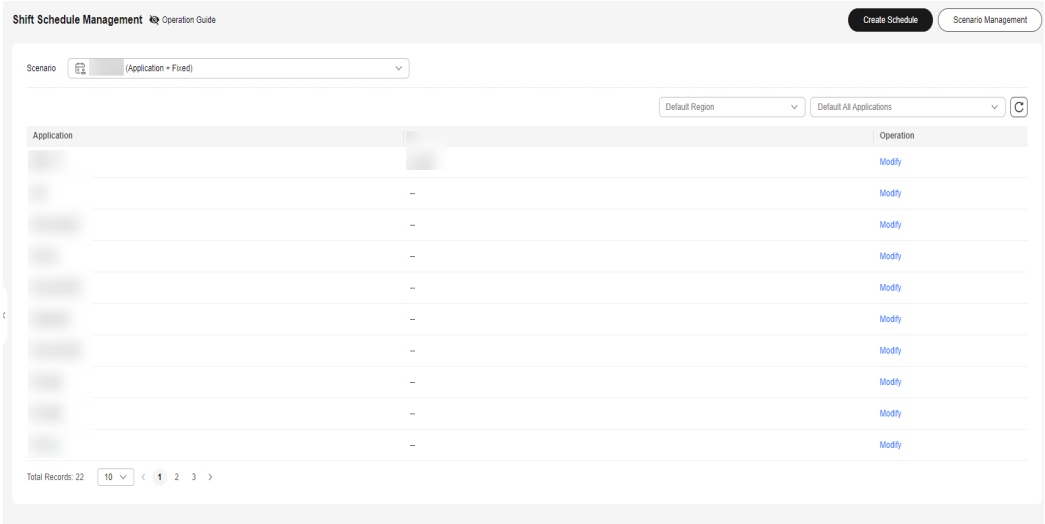
Application scenario: These schedules are applied to specific applications. O&M engineers are fixed in a day.

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

Step 1 Log in to **COC**.

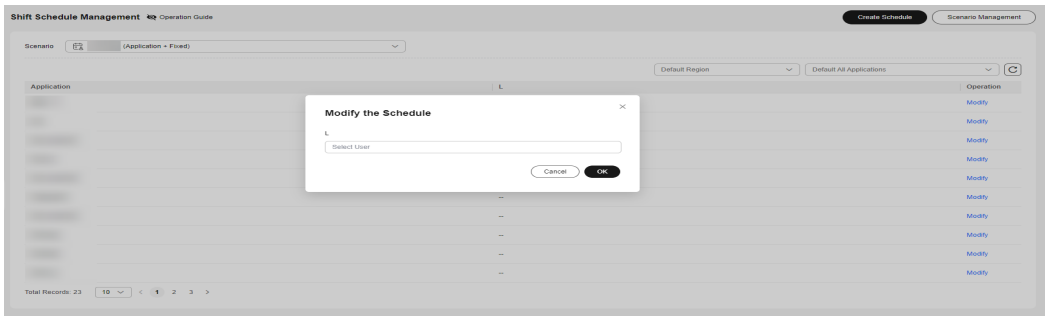
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Shift Schedule Management**. On the displayed page, select a created scenario (**Application + Fixed** is displayed next to the scenario name), region, and application.

Figure 10-11 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 10-12 Adding an engineer



----End

Application-specific Schedule of Rotating Shifts

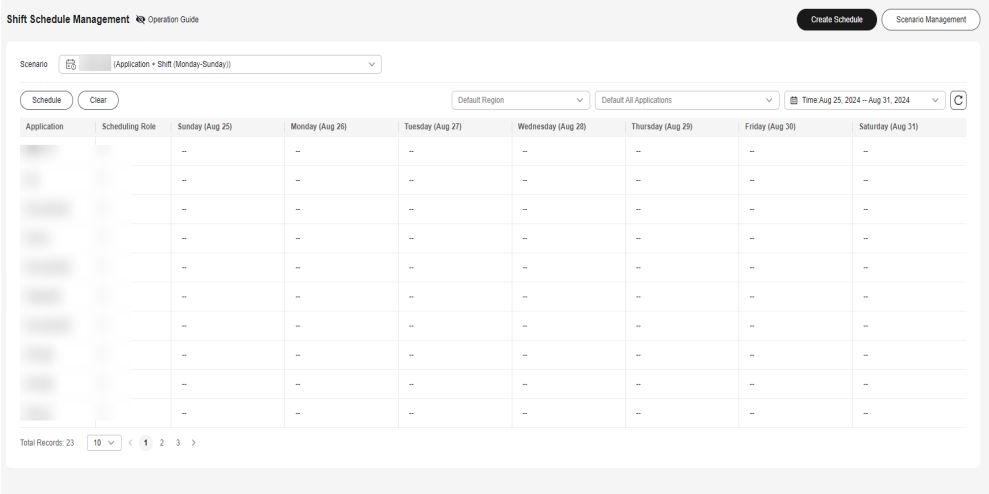
Application scenario: These schedules are applied to specific applications.

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

Step 1 Log in to **COC**.

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 10-13 Applications where the schedules are applied

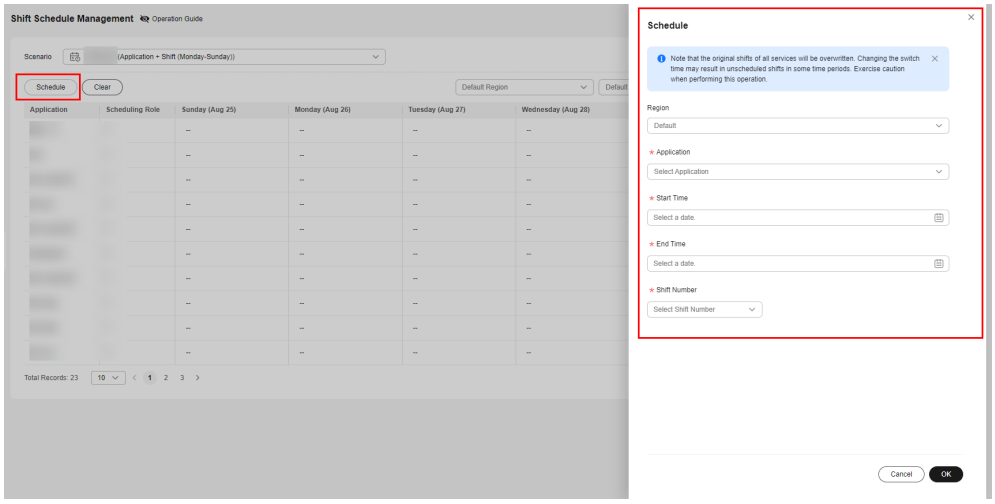


NOTE

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 10-14 Adding engineers to non-fixed shifts



- **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

10.2.1.3 Managing O&M Engineers

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

Scenarios

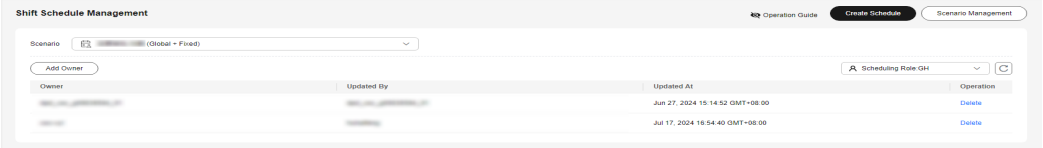
When the engineers in a schedule change, you can modify or delete the information about the changes. The method of changing the engineers varies according to the scenario.

Global Schedule of Fixed Shifts

Step 1 Log in to **COC**.

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

Figure 10-15 Deleting an engineer



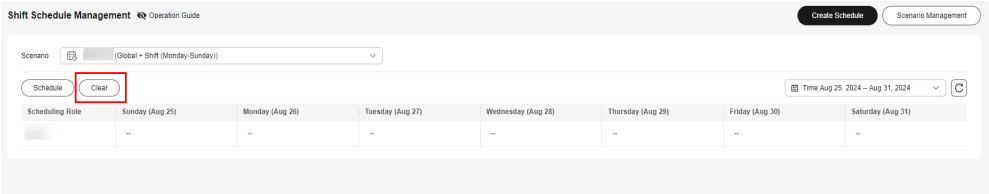
----End

Global Schedule of Rotating Shifts

Step 1 Log in to **COC**.

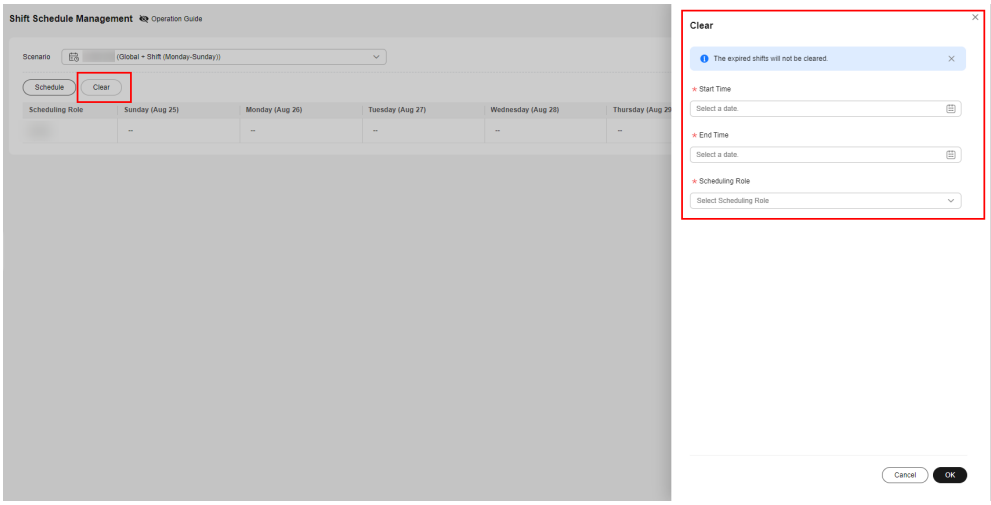
Step 2 In the navigation pane, choose **Basic Configuration** > **Shift Schedule Management**. Select a scheduling scenario and click **Clear**.

