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/

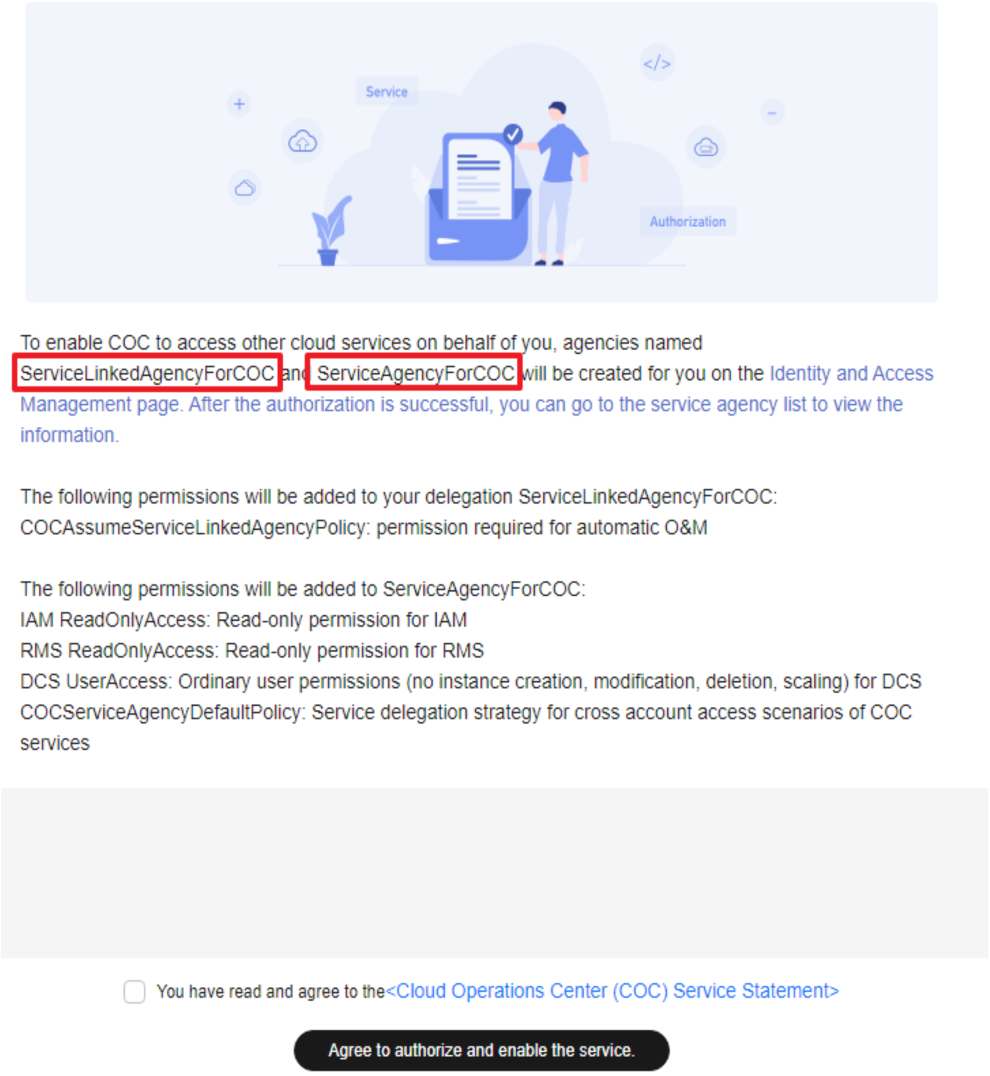
Contents

1 COC Enablement and Permissions Granting

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



To enable COC to access other cloud services on behalf of you, agencies named ServiceLinkedAgencyForCOC and ServiceAgencyForCOC will be created for you on the Identity and Access Management page. After the authorization is successful, you can go to the service agency list to view the information.

The following permissions will be added to your delegation ServiceLinkedAgencyForCOC:
COCAssumeServiceLinkedAgencyPolicy: permission required for automatic O&M

The following permissions will be added to ServiceAgencyForCOC:
IAM ReadOnlyAccess: Read-only permission for IAM
RMS ReadOnlyAccess: Read-only permission for RMS
DCS UserAccess: Ordinary user permissions (no instance creation, modification, deletion, scaling) for DCS
COCServiceAgencyDefaultPolicy: Service delegation strategy for cross account access scenarios of COC services

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

Agree to authorize and enable the service.

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:deleteServiceLinkedAgen-cyV5	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.

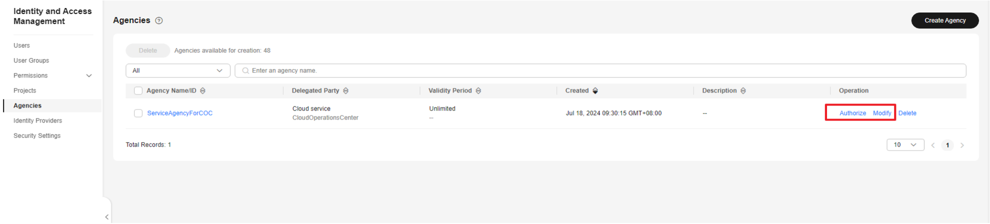
Permission	Action	Application Scenario
Listing roots of an organization	organizations:roots:list	Used to query organization roots in the cross-account scenario.

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



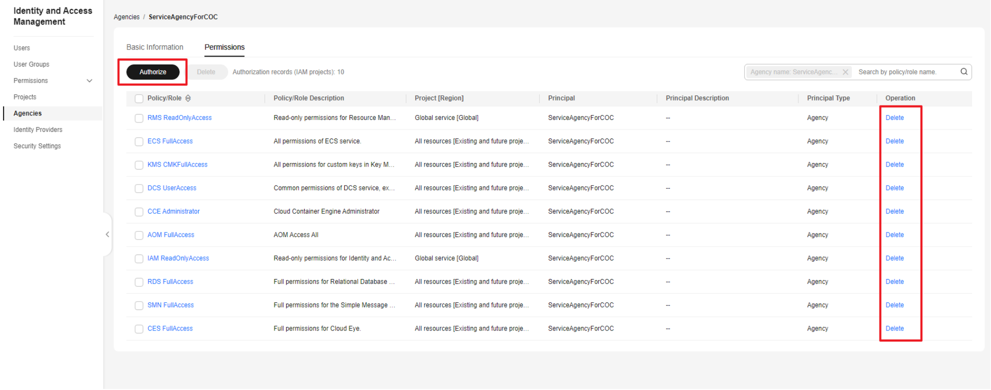
Agencies available for creation: 48

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

Total Records: 1

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

Figure 1-3 Permission granting records



Authorization records (IAM projects): 10

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

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 Learning About RBAC

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

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing COC resources.
- Grant 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 Huawei Cloud account does not require individual IAM users, skip this chapter.

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 an IAM user and add it to a 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, choose **Task Management** > **To-do Center** in the navigation pane on the left. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task fails to be created (assume that you have only the **COC ReadOnlyAccess** permission), the **COC ReadOnlyAccess** permission has taken effect.
   - Log in to COC, choose **Task Management** > **To-do Center** in the navigation pane on the left. In the upper right corner of the displayed page, click **Create Ticket**. If a to-do task can be created (assume that you have only the **COC FullAccess** permission), the **COC FullAccess** permission has 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 Learning About ABAC

N/A

2 Overview

You can have an overview of your cloud resources, including their health status, monitoring data, and security details, and can also learn about the O&M capabilities of the platform and the system updates.

2.1 O&M Operations Center

You can query and follow up O&M to-do tasks.

Scenarios

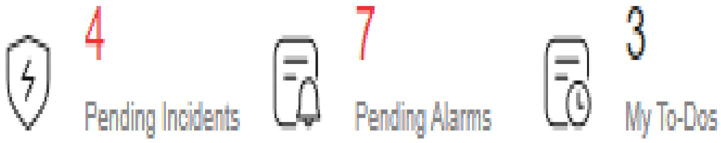
Query and follow up O&M to-do tasks on COC.

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 O&M transaction tracking



Step 3 Click **Pending Incidents**, **Pending Alarms**, or **My To-Dos** to go to the corresponding O&M transaction page.

----End

2.2 Quick Configuration Center

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

Scenarios

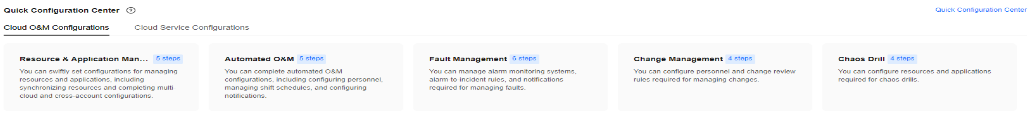
You can use the quick configuration center to quickly configure resources in different scenarios.

COC Configurations

Step 1 Log in to COC.

Step 2 On the **Overview** page of COC, you can view the quick configuration center module.

Figure 2-2 Quick configuration center



Quick Configuration Center

Quick Configuration Center

Cloud O&M Configurations Cloud Service Configurations

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

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

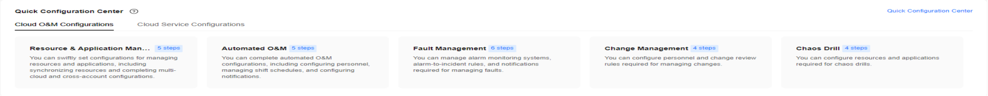
Fault Management 6 steps
You can manage alarm monitoring systems, alarm-to-incident rules, and notifications required for managing faults.

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

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

If the quick configuration center (shown in Figure 1) module is not displayed on the **Overview** page, click **Quick Configuration Center** on the top to access it.

Figure 2-3 Quick configuration center entry



Quick Configuration Center

Quick Configuration Center

Cloud O&M Configurations Cloud Service Configurations

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

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

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

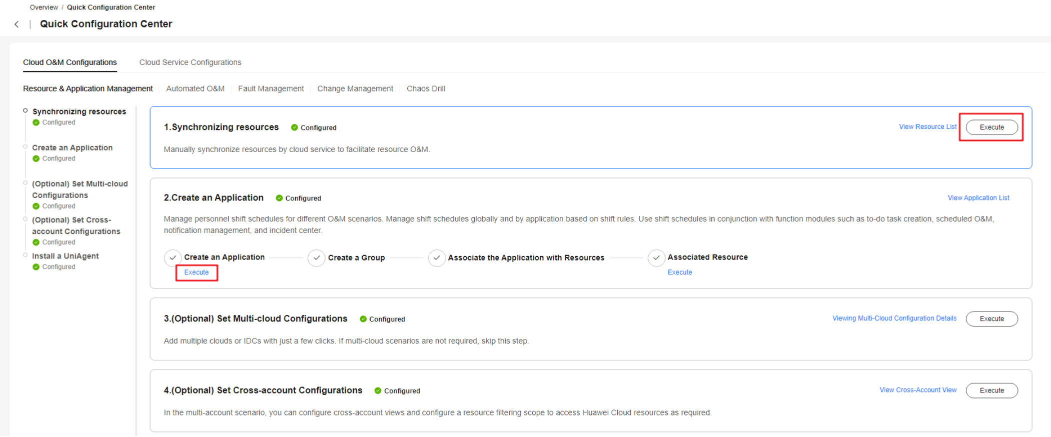
Change Management 4 steps
You can configure personnel and change review rules required for managing changes.

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

Step 3 Click a card for a specific O&M scenario to go to the configuration page of the corresponding scenario.

Step 4 Go to the **Quick Configuration Center** page and click **Execute** corresponding to different types of configuration tasks.

Figure 2-4 Selecting a scenario for configuration



Overview / Quick Configuration Center

< | Quick Configuration Center

Cloud O&M Configurations | Cloud Service Configurations

Resource & Application Management | Automated O&M | Fault Management | Change Management | Chaos Drill

- Synchronizing resources ● Configured
- Create an Application ● Configured
- (Optional) Set Multi-cloud Configurations ● Configured
- (Optional) Set Cross-account Configurations ● Configured
- Install a UniAgent ● Configured

1.Synchronizing resources ● Configured — View Resource List — Execute

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

2.Create an Application ● Configured — View Application List

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

✓ Create an Application (Execute) — ✓ Create a Group — ✓ Associate the Application with Resources — ✓ Associated Resource (Execute)

3.(Optional) Set Multi-cloud Configurations ● Configured — Viewing Multi-Cloud Configuration Details — Execute

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

4.(Optional) Set Cross-account Configurations ● Configured — View Cross-Account View — Execute

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

----End

2.3 Resource Overview

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

Scenarios

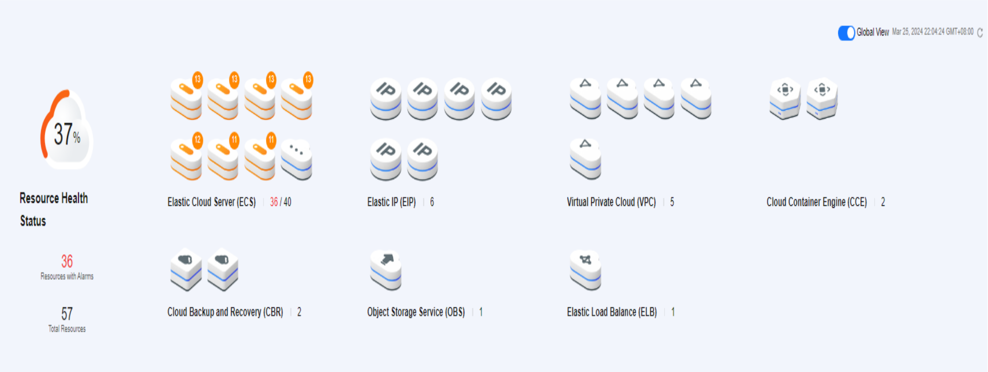
View resources (including ECSs, EIPs, and cloud databases) on COC.

Procedure

Step 1 Log in to **COC**.

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

Figure 2-5 Resource information



Global View Mar 25, 2024 22:04:24 GMT+08:00

37%

Resource Health Status

36 Resources with Alarms

57 Total Resources

Elastic Cloud Server (ECS) | 36 / 40

Elastic IP (EIP) | 6

Virtual Private Cloud (VPC) | 5

Cloud Container Engine (CCE) | 2

Cloud Backup and Recovery (CBR) | 2

Object Storage Service (OBS) | 1

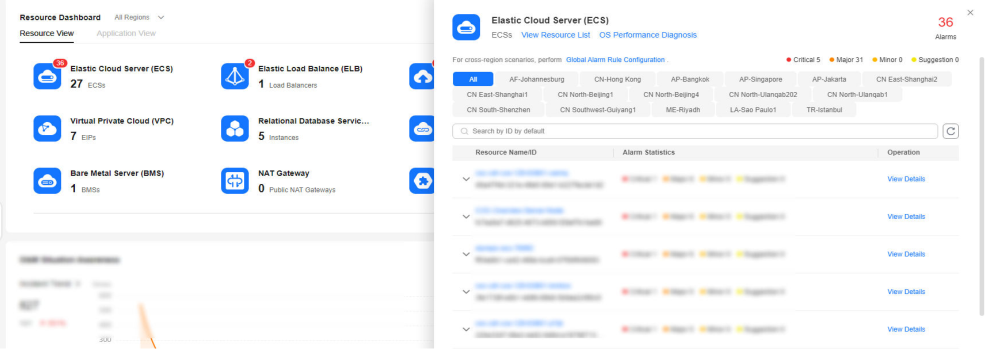
Elastic Load Balance (ELB) | 1

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.

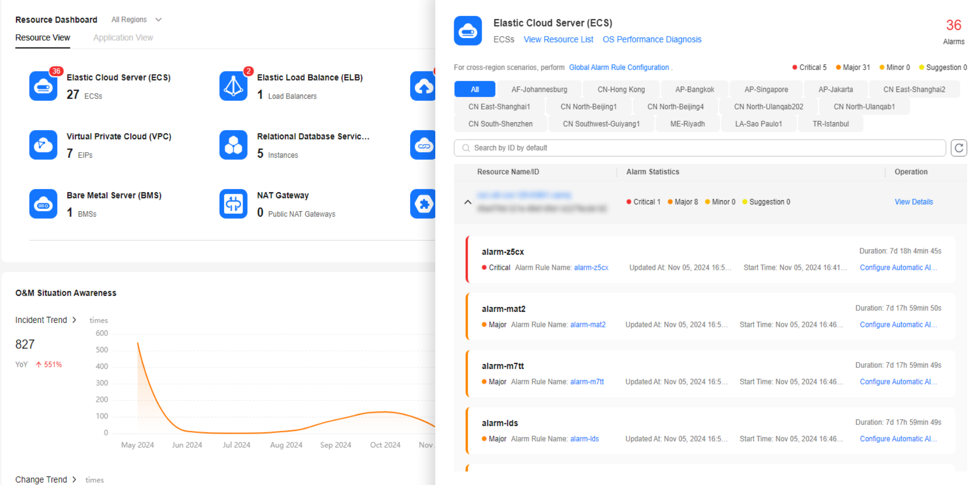
Figure 2-6 Resources in different regions



Resource Name/ID	Alarm Statistics	Operation
[redacted]	[redacted]	View Details
[redacted]	[redacted]	View Details
[redacted]	[redacted]	View Details
[redacted]	[redacted]	View Details
[redacted]	[redacted]	View Details

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

Figure 2-7 Alarm information



Resource Name/ID	Alarm Statistics	Operation
[redacted]	● Critical 1 ● Major 8 ● Minor 0 ● Suggestion 0	View Details

alarm-z5cx
● Critical Alarm Rule Name: alarm-z5cx Updated At: Nov 05, 2024 16:5... Start Time: Nov 05, 2024 16:41... Duration: 7d 18h 4min 45s Configure Automatic Al...

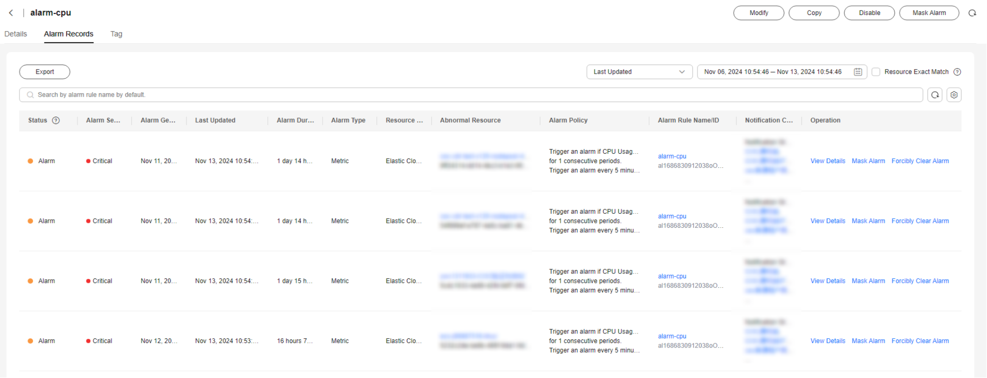
alarm-mat2
● Major Alarm Rule Name: alarm-mat2 Updated At: Nov 05, 2024 16:5... Start Time: Nov 05, 2024 16:46... Duration: 7d 17h 59min 50s Configure Automatic Al...

alarm-m7tt
● Major Alarm Rule Name: alarm-m7tt Updated At: Nov 05, 2024 16:5... Start Time: Nov 05, 2024 16:46... Duration: 7d 17h 59min 49s Configure Automatic Al...

alarm-lds
● Major Alarm Rule Name: alarm-lds Updated At: Nov 05, 2024 16:5... Start Time: Nov 05, 2024 16:46... Duration: 7d 17h 59min 49s Configure Automatic Al...

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

Figure 2-8 More alarm information



Status	Alarm Se...	Alarm Ge...	Last Updated	Alarm Dur...	Alarm Type	Resource ...	Abnormal Resource	Alarm Policy	Alarm Rule Name/ID	Notification C...	Operation
● Alarm	● Critical	Nov 11, 20...	Nov 13, 2024 10:54:...	1 day 14 h...	Metric	Elastic Clo...	[redacted]	Trigger an alarm if CPU Usag... for 1 consecutive periods. Trigger an alarm every 5 minu...	alarm-cpu al1686830912038oO...	[redacted]	View Details Mask Alarm Forcibly Clear Alarm
● Alarm	● Critical	Nov 11, 20...	Nov 13, 2024 10:54:...	1 day 14 h...	Metric	Elastic Clo...	[redacted]	Trigger an alarm if CPU Usag... for 1 consecutive periods. Trigger an alarm every 5 minu...	alarm-cpu al1686830912038oO...	[redacted]	View Details Mask Alarm Forcibly Clear Alarm
● Alarm	● Critical	Nov 11, 20...	Nov 13, 2024 10:54:...	1 day 15 h...	Metric	Elastic Clo...	[redacted]	Trigger an alarm if CPU Usag... for 1 consecutive periods. Trigger an alarm every 5 minu...	alarm-cpu al1686830912038oO...	[redacted]	View Details Mask Alarm Forcibly Clear Alarm
● Alarm	● Critical	Nov 12, 20...	Nov 13, 2024 10:53:...	16 hours 7...	Metric	Elastic Clo...	[redacted]	Trigger an alarm if CPU Usag... for 1 consecutive periods. Trigger an alarm every 5 minu...	alarm-cpu al1686830912038oO...	[redacted]	View Details Mask Alarm Forcibly Clear Alarm

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

----End

2.4 Resource Monitoring

You can view the monitoring information provided by Cloud Eye.

Scenarios

View resources monitored by Cloud Eye 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.

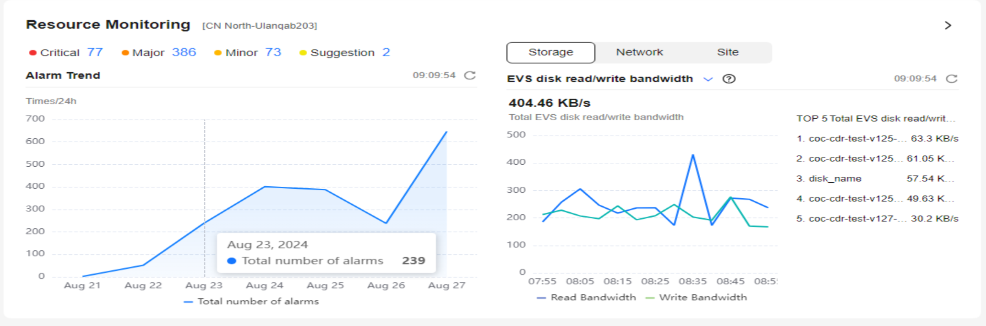


Figure 2-9 CES monitoring information

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

2.5 Application Monitoring

You can create custom applications and view application monitoring information.

Scenarios

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

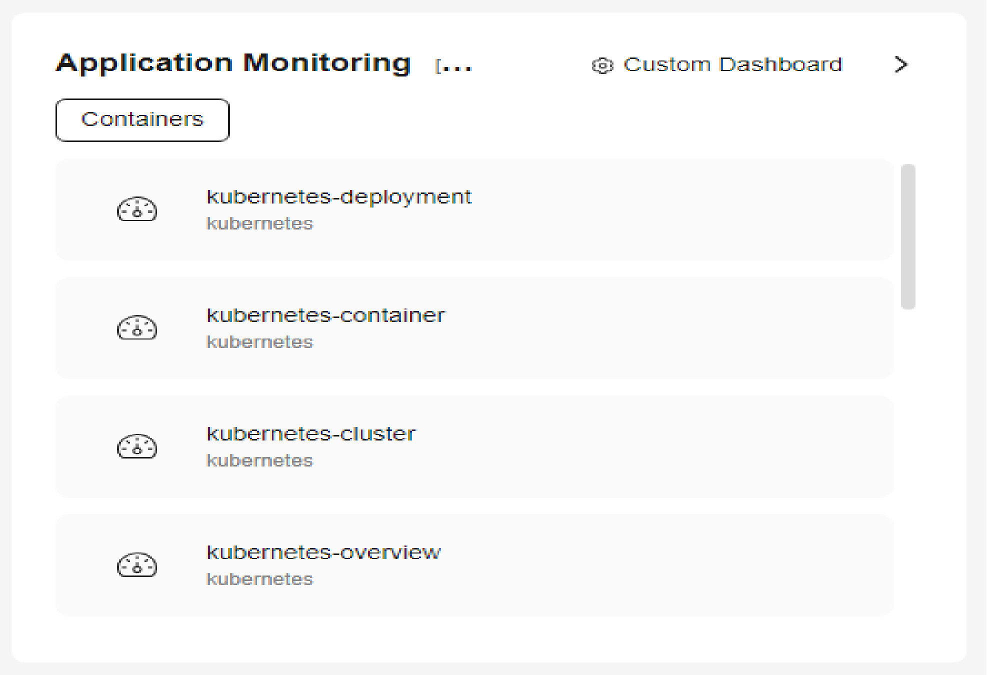
Procedure

Step 1 Log in to COC.

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

Step 3 Click **Custom Dashboard** to configure the applications to be monitored.

Figure 2-10 Application monitoring information



Application Monitoring [...
Custom Dashboard >

Containers

kubernetes-deployment
kubernetes

kubernetes-container
kubernetes

kubernetes-cluster
kubernetes

kubernetes-overview
kubernetes

----End

2.6 Security Overview

You can view the security monitoring information from SecMaster.

Scenarios

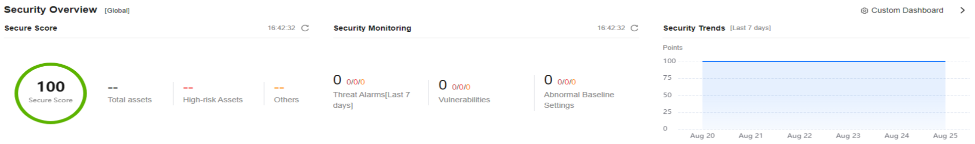
View the security monitoring information provided by SecMaster on COC.

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 2-11 Security monitoring information from SecMaster



Security Overview [Global]
Custom Dashboard >

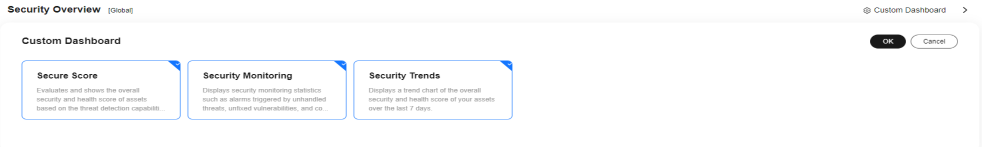
Secure Score 16:42:32
100 Secure Score
-- Total assets
-- High-risk Assets
-- Others

Security Monitoring 16:42:32
0 0/0/0 Threat Alarms[Last 7 days]
0 0/0/0 Vulnerabilities
0 0/0/0 Abnormal Baseline Settings

Security Trends [Last 7 days]

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

Figure 2-12 Customizing security monitoring dashboard



Secure Score
Evaluates and shows the overall security and health score of assets based on the threat detection capabiliti...

Security Monitoring
Displays security monitoring statistics such as alarms triggered by unhandled threats, unfixed vulnerabilities, and co...

Security Trends
Displays a trend chart of the overall security and health score of your assets over the last 7 days.

----End

2.7 O&M Situational Awareness

COC provides O&M situation awareness capabilities through monitoring of changes, incidents, alarms, security compliance, 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.
- Organization administrators or delegated administrators can view the O&M situation data of organization member accounts across accounts, and aggregate data of multiple regions and applications across accounts.

Prerequisites

If you use the O&M situation awareness function in the single-account scenario, skip this section and see **Procedure**.

If you use the O&M situation awareness function across accounts, the following prerequisites must be completed:

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

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

Scenarios

View O&M situation data of your applications on COC.

Procedure

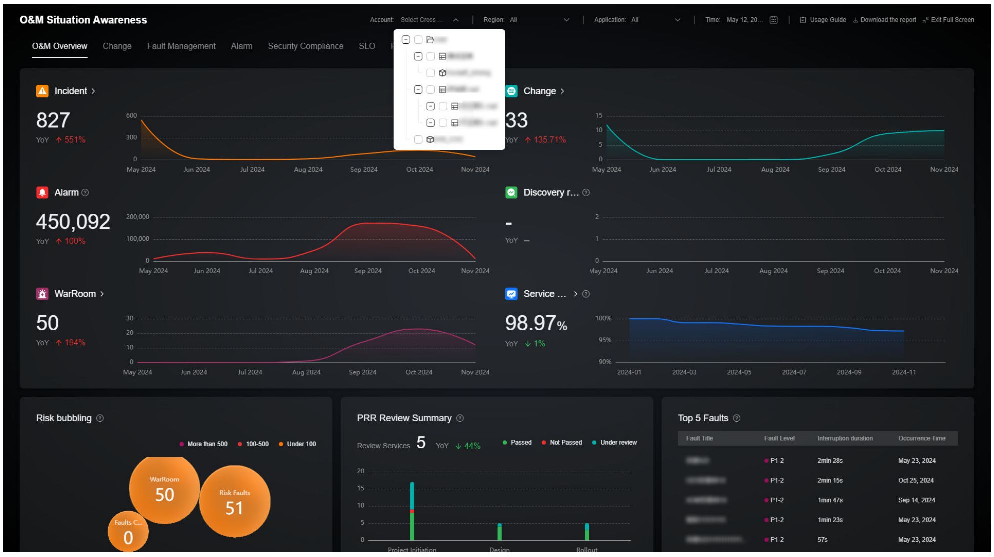
Step 1 Log in to **COC**.

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

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

Step 4 Filter O&M situation information by organization account, region, application, and date.

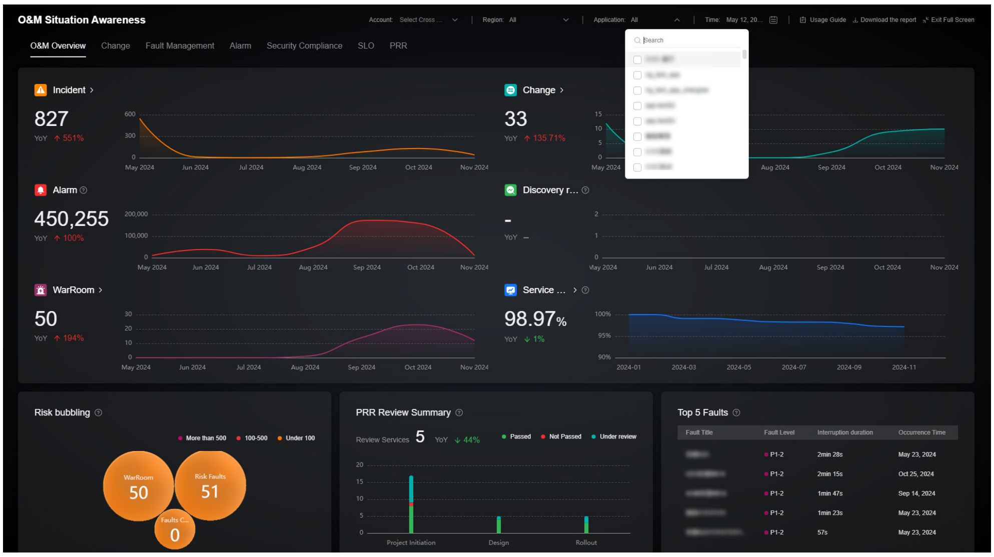
Figure 2-13 Filtering data by organization account



NOTE

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

Figure 2-14 Application data aggregation in cross-account scenarios



----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 2-15 O&M overview

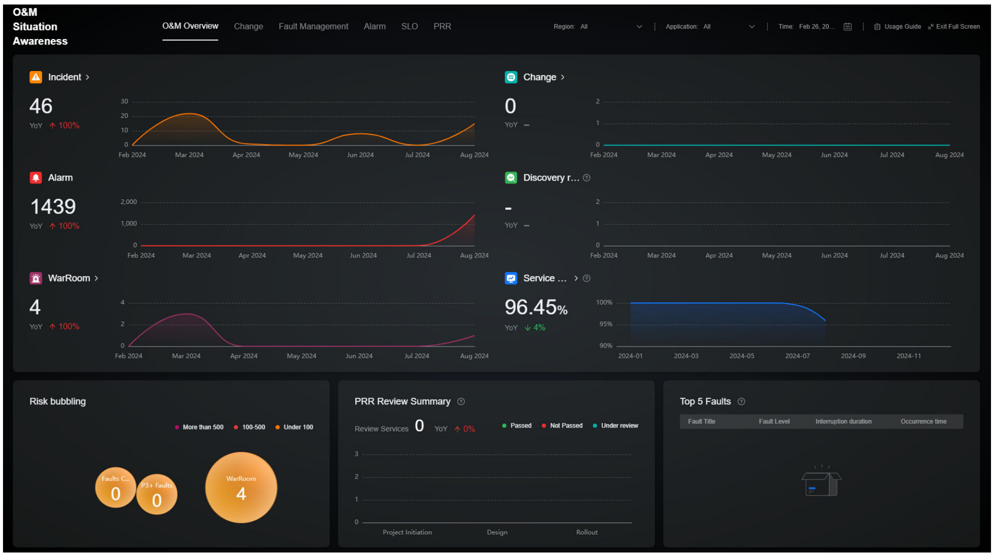


Table 2-1 Metrics in the O&M overview

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
	War Rooms	War rooms	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 2-16 Changes

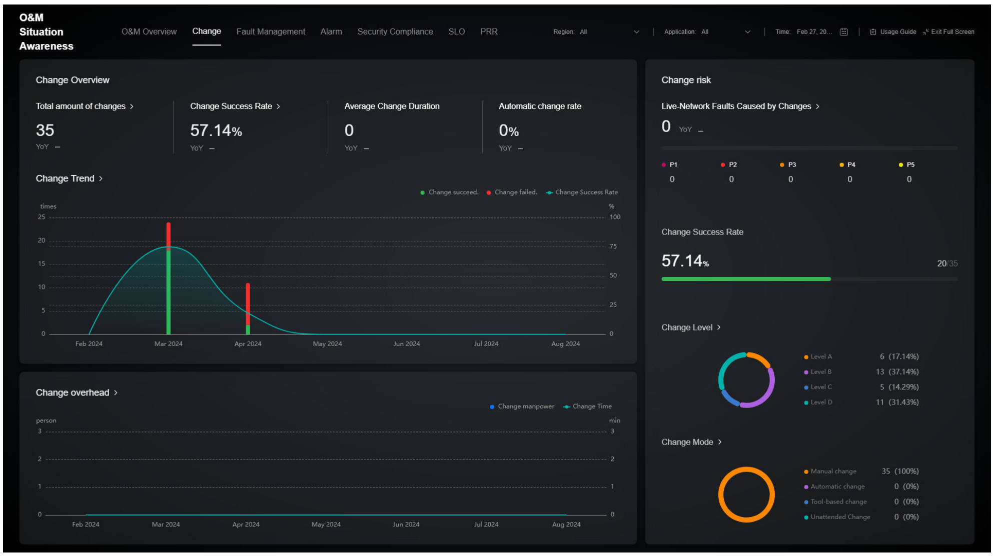

Region: All
Application: All
Time: Feb 27, 20...