Figure 10-16 Deleting engineers



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

Figure 10-17 Clearing personnel from a schedule



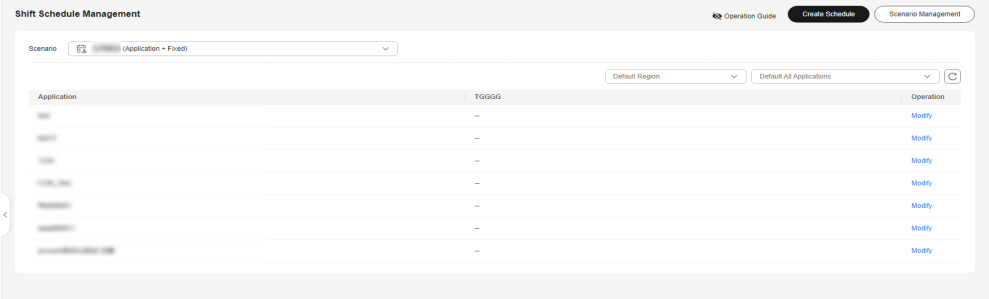
----End

Application-specific Schedule of Fixed Shifts

Step 1 Log in to **COC**.

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 10-18 Modifying a fixed shift



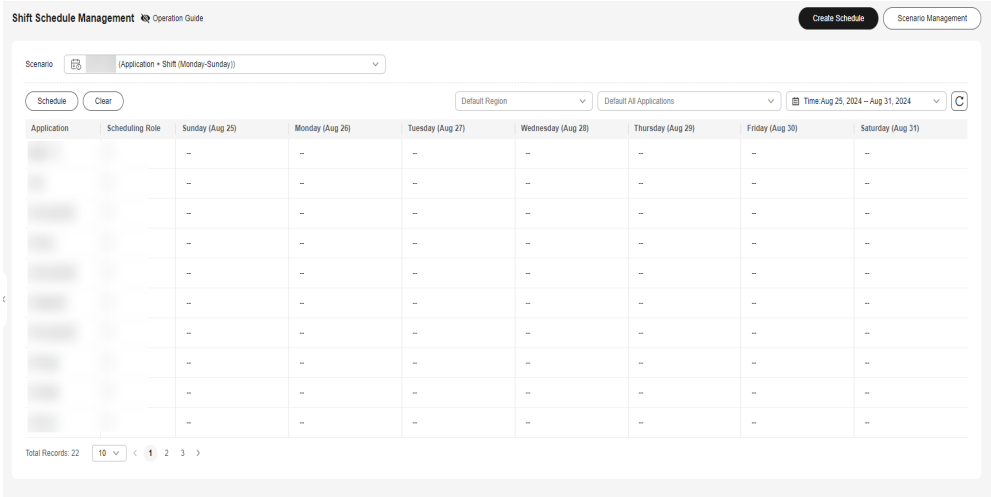
----End

Application-specific Schedule of Rotating Shifts

Step 1 Log in to **COC**.

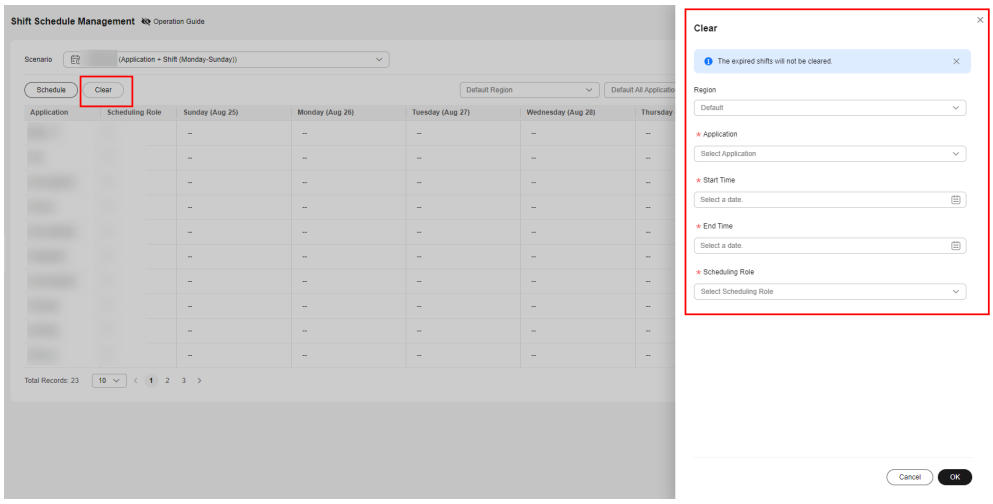
Step 2 In the navigation pane, choose **Basic Configuration** > **Shift Schedule Management**. Select a scheduling scenario and click **Clear**.

Figure 10-19 Clearing schedules



Step 3 In the **Clear** drawer, select regions and applications, enter the start time and end time, select scheduling roles, and click **OK**.

Figure 10-20 Clearing schedules



----End

10.2.2 Managing Scheduling Scenarios

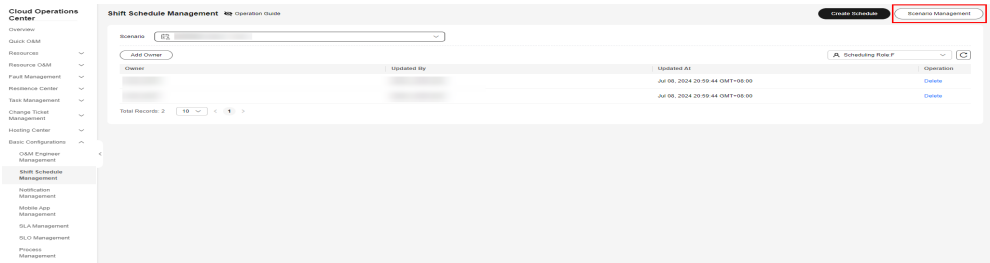
This topic describes how to manage scheduling scenarios and scheduling roles.

Creating a Scheduling Scenario

Step 1 Log in to **COC**.

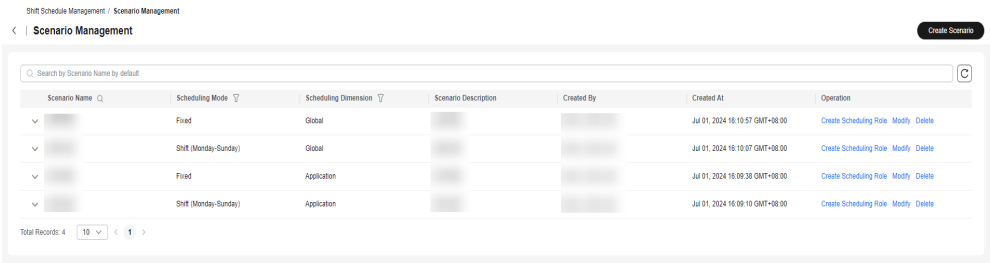
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Shift Schedule Management**. On the displayed page, click **Scenario Management**.

Figure 10-21 Scenario management



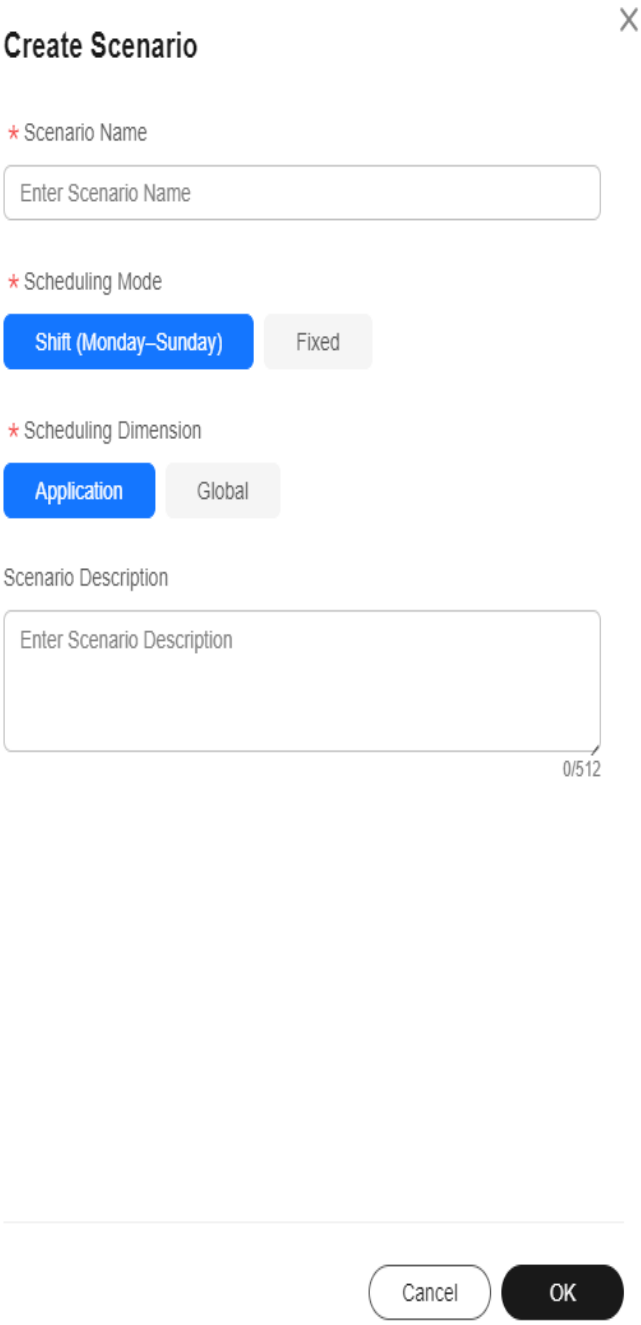
Step 3 Click **Create Scenario**.

Figure 10-22 Scenario list



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

Figure 10-23 Creating a scheduling scenario



- **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.

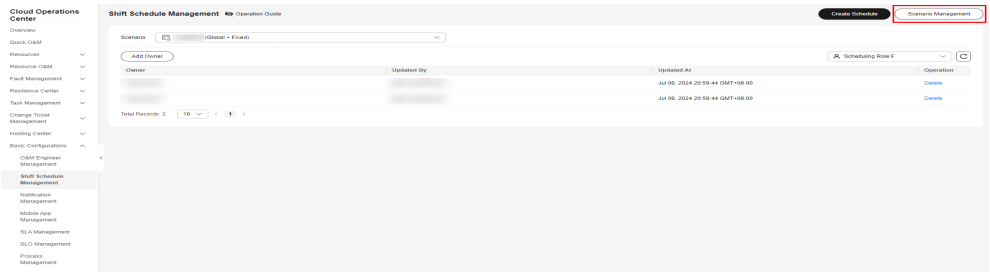
----End

Querying a Scheduling Scenario

Step 1 Log in to **COC**.

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

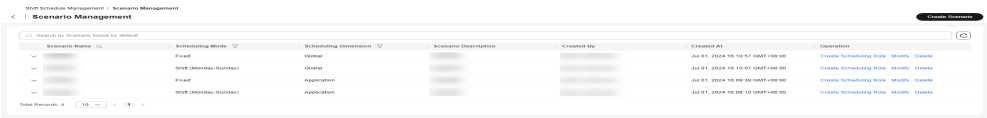
Figure 10-24 Scenario management



Step 3 In the scenario list, enter the search criteria.

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

Figure 10-25 View roles



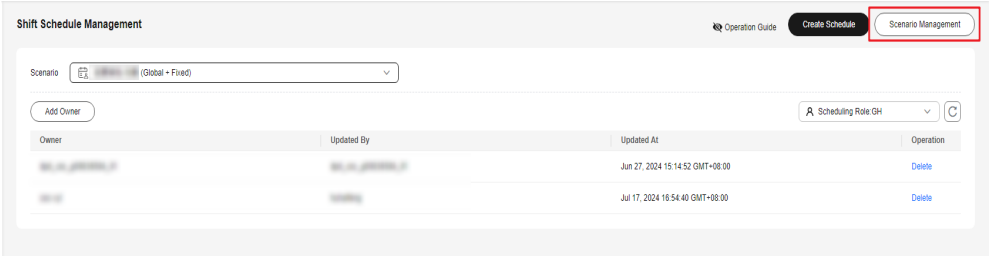
----End

Modifying a Scheduling Scenario

Step 1 Log in to **COC**.

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

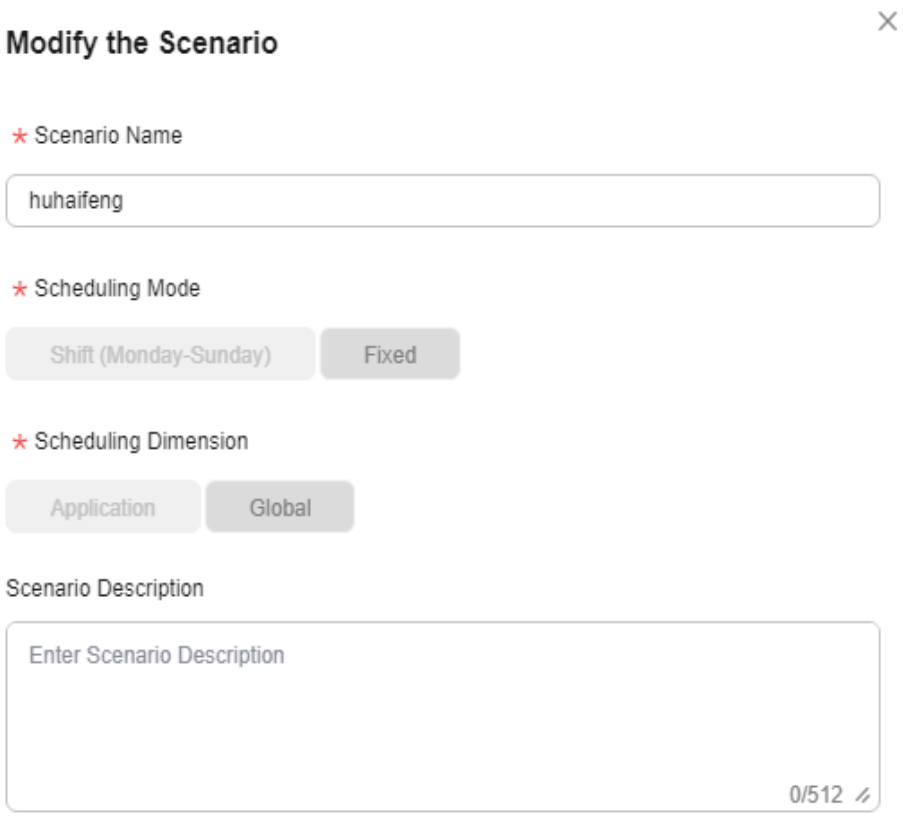
Figure 10-26 Scenario management



Step 3 In the scenario list, locate a scenario and click **Modify** in the **Operation** column.

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

Figure 10-27 Modifying a scenario

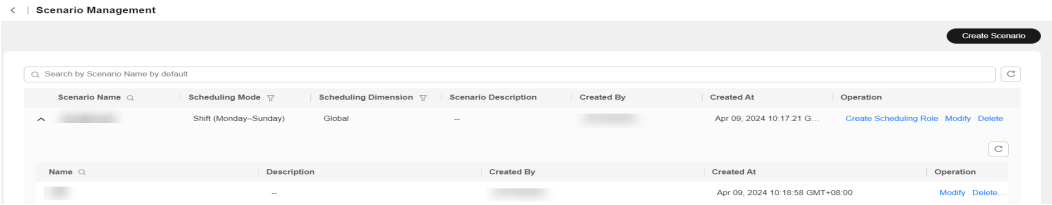


NOTE

The scheduling mode and scheduling dimension in a scenario cannot be modified. You can create a schedule to specify the mode and dimension you need as described in **Creating a Schedule**.

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 10-28 Modifying a scheduling role



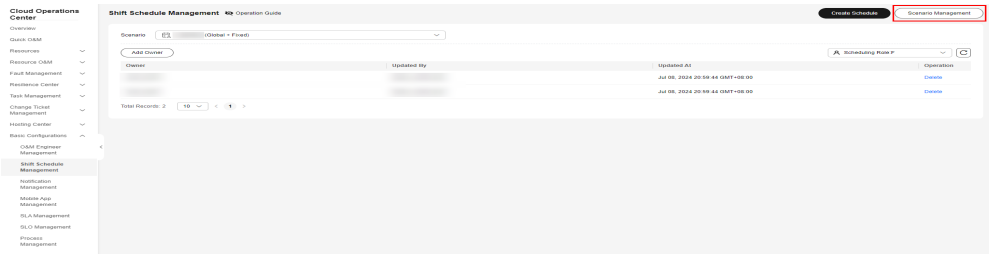
----End

Deleting a Scheduling Scenario

Step 1 Log in to **COC**.

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

Figure 10-29 Scenario management



Step 3 In the scenario list, locate a scenario and click **Delete** in the **Operation** column.

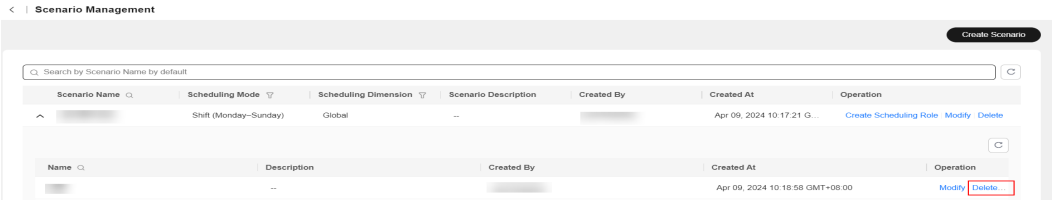
Step 4 In the displayed dialog box, click **OK**.

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, locate a role, and click **Delete** in the **Operation** column of the scheduling role.

Figure 10-30 Deleting a scheduling role



----End

10.3 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.

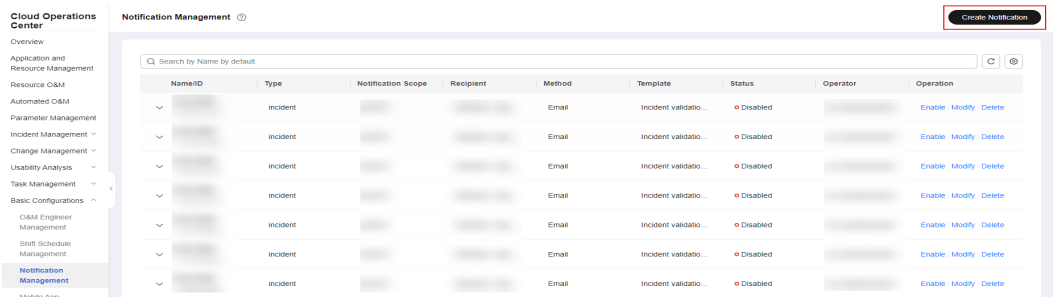
Creating a Notification

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 10-31 Clicking Create Notification



Step 3 Enter the parameters for creating a notification and click **OK**. **Table 10-1** describes the parameters for creating a notification.

Figure 10-32 Entering the notification parameters

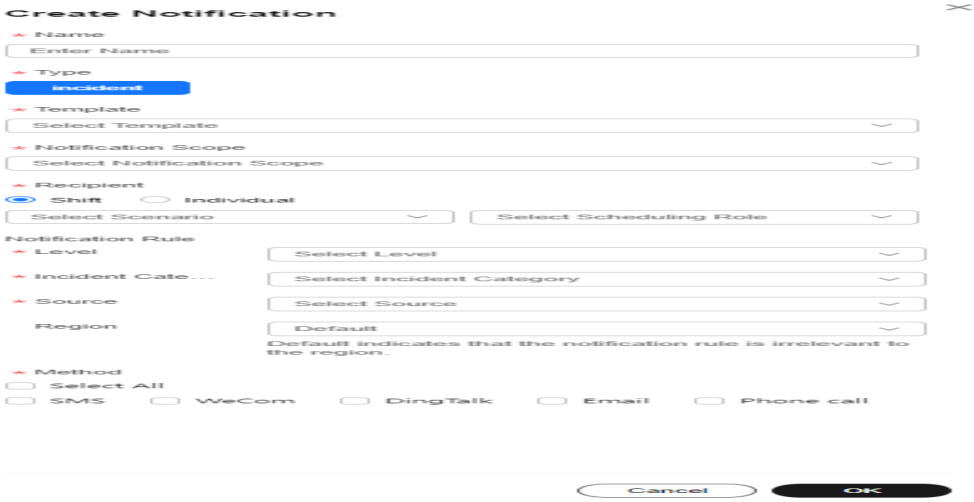


Table 10-1 Notification parameters

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.