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

Fault 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 2-17 Fault management

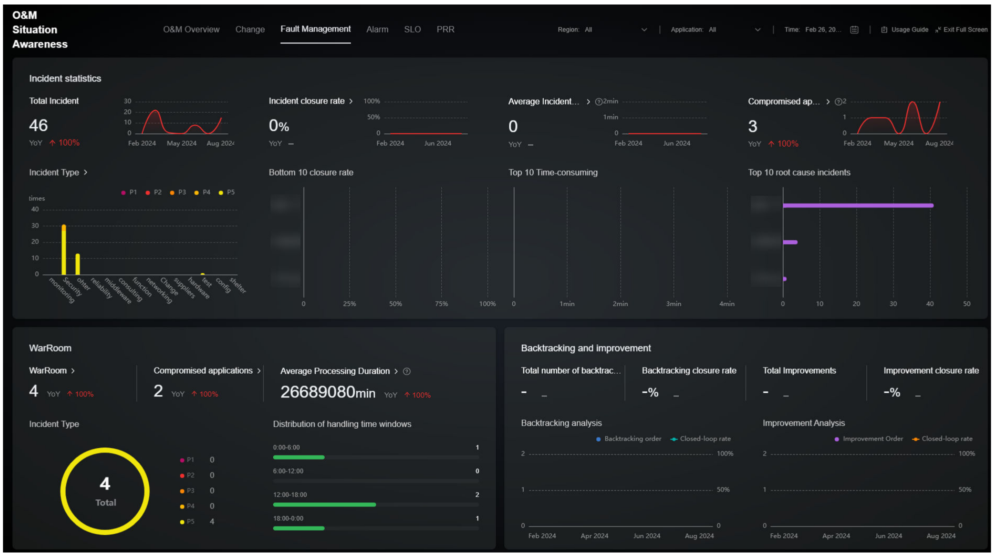


Table 2-3 Incident management data dictionary

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Incident statistics	Total Incidents	Incident management	Collects 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.	Collect the number of incident tickets of each type and level within a selected time range.	Day or month	Count
	Incident Closure Rate	Incident management	Collects the closure rate 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
War rooms	WarRoom Requests	War rooms	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 war room request.	Day or month	Count

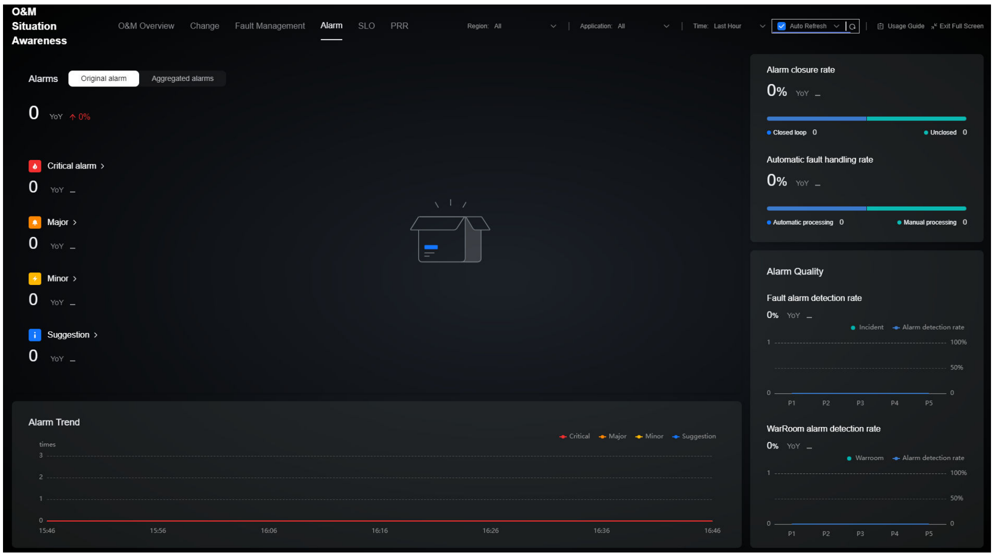
Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Affected Applications	War rooms	Collects the number of affected applications for a war room request.	Calculate the number of affected applications for a WarRoom request after deduplication.	Day or month	Count
	Average Recovery Duration	War rooms	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	War rooms	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 2-18 Monitoring and alerting



Region: All
Application: All
Time: Last Hour
☑ Auto Refresh

Table 2-4 Monitoring alarm data dictionary

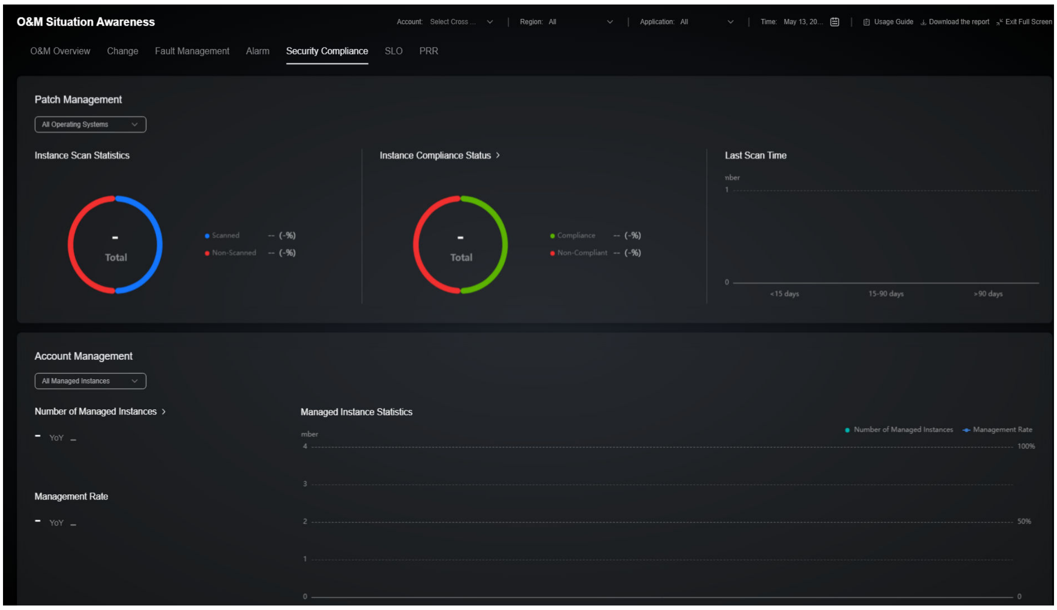
Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Alarm analysis	Alarms	Alarms	Collects the total number of alarms.	Collects the number of alarms generated in a selected period.	Day/Month	Count
	Alarm Severity	Alarms	Collects the number of alarms of each 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	War rooms	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

Security Compliance

The security compliance module includes statistics on the number of scanned patches and account management data (coming soon). Patch scanning allows you to view instance compliance data by region, application, and OS, and display the number of scanned instances by time range.

Figure 2-19 Security compliance



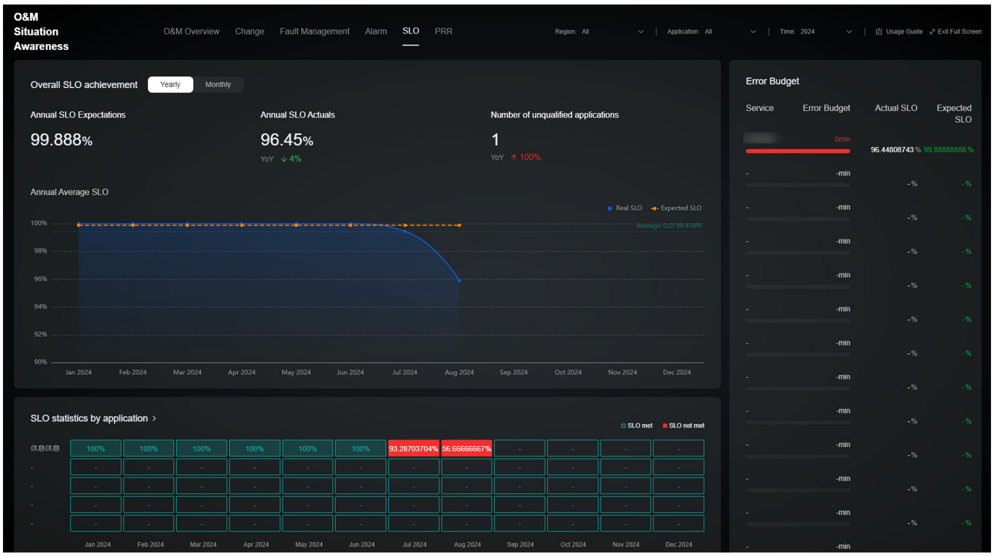
Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
Patch Management	Instance scanning status	Patch management/CloudCMDB	Number of ECSs where patches have been scanned and have not been scanned under a tenant account	Unscanned instances = Total instances – Scanned instances	Area and application	Count
	Instance compliance status	Patch management	Number of compliant and non-compliant instances in the scanned instances	Collects statistics on the number of instances in each compliance status in patch management.	Area and application	Count
	Last Scan Time	Patch management	Collect statistics on the latest scanning time range of scanned instances.	Collect statistics on the latest scanning time range of scanned instances.	Area and application	Count
Account Management	Managed Instances	Account Management	Number of managed cloud service instances in account management	Number of managed cloud service instances in account management	Area and application	Count
	Management Rate	Account management	Proportion of the managed cloud service instances to all instances	Management rate = Number of managed instances/Total number of instances x 100%	Area and application	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Managed Instance Statistics	Account management	This metric displays the instance management trend by time period.	This metric displays the instance management trend by time period.	Area and application	-

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 2-20 SLO dashboard



Annual SLO Expectations: 99.888%

Annual SLO Actuals: 96.45% YoY ↓ 4%

Number of unqualified applications: 1 YoY ↑ 100%

	Jan 2024	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024	Jul 2024	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024
休息休息	100%	100%	100%	100%	100%	100%	93.28703704%	56.66666667%	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-

Service	Error Budget	Actual SLO	Expected SLO
[redacted]	0min	96.44808743 %	99.88888888 %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min	- %	- %
-	-min		

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	Collects the actual SLO achievement of an application in a year.	Actual SLO value in a year = 1 – (Annual service unavailability duration/Total application duration in a year) 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	Collects the expected SLO achievement of an application in a month.	Expected SLO value = Expected SLO value set in the SLO management module Expected SLO value of multiple applications = Average expected SLO value of applications	Day or month	%

Module	Metric	Data Source	Metric Definition	Calculation Rule	Statistical Period	Measurement Unit
	Monthly Actual SLO Value	SLO management	Collects the actual SLO achievement in a month.	Actual SLO value in a month = 1 – (Monthly service unavailability duration/Total service duration in a month) 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 2-21 PRR dashboard

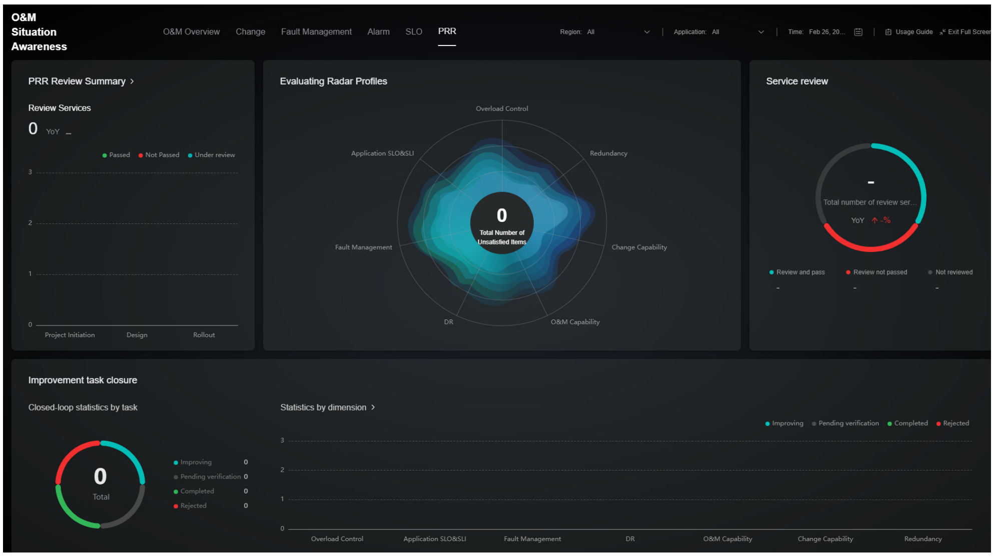


Table 2-6 PRR dashboard data dictionary

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

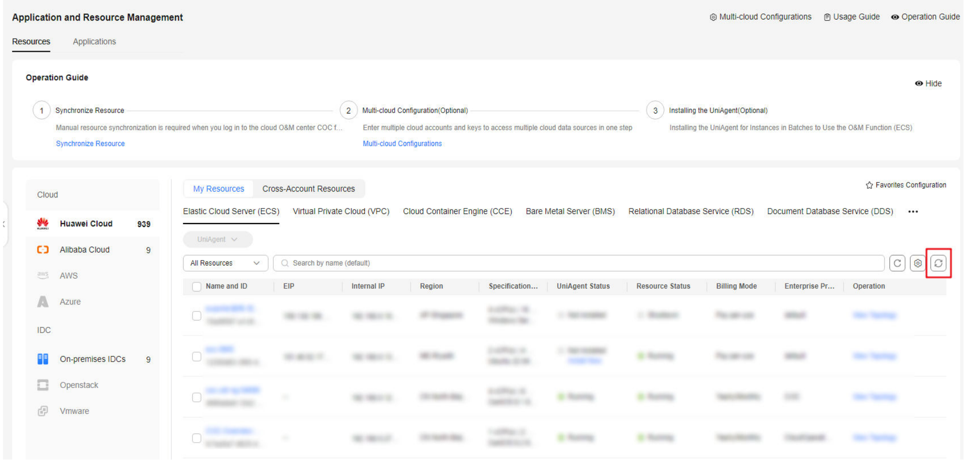
After resource synchronization is triggered, wait until the synchronization task is executed. The synchronization duration depends on the total amount of resource data to be synchronized.

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



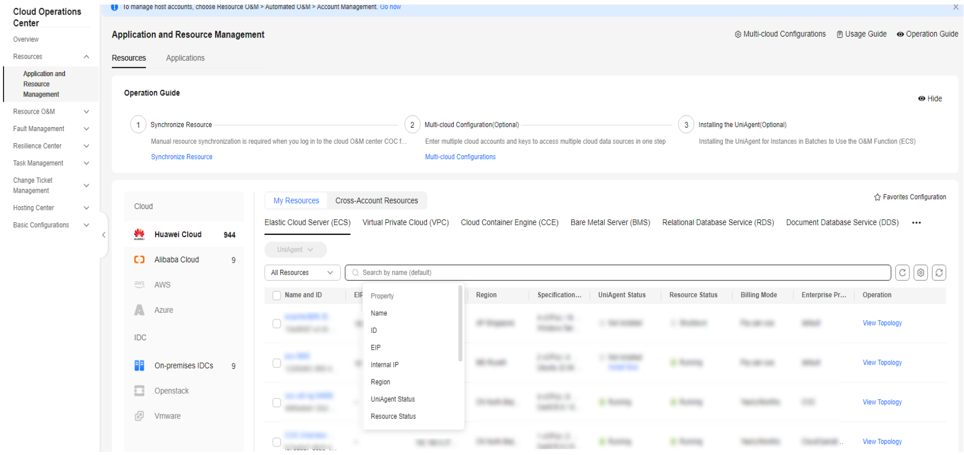
Manual resource synchronization is required when you log in to the cloud O&M center COC f...

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

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

Figure 3-2 Filtering resources



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

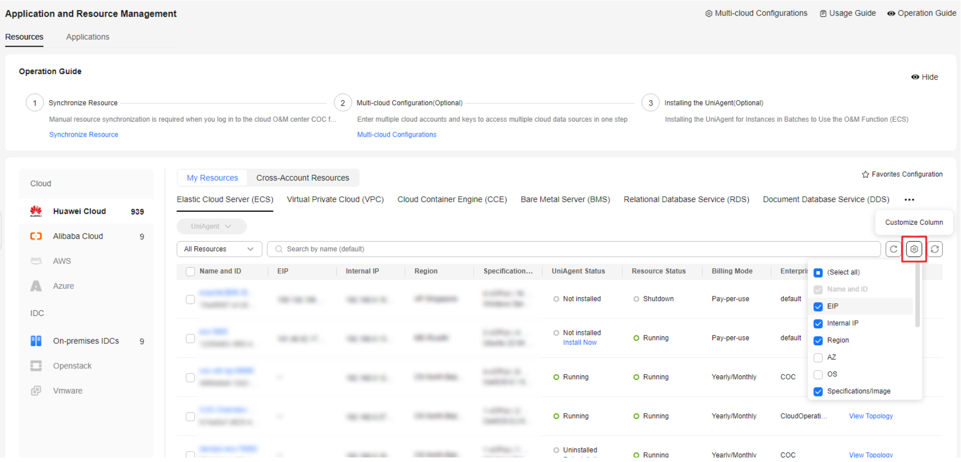
Manual resource synchronization is required when you log in to the cloud O&M center COC f...

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Step 4 Click ⚙ to select the columns to display.

Figure 3-3 Column display control



Manual resource synchronization is required when you log in to the cloud O&M center COC f...

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

----End

3.1.2 Configuring a UniAgent

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

Scenarios

Install, reinstall, and upgrade, unstall, and synchronize status of a UniAgent on and uninstall a UniAgent from corresponding nodes on COC.

Precautions

- Currently, you can only perform operations on UniAgent for ECSs.
- OS usage restrictions

Table 3-1 Linux operating systems and versions supported by a UniAgent

OS	Version				
Euler OS	1.1 64bit	2.0 64bit			
CentOS	7.1 64bit	7.2 64bit	7.3 64bit	7.4 64bit	7.5 64bit
	7.6 64bit	7.7 64bit	7.8 64bit	7.9 64bit	8.0 64bit
Ubuntu	16.04 server 64bit	18.04 server 64bit	20.04 server 64bit	22.04 server 64bit	

NOTE

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

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**.

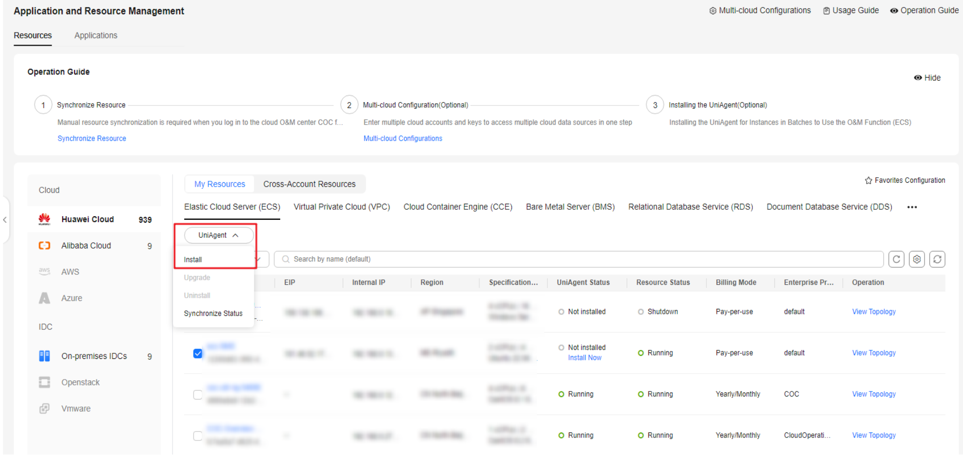


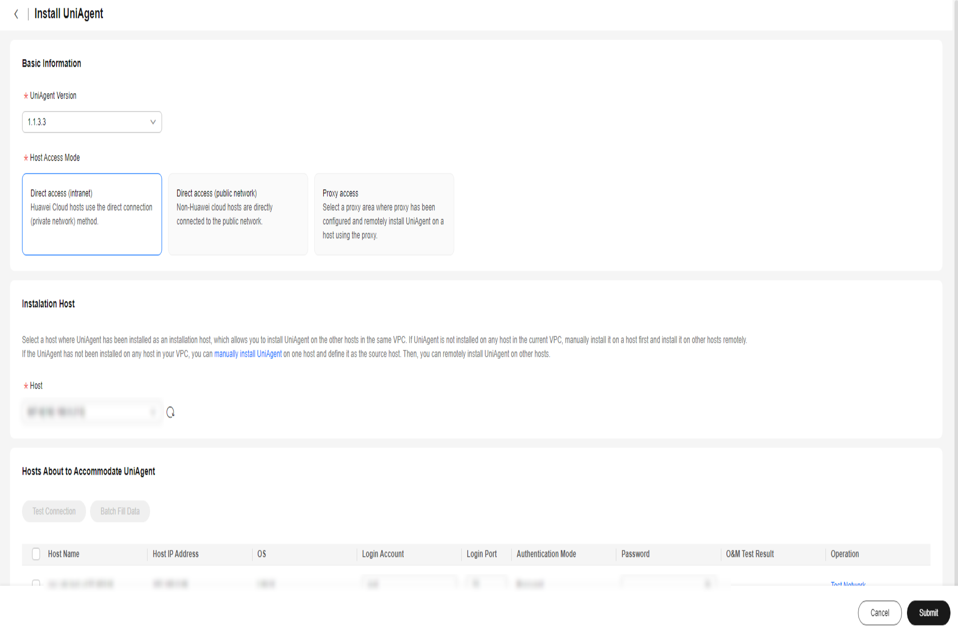
Figure 3-4 Installing a UniAgent

NOTE

When installing a UniAgent for ECSs in the same VPC, you need to manually install a UniAgent for the first ECS and set this ECS as the installation node. For details, see **Installing a UniAgent for the First Time**.

Step 3 On the displayed **Install UniAgent** page, specify required information by referring to **Table 3-2** and click **Submit** to trigger the automated installation process. Wait until the installation is complete.

Figure 3-5 Setting parameters



Install UniAgent

Basic Information

* UniAgent Version

1.1.3.3

* Host Access Mode

Direct access (intranet)
Huawei Cloud hosts use the direct connection (private network) method.

Direct access (public network)
Non-Huawei cloud hosts are directly connected to the public network.

Proxy access
Select a proxy area where proxy has been configured and remotely install UniAgent on a host using the proxy.

Instalation Host

Select a host where UniAgent has been installed as an installation host, which allows you to install UniAgent on the other hosts in the same VPC. If UniAgent is not installed on any host in the current VPC, manually install it on a host first and install it on other hosts remotely.
If the UniAgent has not been installed on any host in your VPC, you can manually install UniAgent on one host and define it as the source host. Then, you can remotely install UniAgent on other hosts.

* Host

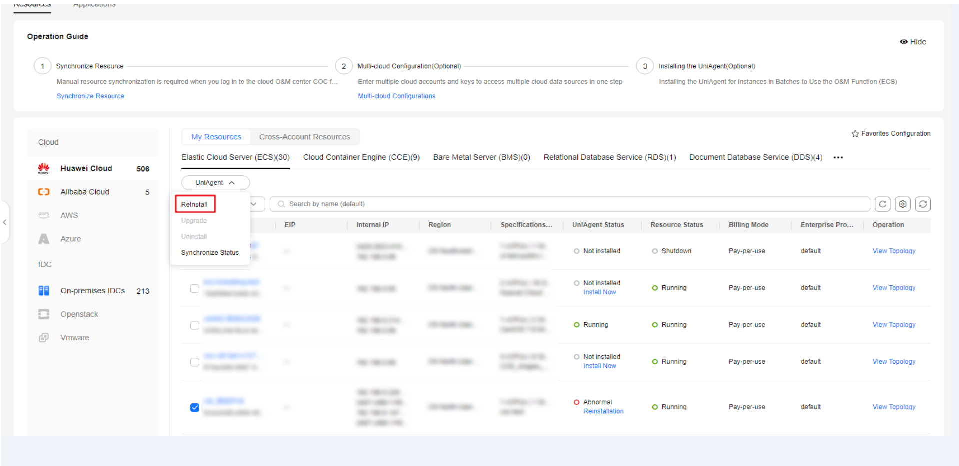
[redacted]

Hosts About to Accommodate UniAgent

□ Host Name	Host IP Address	OS	Login Account	Login Port	Authentication Mode	Password	O&M Test Result	Operation

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 **Uninstalled**, and choose **UniAgent** > **Reinstall**. For an instance whose UniAgent status is uninstalled, locate the instance, and click **Reinstall** in the **UniAgent Status** column.

Figure 3-6 Reinstalling a UniAgent



Operation Guide

1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC f...
Synchronize Resource

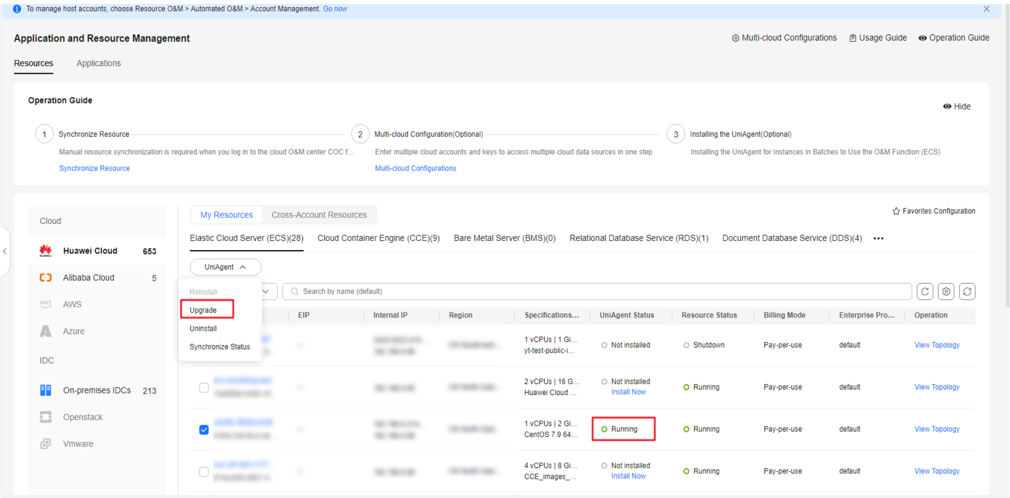
2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud data sources in one step
Multi-cloud Configurations

3 Installing the UniAgent(Optional)
Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

	EIP	Internal IP	Region	Specifications...	UniAgent Status	Resource Status	Billing Mode	Enterprise Pro...	Operation
[redacted]	-	[redacted]	[redacted]	[redacted]	○ Not installed	○ Shutdown	Pay-per-use	default	View Topology
□ [redacted]	-	[redacted]	[redacted]	[redacted]	○ Not installed Install Now	○ Running	Pay-per-use	default	View Topology
□ [redacted]	-	[redacted]	[redacted]	[redacted]	○ Running	○ Running	Pay-per-use	default	View Topology
□ [redacted]	-	[redacted]	[redacted]	[redacted]	○ Not installed Install Now	○ Running	Pay-per-use	default	View Topology
☑ [redacted]	-	[redacted]	[redacted]	[redacted]	○ Abnormal Reinstallation	○ Running	Pay-per-use	default	View Topology

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



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

Application and Resource Management

Operation Guide

1 Synchronize Resource — Manual resource synchronization is required when you log in to the cloud O&M center COC f... Synchronize Resource

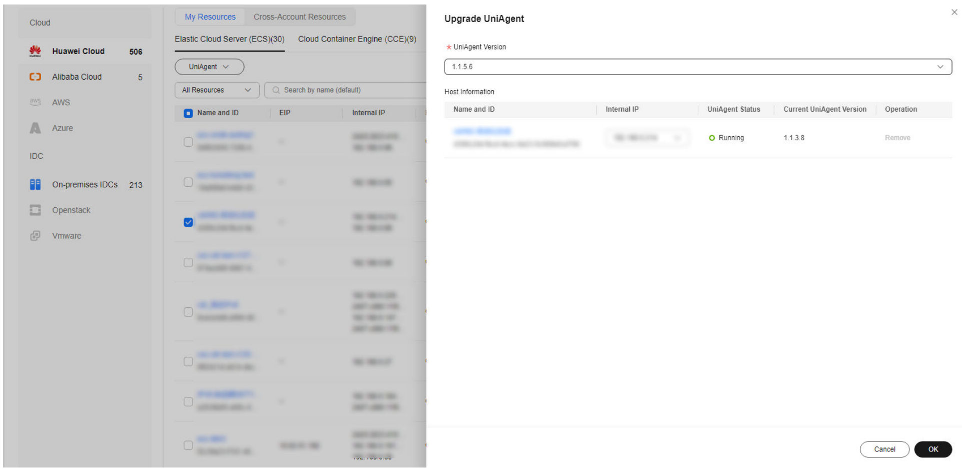
2 Multi-cloud Configuration(Optional) — Enter multiple cloud accounts and keys to access multiple cloud data sources in one step. Multi-cloud Configurations

3 Installing the UniAgent(Optional) — Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

	EIP	Internal IP	Region	Specifications...	UniAgent Status	Resource Status	Billing Mode	Enterprise Pro...	Operation
[illegible]	-	[illegible]	[illegible]	1 vCPUs | 1 Gi... yt-test-public-i...	○ Not installed	○ Shutdown	Pay-per-use	default	View Topology
□ [illegible]	-	[illegible]	[illegible]	2 vCPUs | 16 G... Huawei Cloud ...	○ Not installed Install Now	○ Running	Pay-per-use	default	View Topology
☑ [illegible]	-	[illegible]	[illegible]	1 vCPUs | 2 Gi... CentOS 7.9 64...	○ Running	○ Running	Pay-per-use	default	View Topology
□ [illegible]	-	[illegible]	[illegible]	4 vCPUs | 8 Gi... CCE_images_...	○ Not installed Install Now	○ Running	Pay-per-use	default	View Topology

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



Upgrade UniAgent

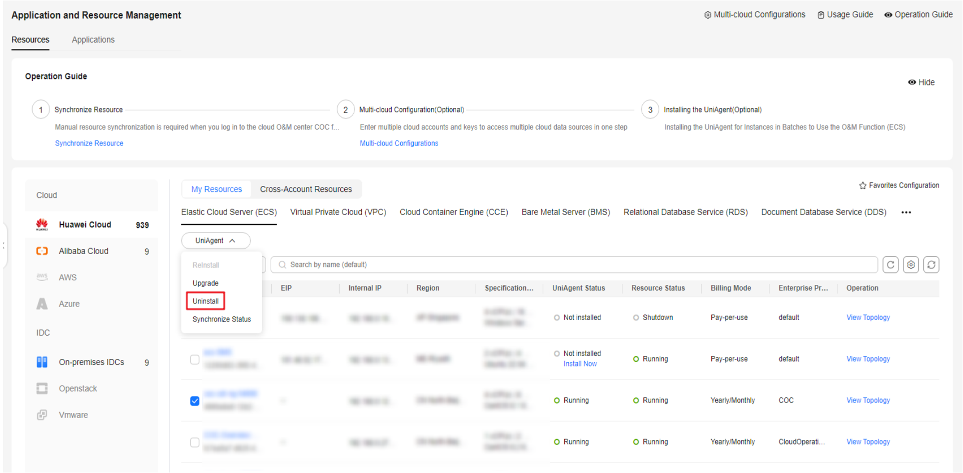
* UniAgent Version: 1.1.5.6

Host Information

Name and ID	Internal IP	UniAgent Status	Current UniAgent Version	Operation
[illegible]	[illegible]	○ Running	1.1.3.8	Remove

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.

Step 9 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** > **Synchronize Status**.

Figure 3-10 Status synchronization

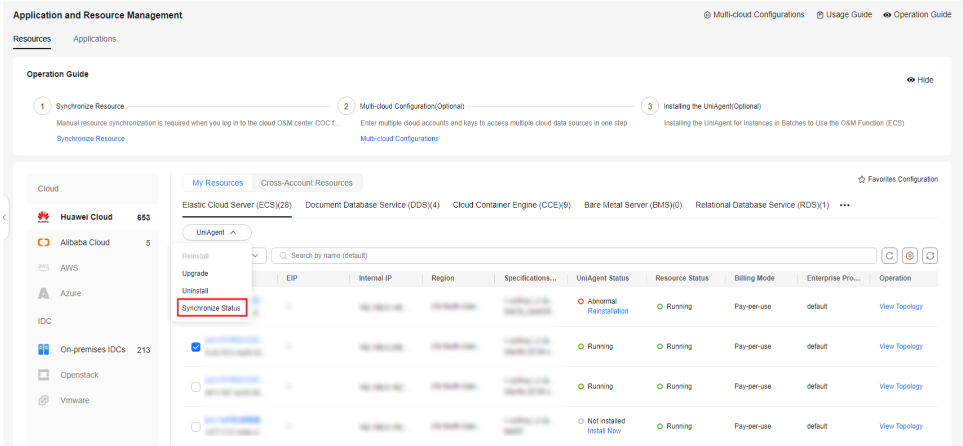


Table 3-2 UniAgent parameters

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

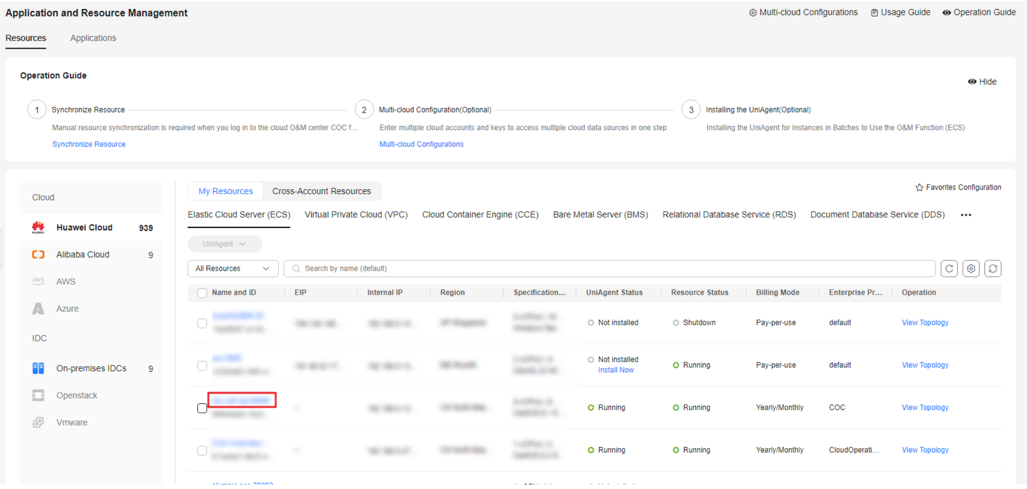
View resource details on COC.

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, locate the instances whose details you want to check and click the instance name.

Figure 3-11 Viewing details



1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC f...
Synchronize Resource

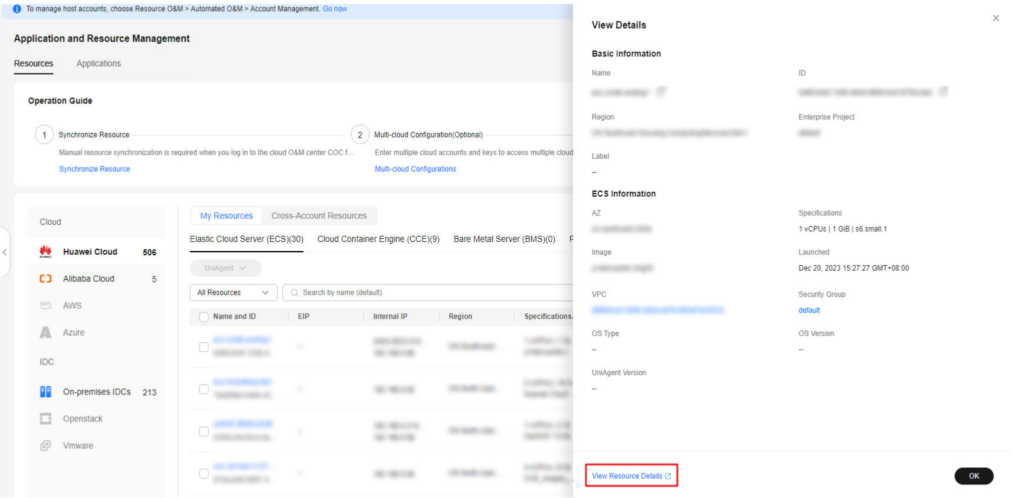
2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud data sources in one step
Multi-cloud Configurations

3 Installing the UniAgent(Optional)
Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Name and ID	EIP	Internal IP	Region	Specification...	UniAgent Status	Resource Status	Billing Mode	Enterprise Pr...	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Not installed	Shutdown	Pay-per-use	default	View Topology
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Not installed Install Now	Running	Pay-per-use	default	View Topology
[redacted]	--	[redacted]	[redacted]	[redacted]	Running	Running	Yearly/Monthly	COC	View Topology
[redacted]	--	[redacted]	[redacted]	[redacted]	Running	Running	Yearly/Monthly	CloudOperati...	View Topology

Step 3 In the drawer that is displayed on the right, click **View Resource Details** in the lower left part to go to the resource details page.