Parameter	Mandatory	Radio/Checkbox	Description
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.
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 *A* is set to *a*, in an incident ticket, the value of rule *A* is *a*, not considering other matching rules, the subscription instance will take effect and a notification is sent based on the subscription instance. However, if the value of rule *A* in the incident ticket is *b*, the subscription instance will not take effect, and no notification is sent.
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.

Parameter	Mandatory	Radio/Checkbox	Description
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

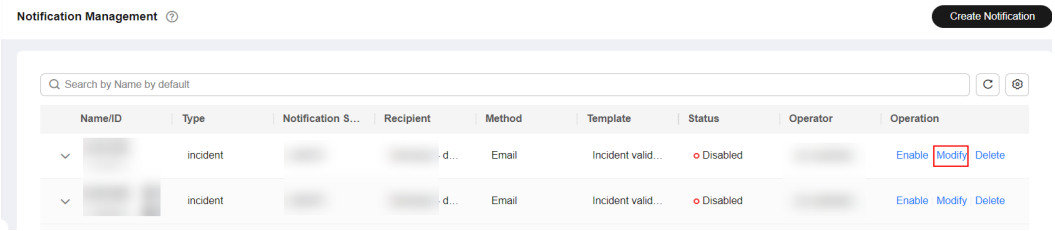
Editing Notifications

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 10-33 Modifying notifications



Step 3 Modify the notification instance and save the modification. For details, see **Step 3**.

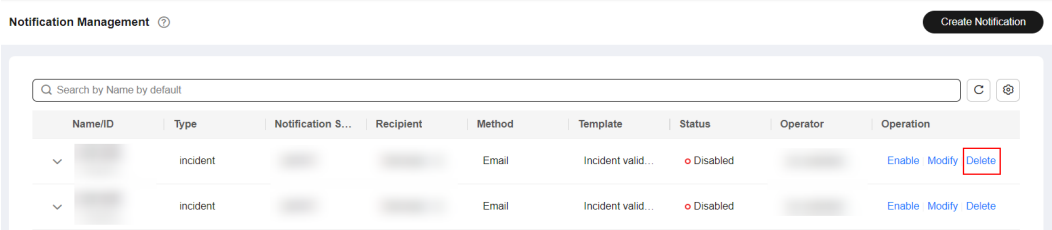
----End

Deleting a Notification

Step 1 Log in to **COC**.

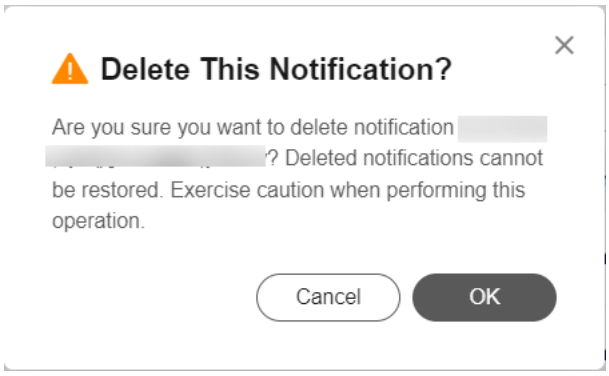
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Notification Management**. On the displayed page, locate the notification to be deleted and click **Delete** in the **Operation** column.

Figure 10-34 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 10-35 Confirming the deletion



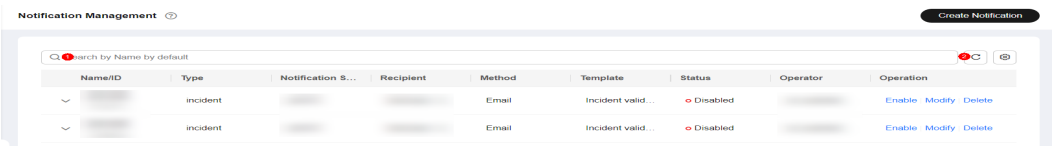
----End

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 10-36 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.

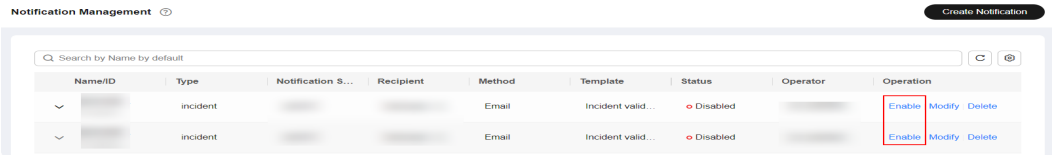
----End

Enabling and Disabling a Notification Instance

Step 1 Log in to **COC**.

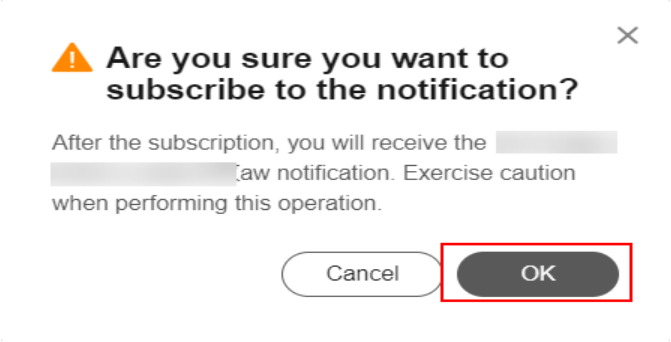
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Notification Management**. On the displayed page, locate the notification to be enabled or disabled, click **Enable** or **Disable** in the **Operation** column.

Figure 10-37 Enabling/Disabling Notifications



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

Figure 10-38 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.

10.4 Mobile Application Management

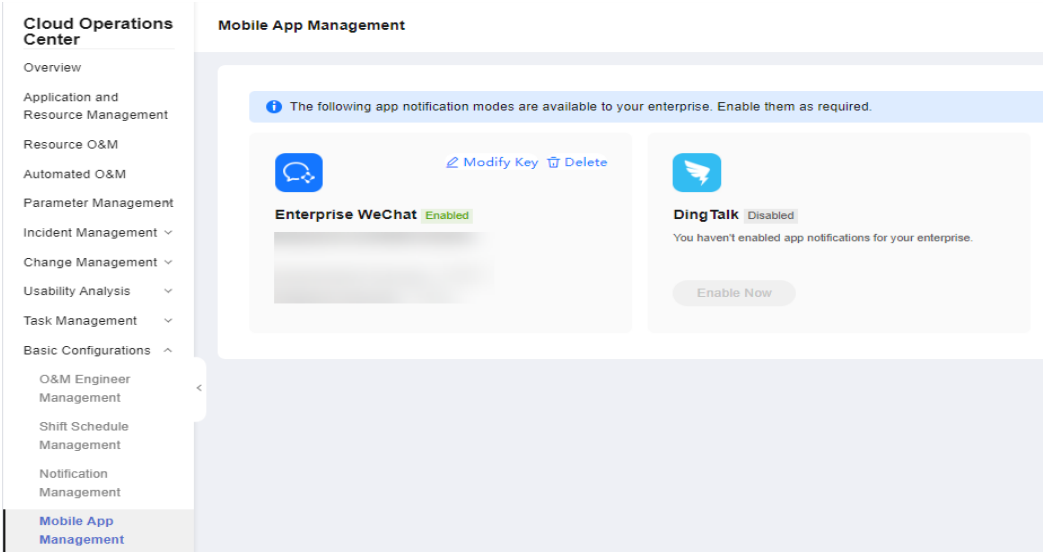
Mobile Application Management is used to manage the enterprise WeChat configuration information required for creating an enterprise WeChat WarRoom.

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 10-39 Mobile application management



NOTE

Currently, only enterprise WeChat is supported.

----End

Adding a Mobile Application

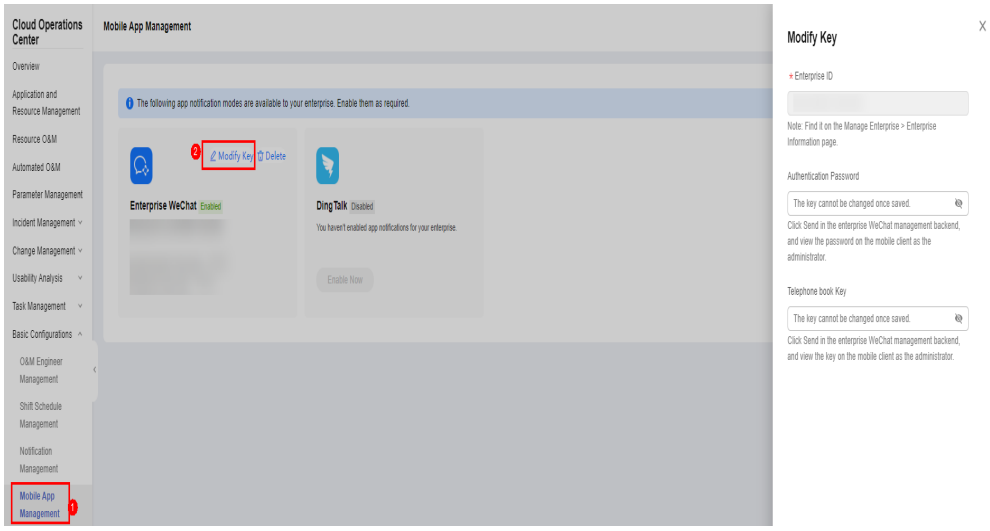
Step 1 Log in to **COC**.

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 10-40 Creating a mobile application



----End

Deleting a Mobile Application

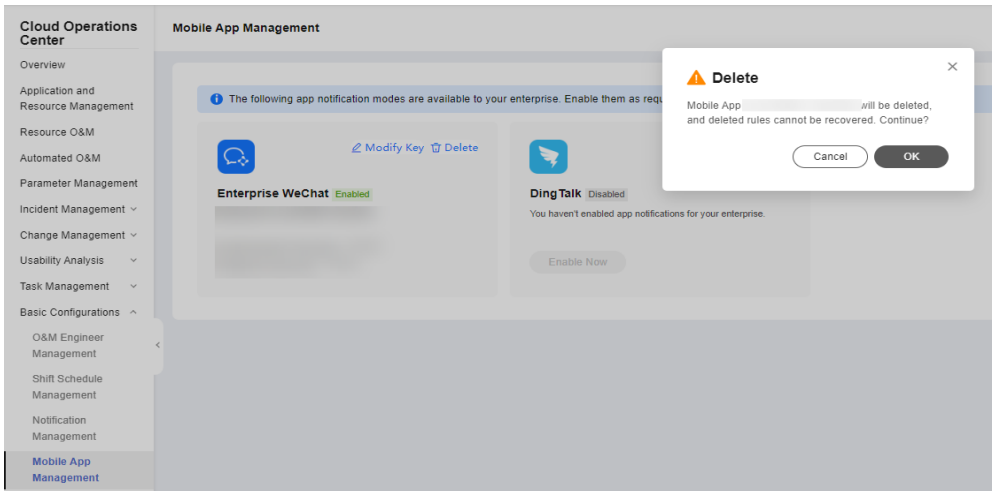
Step 1 Log in to **COC**.

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 10-41 Deleting a Mobile Application



----End

10.5 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.

10.5.1 Custom SLA

Tenants can customize SLA as required.

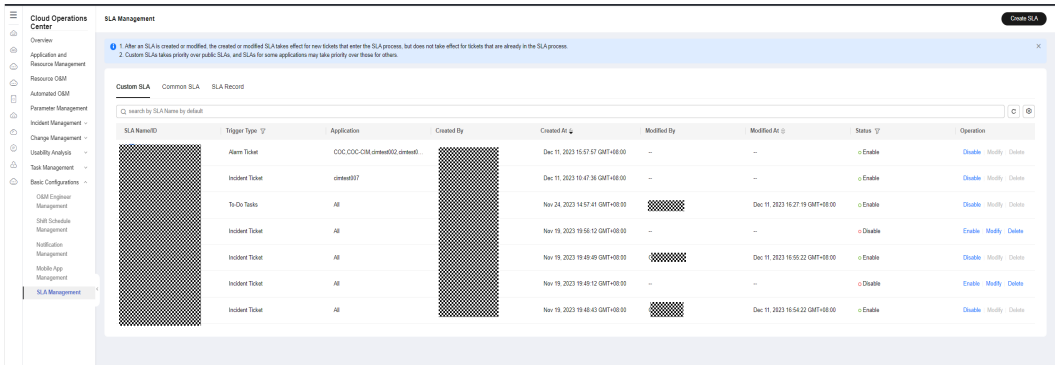
Querying a Custom SLA

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 10-42 SLA list

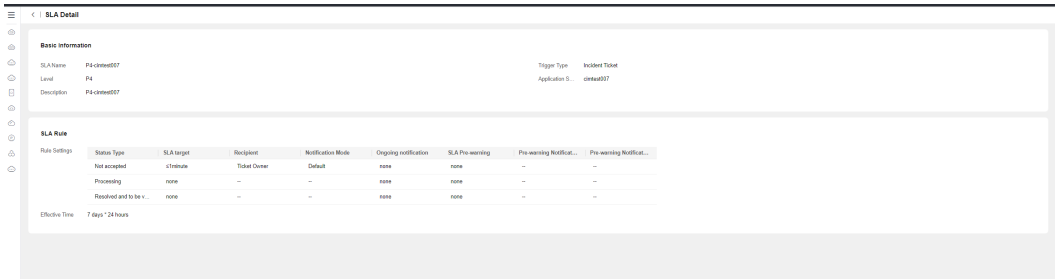


Step 4 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 10-43 Filtering SLA rules

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

Figure 10-44 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

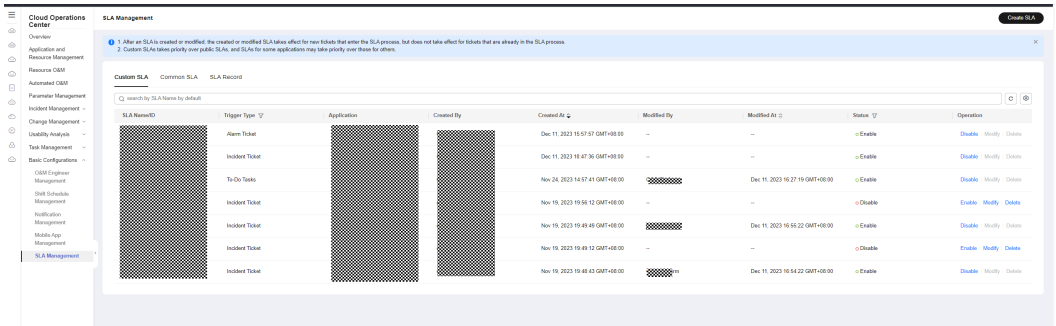
Creating a Custom SLA

Step 1 Log in to **COC**.

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

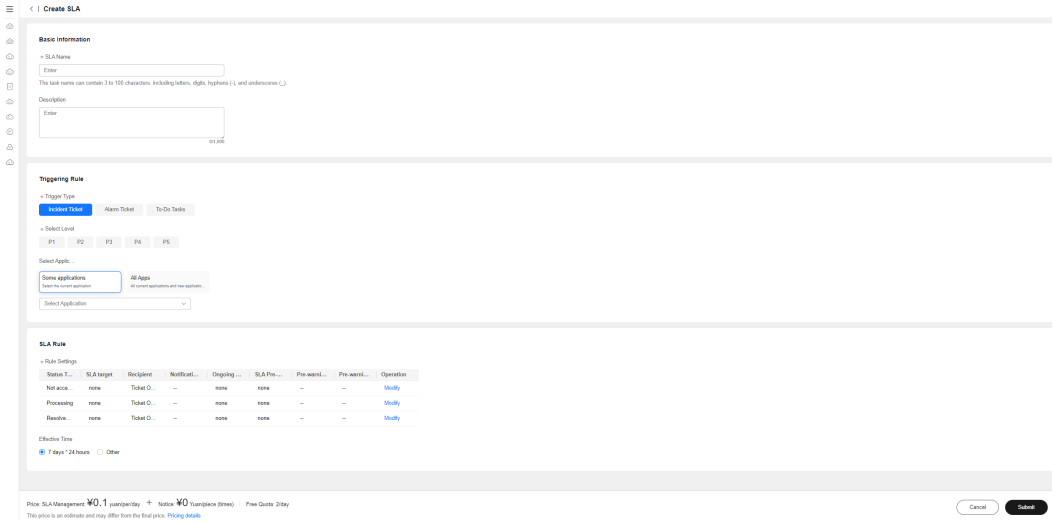
Step 3 Click the **Custom SLA** tab.

Figure 10-45 Querying the SLA List



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

Figure 10-46 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 10-2** describes the required parameters.

Figure 10-47 Selecting applications

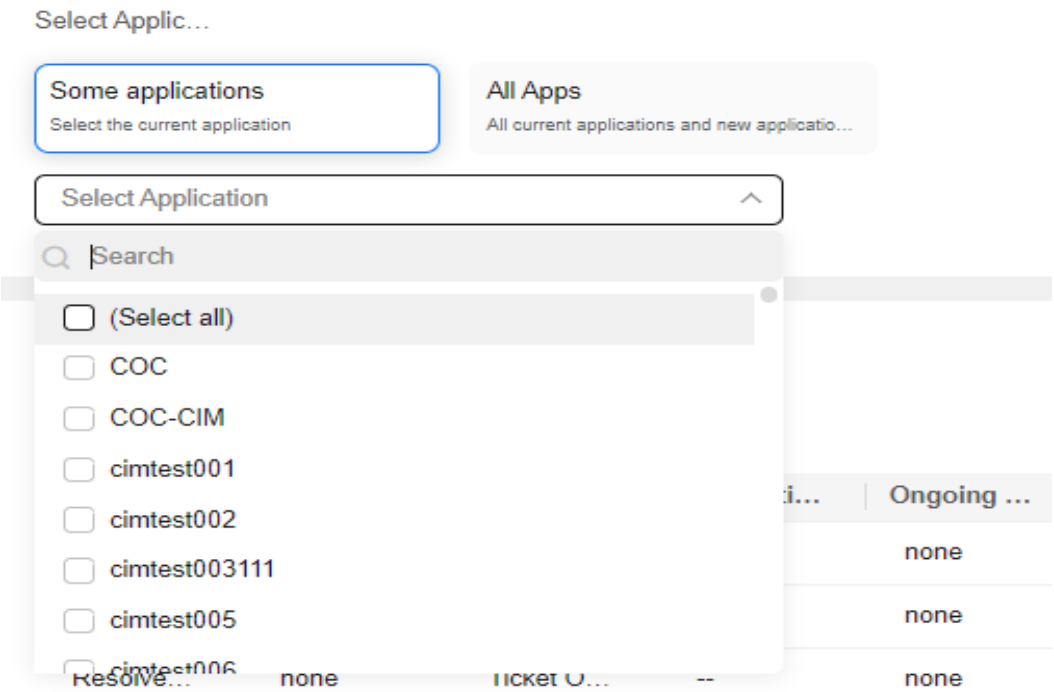


Table 10-2 Description

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: ● Incident Ticket ● Alarm Ticket ● To-Do Task
Select Level	When the trigger type is incident ticket, the levels are as follows: ● P1 ● P2 ● P3 ● P4 ● P5 When the trigger type is Alarm Ticket, the levels include: ● **Critical** ● **Major** ● **Minor** ● **Suggestion** When the trigger type is To-Do Task, the levels include: ● **Critical** ● **Major** ● **Minor** ● **Suggestion**
Select Application	Options: ● Some applications ● All Apps

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

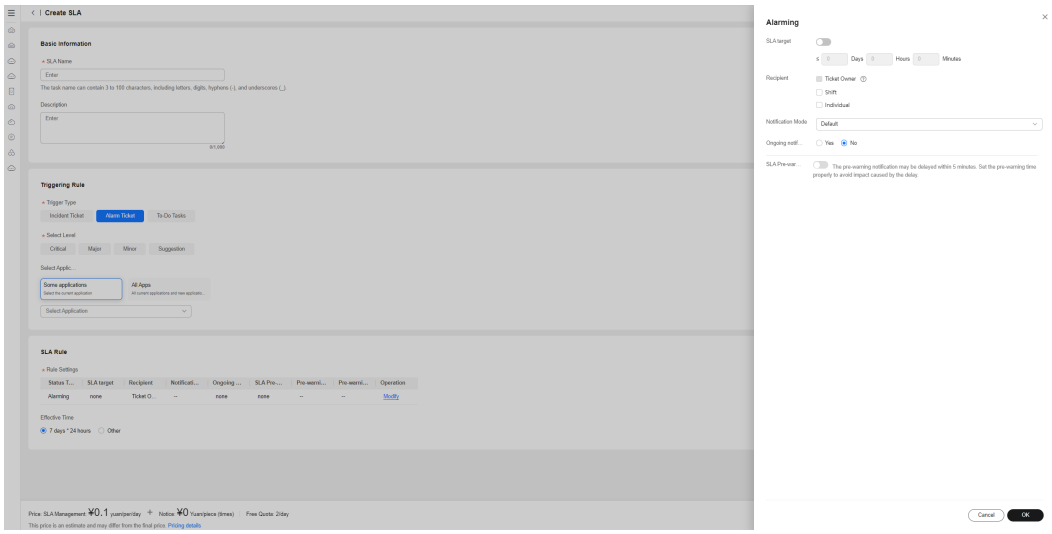
Step 7 Set SLA target, notification object, and notification channel in the dialog box that is displayed.