Figure 3-12 Resource details



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC f...
Synchronize Resource

2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud
Multi-cloud Configurations

View Details

Basic Information

Name: [redacted]
ID: [redacted]
Region: [redacted]
Enterprise Project: [redacted]
Label: --

ECS Information

AZ: [redacted]
Specifications: 1 vCPUs | 1 GiB | s6.small.1
Image: [redacted]
Launched: Dec 20, 2023 15:27:27 GMT+08:00
VPC: [redacted]
Security Group: default
OS Type: --
OS Version: --
UniAgent Version: --

----End

3.1.4 Viewing Resource Topologies

You can view resource topologies.

Scenarios

View resource topologies on COC.

Precautions

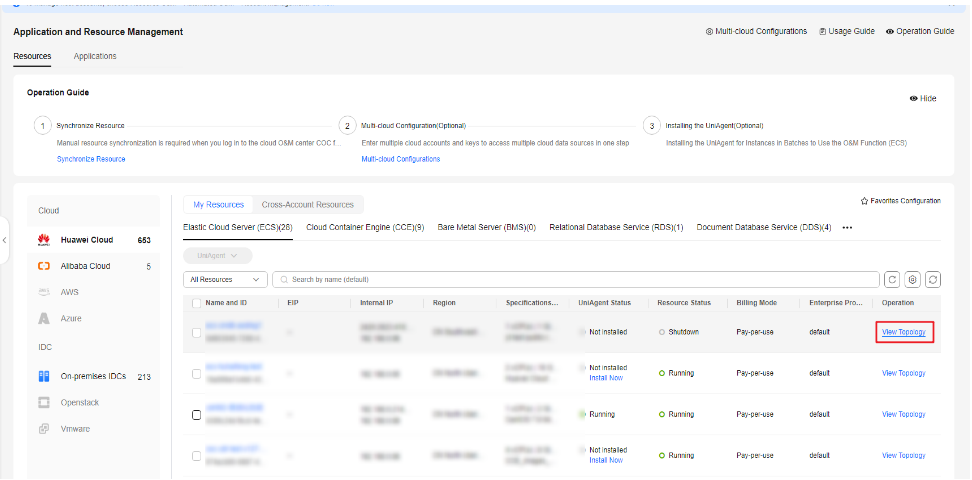
Currently, only the topologies of instances of Elastic Cloud Servers (ECS), MapReduce Services (MRS) instance, Bare Metal Server (BMS), and Cloud Container Engine (CCE) can be viewed.

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 3-13 Viewing resource topologies



Application and Resource Management

⚙ Multi-cloud Configurations   Usage Guide   Operation Guide

Resources   Applications

Operation Guide   Hide

1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC f...
Synchronize Resource

2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud data sources in one step
Multi-cloud Configurations

3 Installing the UniAgent(Optional)
Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Cloud	
Huawei Cloud	653
Alibaba Cloud	5
AWS	
Azure	
IDC	
On-premises IDCs	213
Openstack	
Vmware	

My Resources   Cross-Account Resources   ☆ Favorites Configuration

Elastic Cloud Server (ECS)(28)   Cloud Container Engine (CCE)(9)   Bare Metal Server (BMS)(0)   Relational Database Service (RDS)(1)   Document Database Service (DDS)(4)   •••

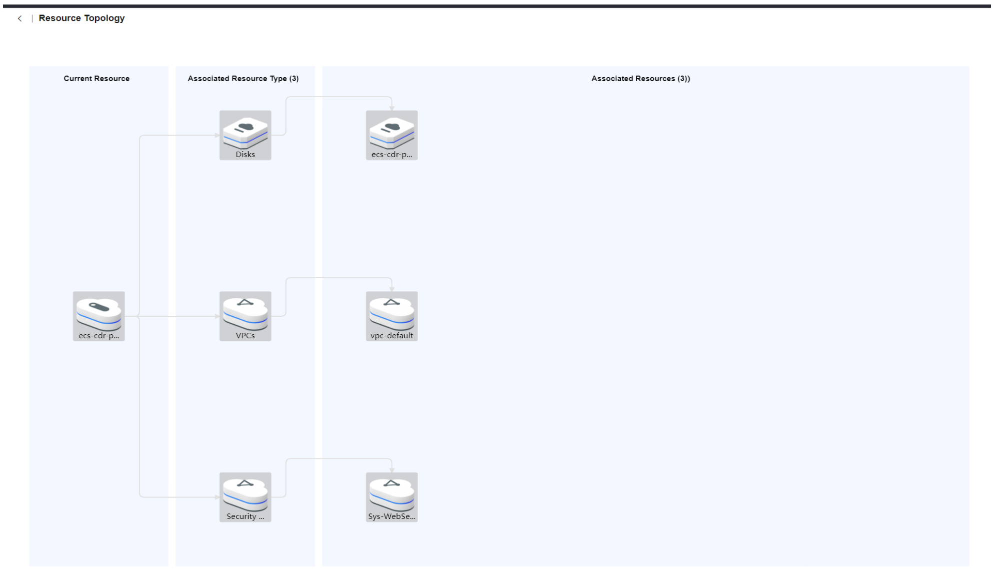
UniAgent ⌄

All Resources ⌄   Search by name (default)

□ Name and ID	EIP	Internal IP	Region	Specifications...	UniAgent Status	Resource Status	Billing Mode	Enterprise Pro...	Operation
□ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Not installed	○ Shutdown	Pay-per-use	default	View Topology
□ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Not installed Install Now	○ Running	Pay-per-use	default	View Topology
□ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Running	○ Running	Pay-per-use	default	View Topology
□ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Not installed Install Now	○ Running	Pay-per-use	default	View Topology

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

Figure 3-14 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 application.

Scenarios

Create an application on COC.

Precautions

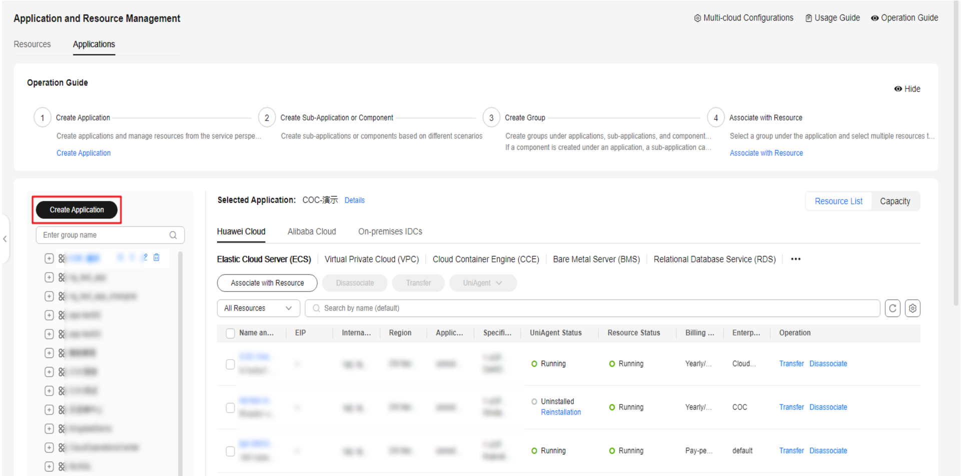
An application cannot contain both sub-applications and components.

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**.

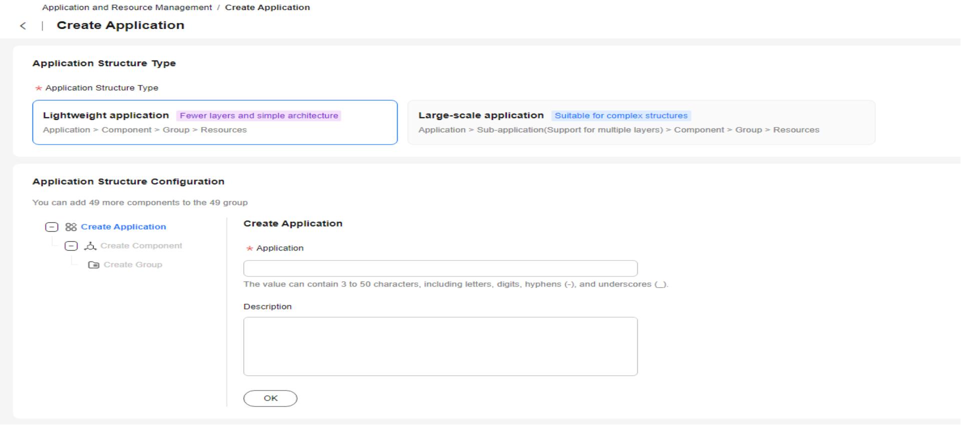
Figure 3-15 Creating an application


Application and Resource Management
Multi-cloud Configurations
Usage Guide
Operation Guide
Resources
Applications
Operation Guide
Hide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios
3 Create Group
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
Selected Application: COC-演示 Details
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)
Virtual Private Cloud (VPC)
Cloud Container Engine (CCE)
Bare Metal Server (BMS)
Relational Database Service (RDS)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)

Name an...	EIP	Interna...	Region	Applic...	Specifi...	UniAgent Status	Resource Status	Billing ...	Enterp...	Operation
[illegible]	-	[illegible]	[illegible]	[illegible]	[illegible]	Running	Running	Yearly/...	Cloud...	Transfer Disassociate
[illegible]	-	[illegible]	[illegible]	[illegible]	[illegible]	Uninstalled Reinstallation	Running	Yearly/...	COC	Transfer Disassociate
[illegible]	-	[illegible]	[illegible]	[illegible]	[illegible]	Running	Running	Pay-pe...	default	Transfer Disassociate

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

Figure 3-16 Setting parameters



Application and Resource Management / Create Application

< | Create Application

Application Structure Type

* Application Structure Type

Lightweight application Fewer layers and simple architecture
Application > Component > Group > Resources

Large-scale application Suitable for complex structures
Application > Sub-application(Support for multiple layers) > Component > Group > Resources

Application Structure Configuration

You can add 49 more components to the 49 group

Create Application

* Application

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

Description

NOTE

Configure the mandatory fields of each level and click **Save**. Then, click **Create** to create an application.

Table 3-3 Parameters for creating an application

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.	-
Subapplication Name	(Mandatory for large-scale applications) In the **Basic Information** area, provide a user-defined sub-application name.	Test sub-application
Description	(Optional) In the **Basic Information** area, provide a description of the sub-application.	-
Component	(Mandatory) In the **Application Configuration** area, enter the name of the component you want to create.	Test Component
Group	(Mandatory) Group of the component you created. Enter a valid group name.	Test Group
Vendor	(Mandatory) Information about the vendor to which the group belongs.	/

Parameter	Description	Example Value
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
Region	(Mandatory) Region to which a group belongs.	/
Enterprise Project	(Mandatory) Enterprise project. This parameter is displayed when the resource association mode is intelligent association.	/
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
Associate APM Environment	(Optional) Configure the application, component, and environment of the APM service corresponding to the group. APM service performance information can be obtained through this field during fault diagnosis.	-

----End

3.2.2 Modifying an Application

You can modify an application to facilitate resource management by application.

Scenarios

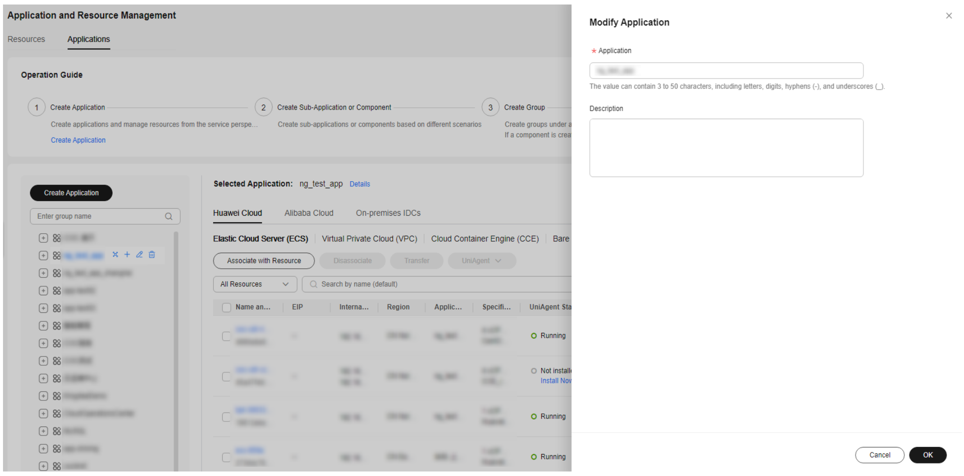
Modify an application on COC.

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 modify in the resource tree on the left, and click ✎.

Figure 3-17 Editing an application



Create applications and manage resources from the service perspe...

Create sub-applications or components based on different scenarios

Create groups under a
If a component is crea

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

Step 3 Set parameters in the **Modify Application** drawer by referring to **Table 3-4** and click **OK**.

Table 3-4 Parameters for modifying 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 an application to facilitate resource management by application.

Scenarios

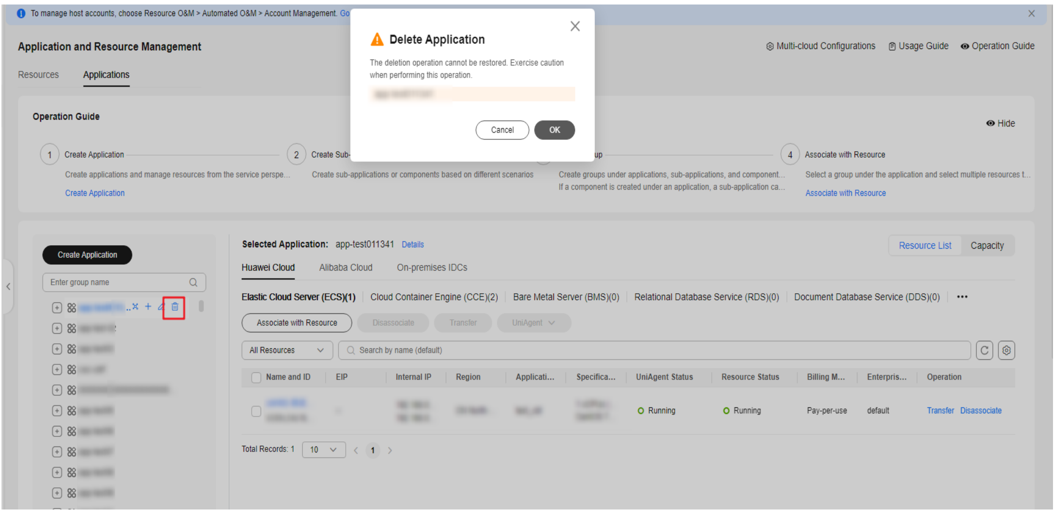
Delete an application on COC.

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 3-18 Deleting an application



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go

Delete Application

The deletion operation cannot be restored. Exercise caution when performing this operation.

[redacted]

Cancel OK

Selected Application: app-test011341 Details

Name and ID	EIP	Internal IP	Region	Applicati...	Specifica...	UniAgent Status	Resource Status	Billing M...	Enterpris...	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Running	Running	Pay-per-use	default	Transfer Disassociate

Total Records: 1

Application and Resource Management
Multi-cloud Configurations
Usage Guide
Operation Guide
Resources
Applications
Operation Guide
Hide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-
Create sub-applications or components based on different scenarios
up
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)(1)
Cloud Container Engine (CCE)(2)
Bare Metal Server (BMS)(0)
Relational Database Service (RDS)(0)
Document Database Service (DDS)(0)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
10
1

Step 3 Click **OK**.

----End

3.2.4 Editing an Application Topology

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

Scenarios

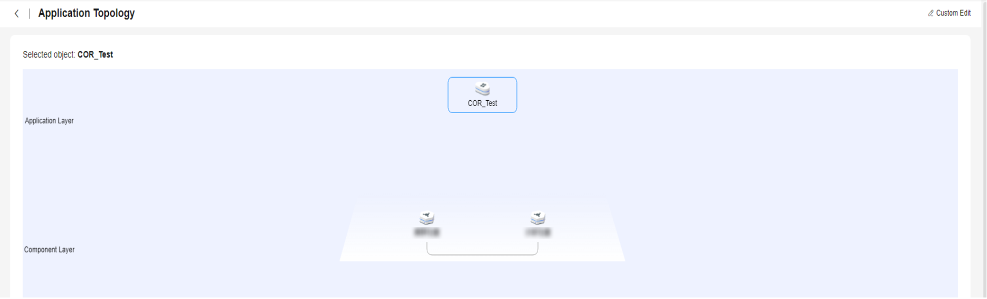
Check the application topology and edit the component invoking connections on COC.

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 ⌘.

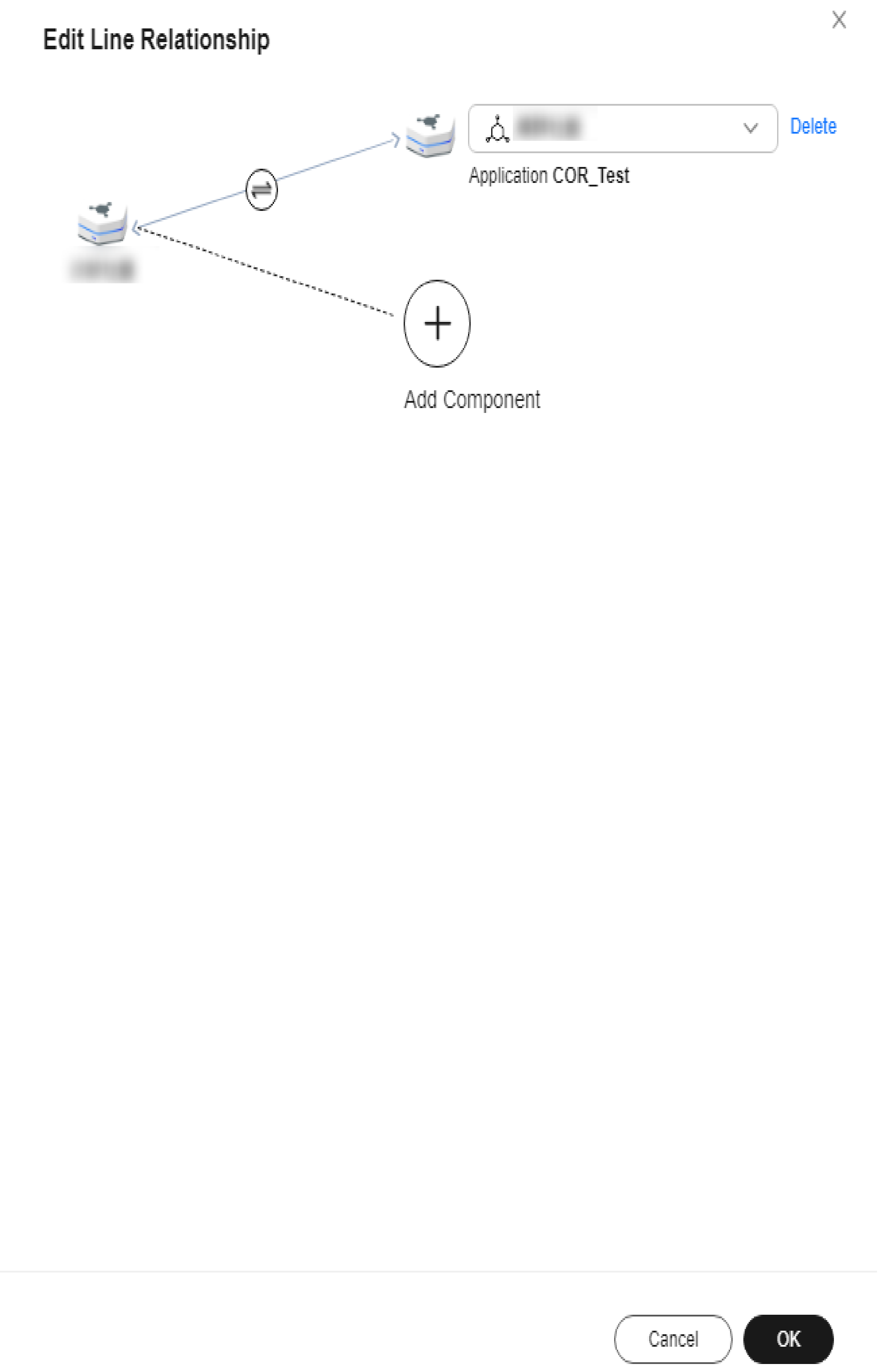
Figure 3-19 Application topology



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**.

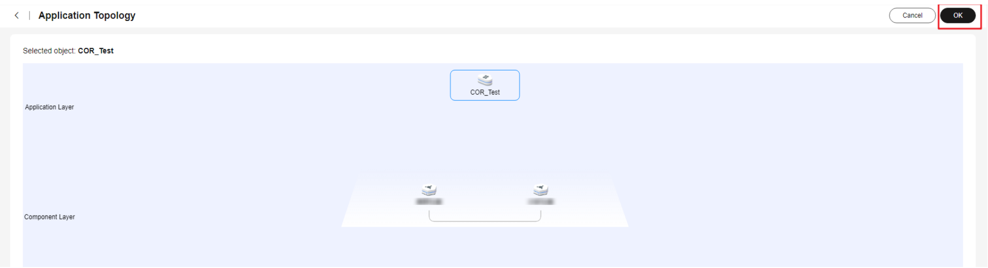
Figure 3-20 Editing component connections



Edit Line Relationship

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

Figure 3-21 Exiting the editing state.



Application Topology

Selected object: COR_Test

----End

3.2.5 Creating a Component

You can create a component to facilitate resource management by component.

Scenarios

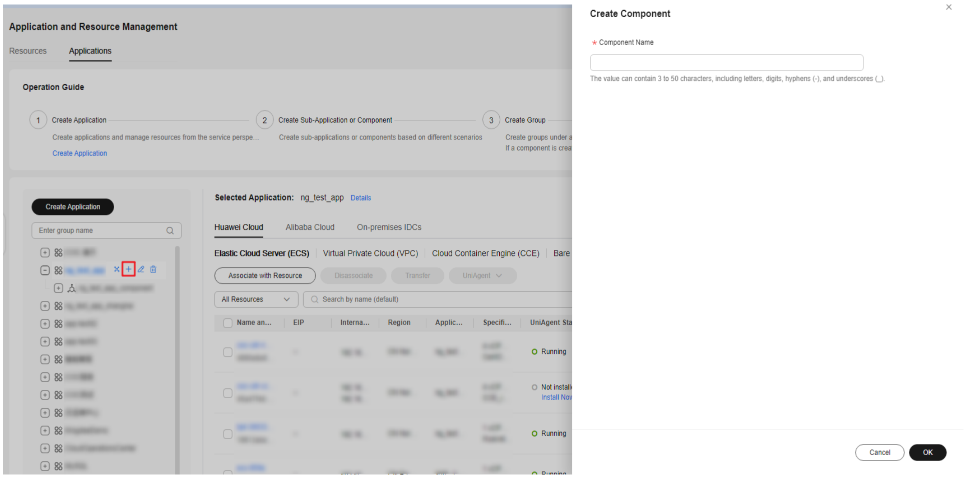
Create a component on COC.

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 3-22 Creating a component



Application and Resource Management

Operation Guide

1 Create Application: Create applications and manage resources from the service perspe...

2 Create Sub-Application or Component: Create sub-applications or components based on different scenarios

3 Create Group: Create groups under a
If a component is crea

Selected Application: ng_test_app Details

Create Component

* Component Name

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

Step 3 Set parameters in the **Create Sub-application/Component** drawer by referring to **Table 3-5** and click **OK**.

Table 3-5 Parameters for creating 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

3.2.6 Modifying a Component

You can modify a component to facilitate resource management by component.

Scenarios

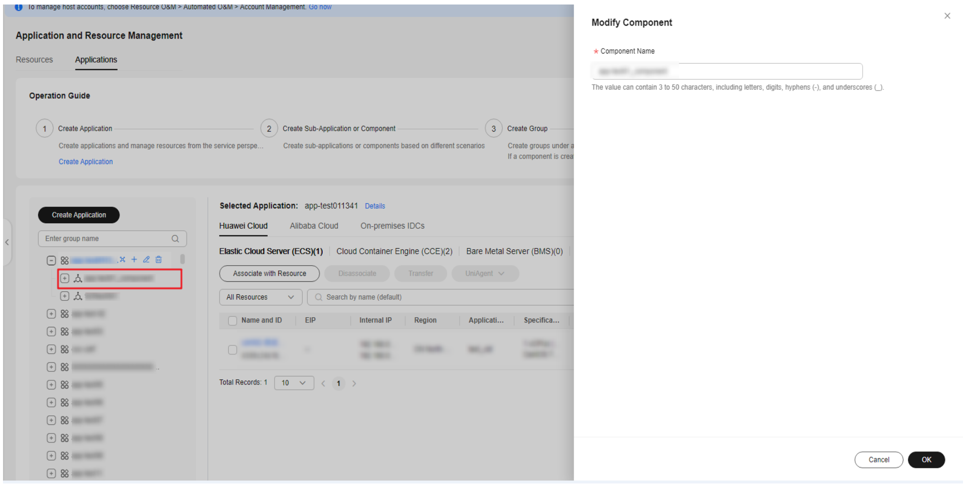
Modify a component on COC.

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 3-23 Editing a component



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

Create applications and manage resources from the service perspe...

Create sub-applications or components based on different scenarios

Create groups under a
If a component is crea

Selected Application: app-test011341

Total Records: 1

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

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

Table 3-6 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 Deleted a Component

You can delete a component to facilitate resource management by component.

Scenarios

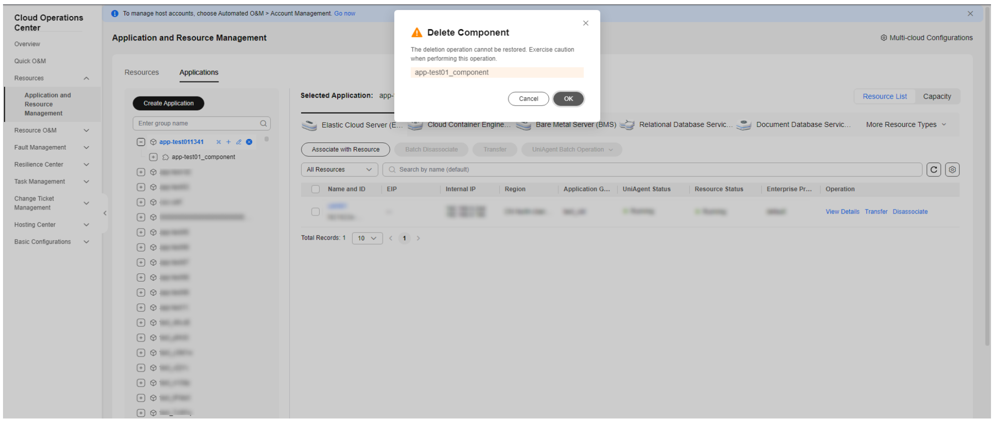
Delete a component on COC.

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 3-24 Deleted a component



Delete Component

The deletion operation cannot be restored. Exercise caution when performing this operation.

app-test01_component

Cancel OK

Step 3 Click **OK**.

----End

3.2.8 Creating a Group

You can create a group to facilitate resource management by group.

Scenarios

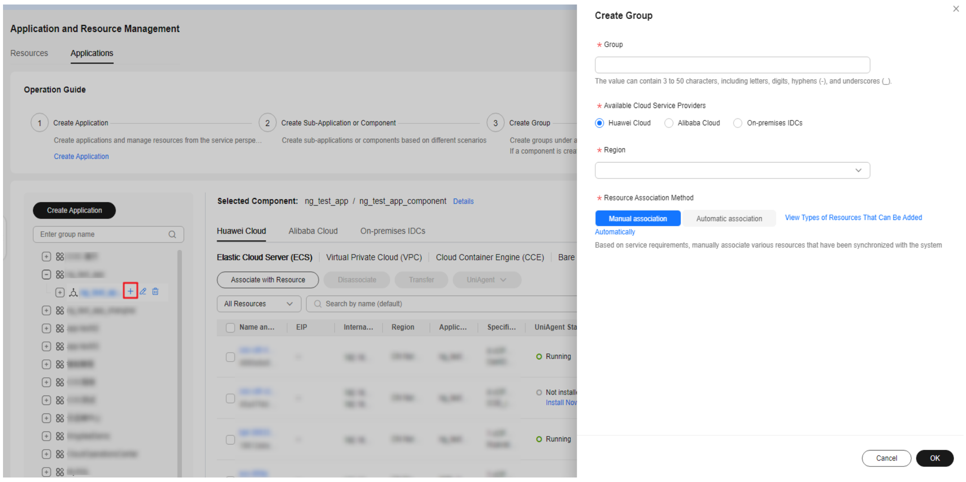
Create a group on COC.

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** tab, expand the target application, locate the component for which you want to create a group in the resource tree on the left, and click the plus sign (+) next to the component.

Figure 3-25 Creating a group



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

Available Cloud Service Providers: ● Huawei Cloud ○ Alibaba Cloud ○ On-premises IDCs

Resource Association Method: Manual association

Based on service requirements, manually associate various resources that have been synchronized with the system

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

Table 3-7 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
Vendor	(Mandatory) Information about the vendor to which the group belongs.	/
Region	(Mandatory) Region to which a group belongs.	/

Parameter	Description	Example Value
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
Enterprise Project	(Mandatory) Enterprise project. This parameter is displayed when the resource association mode is intelligent association.	/
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
Associate APM Environment	(Optional) Configure the application, component, and environment of the APM service corresponding to the group. APM service performance information can be obtained through this field during fault diagnosis.	/

----End

3.2.9 Modifying a Group

You can modify a group to facilitate resource management by group.

Scenarios

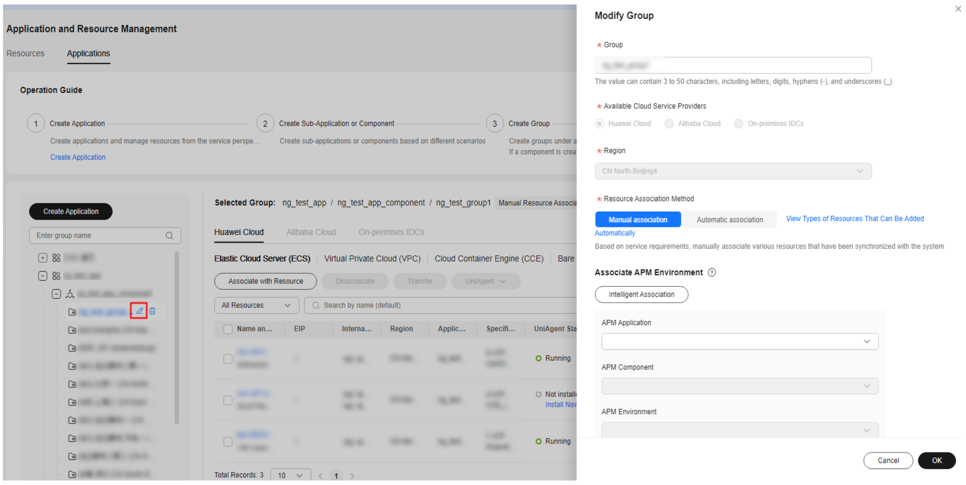
Modify a group on COC.

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 3-26 Modifying a group


Application and Resource Management
Resources
Applications
Operation Guide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios
3 Create Group
Create Application
Enter group name
Selected Group: ng_test_app / ng_test_app_component / ng_test_group1
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)
Virtual Private Cloud (VPC)
Cloud Container Engine (CCE)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Running
Not installed
Install Now
Running
Total Records: 3

Modify Group

* Group

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

* Available Cloud Service Providers

● Huawei Cloud ○ Alibaba Cloud ○ On-premises IDCs

* Region

CN North-Beijing4

* Resource Association Method

Manual association | Automatic association | View Types of Resources That Can Be Added Automatically

Based on service requirements, manually associate various resources that have been synchronized with the system

Associate APM Environment

Intelligent Association

APM Application

APM Component

APM Environment

Cancel OK

Step 3 Set parameters in the **Modify Group** drawer by referring to **Table 3-8** and click **OK**.

Table 3-8 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
Enterprise Project	(Mandatory) Enterprise project. This parameter is displayed when the resource association mode is intelligent association.	/
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

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

----End

3.2.10 Deleting a Group

You can delete a group to facilitate resource management by group.

Scenarios

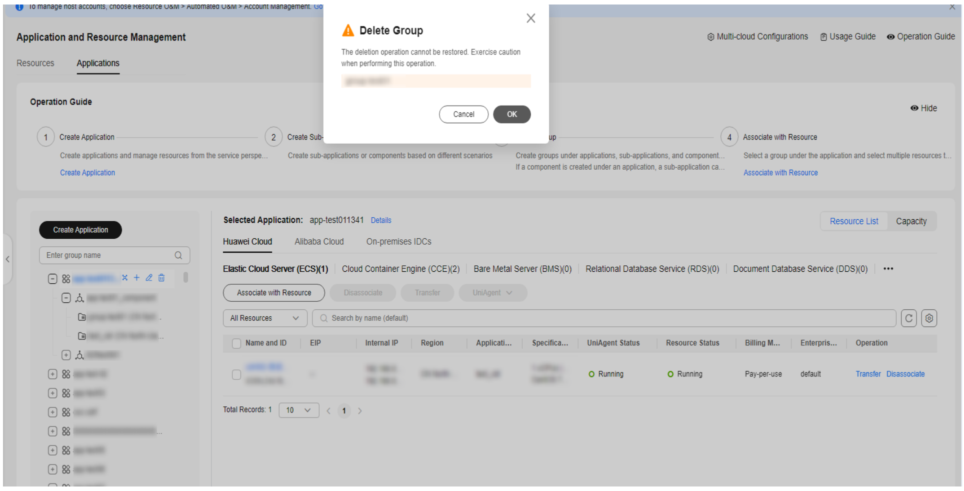
Delete a group on COC.

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 3-27 Deleting a group



Delete Group

The deletion operation cannot be restored. Exercise caution when performing this operation.

To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go
Application and Resource Management
Resources
Applications
Multi-cloud Configurations
Usage Guide
Operation Guide
Cancel
OK
Operation Guide
Hide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-
Create sub-applications or components based on different scenarios
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
Selected Application: app-test011341
Details
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)(1)
Cloud Container Engine (CCE)(2)
Bare Metal Server (BMS)(0)
Relational Database Service (RDS)(0)
Document Database Service (DDS)(0)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Name and ID
EIP
Internal IP
Region
Applicati...
Specifica...
UniAgent Status
Resource Status
Billing M...
Enterpris...
Operation
Running
Running
Pay-per-use
default
Transfer
Disassociate
Total Records: 1
10
1

Step 3 Click **OK**.

----End

3.2.11 Manually Associating Resources with a Group

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

Scenarios

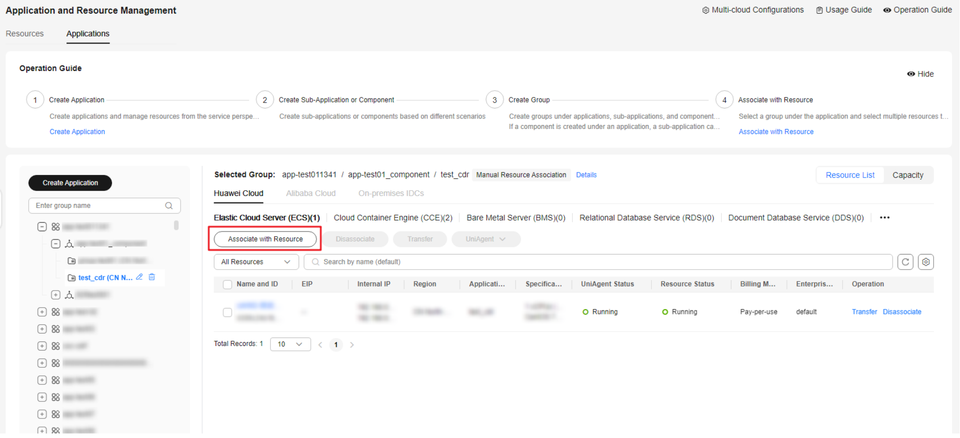
Associate resources with a specified application group.