Table 10-3 Description

Parameter	Description
SLA Status Type	When the trigger type is incident ticket, the status types are as follows: ● Not yet accepted ● Processing ● To-be-verified When Trigger Type is set to Alarm Ticket, the status types are as follows: ● In alarm When Trigger Type is set to Alarm Ticket, the status types are as follows: ● Pending processing ● Processing
SLA target	The SLA target can be enabled. After the SLA target is enabled, a maximum of seven days can be set.
Notification Objects	Notification objects are classified into the following types: ● Ticket owner. ● **Shift** ● **Individual** The case owner is the default notification.
Notification Mode	Notification mode. The options are as follows: ● **Default** ● **SMS** ● **Enterprise WeChat** ● **DingTalk** ● **Email** ● **No notification**

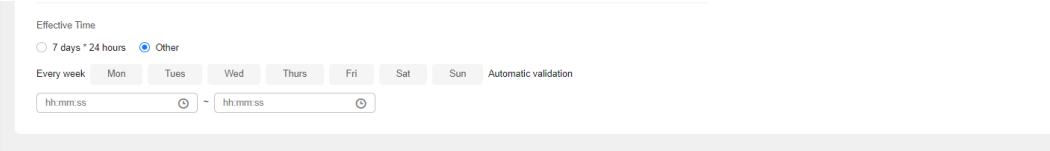
Step 8 Click OK to modify the SLA rule.

Figure 10-48 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 10-49 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

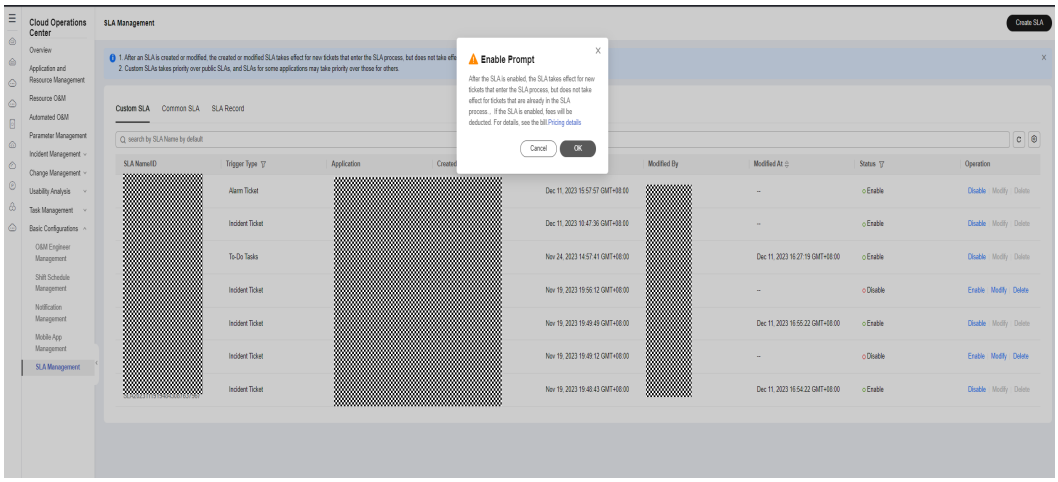
Enabling or Disabling a Custom SLA

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 10-50 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

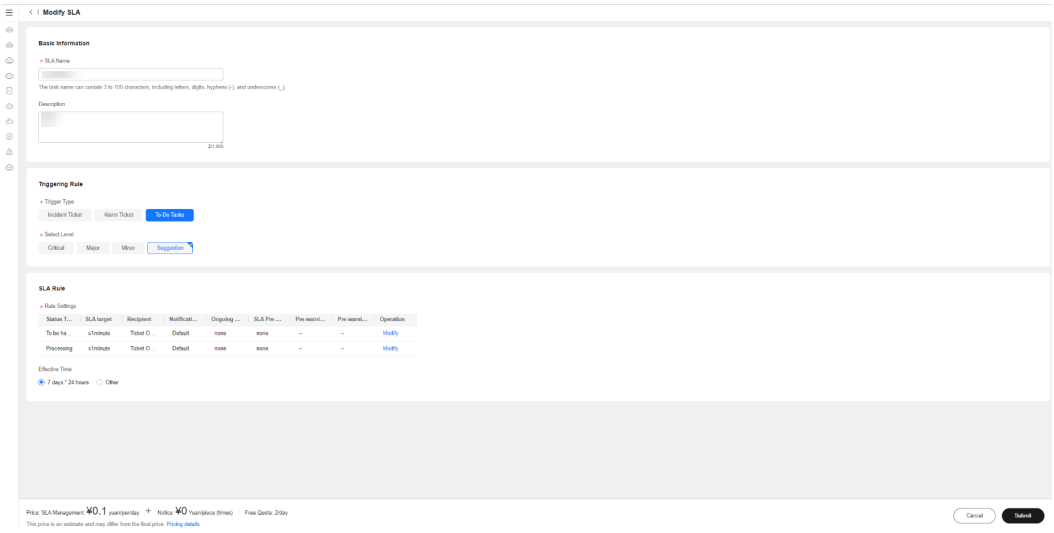
Modifying SLA

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 10-51 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

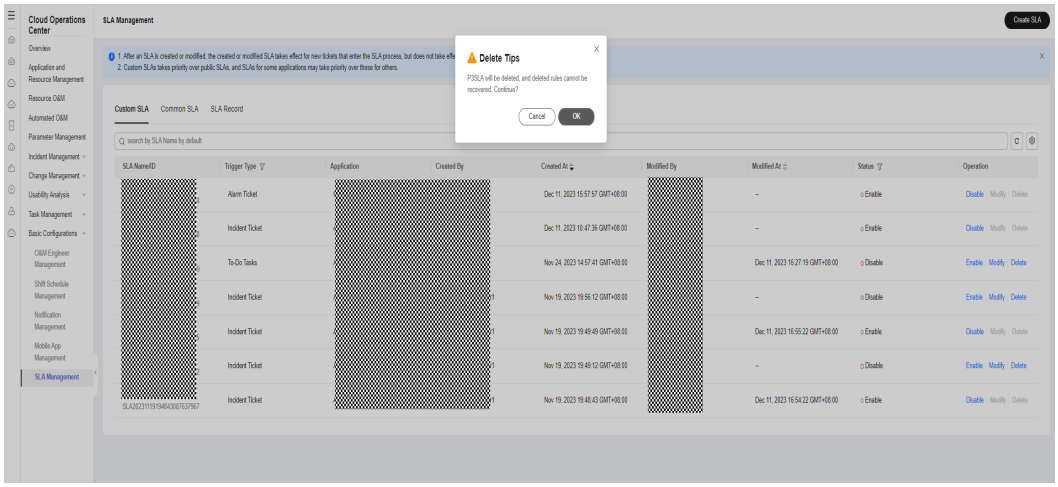
Deleting SLA

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 10-52 Deleting SLA



NOTE

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

----End

10.5.2 Common SLA

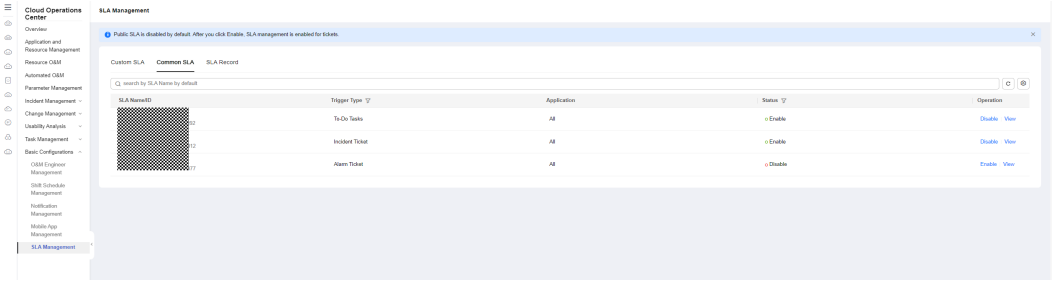
Querying Common SLA

Step 1 Log in to **COC**.

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

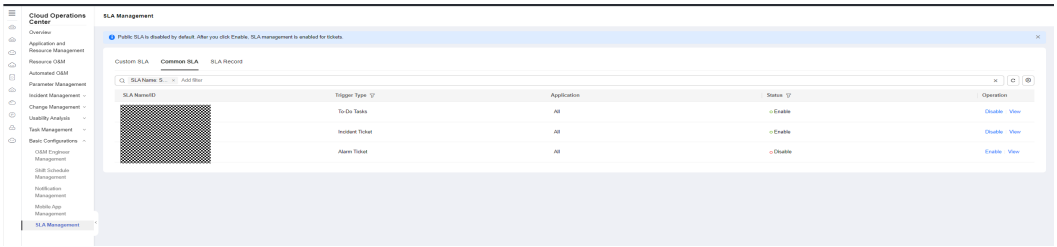
Step 3 Click the **Common SLA** tab.