Procedure

Step 1 Log in to COC.

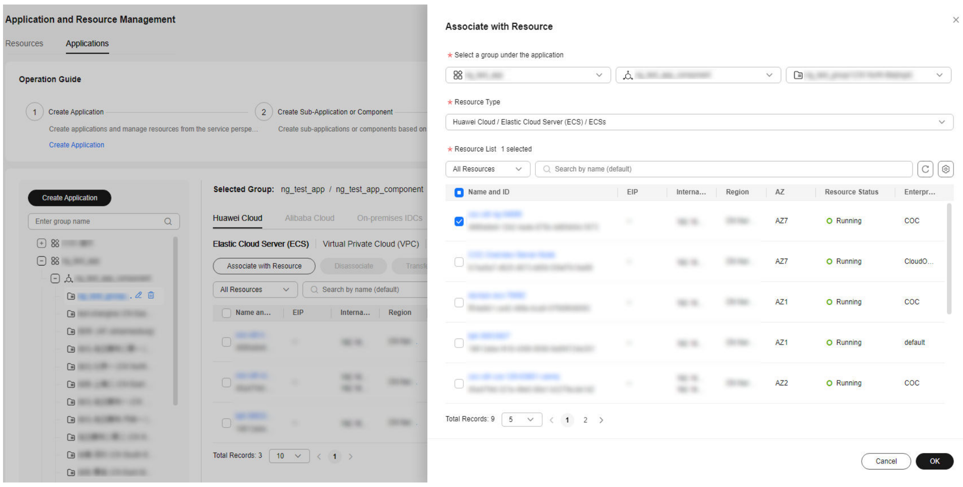
Step 2 In the navigation pane, choose **Resources > Application and Resource Management**. On the displayed page, click the **Applications** tab and click **Associate with Resource**.

Figure 3-28 Manually associating resources with a group


Application and Resource Management
Multi-cloud Configurations
Usage Guide
Operation Guide
Resources
Applications
Operation Guide
Hide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios
3 Create Group
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
test_cdr (CN N...
Selected Group: app-test011341 / app-test01_component / test_cdr
Manual Resource Association
Details
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)(1)
Cloud Container Engine (CCE)(2)
Bare Metal Server (BMS)(0)
Relational Database Service (RDS)(0)
Document Database Service (DDS)(0)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Name and ID
EIP
Internal IP
Region
Applicati...
Specifica...
UniAgent Status
Resource Status
Billing M...
Enterpris...
Operation
Running
Running
Pay-per-use
default
Transfer
Disassociate
Total Records: 1
10
1

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 3-29 Selecting the resources to be associated with the group



----End

3.2.12 Intelligently Associating Resources with a 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

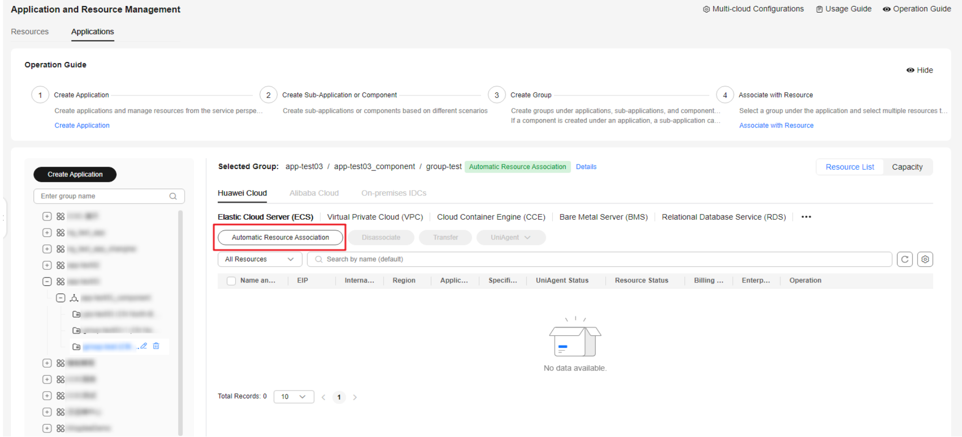
1. Only after you select a group and click the **Intelligent resource association** button above the resource list, can this operation take effect.
2. After intelligent resource association is triggered, wait until the synchronization task is executed. Time the association takes depends on the total 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 3-30 Intelligently associating resources with a group


Application and Resource Management
Multi-cloud Configurations
Usage Guide
Operation Guide
Resources
Applications
Operation Guide
Hide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios
3 Create Group
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
Selected Group: app-test03 / app-test03_component / group-test
Automatic Resource Association
Details
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)
Virtual Private Cloud (VPC)
Cloud Container Engine (CCE)
Bare Metal Server (BMS)
Relational Database Service (RDS)
•••
Automatic Resource Association
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Name an...
EIP
Interna...
Region
Applic...
Specifi...
UniAgent Status
Resource Status
Billing ...
Enterp...
Operation
No data available.
Total Records: 0
10
1

----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

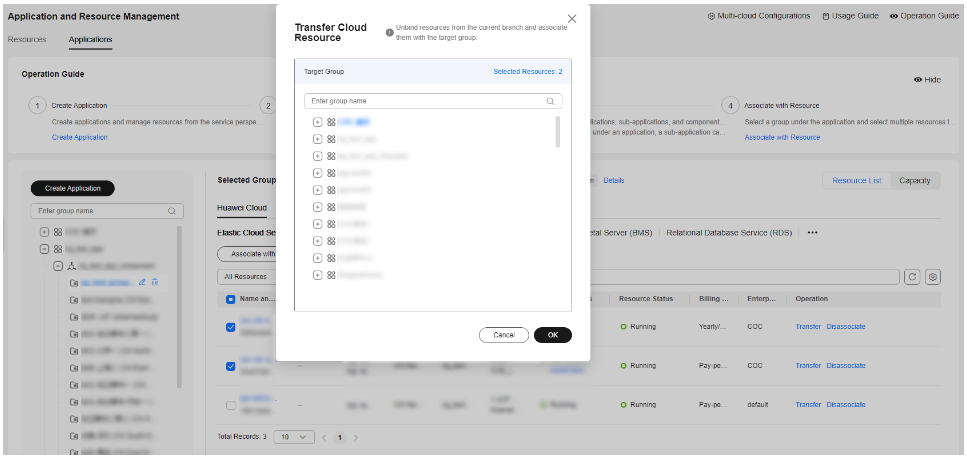
Resources can be transferred to application groups only when they belong to the same enterprise project as the application.

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 3-31 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

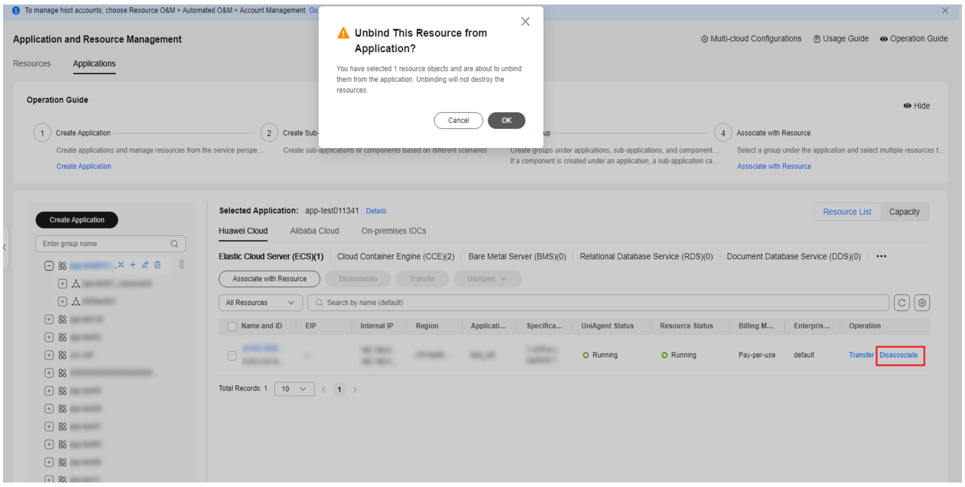
Disassociate resources from groups on COC

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 3-32 Disassociating a resource from a group



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go
Application and Resource Management
Resources
Applications
Multi-cloud Configurations
Usage Guide
Operation Guide
Operation Guide
Hide
Create Application
Create applications and manage resources from the service perspe...
Create Application
Create Sub-
Create sub-applications or components based on different scenarios
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...
Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource
Create Application
Enter group name
Selected Application: app-test011341
Details
Resource List
Capacity
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)(1)
Cloud Container Engine (CCE)(2)
Bare Metal Server (BMS)(0)
Relational Database Service (RDS)(0)
Document Database Service (DDS)(0)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Name and ID
EIP
Internal IP
Region
Applicati...
Specifica...
UniAgent Status
Resource Status
Billing M...
Enterpris...
Operation
Running
Running
Pay-per-use
default
Transfer
Disassociate
Total Records: 1
10

Unbind This Resource from Application?

You have selected 1 resource objects and are about to unbind them from the application. Unbinding will not destroy the resources.

Step 3 Click **OK**.

----End

3.2.15 Viewing Resource Details

You can view resource details.

Scenarios

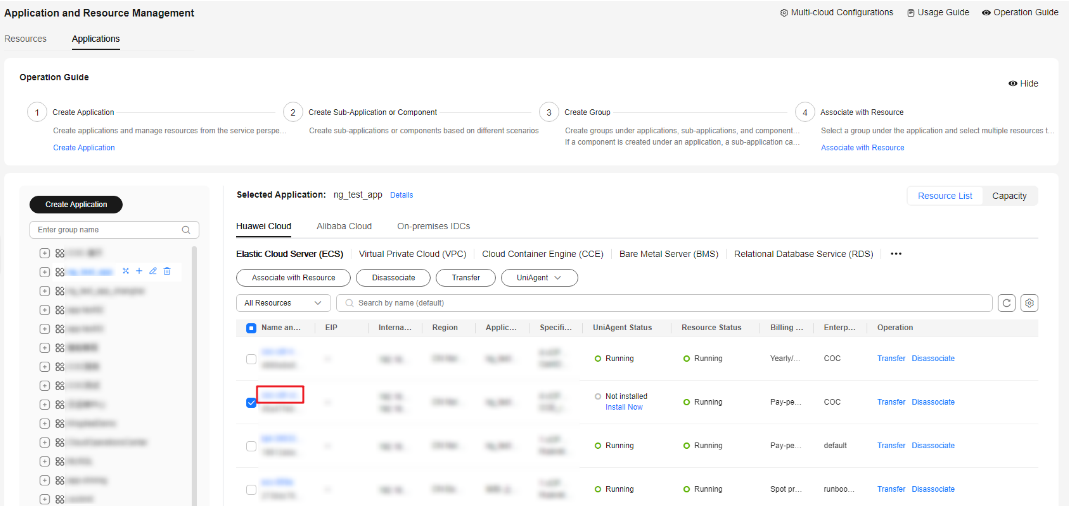
View details about resources associated with applications on COC.

Procedure

Step 1 Log in to **COC**.

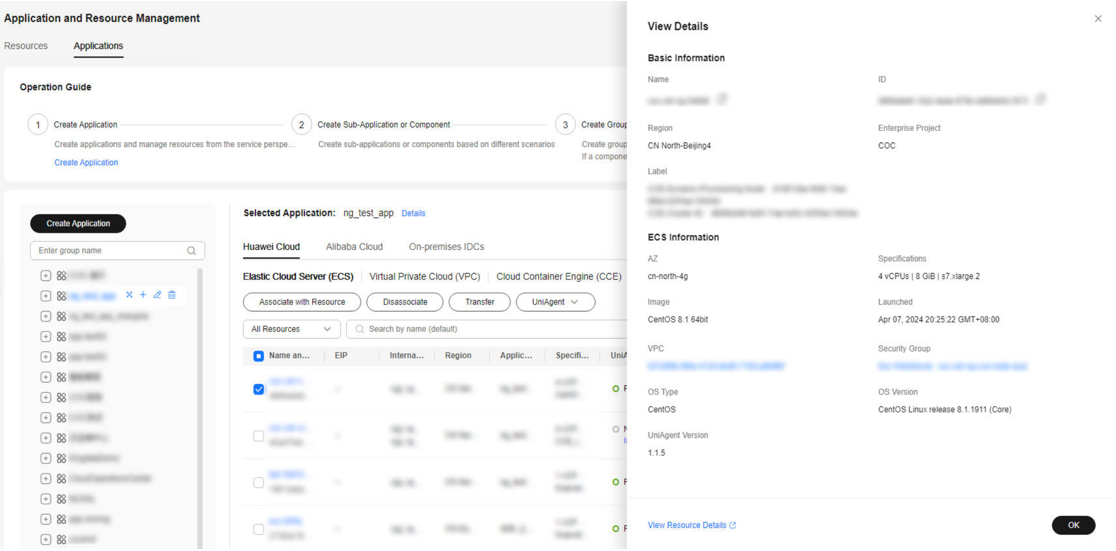
Step 2 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Applications** > **Elastic Cloud Server (ECS)** tab page, above the resource list, locate the ECSs whose details you want to check and click the instance name.

Figure 3-33 Viewing resource details



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

Figure 3-34 Resource details


Application and Resource Management
Resources
Applications
Operation Guide
1 Create Application
Create applications and manage resources from the service perspe...
Create Application
2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios
3 Create Group
Create group
If a compone
Create Application
Enter group name
Selected Application: ng_test_app Details
Huawei Cloud
Alibaba Cloud
On-premises IDCs
Elastic Cloud Server (ECS)
Virtual Private Cloud (VPC)
Cloud Container Engine (CCE)
Associate with Resource
Disassociate
Transfer
UniAgent
All Resources
Search by name (default)
Name an...
EIP
Interna...
Region
Applic...
Specifi...
UniA

View Details

Basic Information

Name: [redacted]

ID: [redacted]

Region: CN North-Beijing4

Enterprise Project: COC

Label: [redacted]

ECS Information

AZ: cn-north-4g

Specifications: 4 vCPUs | 8 GiB | s7.xlarge.2

Image: CentOS 8.1 64bit

Launched: Apr 07, 2024 20:25:22 GMT+08:00

VPC: [redacted]

Security Group: [redacted]

OS Type: CentOS

OS Version: CentOS Linux release 8.1.1911 (Core)

UniAgent Version: 1.1.5

----End

3.2.16 Viewing Capacity Rankings

You can view the capacity rankings of associated resources.

Scenarios

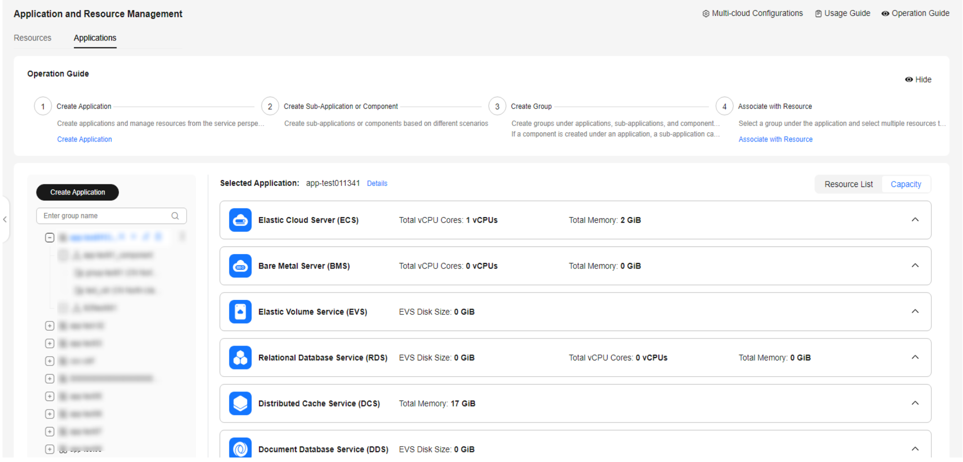
View the capacity rankings of associated resources on COC.

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 3-35 Viewing capacity rankings



Operation Guide

1 Create Application
Create applications and manage resources from the service perspe...
Create Application

2 Create Sub-Application or Component
Create sub-applications or components based on different scenarios

3 Create Group
Create groups under applications, sub-applications, and component...
If a component is created under an application, a sub-application ca...

4 Associate with Resource
Select a group under the application and select multiple resources t...
Associate with Resource

Selected Application: app-test011341 Details

Elastic Cloud Server (ECS) Total vCPU Cores: **1 vCPUs** Total Memory: **2 GiB**

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

Elastic Volume Service (EVS) EVS Disk Size: **0 GiB**

Relational Database Service (RDS) EVS Disk Size: **0 GiB** Total vCPU Cores: **0 vCPUs** Total Memory: **0 GiB**

Distributed Cache Service (DCS) Total Memory: **17 GiB**

Document Database Service (DDS) EVS Disk Size: **0 GiB**

----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

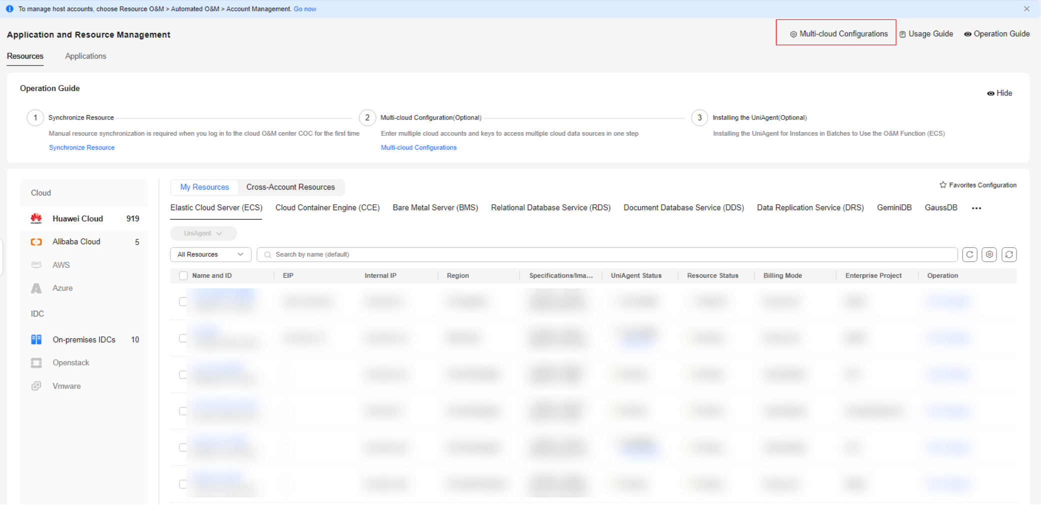
Currently, only Alibaba Cloud accounts can be created.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management**. On the displayed page, click **Multi-cloud Configurations**.

Figure 3-36 Multi-cloud Configurations



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

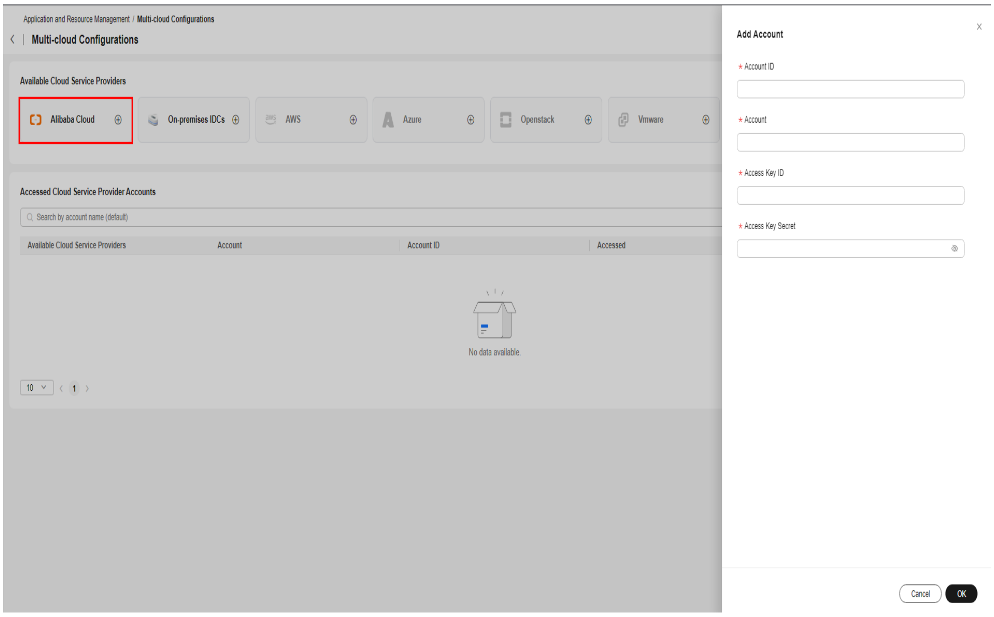
Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Step 3 On the **Multi-cloud Configurations** page, click the target cloud vendor.

Figure 3-37 Creating an account



Application and Resource Management / Multi-cloud Configurations
Multi-cloud Configurations
Available Cloud Service Providers
Alibaba Cloud
On-premises IDCs
AWS
Azure
Openstack
Vmware
Accessed Cloud Service Provider Accounts
Search by account name (default)
Available Cloud Service Providers
Account
Account ID
Accessed
No data available.
10
1
Add Account
* Account ID
* Account
* Access Key ID
* Access Key Secret
Cancel
OK

Step 4 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.	-

Parameter	Description	Example Value
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

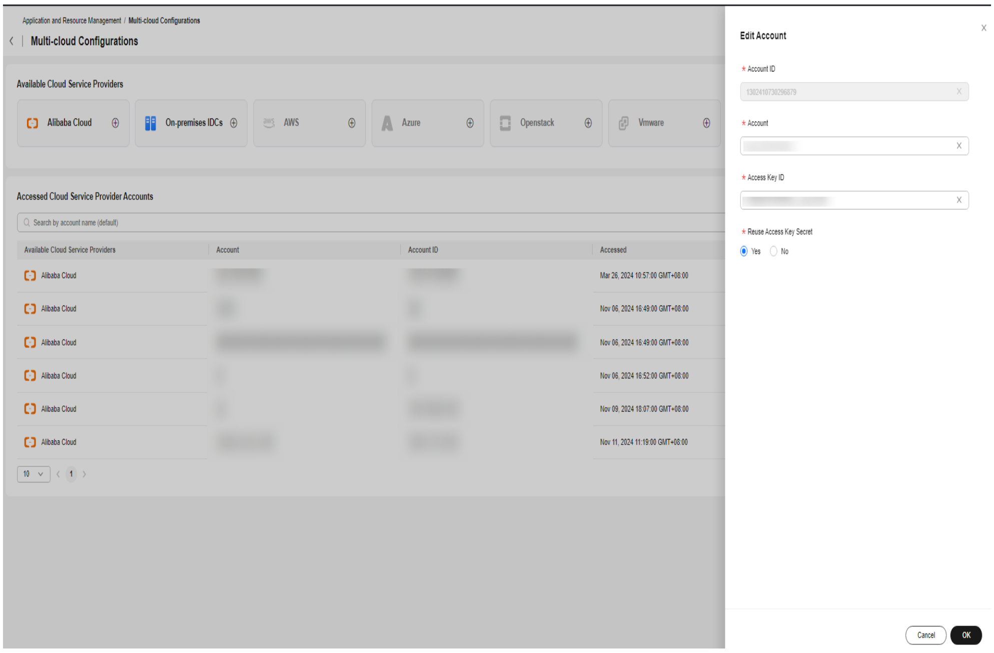
Update a cloud vendor account on COC.

Procedure

Step 1 Log in to COC.

Step 2 On the **Multi-cloud Configurations** page, locate the target cloud service provider account, and click **Modify** in the **Operation** column.

Figure 3-38 Editing an account


Application and Resource Management / Multi-cloud Configurations
Multi-cloud Configurations
Available Cloud Service Providers
Alibaba Cloud
On-premises IDCs
AWS
Azure
Openstack
Vmware
Accessed Cloud Service Provider Accounts
Search by account name (default)
10
1
Edit Account
Cancel
OK

Available Cloud Service Providers	Account	Account ID	Accessed
Alibaba Cloud	[redacted]	[redacted]	Mar 26, 2024 10:57:00 GMT+08:00
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+08:00
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+08:00
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:52:00 GMT+08:00
Alibaba Cloud	[redacted]	[redacted]	Nov 09, 2024 18:07:00 GMT+08:00
Alibaba Cloud	[redacted]	[redacted]	Nov 11, 2024 11:19:00 GMT+08:00

* Account ID: 1302410730296879

* Account: [redacted]

* Access Key ID: [redacted]

* Reuse Access Key Secret: ● Yes ○ No

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.	-

Parameter	Description	Example Value
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

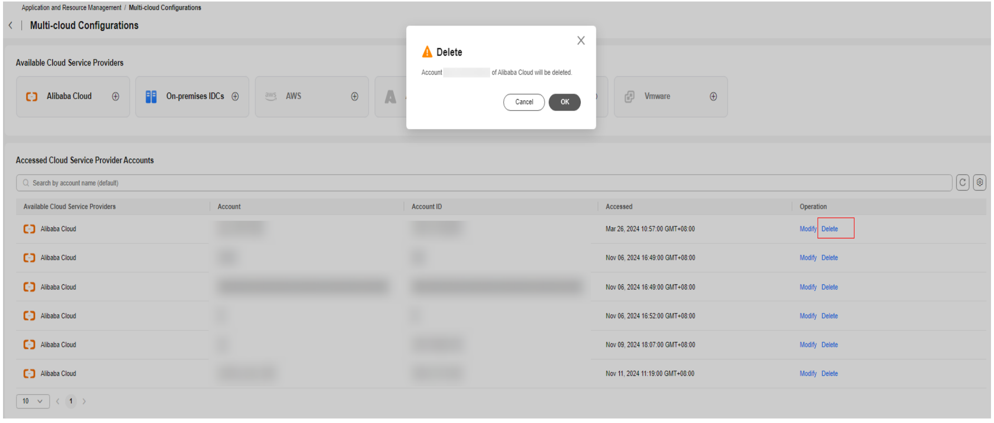
Delete a cloud vendor account on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 On the **Multi-cloud Configurations** page, locate the target cloud vendor account, and click **Delete** in the **Operation** column.

Figure 3-39 Deleting an account



Application and Resource Management / Multi-cloud Configurations

Multi-cloud Configurations

Available Cloud Service Providers

Delete

Account [redacted] of Alibaba Cloud will be deleted.

Accessed Cloud Service Provider Accounts

Search by account name (default)

Available Cloud Service Providers	Account	Account ID	Accessed	Operation
Alibaba Cloud	[redacted]	[redacted]	Mar 26, 2024 10:57:00 GMT+08:00	Modify Delete
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+08:00	Modify Delete
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+08:00	Modify Delete
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:52:00 GMT+08:00	Modify Delete
Alibaba Cloud	[redacted]	[redacted]	Nov 09, 2024 18:07:00 GMT+08:00	Modify Delete
Alibaba Cloud	[redacted]	[redacted]	Nov 11, 2024 11:19:00 GMT+08:00	Modify Delete

Step 3 Click **OK**.

----End

3.3.4 Importing On-premises IDC

You can import on-premises IDCs.

Scenarios

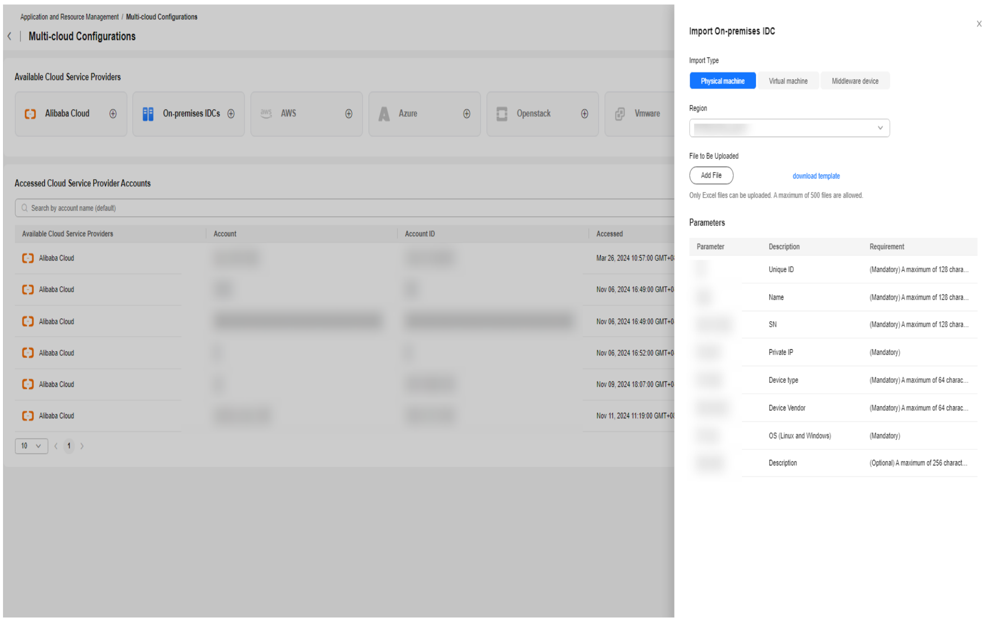
Import on-premises IDCs on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 On the **Multi-cloud Configurations** page, click **On-premises IDCs**.

Figure 3-40 Importing on-premises IDCs



Application and Resource Management / Multi-cloud Configurations

< | Multi-cloud Configurations

Available Cloud Service Providers

Alibaba Cloud ⊕ | On-premises IDCs ⊕ | AWS ⊕ | Azure ⊕ | Openstack ⊕ | Vmware

Accessed Cloud Service Provider Accounts

Search by account name (default)

Available Cloud Service Providers	Account	Account ID	Accessed
Alibaba Cloud	[redacted]	[redacted]	Mar 26, 2024 10:57:00 GMT+0
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+0
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:49:00 GMT+0
Alibaba Cloud	[redacted]	[redacted]	Nov 06, 2024 16:52:00 GMT+0
Alibaba Cloud	[redacted]	[redacted]	Nov 09, 2024 18:07:00 GMT+0
Alibaba Cloud	[redacted]	[redacted]	Nov 11, 2024 11:19:00 GMT+0

10 < 1 >

Import On-premises IDC

Import Type

Physical machine | Virtual machine | Middleware device

Region

[redacted]

File to Be Uploaded

Add File   download template

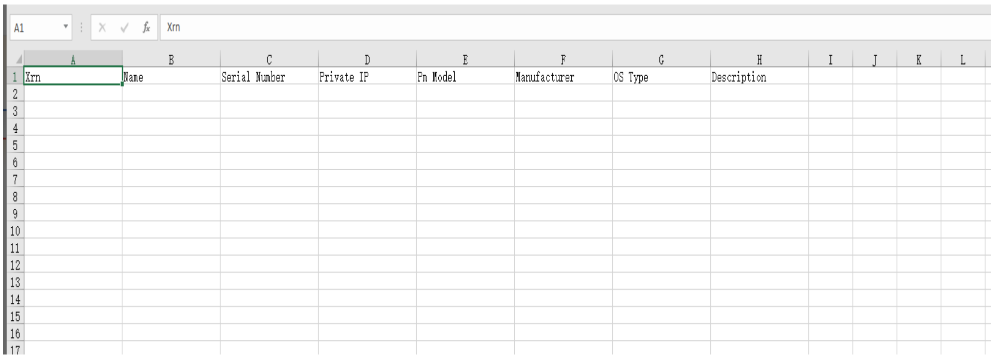
Only Excel files can be uploaded. A maximum of 500 files are allowed.

Parameters

Parameter	Description	Requirement
[redacted]	Unique ID	(Mandatory) A maximum of 128 chara...
[redacted]	Name	(Mandatory) A maximum of 128 chara...
[redacted]	SN	(Mandatory) A maximum of 128 chara...
[redacted]	Private IP	(Mandatory)
[redacted]	Device type	(Mandatory) A maximum of 64 charac...
[redacted]	Device Vendor	(Mandatory) A maximum of 64 charac...
[redacted]	OS (Linux and Windows)	(Mandatory)
[redacted]	Description	(Optional) A maximum of 256 charact...

Step 3 Click **download template** and complete the downloaded template.

Figure 3-41 Entering information in an Excel file



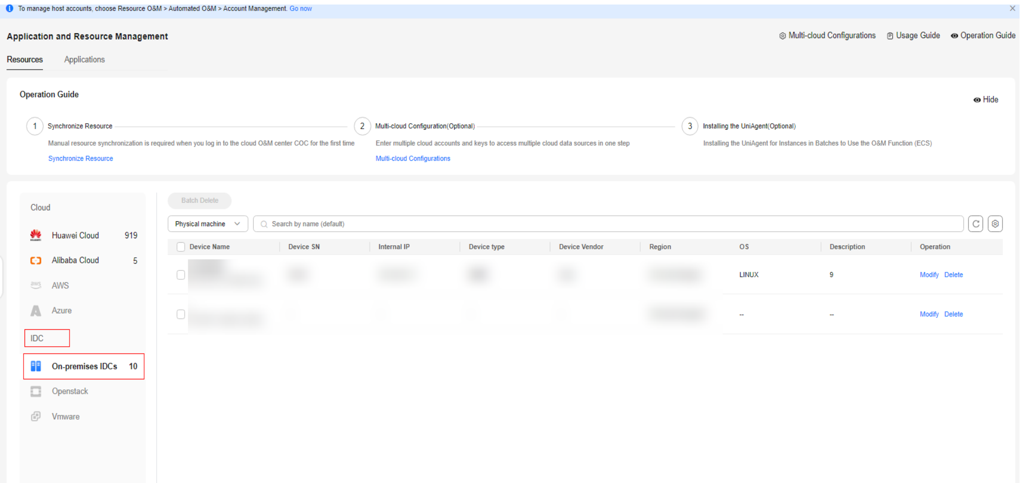
A1 fx Xrn

	A	B	C	D	E	F	G	H	I	J	K	L
1	Xrn	Name	Serial Number	Private IP	Pm Model	Manufacturer	OS Type	Description				

Step 4 Click **Add File** to add the completed excel file.

Step 5 Click < in the upper left corner to return to the **Resources** tab page. You can view the imported on-premises IDC resource information.

Figure 3-42 On-premises IDCs



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

Application and Resource Management

Operation Guide

1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time
Synchronize Resource

2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud data sources in one step
Multi-cloud Configurations

3 Installing the UniAgent(Optional)
Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Device Name	Device SN	Internal IP	Device type	Device Vendor	Region	OS	Description	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	LINUX	9	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	--	Modify Delete

----End

3.3.5 Modifying On-premises IDC Information

You can modify on-premises IDC information.

Scenarios

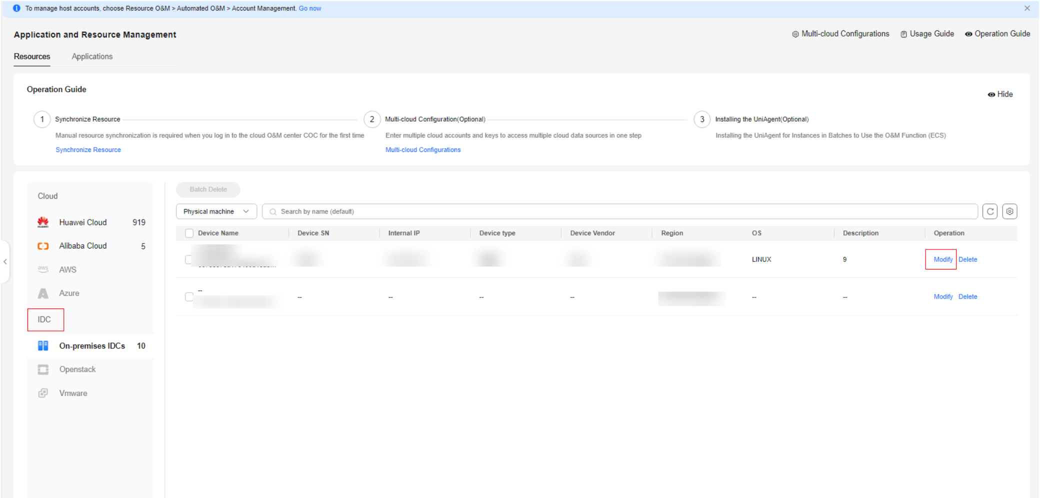
Modify on-premises IDC information on COC.