Figure 10-53 Viewing the SLA list



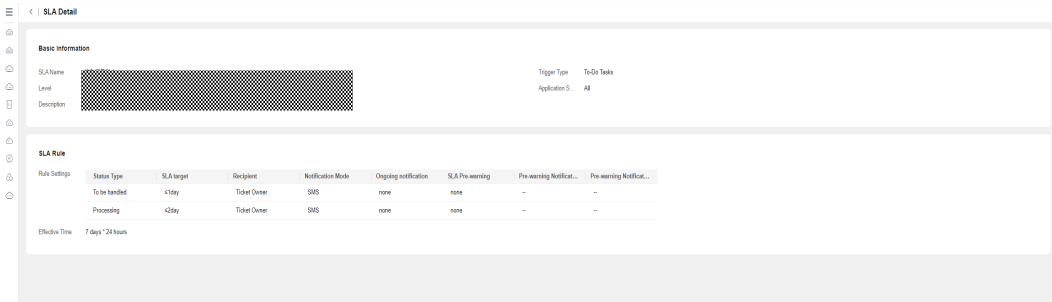
Step 4 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 10-54 Searching for a common SLA templates



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

Figure 10-55 Viewing common SLA details



NOTE

All users can view the preset common SLA.

----End

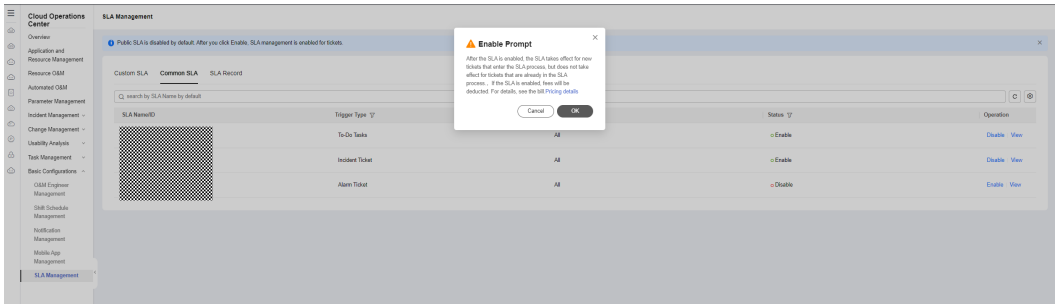
Enabling or Disabling Common SLAs

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 10-56 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

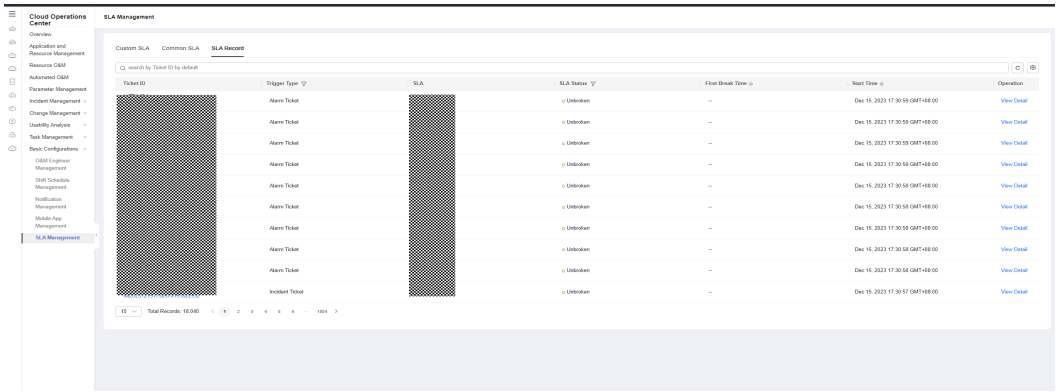
10.5.3 Managing SLA Records

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-based Tickets** tab.

Figure 10-57 Querying SLA records

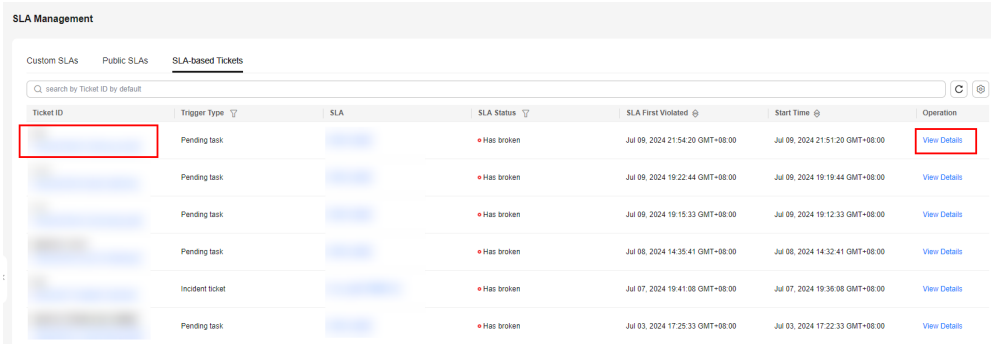


Step 3 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and configure the fields to be displayed in the list.

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

Step 5 Click a ticket ID in the **Ticket ID** column or click **View Details** in the **Operation** column to view the SLA record details.

Figure 10-58 Querying SLA record details



NOTE

- The **SLA Status** column in the **SLA Information** table on the **SLA Record Details** page is strongly associated with the SLA rule configured during SLA template creation. If a service ticket status keeps for a duration that exceeds the specified duration set in the SLA rule, the status automatically changes to **Has Broken**.
- Duration is closely related to the status change of the ticket.

----End

10.6 SLO Management

Overview

Currently, SLO management interconnects with features such as war rooms, fault management, and alarm management, to automatically complete SLO calculation and provide data for the SLO dashboard.

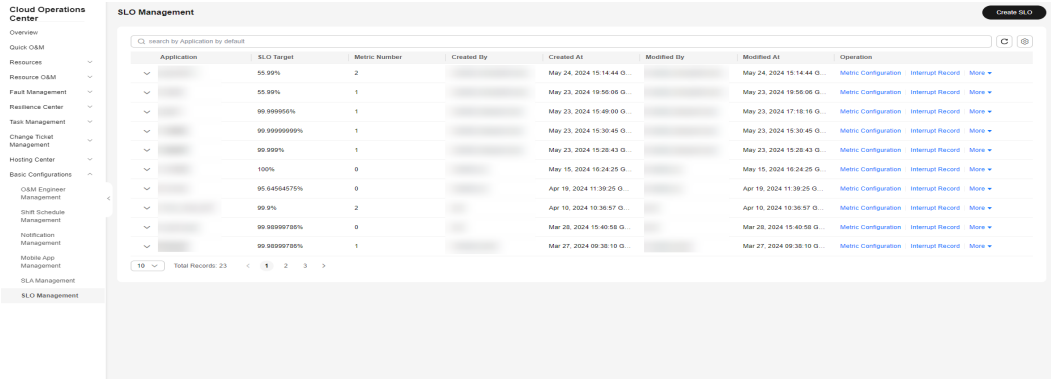
10.6.1 Viewing an SLO

Viewing an SLO

Step 1 Log in to **COC**.

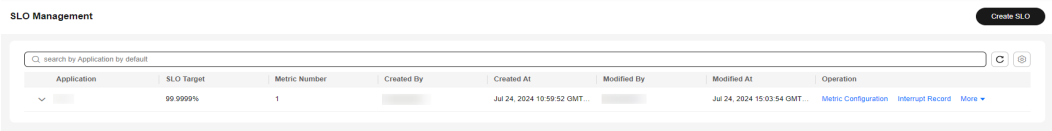
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **SLO Management**.

Figure 10-59 SLOs



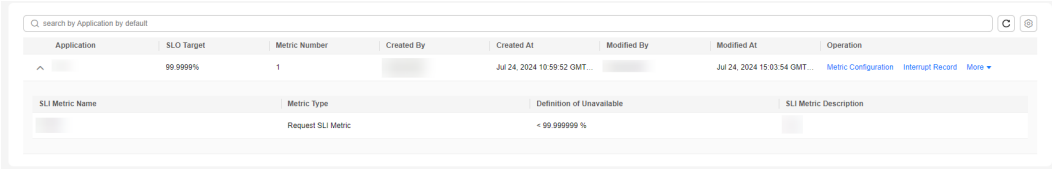
Step 3 Click the search box. The search criteria list is displayed. Select search criteria, enter values, and press **Enter** to search for data. You can click the refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 10-60 Filtering SLOs



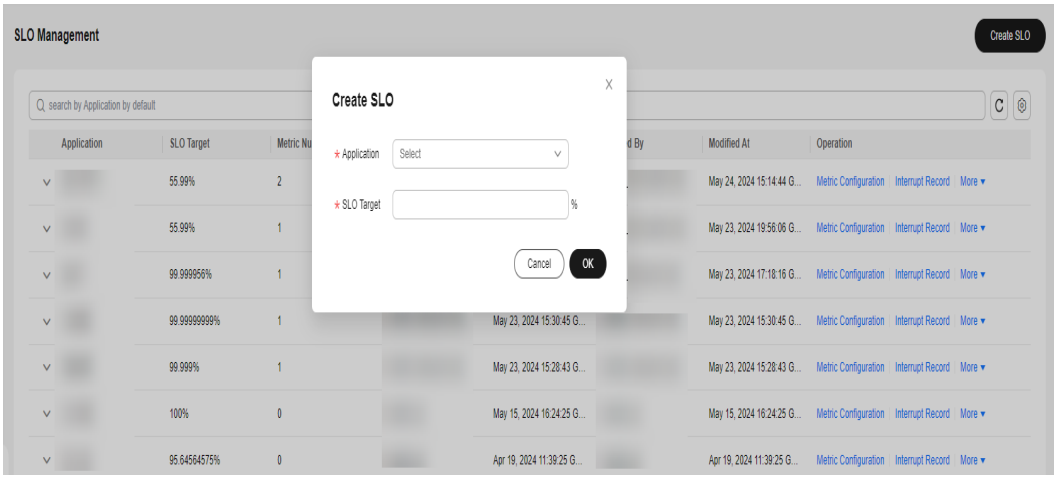
Step 4 Click in the list to view details.