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, click **IDC**, locate the target IDC record, and click **Modify** in the **Operation** column.

Figure 3-43 Modifying on-premises IDC records



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

Application and Resource Management

Operation Guide

1 Synchronize Resource
Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time
Synchronize Resource

2 Multi-cloud Configuration(Optional)
Enter multiple cloud accounts and keys to access multiple cloud data sources in one step
Multi-cloud Configurations

3 Installing the UniAgent(Optional)
Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Device Name	Device SN	Internal IP	Device type	Device Vendor	Region	OS	Description	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	LINUX	9	Modify Delete
[redacted]	--	--	--	--	[redacted]	--	--	Modify Delete

Step 3 Modify the on-premises IDC resource information based on **Table 3-11**, and click **OK**.

Table 3-11 On-premises IDC information parameters

Parameter	Description	Example Value
Device Name	Device name, which is mandatory.	Test device
Device SN	Device SN, which is mandatory.	--
Internal IP	Internal IP address, which is mandatory.	192.168.1.1
Device type	Device type, which is mandatory.	--
Device Vendor	Device vendor, which is mandatory.	--
OS	Operating system (LINUX or WINDOWS), which is mandatory.	LINUX
Description	Description, which is optional.	--

----End

3.3.6 Deleting On-premises IDCs

You can delete on-premises IDC information.

Scenarios

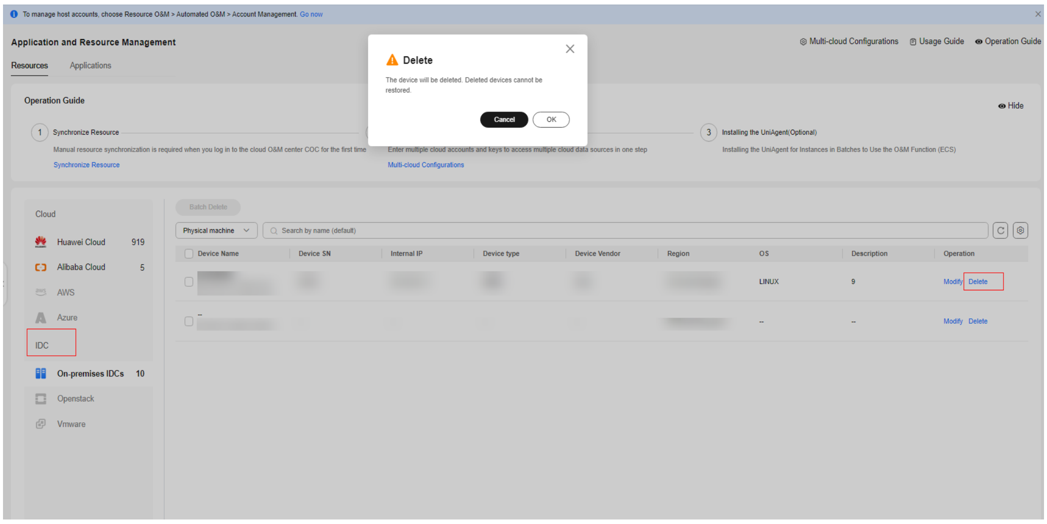
Delete on-premises IDC information on COC.

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, click **IDC**, locate the target IDC record, and click **Delete** in the **Operation** column.

Figure 3-44 Deleting On-premises IDCs



To manage host accounts, choose Resource O&M > Automated O&M > Account Management. Go now

Delete

The device will be deleted. Deleted devices cannot be restored.

Synchronize Resource: Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent(Optional): Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Device Name	Device SN	Internal IP	Device type	Device Vendor	Region	OS	Description	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	LINUX	9	Modify Delete
-- [redacted]					[redacted]	--	--	Modify Delete

Step 3 Click **OK**.

----End

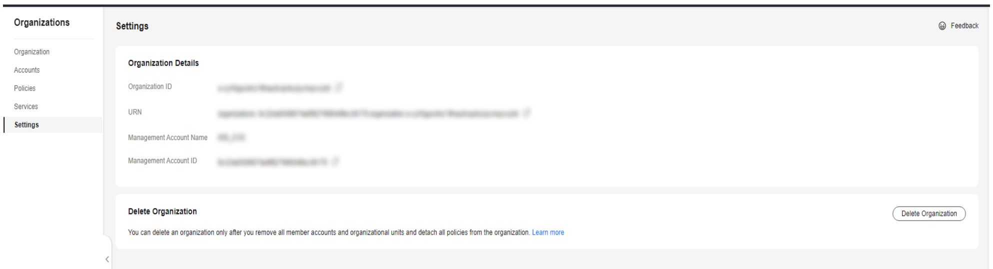
3.4 Cross-Account Resources

Prerequisites

Before performing cross-account resource operations on COC, you need to meet the following prerequisites:

1. You have enabled organizations or joined an organization. You can view the information on the organization service page.

Figure 3-45 Organizations



Organization Details

Organization ID [redacted]

URN [redacted]

Management Account Name [redacted]

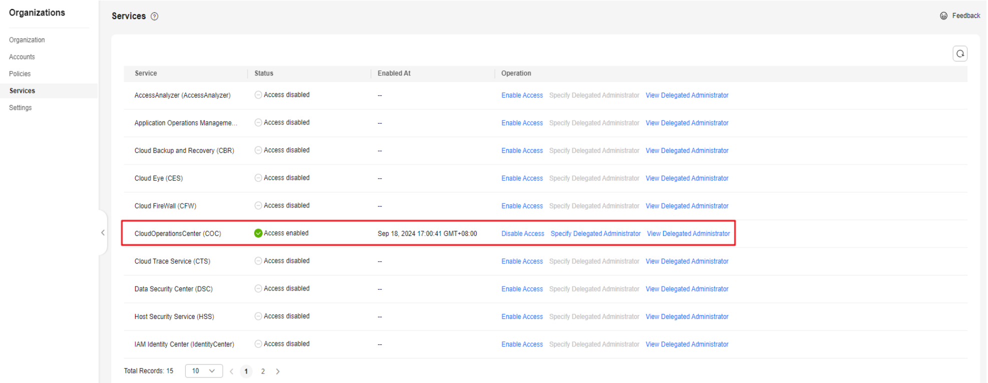
Management Account ID [redacted]

Delete Organization

You can delete an organization only after you remove all member accounts and organizational units and detach all policies from the organization. Learn more

2. The organization to which the user belongs has set COC as a trusted service. You can view the trusted services on the organization page.

Figure 3-46 Trusted Services

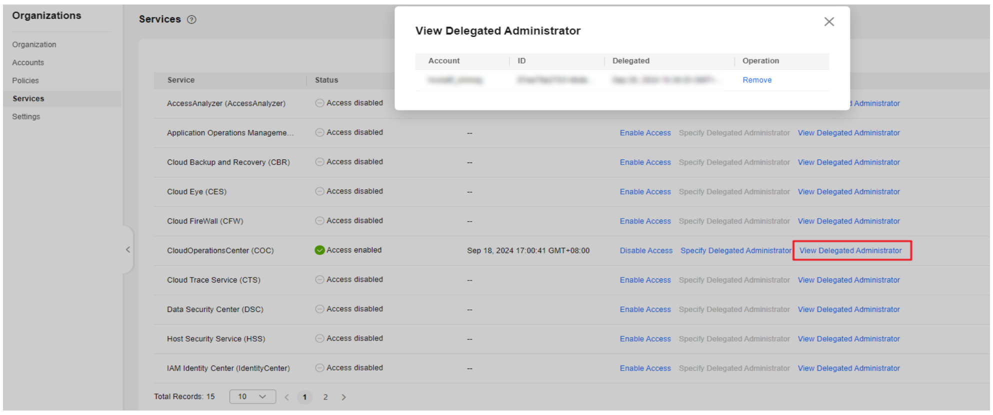


Service	Status	Enabled At	Operation
AccessAnalyzer (AccessAnalyzer)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Application Operations Manageme...	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Backup and Recovery (CBR)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Eye (CES)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud FireWall (CFW)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
CloudOperationsCenter (COC)	Access enabled	Sep 18, 2024 17:00:41 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator
Cloud Trace Service (CTS)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Data Security Center (DSC)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Host Security Service (HSS)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
IAM Identity Center (IdentityCenter)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator

Total Records: 15 10 < 1 2 >

3. The account that performs the cross-account O&M operation is an organization administrator or a delegated administrator assigned by the organization administrator.

Figure 3-47 Delegated administrator



View Delegated Administrator

Account	ID	Delegated	Operation
[redacted]	[redacted]	[redacted]	Remove

Service	Status		Operation
AccessAnalyzer (AccessAnalyzer)	Access disabled		d Administrator
Application Operations Manageme...	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Backup and Recovery (CBR)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud Eye (CES)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Cloud FireWall (CFW)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
CloudOperationsCenter (COC)	Access enabled	Sep 18, 2024 17:00:41 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator
Cloud Trace Service (CTS)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Data Security Center (DSC)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
Host Security Service (HSS)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator
IAM Identity Center (IdentityCenter)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator

Total Records: 15 10 < 1 2 >

3.4.1 Creating a View

Allows users to create views and configure the filter scope to access Huawei Cloud resources across accounts.

Scenarios

Create a view on Cloud Operations Center.

Precautions

A maximum of 10 views can be created.

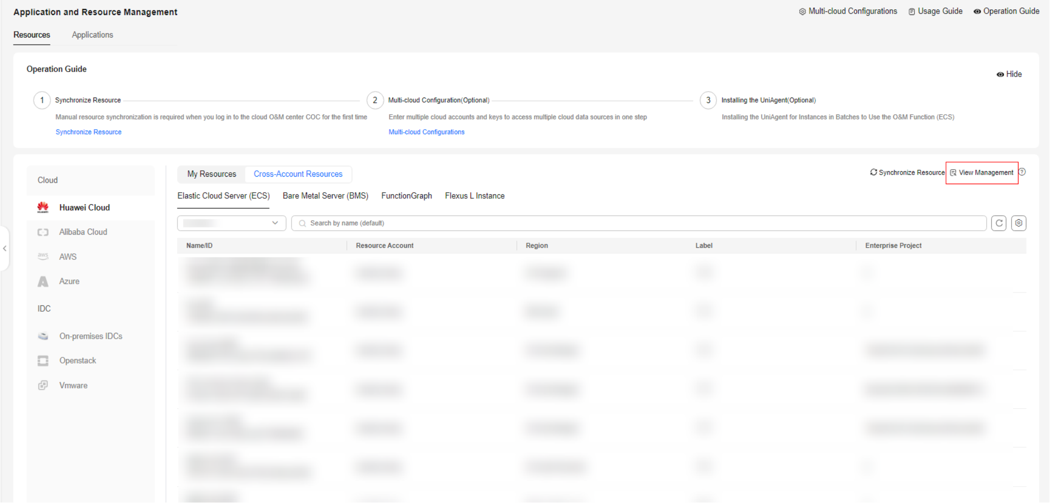
Procedure

Step 1 Log in to **COC**.

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

Step 3 Click **View Management**.

Figure 3-48 View management



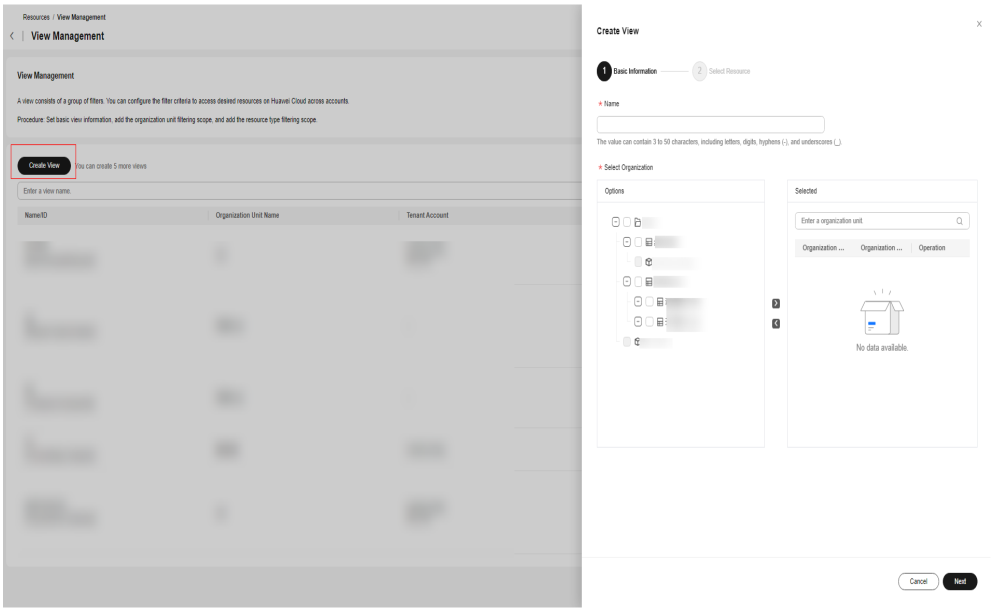
Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

Step 4 Click **Create View**. In the dialog box that is displayed on the right, enter information based on **Table 3-12** and click **OK**.

Figure 3-49 View management



A view consists of a group of filters. You can configure the filter criteria to access desired resources on Huawei Cloud across accounts.

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

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

Table 3-12 Parameters for creating a view

Parameter	Description	Example Value
Authorization Model	Basic information, view name (mandatory)	-
Organization Unit Name	Basic information, organization unit (mandatory)	-
Resource	Basic information, resource (mandatory)	-

----End

3.4.2 Managing a View

Allows users to edit a view.

Scenarios

Edit a view on Cloud Operations Center.

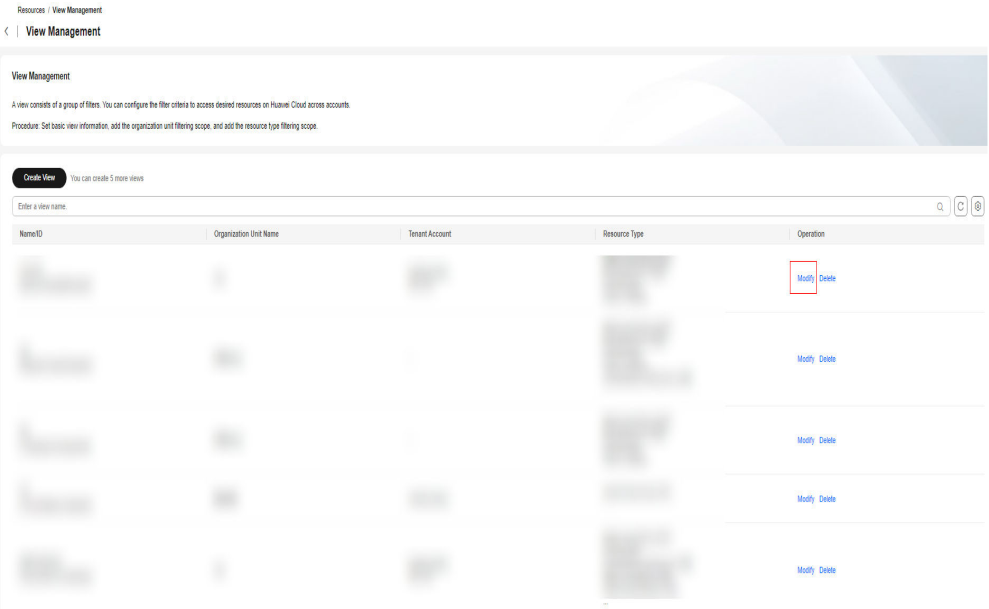
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management** and click **Cross-Account Resources**. Click **View Management**.

Step 3 Click **Modify**. In the dialog box that is displayed on the right, enter information based on **Table 3-12** and click **Submit**.

Figure 3-50 Managing a view



A view consists of a group of filters. You can configure the filter criteria to access desired resources on Huawei Cloud across accounts.

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

You can create 5 more views

Enter a view name.

Name/ID	Organization Unit Name	Tenant Account	Resource Type	Operation
				Modify Delete
				Modify Delete
				Modify Delete
				Modify Delete
				Modify Delete

----End

3.4.3 Deleting a View

Allows users to delete views.

Scenarios

Delete a view on Cloud Operations Center.

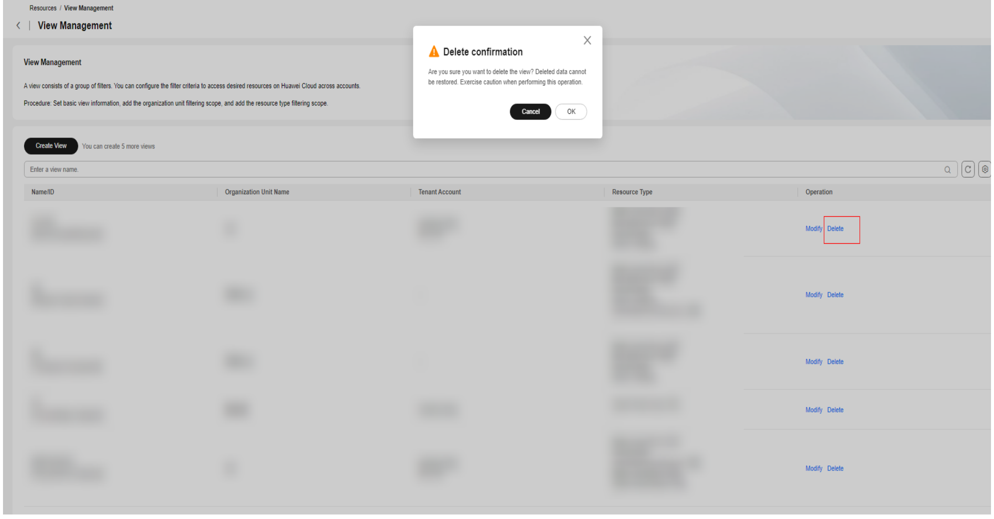
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management** and click **Cross-Account Resources**. Click **View Management**.

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

Figure 3-51 Deleting a view



A view consists of a group of filters. You can configure the filter criteria to access desired resources on Huawei Cloud across accounts.

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

Are you sure you want to delete the view? Deleted data cannot be restored. Exercise caution when performing this operation.

----End

3.4.4 Synchronizing Resources

Allows users to synchronize resources based on views.

Scenarios

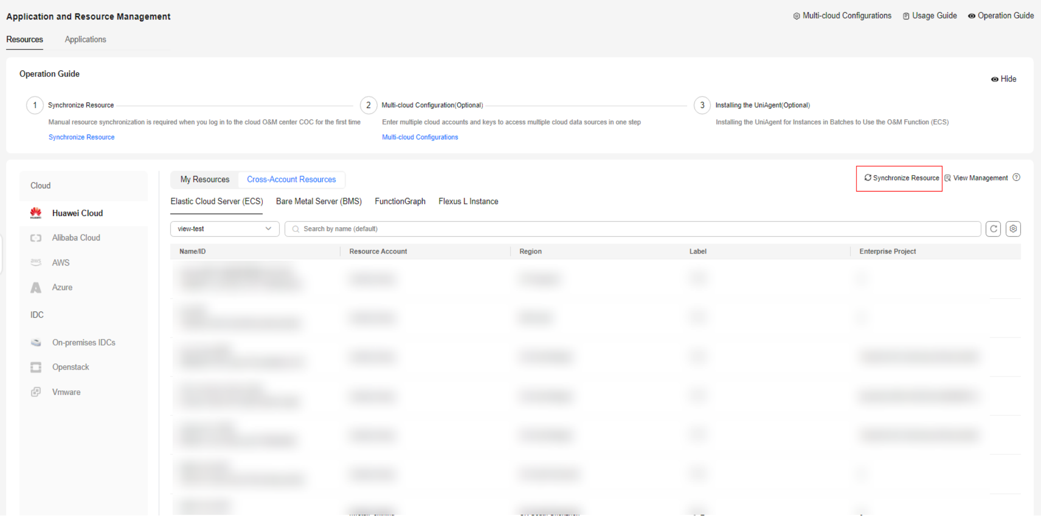
Synchronize view resources on Cloud Operations Center.

Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resources** > **Application and Resource Management** and click **Cross-Account Resources**. Click **Synchronize Resource**.

Figure 3-52 Synchronizing resources



1 Synchronize Resource

Manual resource synchronization is required when you log in to the cloud O&M center COC for the first time

Synchronize Resource

2 Multi-cloud Configuration(Optional)

Enter multiple cloud accounts and keys to access multiple cloud data sources in one step

Multi-cloud Configurations

3 Installing the UniAgent(Optional)

Installing the UniAgent for Instances in Batches to Use the O&M Function (ECS)

----End

4 Resource O&M

4.1 Overview

Resource O&M allows you to perform operations on ECS, RDS, Flexus L, and BMS instances, including starting, stopping, and restarting instances in batches, and change and reinstall OSs.

4.2 Batch Operations on ECSs

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

4.2.1 Batch Starting ECSs

Scenarios

Start ECS instances in batches on COC.

Precautions

Instances that have been started cannot be selected.

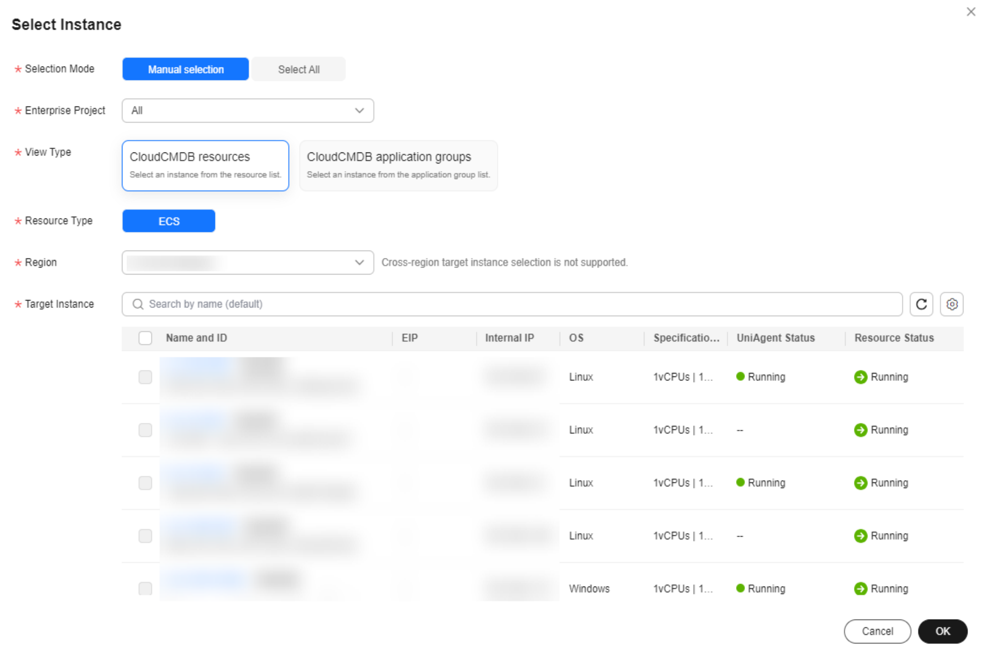
Procedure

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



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS

* Region: [redacted] Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

□	Name and ID	EIP	Internal IP	OS	Specificatio...	UniAgent Status	Resource Status
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	● Running	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	--	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	● Running	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	--	Running
□	[redacted]	[redacted]	[redacted]	Windows	1vCPUs | 1...	● Running	Running

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.

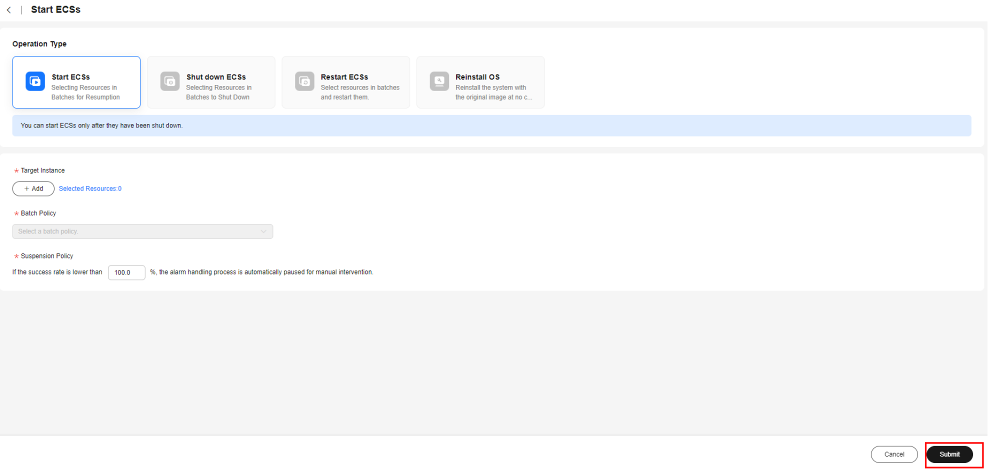
Step 5 Set **Suspension Policy**.

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



< | **Start ECSs**

Operation Type

Start ECSs Selecting Resources in Batches for Resumption

Shut down ECSs Selecting Resources in Batches to Shut Down

Restart ECSs Select resources in batches and restart them.

Reinstall OS Reinstall the system with the original image at no c...

You can start ECSs only after they have been shut down.

* Target Instance

+ Add Selected Resources:0

* Batch Policy

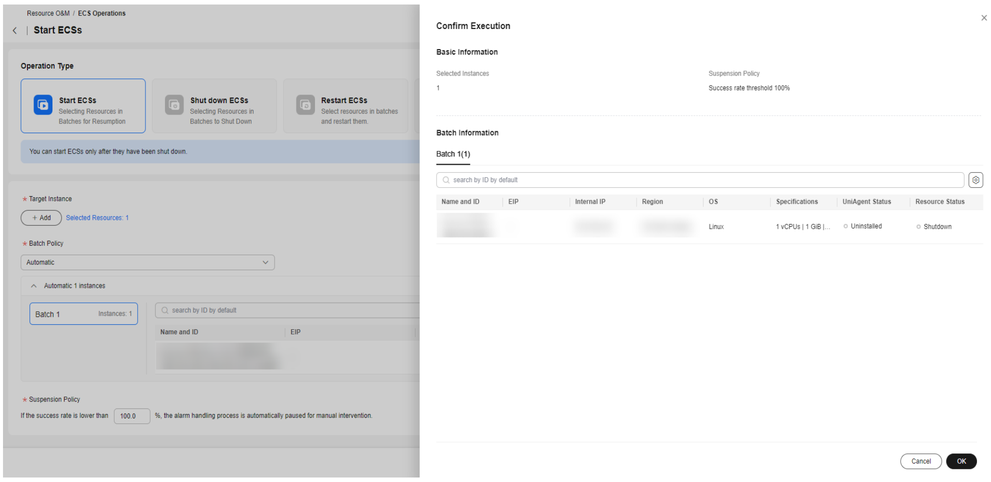
Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

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

Figure 4-3 Confirming the execution



Resource O&M / ECS Operations

< | **Start ECSs**

Operation Type

Start ECSs Selecting Resources in Batches for Resumption

Shut down ECSs Selecting Resources in Batches to Shut Down

Restart ECSs Select resources in batches and restart them.

You can start ECSs only after they have been shut down.

* Target Instance

+ Add Selected Resources: 1

* Batch Policy

Automatic

Automatic 1 instances

Batch 1 Instances: 1

search by ID by default

Name and ID	EIP
[redacted]	

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Confirm Execution

Basic Information

Selected Instances
1

Suspension Policy
Success rate threshold 100%

Batch Information

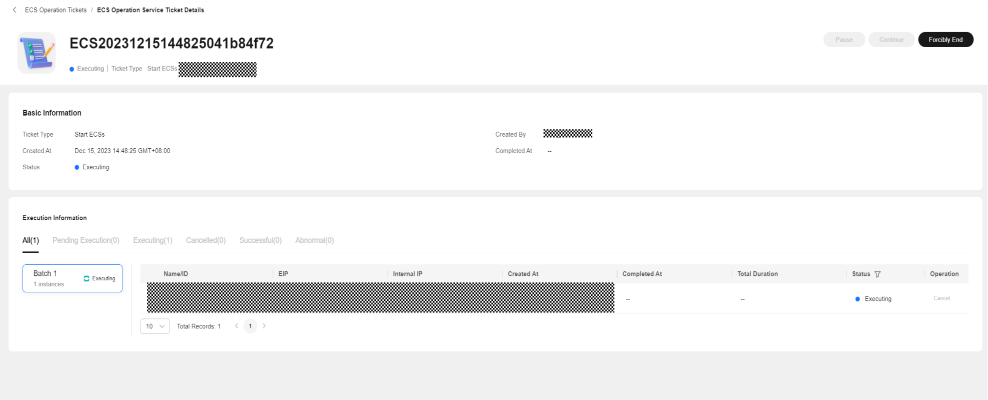
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	Specifications	UniAgent Status	Resource Status
[redacted]		[redacted]	[redacted]	Linux	1 vCPUs | 1 GiB |...	○ Uninstalled	○ Shutdown

Step 8 View the execution result.

Figure 4-4 Viewing the result



< ECS Operation Tickets / **ECS Operation Service Ticket Details**

ECS20231215144825041b84f72

● Executing | Ticket Type Start ECSs [redacted]

Basic Information

Ticket Type	Start ECSs	Created By	[redacted]
Created At	Dec 15, 2023 14:48:25 GMT+08:00	Completed At	--
Status	● Executing		

Execution Information

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

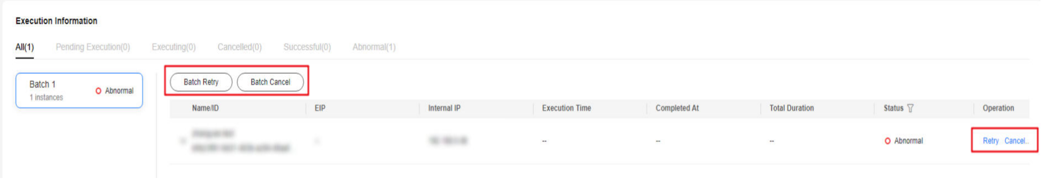
Batch 1 Executing
1 instances

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	--	--	● Executing	Cancel

10 Total Records: 1 < 1 >

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-5 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances
○ Abnormal

Batch Retry | Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.2.2 Batch Stopping ECSs

Scenarios

Stop ECS instances in batches on COC.

Precautions

Stopped instances cannot be selected.

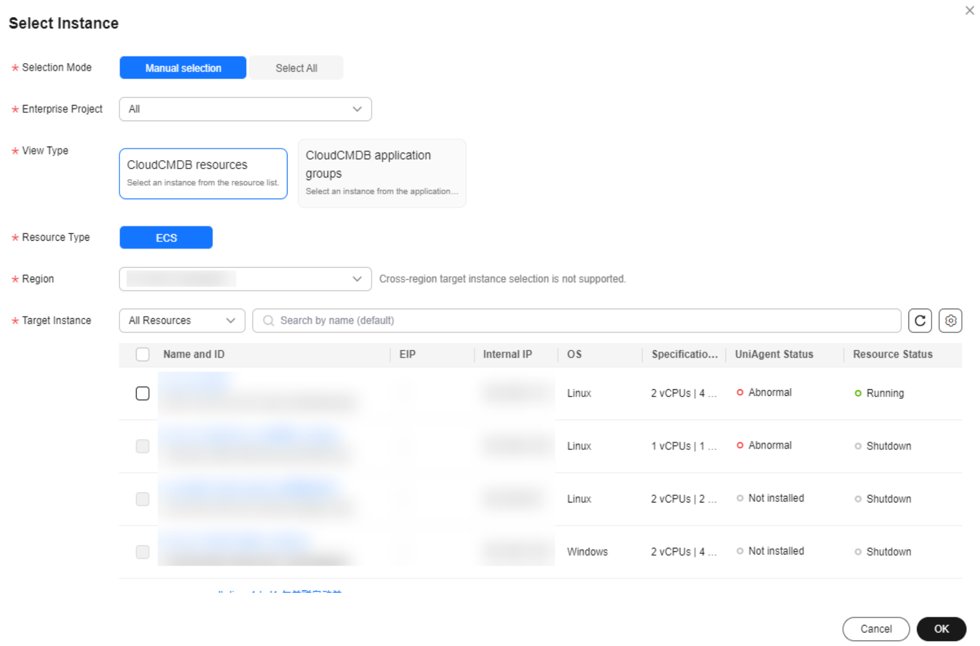
Procedure

Step 1 Log in to **COC**.

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

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

Figure 4-6 Selecting instances



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application...)

* Resource Type: ECS

* Region: [redacted] Cross-region target instance selection is not supported.

* Target Instance: All Resources | Search by name (default)

	Name and ID	EIP	Internal IP	OS	Specificatio...	UniAgent Status	Resource Status
□	[redacted]	[redacted]	[redacted]	Linux	2 vCPUs | 4 ...	○ Abnormal	○ Running
□	[redacted]	[redacted]	[redacted]	Linux	1 vCPUs | 1 ...	○ Abnormal	○ Shutdown
□	[redacted]	[redacted]	[redacted]	Linux	2 vCPUs | 2 ...	○ Not installed	○ Shutdown
□	[redacted]	[redacted]	[redacted]	Windows	2 vCPUs | 4 ...	○ Not installed	○ Shutdown

Cancel | OK

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.

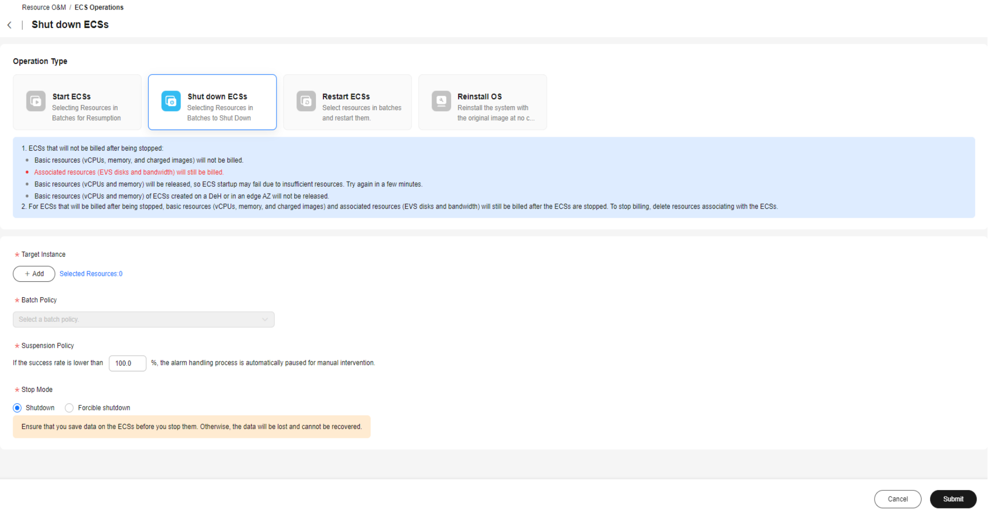
Step 5 Set **Suspension Policy**.

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 4-7 Stopping instances



Resource O&M / ECS Operations

Shut down ECSs

Operation Type

- Start ECSs: Selecting Resources in Batches for Resumption
- Shut down ECSs: Selecting Resources in Batches to Shut Down
- Restart ECSs: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...

1. ECSs that will not be billed after being stopped:
   - Basic resources (vCPUs, memory, and charged images) will not be billed.
   - Associated resources (EVS disks and bandwidth) will still be billed.
   - Basic resources (vCPUs and memory) will be released, so ECS startup may fail due to insufficient resources. Try again in a few minutes.
   - Basic resources (vCPUs and memory) of ECSs created on a DeH or in an edge AZ will not be released.
2. For ECSs that will be billed after being stopped, basic resources (vCPUs, memory, and charged images) and associated resources (EVS disks and bandwidth) will still be billed after the ECSs are stopped. To stop billing, delete resources associating with the ECSs.

* Target Instance

+ Add Selected Resources:0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

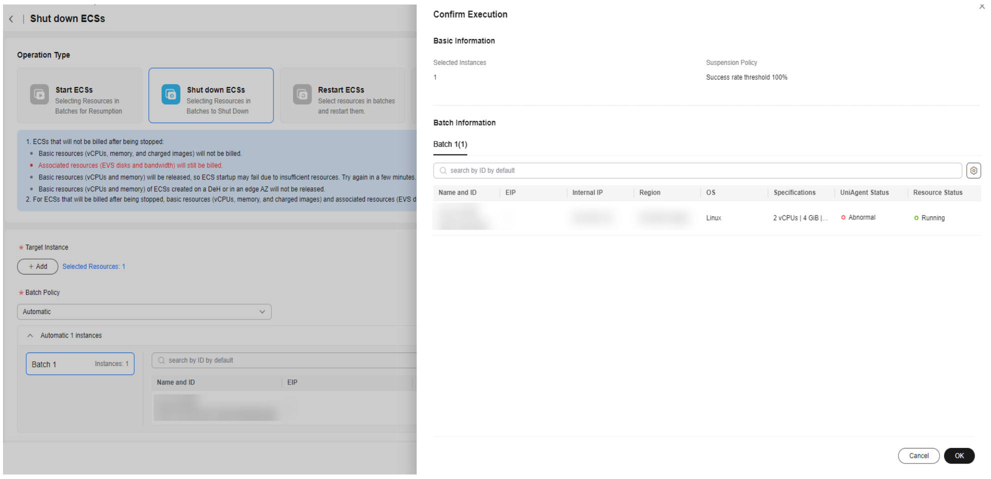
* Stop Mode

● Shutdown ○ Forcible shutdown

Ensure that you save data on the ECSs before you stop them. Otherwise, the data will be lost and cannot be recovered.

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

Figure 4-8 Confirming the execution



Shut down ECSs

Operation Type

- Start ECSs: Selecting Resources in Batches for Resumption
- Shut down ECSs: Selecting Resources in Batches to Shut Down
- Restart ECSs: Select resources in batches and restart them.

1. ECSs that will not be billed after being stopped:
   - Basic resources (vCPUs, memory, and charged images) will not be billed.
   - Associated resources (EVS disks and bandwidth) will still be billed.
   - Basic resources (vCPUs and memory) will be released, so ECS startup may fail due to insufficient resources. Try again in a few minutes.
   - Basic resources (vCPUs and memory) of ECSs created on a DeH or in an edge AZ will not be released.
2. For ECSs that will be billed after being stopped, basic resources (vCPUs, memory, and charged images) and associated resources (EVS d

* Target Instance

+ Add Selected Resources: 1

* Batch Policy

Automatic

Automatic 1 instances

Batch 1 Instances: 1

search by ID by default

Name and ID	EIP
[redacted]	

Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

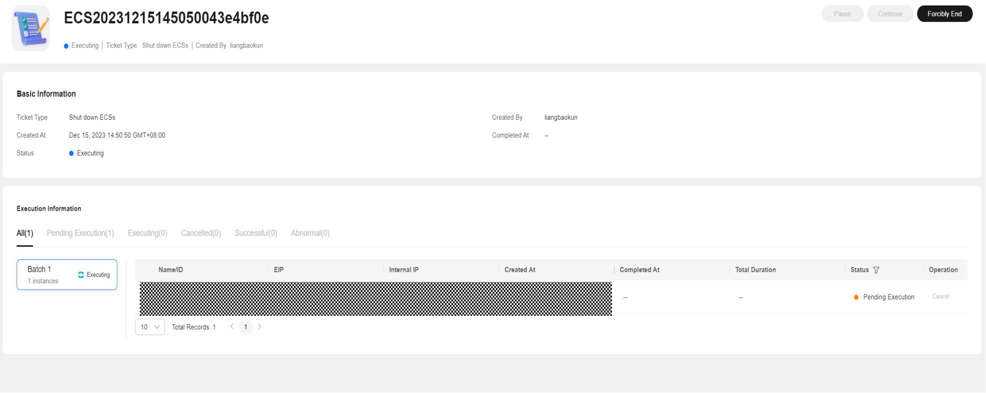
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	Specifications	UniAgent Status	Resource Status
[redacted]		[redacted]	[redacted]	Linux	2 vCPUs | 4 GiB |...	○ Abnormal	○ Running

Step 8 View the execution result.

Figure 4-9 Viewing the result



ECS20231215145050043e4bf0e

● Executing | Ticket Type Shut down ECSs | Created By liangbaokun

Basic Information

Ticket Type	Shut down ECSs	Created By	liangbaokun
Created At	Dec 15, 2023 14:50:50 GMT+08:00	Completed At	--
Status	● Executing		

Execution Information

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

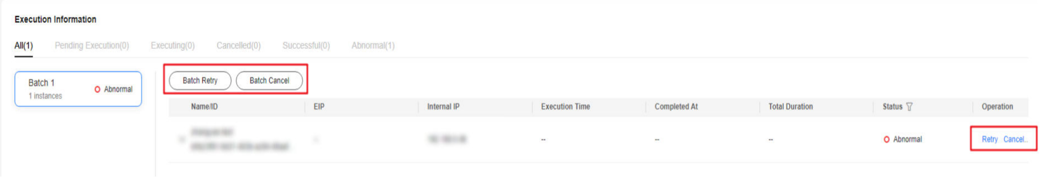
Batch 1
1 instances
Executing

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	--	--	● Pending Execution	Cancel

10 Total Records: 1 < 1 >

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-10 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances
○ Abnormal

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.2.3 Batch Restarting ECSs

Scenarios

Restart ECS instances in batches on COC.

Precautions

Stopped instances cannot be selected.

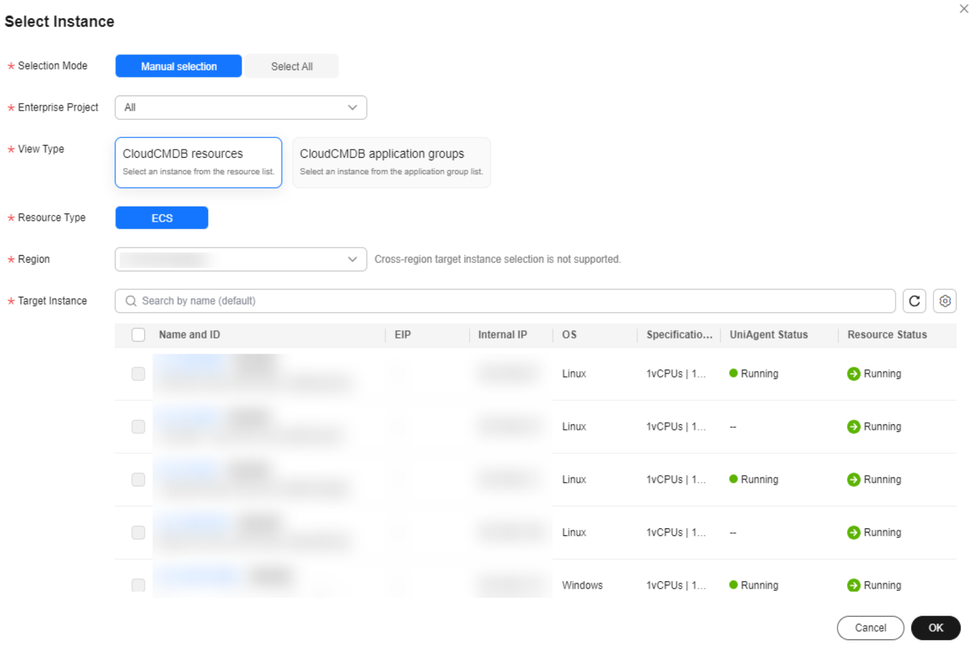
Procedure

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 4-11 Selecting host instances



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS

* Region: [redacted] Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

□	Name and ID	EIP	Internal IP	OS	Specificatio...	UniAgent Status	Resource Status
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	● Running	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	--	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	● Running	Running
□	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	--	Running
□	[redacted]	[redacted]	[redacted]	Windows	1vCPUs | 1...	● Running	Running

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.

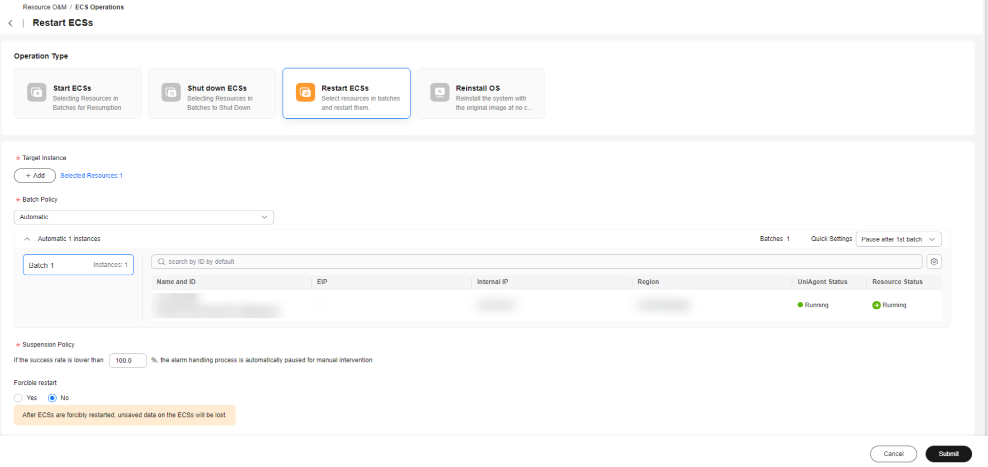
Step 6 Determine whether to forcibly restart ECSs.

NOTE

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

Step 7 Click **Submit**.

Figure 4-12 Restarting instances



Resource O&M / ECS Operations

Restart ECSs

Operation Type

- Start ECSs: Selecting Resources in Batches for Resumption
- Shut down ECSs: Selecting Resources in Batches to Shut Down
- Restart ECSs: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...

* Target Instance

+ Add   Selected Resources:1

* Batch Policy

Automatic

Automatic 1 instances   Batches 1   Quick Settings: Pause after 1st batch

Batch 1   Instances: 1

search by ID by default

Name and ID	EIP	Internal IP	Region	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	● Running	Running

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Forcible restart

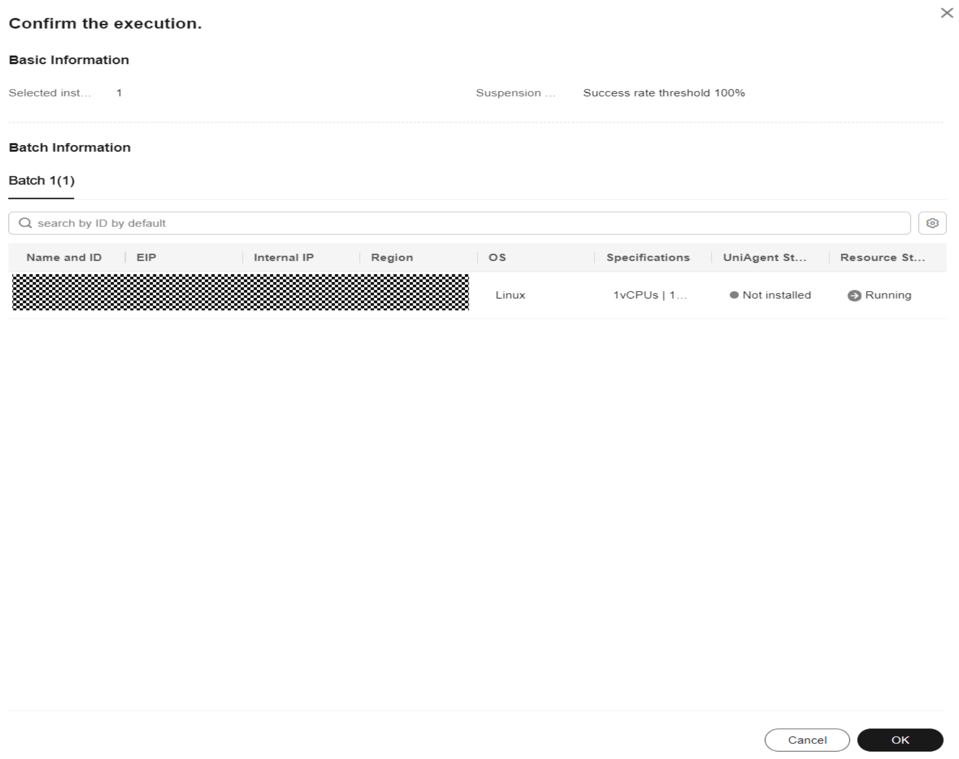
○ Yes ● No

After ECSs are forcibly restarted, unsaved data on the ECSs will be lost.

Cancel   Submit

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

Figure 4-13 Confirming the execution



Confirm the execution.

Basic Information

Selected inst... 1   Suspension ... Success rate threshold 100%

Batch Information

Batch 1(1)

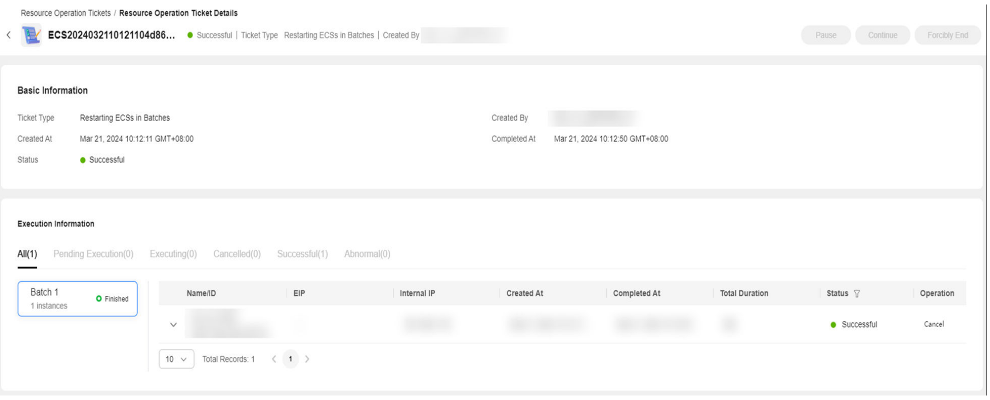
search by ID by default

Name and ID	EIP	Internal IP	Region	OS	Specifications	UniAgent St...	Resource St...
[redacted]	[redacted]	[redacted]	[redacted]	Linux	1vCPUs | 1...	● Not installed	Running

Cancel   OK

Step 9 View the execution result.

Figure 4-14 Viewing the result



Resource Operation Tickets / **Resource Operation Ticket Details**

ECS2024032110121104d86... ● Successful | Ticket Type Restarting ECSs in Batches | Created By

Pause Continue Forcibly End

Basic Information

Ticket Type	Restarting ECSs in Batches	Created By	
Created At	Mar 21, 2024 10:12:11 GMT+08:00	Completed At	Mar 21, 2024 10:12:50 GMT+08:00
Status	● Successful		

Execution Information

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

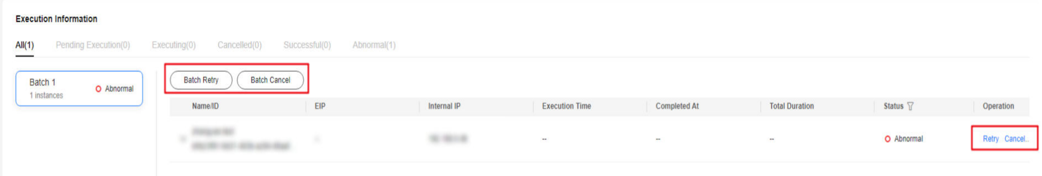
Batch 1 ○ Finished
1 instances

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
						● Successful	Cancel

10 Total Records: 1 < 1 >

Step 10 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-15 Canceling or retrying batch tasks



Execution Information

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

Batch 1 ○ Abnormal
1 instances

Batch Retry Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
			--	--	--	○ Abnormal	Retry Cancel..

----End

4.2.4 Batch Reinstalling OSs

Scenarios

Reinstall OSs of ECS instances in batches on COC.

Precautions

If there are instances that are not stopped, select **Stop now**.

If no instance is stopped, submit the task.

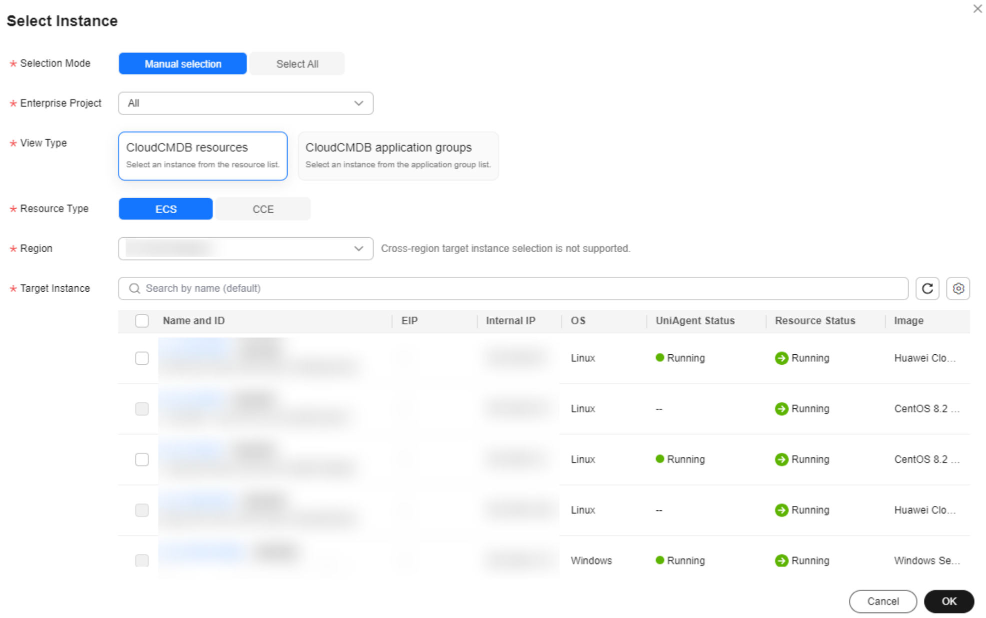
Procedure

Step 1 Log in to COC.

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

Step 3 On the **Reinstall OS** page, click **Add**.

Figure 4-16 Adding instances



Select Instance

* Selection Mode: **Manual selection** | Select All

* Enterprise Project: All

* View Type: **CloudCMDB resources** (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: **ECS** | CCE

* Region: [redacted] Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

□	Name and ID	EIP	Internal IP	OS	UniAgent Status	Resource Status	Image
□	[redacted]	[redacted]	[redacted]	Linux	● Running	Running	Huawei Clo...
□	[redacted]	[redacted]	[redacted]	Linux	--	Running	CentOS 8.2 ...
□	[redacted]	[redacted]	[redacted]	Linux	● Running	Running	CentOS 8.2 ...
□	[redacted]	[redacted]	[redacted]	Linux	--	Running	Huawei Clo...
□	[redacted]	[redacted]	[redacted]	Windows	● Running	Running	Windows Se...

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 reaches the pre-set suspension threshold figure, 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.

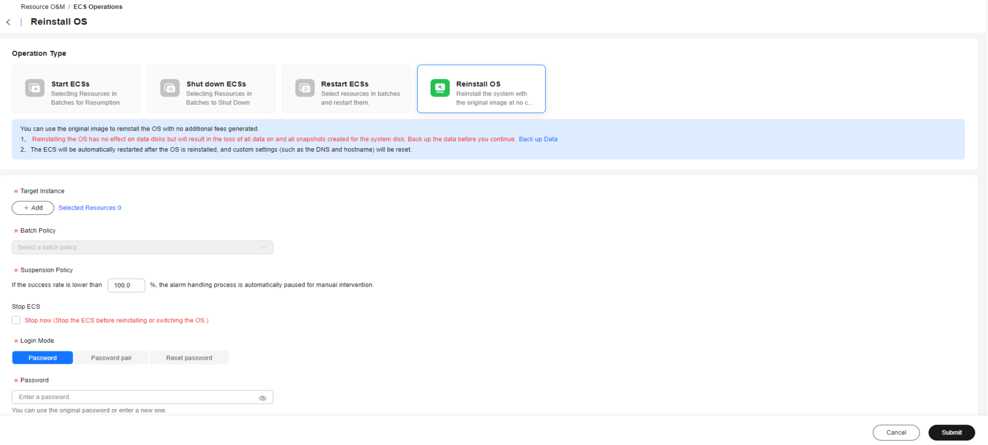
Step 6 Set **Login Mode**.

Login mode:

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

Step 7 Click **Submit**.

Figure 4-17 Reinstalling OSs



Resource O&M / ECS Operations

< | **Reinstall OS**

Operation Type

- **Start ECSs** Selecting Resources in Batches for Resumption
- **Shut down ECSs** Selecting Resources in Batches to Shut Down
- **Restart ECSs** Select resources in batches and restart them.
- **Reinstall OS** Reinstall the system with the original image at no c...

You can use the original image to reinstall the OS with no additional fees generated.

1、 Reinstalling the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system disk. Back up the data before you continue. Back up Data

2、 The ECS will be automatically restarted after the OS is reinstalled, and custom settings (such as the DNS and hostname) will be reset.

* Target Instance

+ Add Selected Resources:0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Stop ECS

□ Stop now (Stop the ECS before reinstalling or switching the OS.)

* Login Mode

Password | Password pair | Reset password

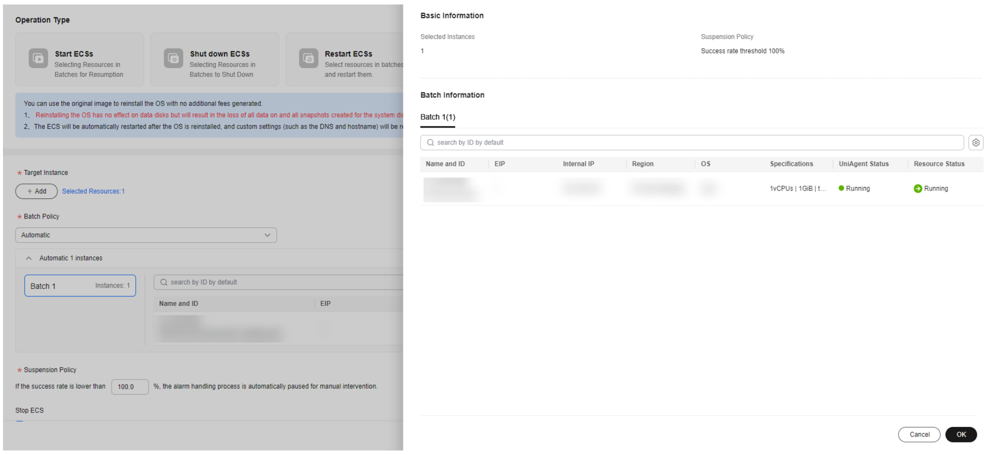
* Password

Enter a password.

You can use the original password or enter a new one.

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

Figure 4-18 Confirming the execution



Operation Type

- **Start ECSs** Selecting Resources in Batches for Resumption
- **Shut down ECSs** Selecting Resources in Batches to Shut Down
- **Restart ECSs** Select resources in batches and restart them.

You can use the original image to reinstall the OS with no additional fees generated.

1、 Reinstalling the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system di

2、 The ECS will be automatically restarted after the OS is reinstalled, and custom settings (such as the DNS and hostname) will be r

* Target Instance

+ Add Selected Resources:1

* Batch Policy

Automatic

Automatic 1 instances

Batch 1 Instances: 1

search by ID by default

Name and ID	EIP
[redacted]	

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Stop ECS

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

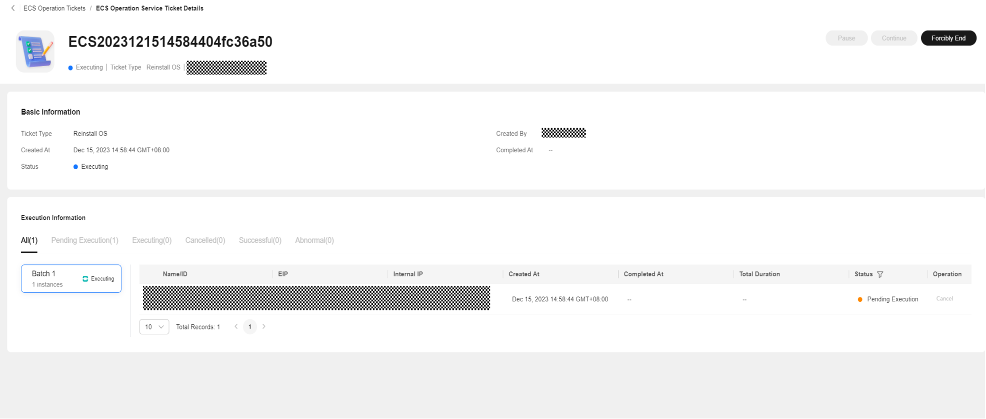
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	Specifications	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1vCPUs | 1GiB | t...	● Running	Running

Step 9 View the execution result.

Figure 4-19 Viewing the execution result



< ECS Operation Tickets / **ECS Operation Service Ticket Details**

ECS2023121514584404fc36a50

● Executing | Ticket Type Reinstall OS | [redacted]

Basic Information

Ticket Type	Reinstall OS	Created By	[redacted]
Created At	Dec 15, 2023 14:58:44 GMT+08:00	Completed At	--
Status	● Executing		

Execution Information

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

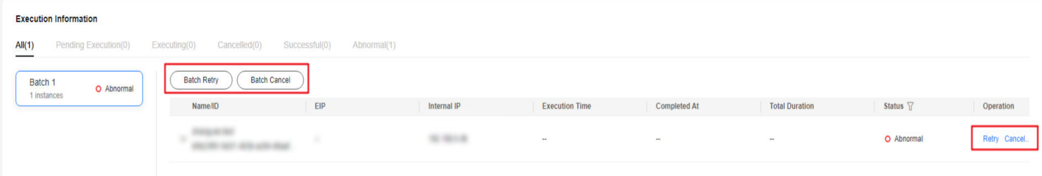
Batch 1 Executing
1 instances

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
[redacted]			Dec 15, 2023 14:58:44 GMT+08:00	--	--	● Pending Execution	Cancel

10 Total Records: 1 < 1 >

Step 10 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-20 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances
○ Abnormal

Batch Retry | Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[illegible]	[illegible]	[illegible]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.2.5 Batch Changing OSs

Scenarios

Change OSs of ECS instances on COC.

Precautions

If there are instances that are not stopped, select **Stop now**.

If no instance is stopped, submit the task.

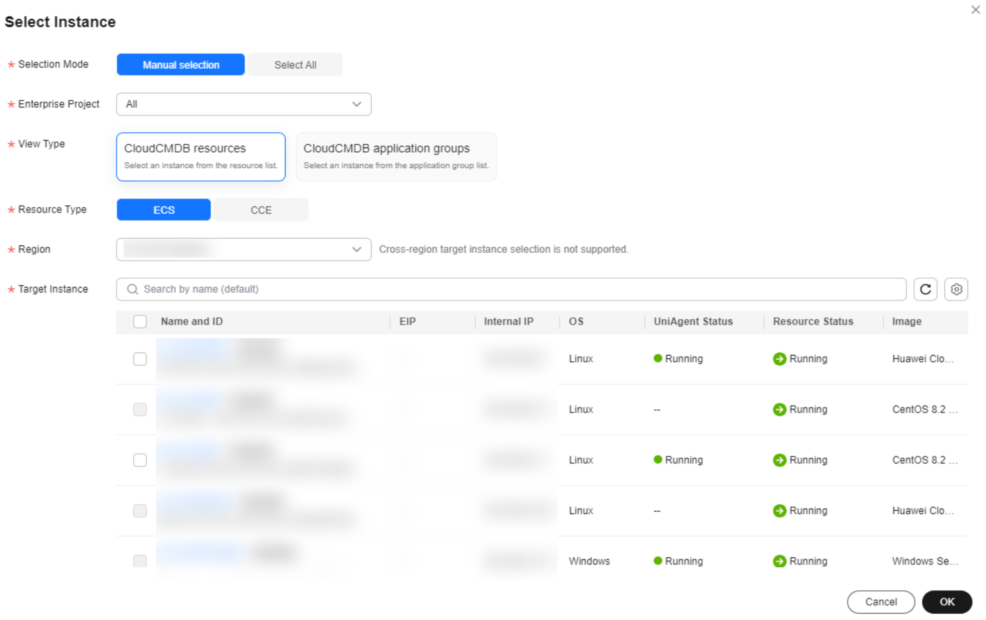
Procedure

Step 1 Log in to **COC**.

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

Step 3 On the **Change OS** page, click **Add**.

Figure 4-21 Changing OSs



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS | CCE

* Region: [illegible] Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

□	Name and ID	EIP	Internal IP	OS	UniAgent Status	Resource Status	Image
□	[illegible]	[illegible]	[illegible]	Linux	● Running	Running	Huawei Clo...
□	[illegible]	[illegible]	[illegible]	Linux	--	Running	CentOS 8.2 ...
□	[illegible]	[illegible]	[illegible]	Linux	● Running	Running	CentOS 8.2 ...
□	[illegible]	[illegible]	[illegible]	Linux	--	Running	Huawei Clo...
□	[illegible]	[illegible]	[illegible]	Windows	● Running	Running	Windows Se...

Cancel | OK

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 Specify **Image** .

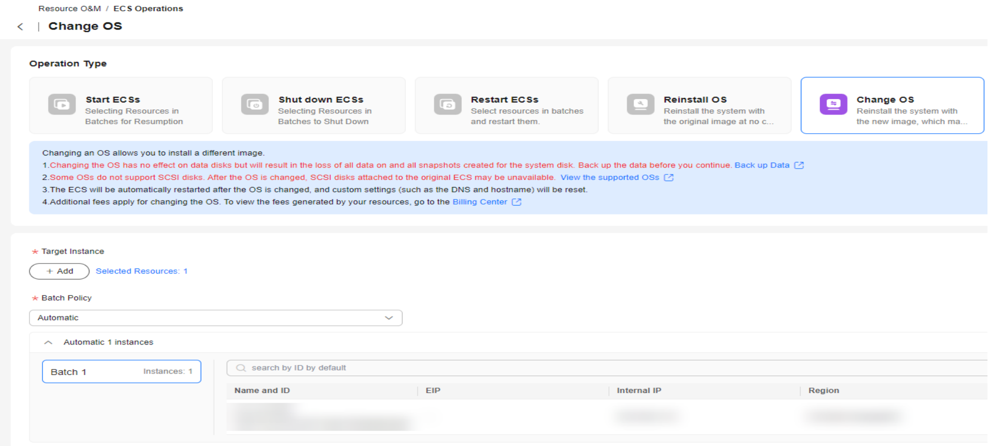
Step 7 Set the login mode.

Login mode:

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

Step 8 Click **Submit**.

Figure 4-22 Changing OSs


Resource O&M / ECS Operations
Change OS
Operation Type
Start ECSs
Selecting Resources in Batches for Resumption
Shut down ECSs
Selecting Resources in Batches to Shut Down
Restart ECSs
Select resources in batches and restart them.
Reinstall OS
Reinstall the system with the original image at no c...
Change OS
Reinstall the system with the new image, which ma...

Changing an OS allows you to install a different image.
1.Changing the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system disk. Back up the data before you continue. Back up Data
2.Some OSs do not support SCSI disks. After the OS is changed, SCSI disks attached to the original ECS may be unavailable. View the supported OSs
3.The ECS will be automatically restarted after the OS is changed, and custom settings (such as the DNS and hostname) will be reset.
4.Additional fees apply for changing the OS. To view the fees generated by your resources, go to the Billing Center

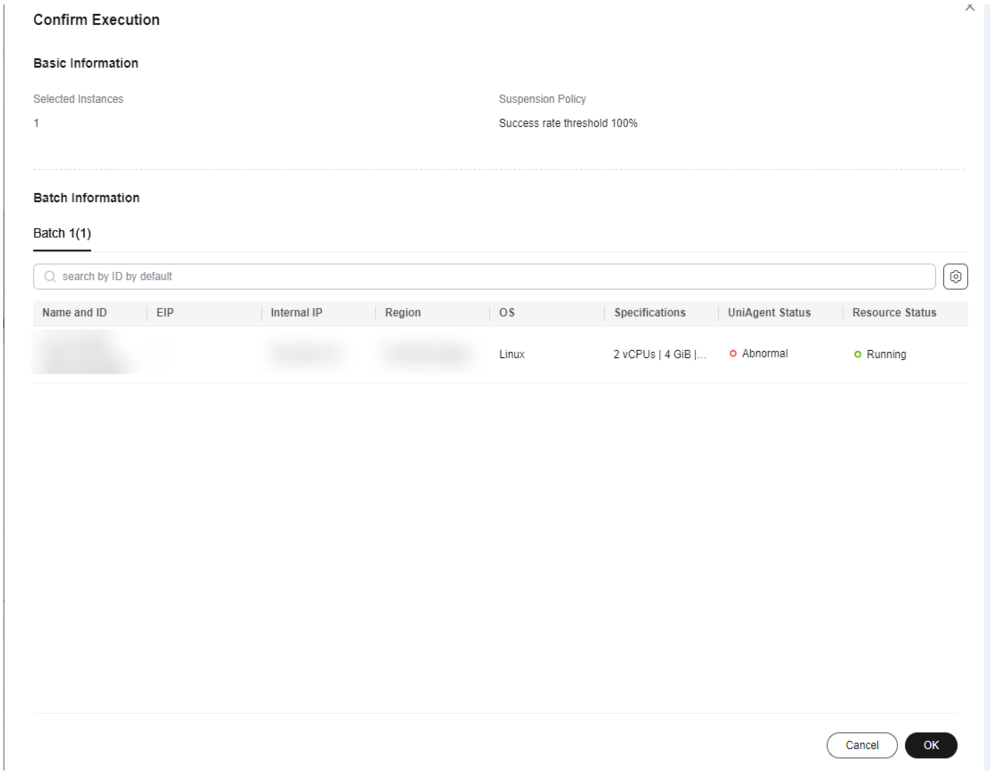
* Target Instance: Selected Resources: 1

* Batch Policy: Automatic

Name and ID	EIP	Internal IP	Region
[redacted]		[redacted]	[redacted]

Step 9 In the **Confirm Execution** dialog box, click **OK**.

Figure 4-23 Confirming the execution



Confirm Execution

Basic Information

Selected Instances
1

Suspension Policy
Success rate threshold 100%

Batch Information

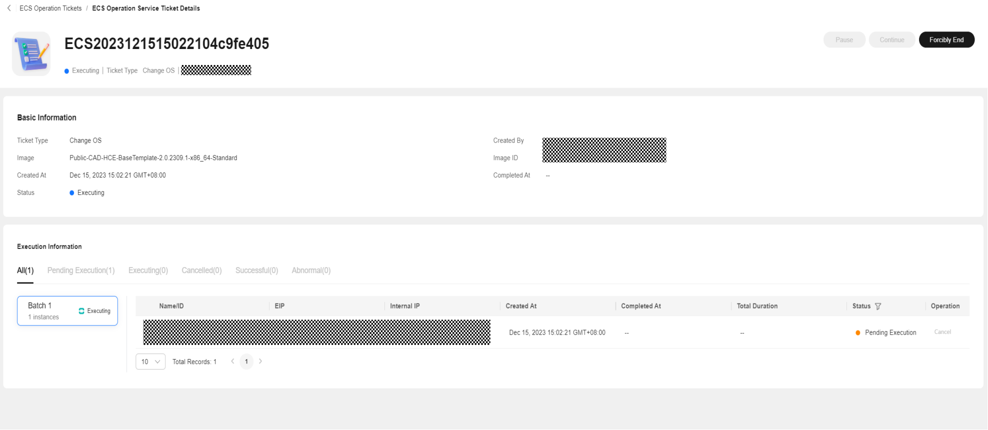
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	Specifications	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	2 vCPUs | 4 GiB |...	○ Abnormal	○ Running

Step 10 View the execution result.