Figure 10-61 SLO details



Step 5 Click **Create SLO** in the upper right corner, and select the corresponding application and SLO target value to create an SLO.

Figure 10-62 Creating an SLO



Step 6 In the SLO management list, locate an SLO metric, click **More** > **Modify** in the **Operation** column to modify the SLO metric.

Step 7 In the SLO management list, locate an SLO metric, click **More** > **Delete** in the **Operation** column to delete the SLO metric.

----End

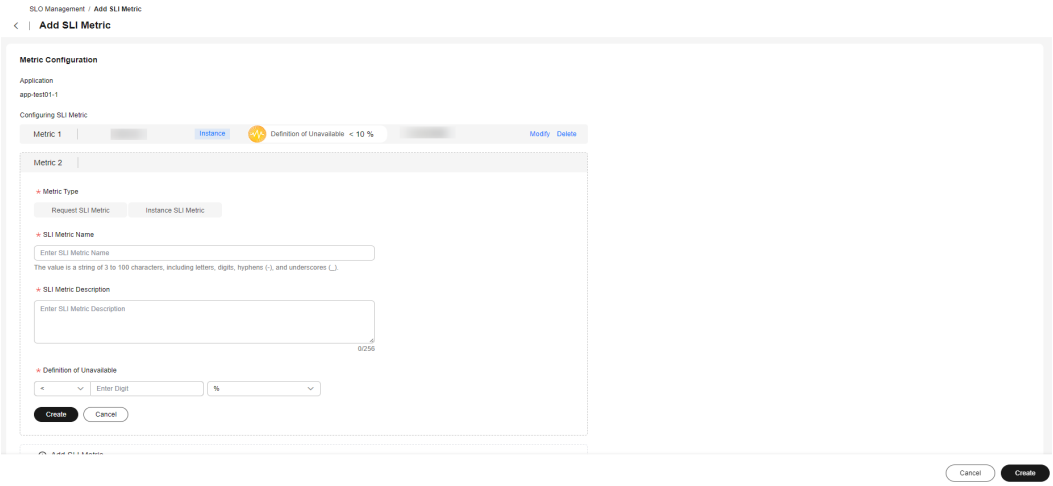
10.6.2 Configuring SLO Metrics

Step 1 Log in to **COC**.

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

Step 3 In the SLO management list, locate a target metric, click **Metric Configuration** in the **Operation** column. On the displayed page, you can add, modify, or delete SLI metrics.

Figure 10-63 Configuring SLI metrics



Step 4 Click **Create** in the lower right corner.

----End

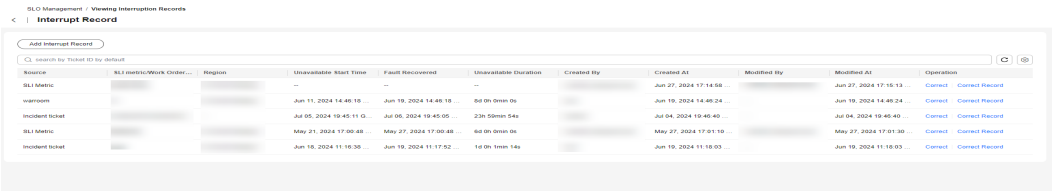
10.6.3 Viewing the SLO Interruption Records

Step 1 Log in to **COC**.

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

Step 3 In the SLO management list, locate the target metric, click **Interrupt Record** in the **Operation** column.

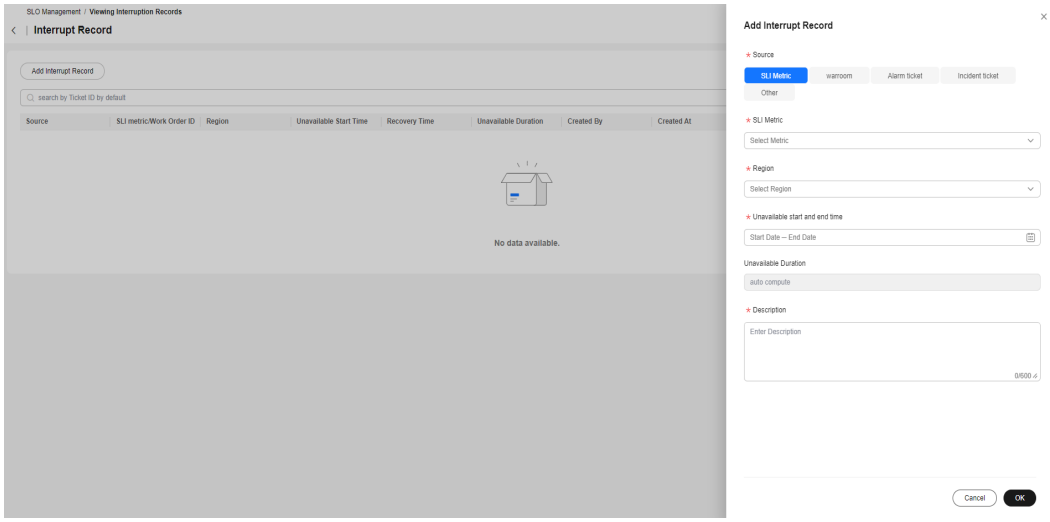
Figure 10-64 Viewing the SLO interruption records



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 configure the fields to be displayed in the list.

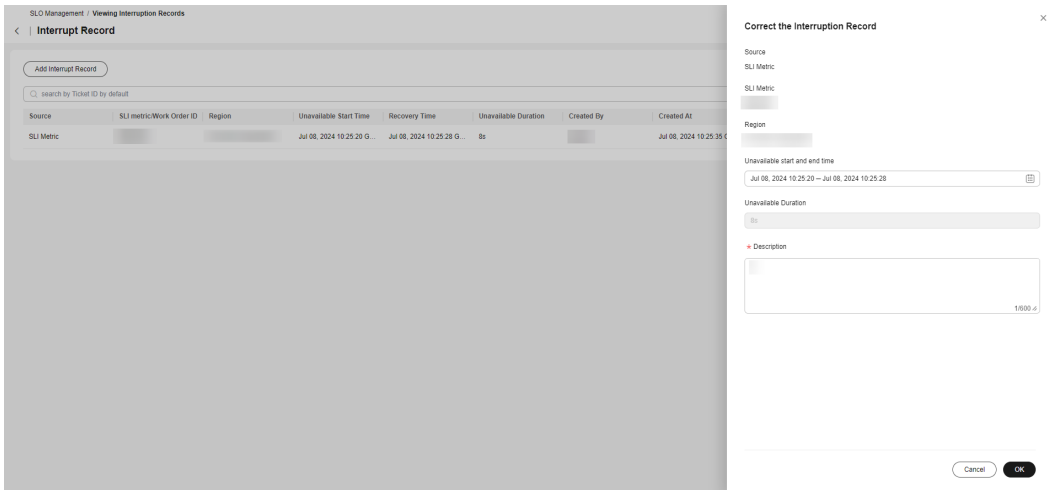
Step 5 Click **Add Interrupt Record**. The **Add Interrupt Record** drawer is displayed. Set the corresponding parameters and click **OK**.

Figure 10-65 Adding an interrupt record



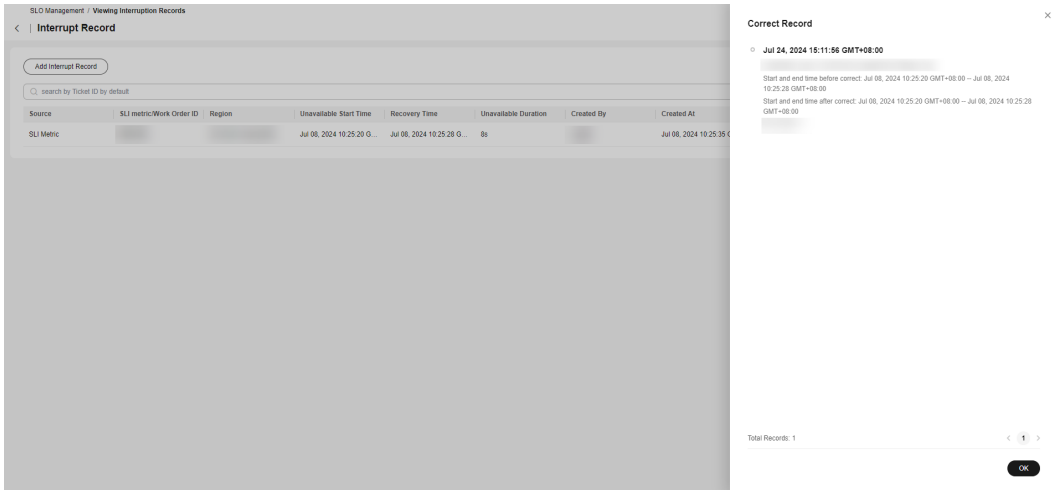
Step 6 Click **Correct** in the **Operation** column. The **Correct the Interruption Record** page is displayed on the right. You can modify the unavailable duration of the interruption.

Figure 10-66 Modifying an interruption record



Step 7 Click **Correct Record** in the **Operation** column. The **Correct Record** dialog box is displayed on the right. You can view the modification history.

Figure 10-67 Viewing interrupt modification records



----End

11 Viewing Logs

With Cloud Trace Service (CTS), you can record operations associated with COC for later query, audit, and backtracking. **Table 11-1** lists the key operations.

Table 11-1 Key COC operations recorded by CTS

Action	Resource	Trace
Creating a war room	WarRoom	createWarRoom
Creating a war room initiation rule	MeetingRule	createMeetingRule
Deleting a war room initiation rule	MeetingRule	deleteMeetingRule
Modifying a war room initiation rule	MeetingRule	updateMeetingRule
Modifying war room information	WarRoom	modifyWarRoomInfo
Sending notifications using war room	NotificationBriefing	sendNotificationBriefing
Adding war room members	WarRoom	addWarRoomMember
Removing a war room member	WarRoom	deleteWarRoomMember
Creating the war room affected applications	ImpactApplication	createImpactApplication
Modifying the war room affected applications	ImpactApplication	updateImpactApplication
Deleting the war room affected applications	ImpactApplication	deleteImpactApplication
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