Figure 4-24 Execution result



ECS Operation Tickets / ECS Operation Service Ticket Details

ECS2023121515022104c9fe405

● Executing | Ticket Type Change OS | [redacted]

Basic Information

Ticket Type	Change OS	Created By	[redacted]
Image	Public-CAD-HCE-BaseTemplate-2.0.2309.1-x86_64-Standard	Image ID	
Created At	Dec 15, 2023 15:02:21 GMT+08:00	Completed At	--
Status	● Executing		

Execution Information

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

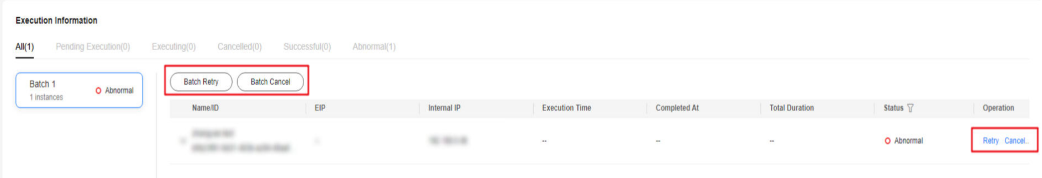
Batch 1 Executing
1 instances

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Dec 15, 2023 15:02:21 GMT+08:00	--	--	● Pending Execution	Cancel

10 Total Records: 1 < 1 >

Step 11 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-25 Canceling or retrying batch tasks



Execution Information

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
			--	--	--	Abnormal	Retry Cancel..

----End

4.3 Batch Operations on RDS Instances

You can batch manage RDS DB instances, including starting, stopping, and restarting RDS DB instances in batches.

4.3.1 Batch Starting RDS Instances

Scenarios

Start RDS database instances in batches on COC.

Precautions

Instances that have been started cannot be selected.

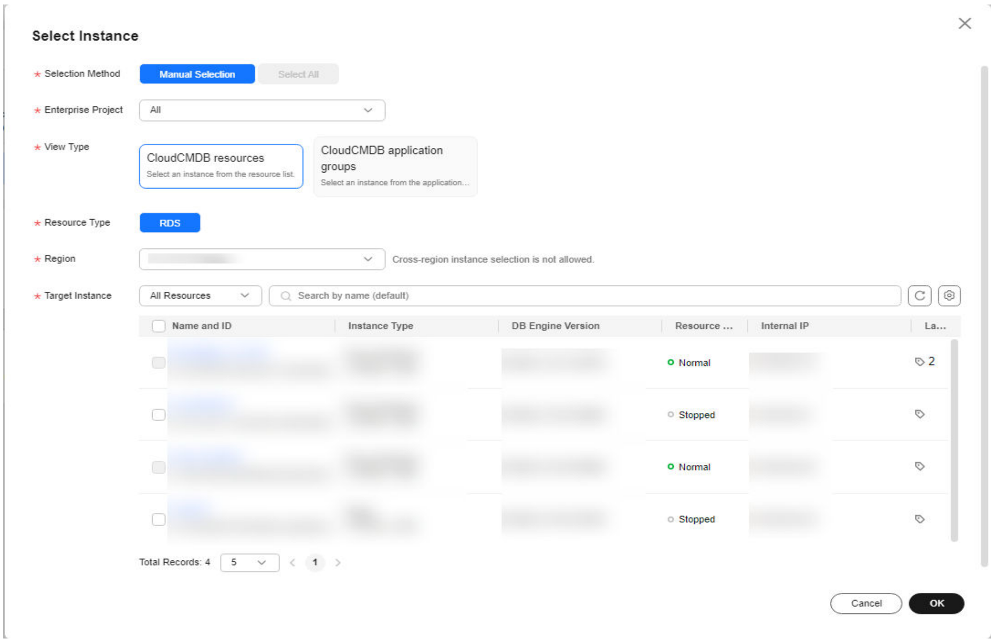
Procedure

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 RDS** in **RDS Operations**.

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

Figure 4-26 Selecting instances



Select Instance

* Selection Method: Manual Selection

* Enterprise Project: All

* View Type: CloudCMDB resources — Select an instance from the resource list.

* Resource Type: RDS

* Region: Cross-region instance selection is not allowed.

* Target Instance: All Resources

Select All
CloudCMDB application groups
Select an instance from the application...
Search by name (default)
Cancel
OK

Name and ID	Instance Type	DB Engine Version	Resource ...	Internal IP	La...
			Normal		2
			Stopped		
			Normal		
			Stopped		

Total Records: 4 5 1

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 target instances are in the same batch.

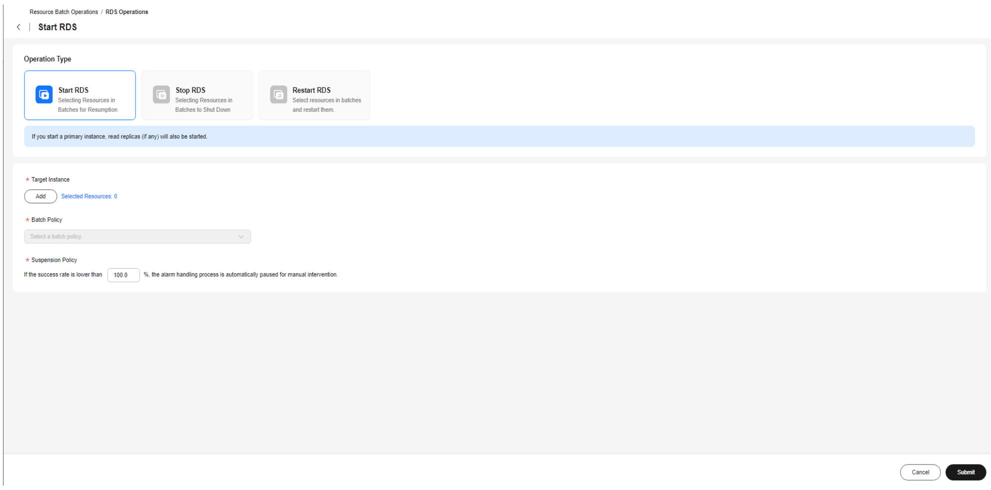
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-27 Starting instances



Resource Batch Operations / RDS Operations

Start RDS

Operation Type

Start RDS
Selecting Resources in Batches for Resumption

Stop RDS
Selecting Resources in Batches to Shut Down

Restart RDS
Select resources in batches and restart them.

If you start a primary instance, read replicas (if any) will also be started.

* Target Instance

Add Selected Resources: 0

* Batch Policy

Select a batch policy.

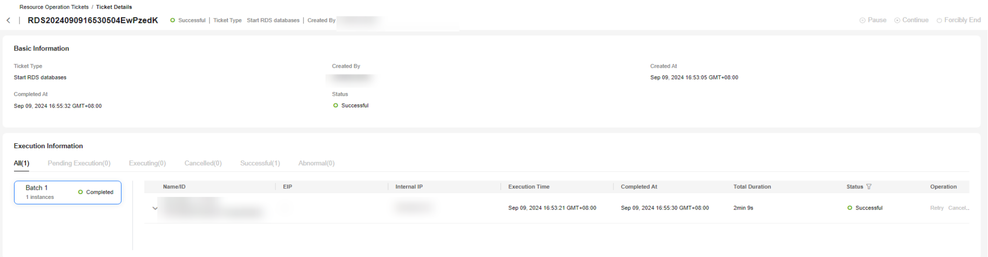
* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Cancel Submit

Step 7 View the execution result.

Figure 4-28 Execution result



Resource Operation Tickets / Ticket Details

RDS2024090916530504EwPzedK ○ Successful | Ticket Type Start RDS databases | Created By [redacted]

Pause Continue Forcibly End

Basic Information

Ticket Type
Start RDS databases

Created By
[redacted]

Created At
Sep 09, 2024 16:53:05 GMT+08:00

Completed At
Sep 09, 2024 16:55:32 GMT+08:00

Status
○ Successful

Execution Information

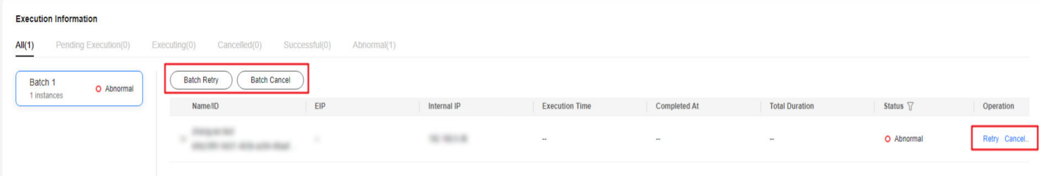
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1
1 instances
○ Completed

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]		[redacted]	Sep 09, 2024 16:53:21 GMT+08:00	Sep 09, 2024 16:55:30 GMT+08:00	2min 9s	○ Successful	Retry Cancel..

Step 8 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-29 Canceling or retrying batch tasks



Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	Abnormal	Retry Cancel..

----End

4.3.2 Batch Stopping RDS Instances

Scenarios

Stop RDS database instances in batches on COC.

Precautions

Instances that have been stopped cannot be selected.

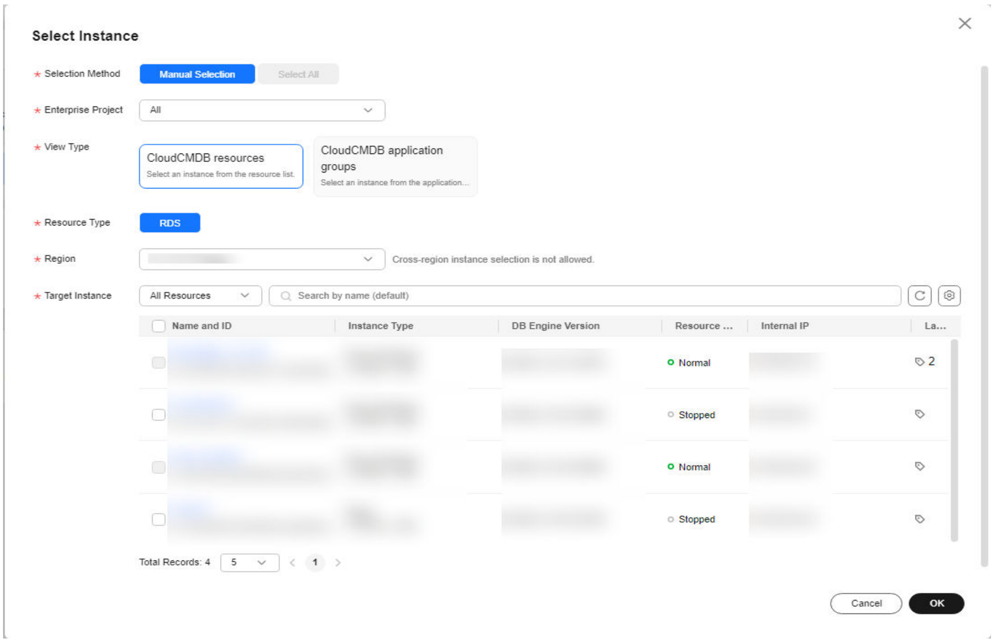
Procedure

Step 1 Log in to **COC**.

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

Step 3 On the **Stop RDS** page, click **Add**.

Figure 4-30 Selecting instances



Select Instance

- * Selection Method: Manual Selection / Select All
- * Enterprise Project: All
- * View Type: CloudCMDB resources (Select an instance from the resource list.) / CloudCMDB application groups (Select an instance from the application...)
- * Resource Type: RDS
- * Region: [redacted] Cross-region instance selection is not allowed.
- * Target Instance: All Resources / Search by name (default)

	Name and ID	Instance Type	DB Engine Version	Resource ...	Internal IP	La...
□	[redacted]	[redacted]	[redacted]	Normal	[redacted]	2
□	[redacted]	[redacted]	[redacted]	Stopped	[redacted]	
□	[redacted]	[redacted]	[redacted]	Normal	[redacted]	
□	[redacted]	[redacted]	[redacted]	Stopped	[redacted]	

Total Records: 4   5   < 1 >

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 target instances are in the same batch.

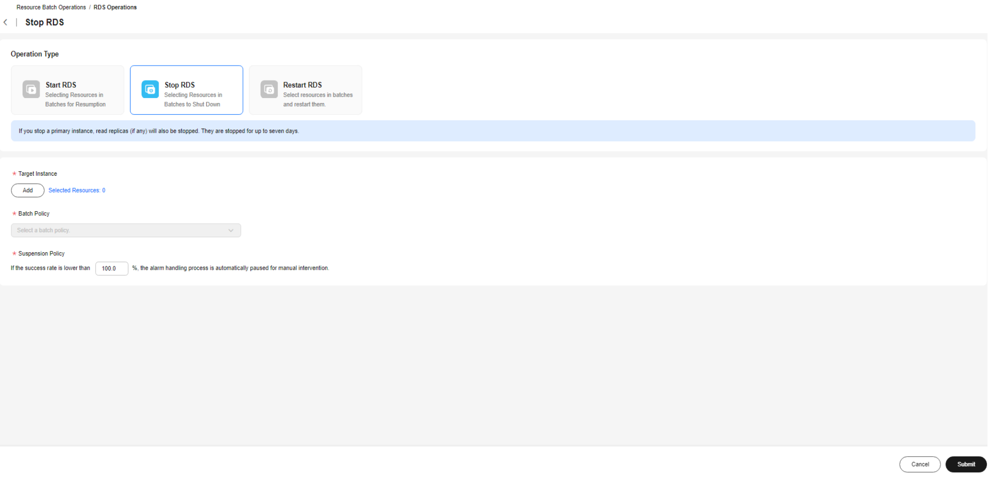
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-31 Stopping RDS instances



Resource Batch Operations / RDS Operations

Stop RDS

Operation Type

Start RDS
Selecting Resources in Batches for Resumption

Stop RDS
Selecting Resources in Batches to Shut Down

Restart RDS
Select resources in batches and restart them.

If you stop a primary instance, read replicas (if any) will also be stopped. They are stopped for up to seven days.

* Target Instance

Add Selected Resources: 0

* Batch Policy

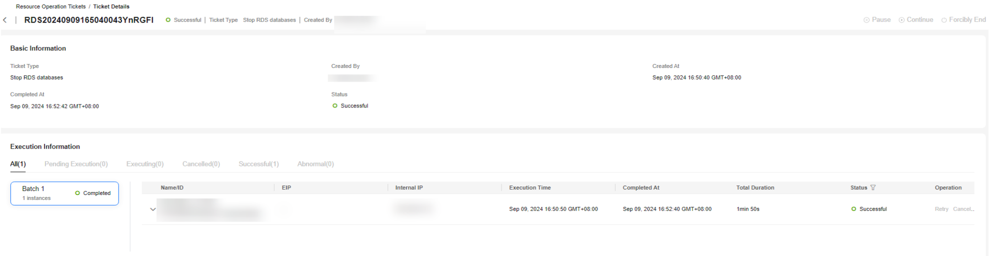
Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 7 View the execution result.

Figure 4-32 Execution result



Resource Operation Tickets / Ticket Details

RDS20240909165040043YnRGFI ○ Successful | Ticket Type Stop RDS databases | Created By [redacted]

Basic Information

Ticket Type: Stop RDS databases

Created By: [redacted]

Created At: Sep 09, 2024 16:50:40 GMT+08:00

Completed At: Sep 09, 2024 16:52:42 GMT+08:00

Status: ○ Successful

Execution Information

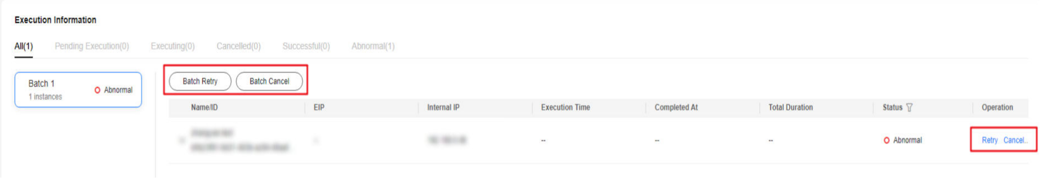
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1 ○ Completed
1 instances

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]		[redacted]	Sep 09, 2024 16:50:50 GMT+08:00	Sep 09, 2024 16:52:40 GMT+08:00	1min 50s	○ Successful	Retry Cancel..

Step 8 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-33 Canceling or retrying batch tasks



Execution Information

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

Batch 1 — 1 instances — Abnormal

Batch Retry | Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	Abnormal	Retry Cancel..

----End

4.3.3 Batch Restarting RDS Instances

Scenarios

Restart RDS database instances in batches on COC.

Precautions

Instances that have been stopped cannot be selected.

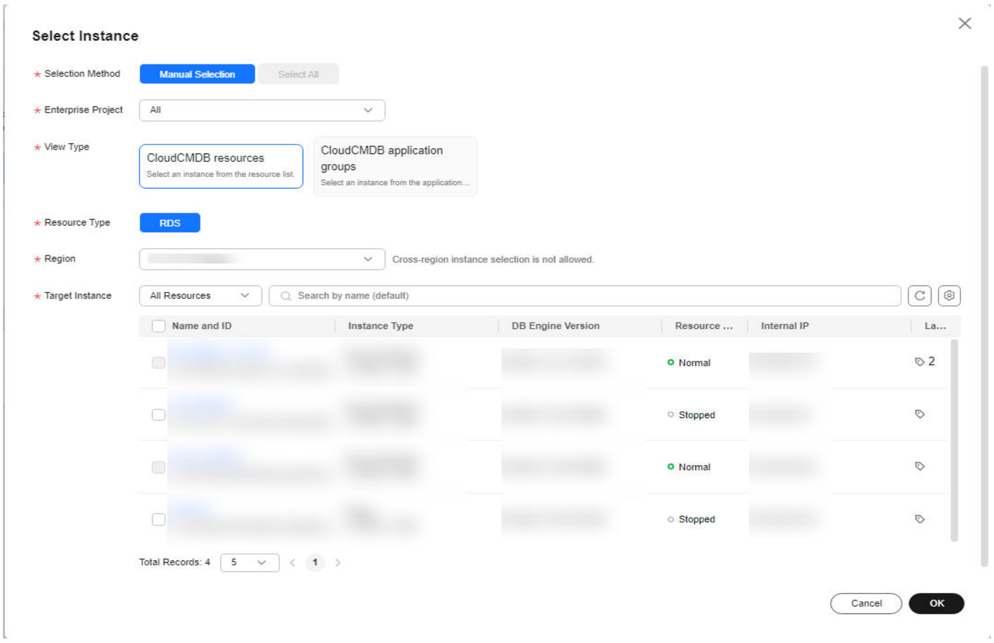
Procedure

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 RDS** in **RDS Operations**.

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

Figure 4-34 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application...)

* Resource Type: RDS

* Region: [redacted] — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

Name and ID	Instance Type	DB Engine Version	Resource ...	Internal IP	La...
[redacted]	[redacted]	[redacted]	Normal	[redacted]	2
[redacted]	[redacted]	[redacted]	Stopped	[redacted]	
[redacted]	[redacted]	[redacted]	Normal	[redacted]	
[redacted]	[redacted]	[redacted]	Stopped	[redacted]	

Total Records: 4 | 5 | < 1 >

Cancel | OK

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 target instances are in the same batch.

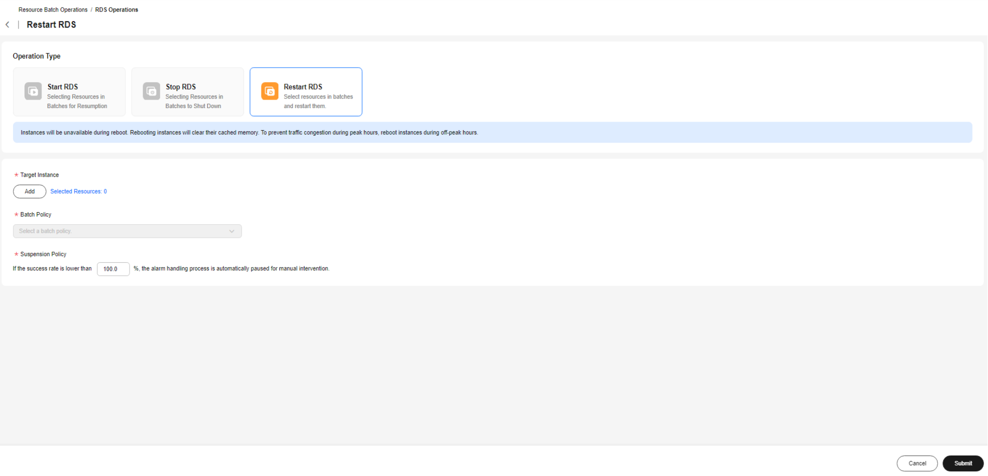
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-35 Restarting RDS instances



Resource Batch Operations / RDS Operations

Restart RDS

Operation Type

Start RDS
Selecting Resources in Batches for Resumption

Stop RDS
Selecting Resources in Batches to Shut Down

Restart RDS
Select resources in batches and restart them.

Instances will be unavailable during reboot. Rebooting instances will clear their cached memory. To prevent traffic congestion during peak hours, reboot instances during off-peak hours.

* Target Instance

Add Selected Resources: 0

* Batch Policy

Select a batch policy.

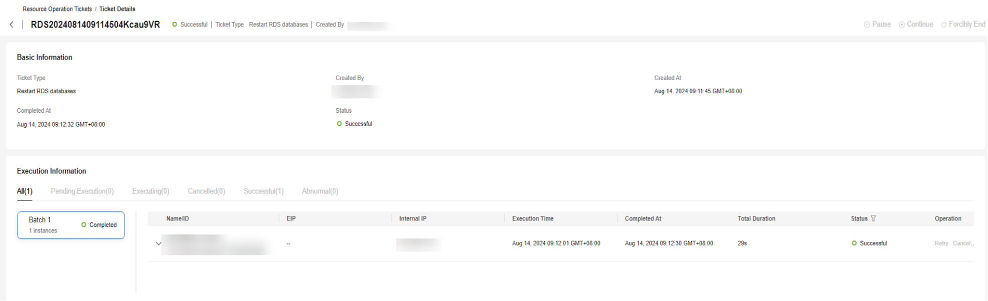
* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Cancel Submit

Step 7 View the execution result.

Figure 4-36 Execution result



Resource Operation Tickets / Ticket Details

RDS2024081409114504Kcau9VR ○ Successful | Ticket Type Restart RDS databases | Created By [redacted]

Pause Continue Forcibly End

Basic Information

Ticket Type
Restart RDS databases

Created By
[redacted]

Created At
Aug 14, 2024 09:11:45 GMT+08:00

Completed At
Aug 14, 2024 09:12:32 GMT+08:00

Status
○ Successful

Execution Information

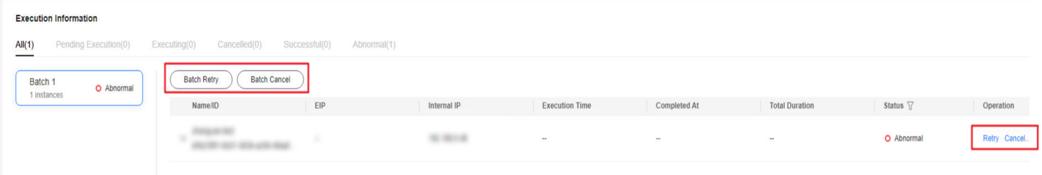
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1 ○ Completed
1 instances

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	--	[redacted]	Aug 14, 2024 09:12:01 GMT+08:00	Aug 14, 2024 09:12:30 GMT+08:00	29s	○ Successful	Retry Cancel..

Step 8 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-37 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances
Abnormal

Batch Retry | Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	Abnormal	Retry Cancel..

----End

4.4 Batch Operations on Flexus L Instances

You can manage Flexus L instances, including starting, stopping, and restarting instances, and reinstalling and changing OSs in batches.

4.4.1 Batch Starting Flexus L Instances

Scenarios

Start Flexus L instances in batches on COC.

Precautions

Instances that have been started cannot be selected.

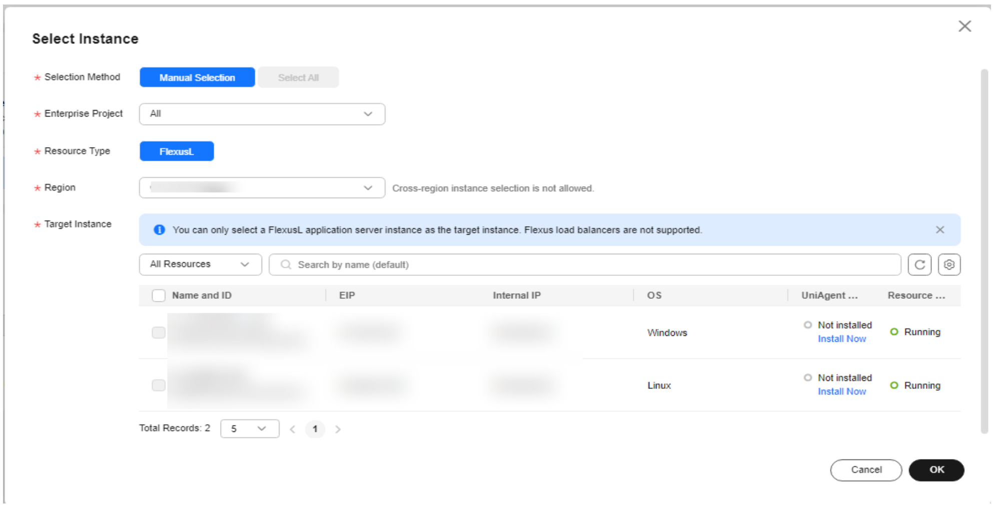
Procedure

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 FlexusL** in **Batch FlexusL Operations**.

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

Figure 4-38 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* Resource Type: FlexusL

* Region: [redacted] Cross-region instance selection is not allowed.

* Target Instance: You can only select a FlexusL application server instance as the target instance. Flexus load balancers are not supported.

All Resources | Search by name (default)

Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
[redacted]	[redacted]	[redacted]	Windows	Not installed Install Now	Running
[redacted]	[redacted]	[redacted]	Linux	Not installed Install Now	Running

Total Records: 2 | 5 | 1

Cancel | OK

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 target instances are in the same batch.

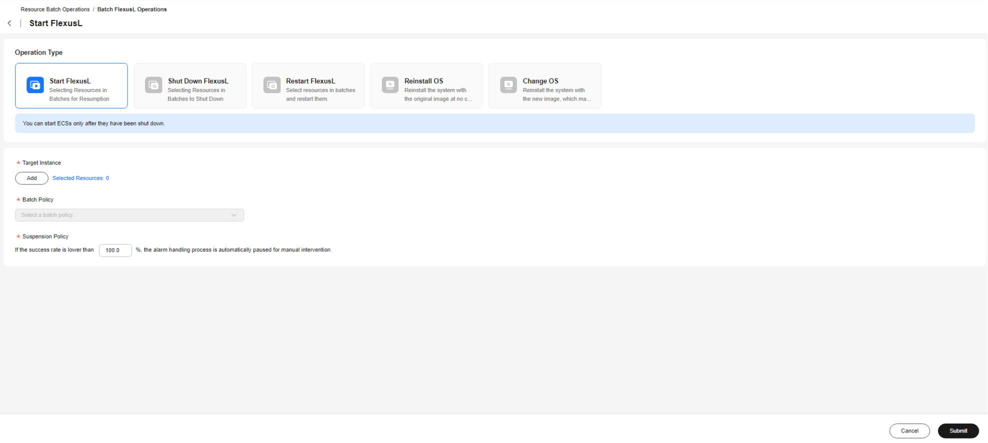
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-39 Starting instances



Resource Batch Operations / Batch FlexusL Operations

Start FlexusL

Operation Type

Start FlexusL — Selecting Resources in Batches for Resumption

Shut Down FlexusL — Selecting Resources in Batches to Shut Down

Restart FlexusL — Select resources in batches and restart them.

Reinstall OS — Reinstall the system with the original image at no c...

Change OS — Reinstall the system with the new image, which ma...

You can start ECSs only after they have been shut down.

* Target Instance

Add Selected Resources: 0

* Batch Policy

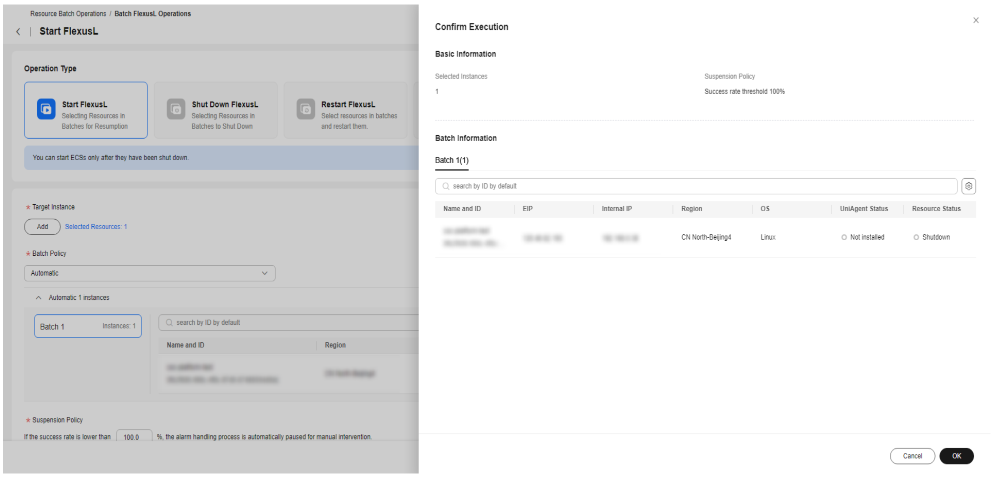
Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

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

Figure 4-40 Confirming the execution



Resource Batch Operations / Batch FlexusL Operations

Start FlexusL

Operation Type

Start FlexusL — Selecting Resources in Batches for Resumption

Shut Down FlexusL — Selecting Resources in Batches to Shut Down

Restart FlexusL — Select resources in batches and restart them.

You can start ECSs only after they have been shut down.

* Target Instance

Add Selected Resources: 1

* Batch Policy

Automatic

Automatic 1 instances

Batch 1 Instances: 1

search by ID by default

Name and ID	Region
[redacted]	[redacted]

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

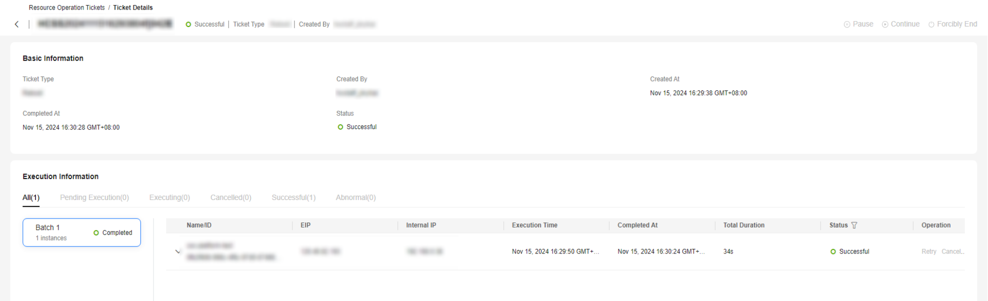
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	CN North-Beijing4	Linux	○ Not installed	○ Shutdown

Step 8 View the execution result.

Figure 4-41 Viewing the result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type [redacted] | Created By [redacted]

Pause Continue Forcibly End

Basic Information

Ticket Type [redacted]	Created By [redacted]	Created At Nov 15, 2024 16:29:38 GMT+08:00
Completed At Nov 15, 2024 16:30:28 GMT+08:00	Status ○ Successful	

Execution Information

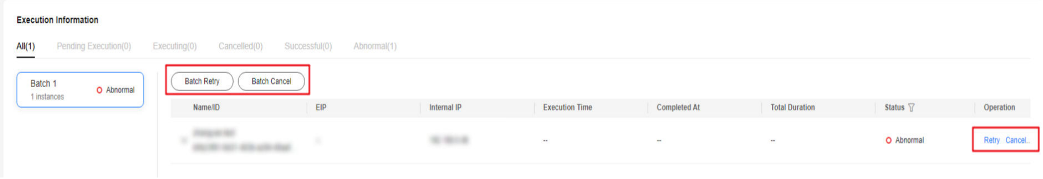
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1 ○ Completed
1 instances

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Nov 15, 2024 16:29:50 GMT+...	Nov 15, 2024 16:30:24 GMT+...	34s	○ Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-42 Canceling or retrying batch tasks



Execution Information

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

Batch 1 ○ Abnormal
1 instances

Batch Retry Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.4.2 Batch Stopping Flexus L Instances

Scenarios

Stop Flexus L instances in batches on COC.

Precautions

Stopped instances cannot be selected.

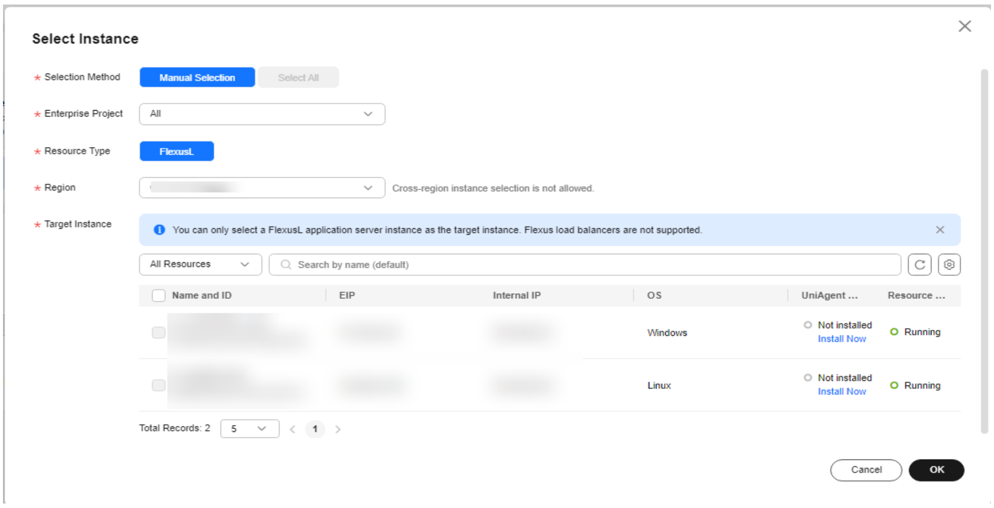
Procedure

Step 1 Log in to COC.

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

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

Figure 4-43 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* Resource Type: FlexusL

* Region: Cross-region instance selection is not allowed.

* Target Instance

You can only select a FlexusL application server instance as the target instance. Flexus load balancers are not supported.

All Resources | Search by name (default)

Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
			Windows	Not installed Install Now	Running
			Linux	Not installed Install Now	Running

Total Records: 2 | 5 | 1

Cancel | OK

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 target instances are in the same batch.

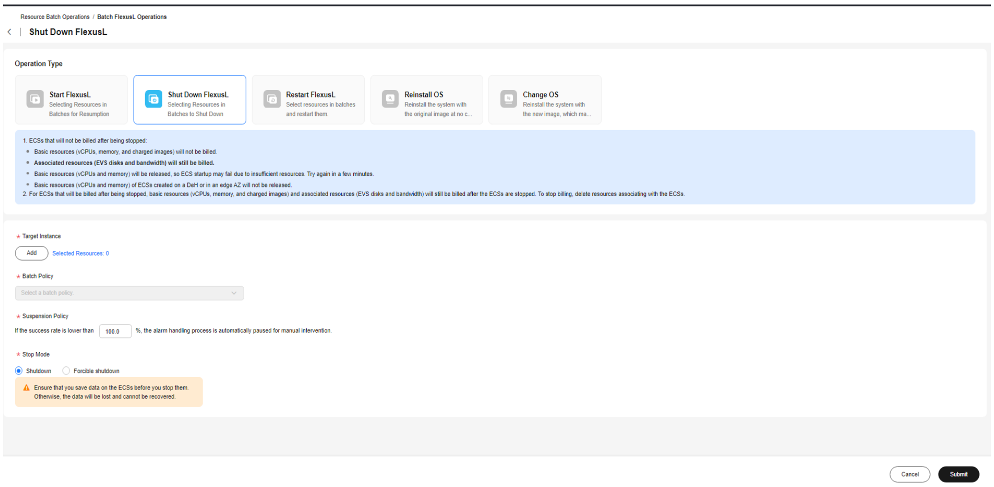
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-44 Stopping instances



Resource Batch Operations / Batch FlexusL Operations

Shut Down FlexusL

Operation Type

- Start FlexusL: Selecting Resources in Batches for Resumption
- Shut Down FlexusL: Selecting Resources in Batches to Shut Down
- Restart FlexusL: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...
- Change OS: Reinstall the system with the new image, which ma...

1. ECSs that will not be billed after being stopped:
   - Basic resources (vCPUs, memory, and charged images) will not be billed.
   - **Associated resources (EVS disks and bandwidth) will still be billed.**
   - Basic resources (vCPUs and memory) will be released, so ECS startup may fail due to insufficient resources. Try again in a few minutes.
   - Basic resources (vCPUs and memory) of ECSs created on a DeH or in an edge AZ will not be released.
2. For ECSs that will be billed after being stopped, basic resources (vCPUs, memory, and charged images) and associated resources (EVS disks and bandwidth) will still be billed after the ECSs are stopped. To stop billing, delete resources associating with the ECSs.

* Target Instance

Add | Selected Resources: 0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

* Stop Mode

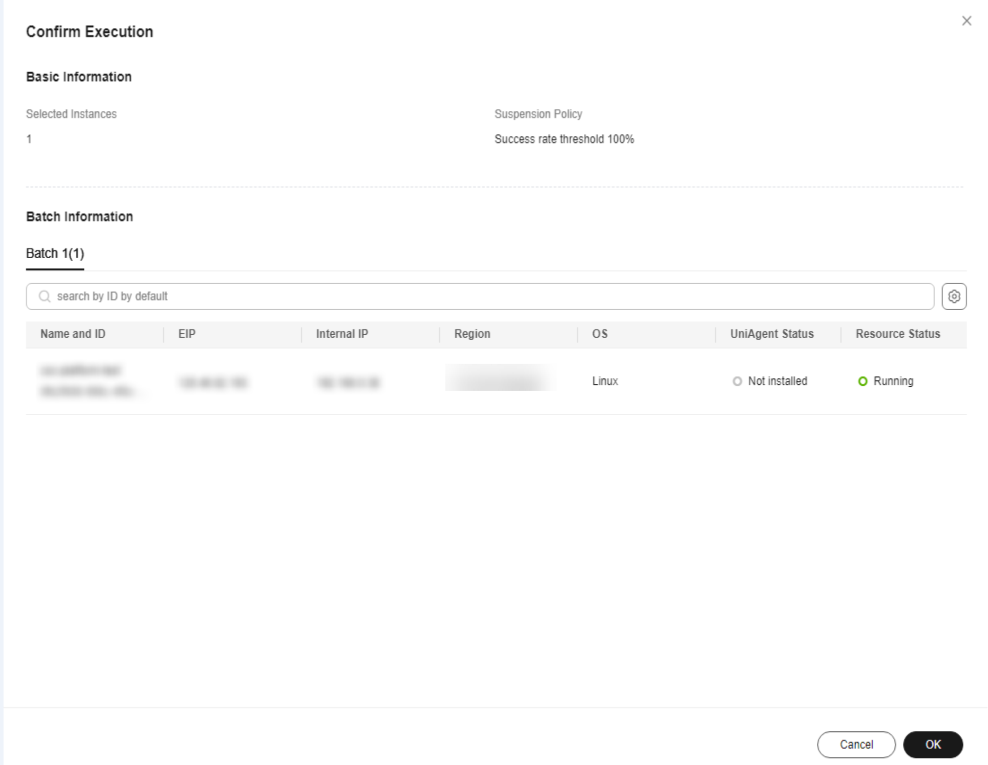
● Shutdown ○ Forcible shutdown

Ensure that you save data on the ECSs before you stop them. Otherwise, the data will be lost and cannot be recovered.

Cancel | Submit

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

Figure 4-45 Confirming the execution



Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

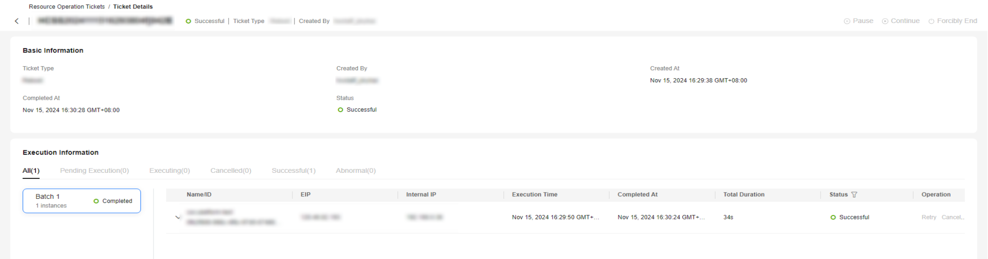
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	○ Not installed	○ Running

Step 8 View the execution result.

Figure 4-46 Viewing the result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type [redacted] | Created By [redacted]

Basic Information

Ticket Type: [redacted]

Created By: [redacted]

Created At: Nov 15, 2024 16:29:38 GMT+08:00

Completed At: Nov 15, 2024 16:30:28 GMT+08:00

Status: ○ Successful

Execution Information

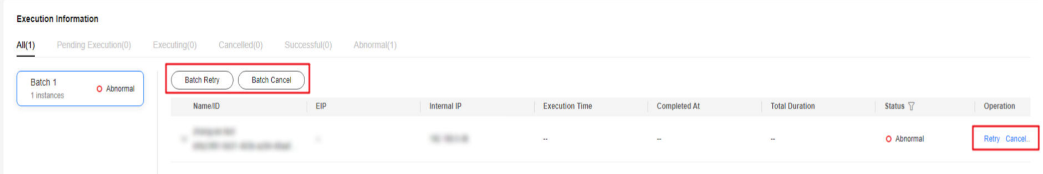
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1, 1 instances, ○ Completed

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Nov 15, 2024 16:29:50 GMT+...	Nov 15, 2024 16:30:24 GMT+...	34s	○ Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-47 Canceling or retrying batch tasks



Execution Information

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

Batch 1, 1 instances, ○ Abnormal

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.4.3 Batch Restarting Flexus L Instances

Scenarios

Restart Flexus L instances in batches on COC.

Precautions

Stopped instances cannot be selected.

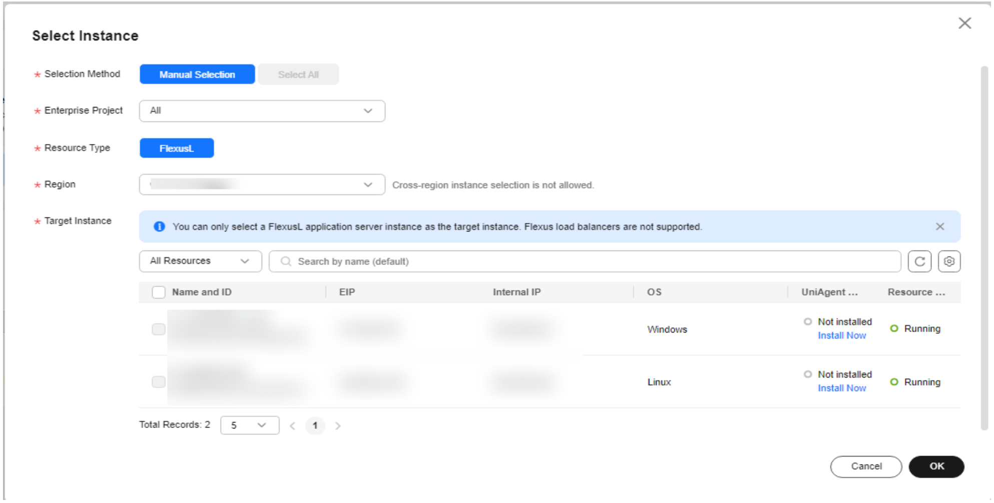
Procedure

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 FlexusL** in **Batch FlexusL Operations**.

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

Figure 4-48 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* Resource Type: FlexusL

* Region: [redacted] Cross-region instance selection is not allowed.

* Target Instance

You can only select a FlexusL application server instance as the target instance. Flexus load balancers are not supported.

All Resources | Search by name (default)

□ Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
□ [redacted]	[redacted]	[redacted]	Windows	○ Not installed Install Now	○ Running
□ [redacted]	[redacted]	[redacted]	Linux	○ Not installed Install Now	○ Running

Total Records: 2 | 5 | < 1 >

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 target instances are in the same batch.

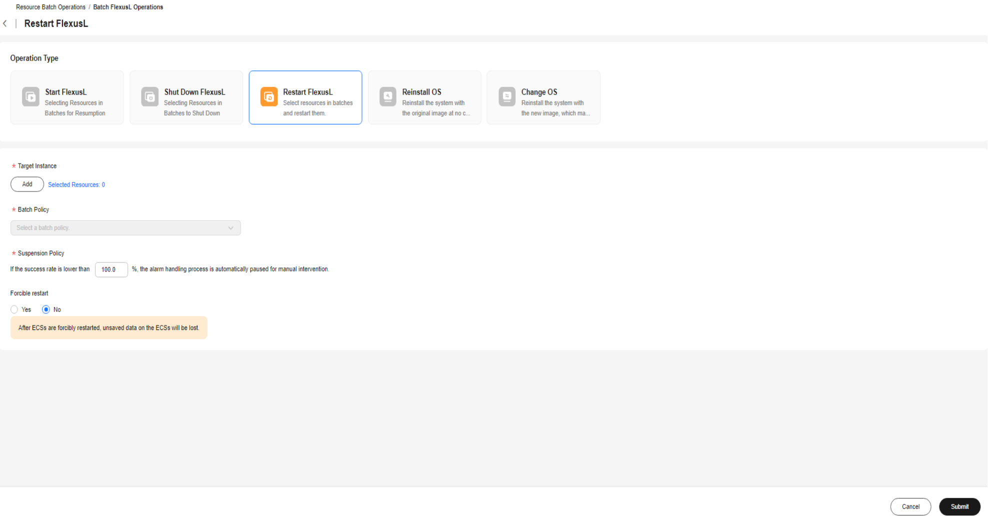
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Click **Submit**.

Figure 4-49 Restarting instances



Resource Batch Operations / Batch FlexusL Operations

Restart FlexusL

Operation Type

- Start FlexusL: Selecting Resources in Batches for Resumption
- Shut Down FlexusL: Selecting Resources in Batches to Shut Down
- Restart FlexusL: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...
- Change OS: Reinstall the system with the new image, which ma...

* Target Instance

Add Selected Resources: 0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

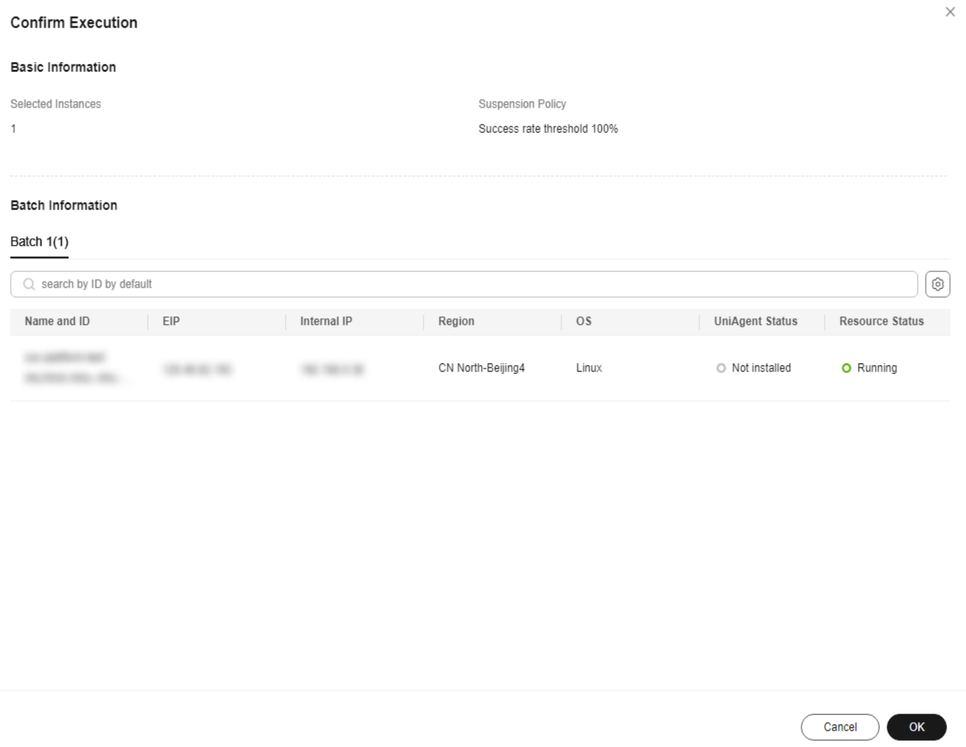
Forcible restart

○ Yes ● No

After ECSs are forcibly restarted, unsaved data on the ECSs will be lost.

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

Figure 4-50 Confirming the execution



Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

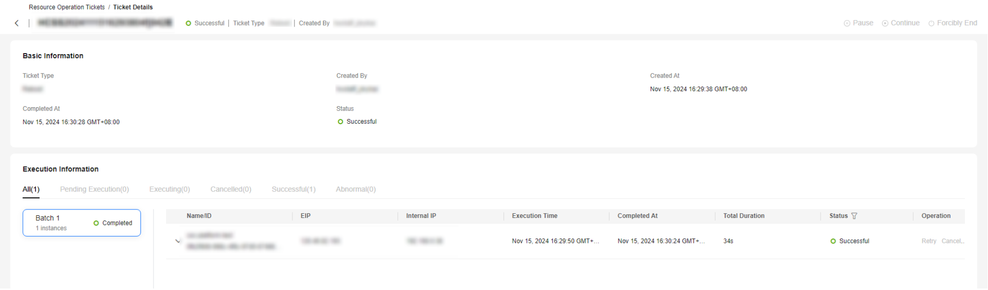
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	CN North-Beijing4	Linux	○ Not installed	○ Running

Step 8 View the execution result.

Figure 4-51 Viewing the result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type [redacted] | Created By [redacted]

○ Pause ○ Continue ○ Forcibly End

Basic Information

Ticket Type [redacted]	Created By [redacted]	Created At Nov 15, 2024 16:29:38 GMT+08:00
Completed At Nov 15, 2024 16:30:28 GMT+08:00	Status ○ Successful	

Execution Information

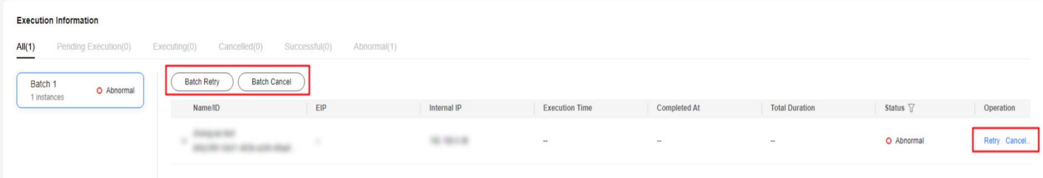
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1
1 instances ○ Completed

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Nov 15, 2024 16:29:50 GMT+...	Nov 15, 2024 16:30:24 GMT+...	34s	○ Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-52 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances ○ Abnormal

Batch Retry Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.4.4 Batch Reinstalling OSs

Scenarios

Reinstall the OSs of FlexusL instances in batches on COC.

Precautions

If there are instances that are not stopped, select **Stop now**.

If no instance is stopped, submit the task.

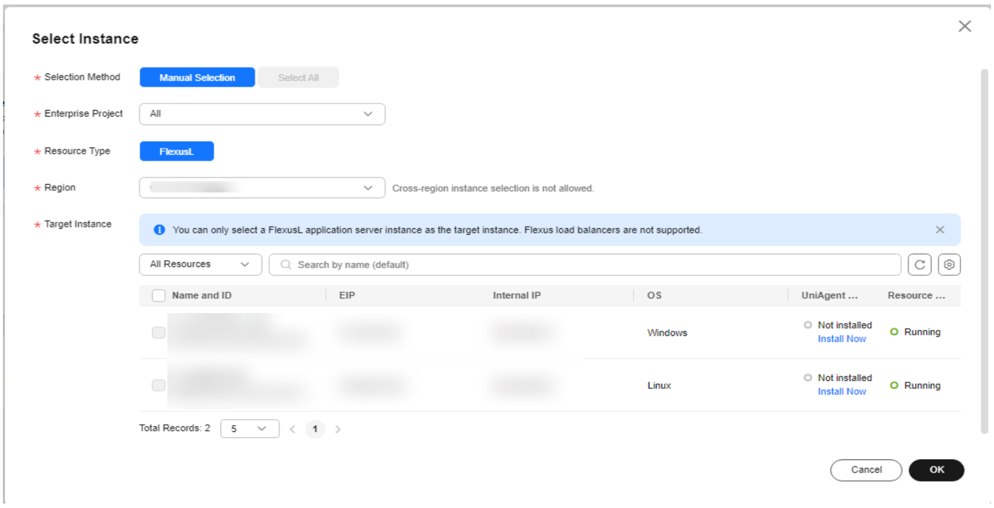
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**, and click **Reinstall OS** in **Batch FlexusL Operations**.

Step 3 On the **Reinstall OS** page, click **Add**.

Figure 4-53 Reinstalling OSs



Select Instance

- * Selection Method: **Manual Selection** | Select All
- * Enterprise Project: All
- * Resource Type: **FlexusL**
- * Region: Cross-region instance selection is not allowed.
- * Target Instance: You can only select a FlexusL application server instance as the target instance. Flexus load balancers are not supported.

All Resources | Search by name (default)

☐ Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
☐			Windows	○ Not installed Install Now	○ Running
☐			Linux	○ Not installed Install Now	○ Running

Total Records: 2 | 5 | 1

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 target instances are in the same batch.

Step 5 Set **Suspension Policy**.

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

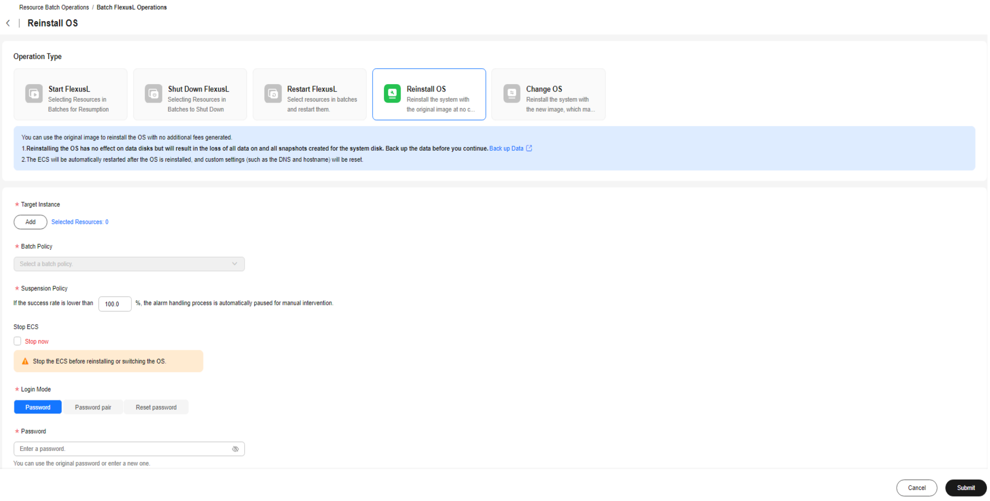
Step 6 Set **Login Mode**.

Login mode:

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

Step 7 Click **Submit**.

Figure 4-54 Reinstalling OSs



Resource Batch Operations / Batch FlexusL Operations

Reinstall OS

Operation Type

Start FlexusL
Selecting Resources in Batches for Resumption
Shut Down FlexusL
Selecting Resources in Batches to Shut Down
Restart FlexusL
Select resources in batches and restart them.
Reinstall OS
Reinstall the system with the original image at no c...
Change OS
Reinstall the system with the new image, which ma...

You can use the original image to reinstall the OS with no additional fees generated.
1.Reinstalling the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system disk. Back up the data before you continue. Back up Data
2.The ECS will be automatically restarted after the OS is reinstalled, and custom settings (such as the DNS and hostname) will be reset.

* Target Instance
Add Selected Resources: 0

* Batch Policy
Select a batch policy.

* Suspension Policy
If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Stop ECS
□ Stop now

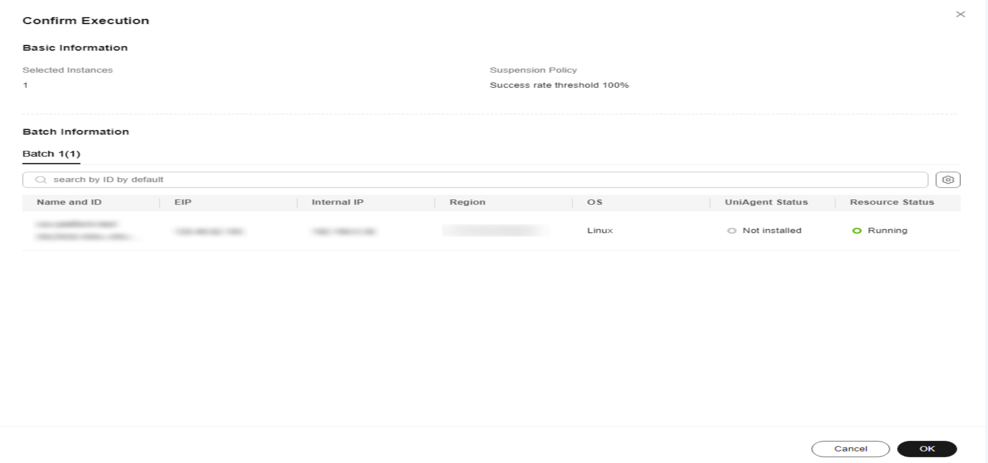
Stop the ECS before reinstalling or switching the OS.

* Login Mode
Password | Password pair | Reset password

* Password
Enter a password.
You can use the original password or enter a new one.

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

Figure 4-55 Confirming the execution



Confirm Execution

Basic Information

Selected Instances
1

Suspension Policy
Success rate threshold 100%

Batch Information

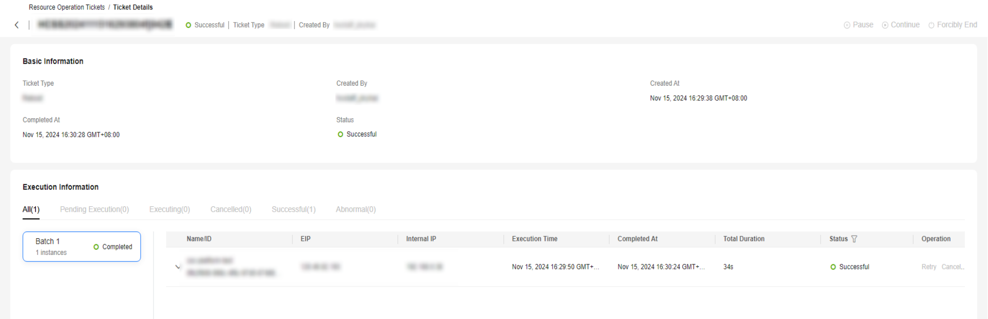
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	○ Not installed	○ Running

Step 9 View the execution result.

Figure 4-56 Viewing the execution result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type [redacted] | Created By [redacted]

Basic Information

Ticket Type
[redacted]

Created By
[redacted]

Created At
Nov 15, 2024 16:29:38 GMT+08:00

Completed At
Nov 15, 2024 16:30:28 GMT+08:00

Status
○ Successful

Execution Information

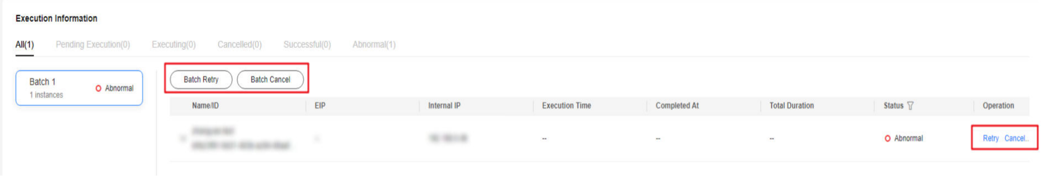
All(1) | Pending Execution(0) | Executing(0) | Cancelled(0) | Successful(1) | Abnormal(0)

Batch 1 ○ Completed
1 instances

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Nov 15, 2024 16:29:50 GMT+...	Nov 15, 2024 16:30:24 GMT+...	34s	○ Successful	Retry Cancel..

Step 10 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-57 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances ○ Abnormal

Batch Retry Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.4.5 Batch Changing OSs

Scenarios

Change the OSs of Flexus L instances in batches on COC.

Precautions

If there are instances that are not stopped, select **Stop now**.

If no instance is stopped, submit the task.

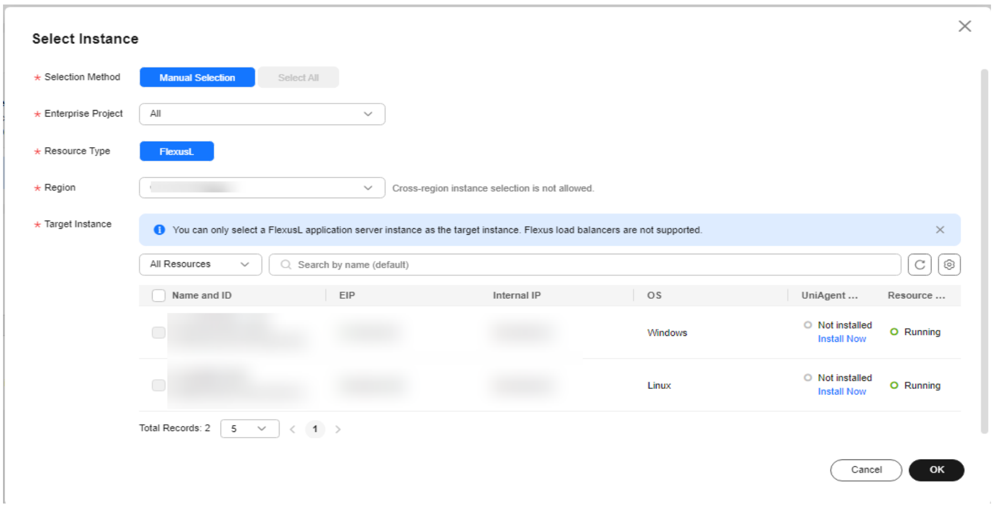
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**, and click **Change OS** in **Batch FlexusL Operations**.

Step 3 On the **Change OS** page, click **Add**.

Figure 4-58 Changing OSs



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* Resource Type: FlexusL

* Region: [redacted] Cross-region instance selection is not allowed.

* Target Instance: You can only select a FlexusL application server instance as the target instance. Flexus load balancers are not supported.

All Resources | Search by name (default)

□ Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
□ [redacted]	[redacted]	[redacted]	Windows	○ Not installed Install Now	○ Running
□ [redacted]	[redacted]	[redacted]	Linux	○ Not installed Install Now	○ Running

Total Records: 2 | 5 | < 1 >

Cancel OK

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 target instances are in the same batch.

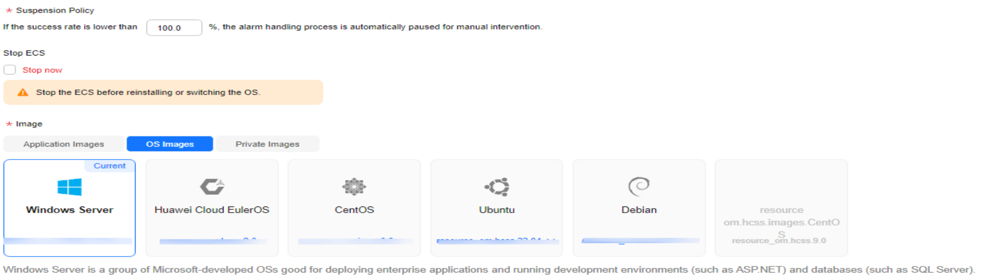
Step 5 Set **Suspension Policy**.

NOTE

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

Step 6 Select the image that you want to switch to.

Figure 4-59 Switching images



* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Stop ECS

□ Stop now

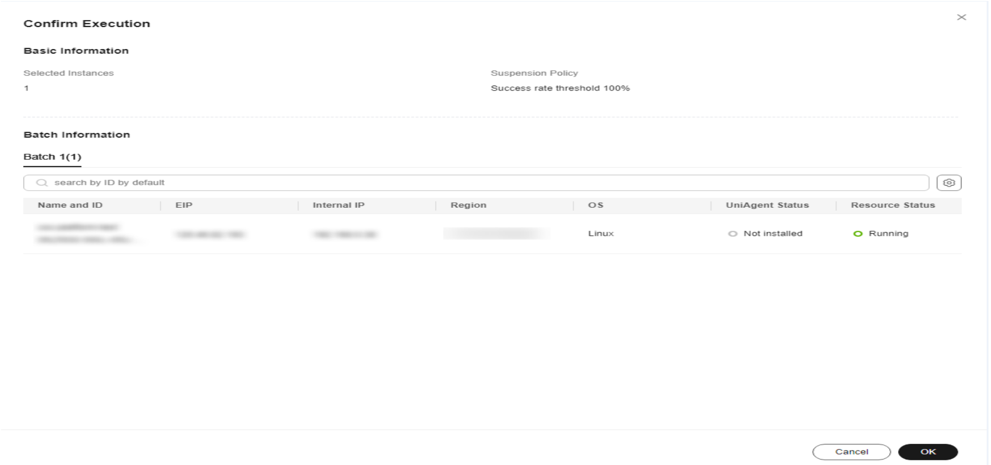
Stop the ECS before reinstalling or switching the OS.

* Image

Windows Server is a group of Microsoft-developed OSs good for deploying enterprise applications and running development environments (such as ASP.NET) and databases (such as SQL Server).

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

Figure 4-60 Confirming the execution



Confirm Execution

Basic Information

Selected Instances
1

Suspension Policy
Success rate threshold 100%

Batch Information

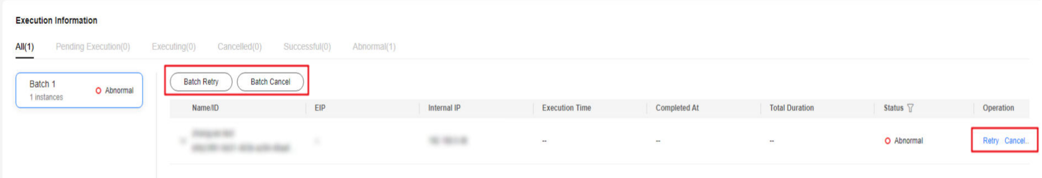
Batch 1(1)

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	○ Not installed	○ Running

Step 8 View the execution result.

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-61 Canceling or retrying batch tasks



Execution Information

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

Batch 1 ○ Abnormal
1 instances

Batch Retry | Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.5 Batch Operations on BMSs

You can manage MBS instances, including starting, stopping, and restarting instances, and reinstalling OSs in batches.

4.5.1 Batch Starting BMSs

Scenarios

Start BMSs in batches on COC.

Precautions

Instances that have been started cannot be selected.

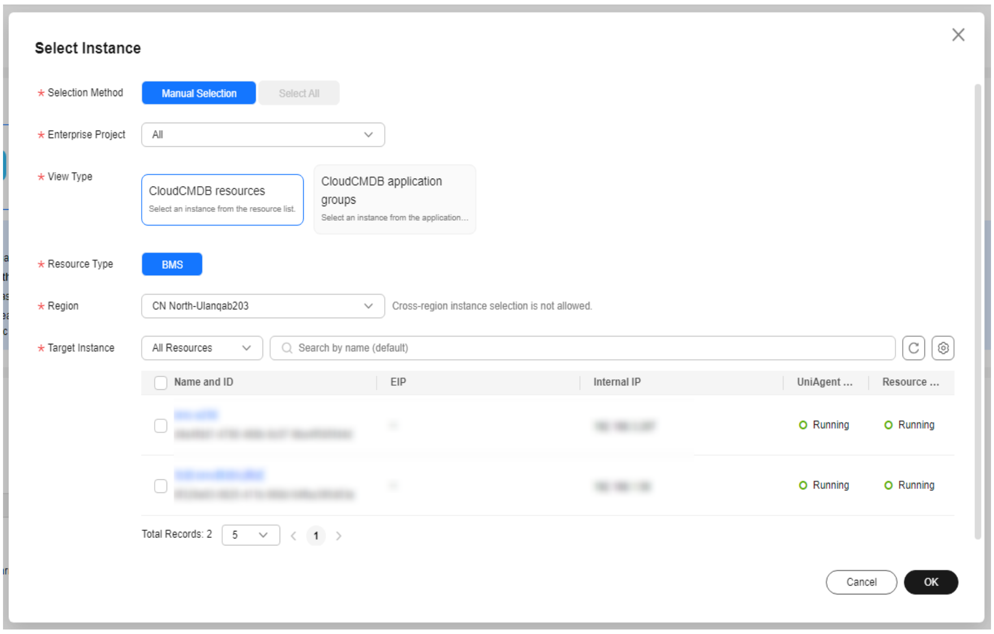
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**. On the displayed page, click the **Bare Metal Server (BMS)** tab, and then click the **Start BMSs** card on the tab page.

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

Figure 4-62 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources — Select an instance from the resource list. | CloudCMDB application groups — Select an instance from the application...

* Resource Type: BMS

* Region: CN North-Ulanqab203 — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

□ Name and ID	EIP	Internal IP	UniAgent ...	Resource ...
□ [redacted]	[redacted]	[redacted]	○ Running	○ Running
□ [redacted]	[redacted]	[redacted]	○ Running	○ Running

Total Records: 2 | 5 | < 1 >

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 target instances are in the same batch.

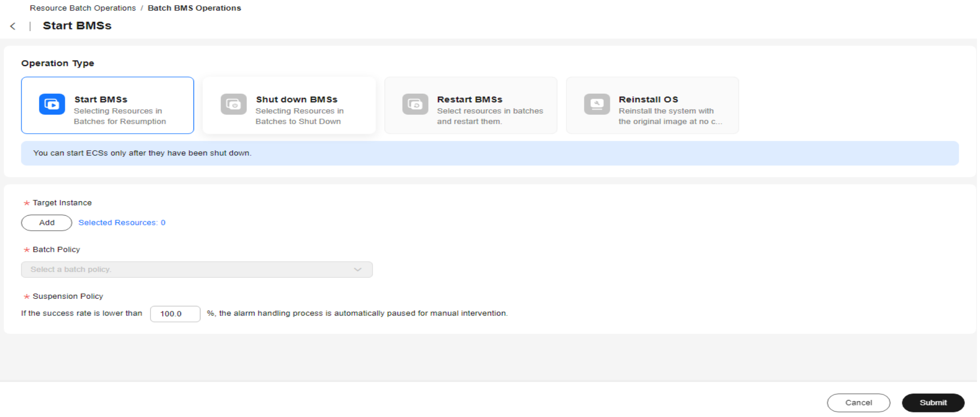
Step 5 Set **Suspension Policy**.

NOTE

- You can set the execution success rate. When the number of failed instances reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
- The value is from 0 to 100 and can be accurate to one decimal place.

Step 6 Click **Submit**.

Figure 4-63 Starting instances



Resource Batch Operations / Batch BMS Operations

Start BMSs

Operation Type

- Start BMSs — Selecting Resources in Batches for Resumption
- Shut down BMSs — Selecting Resources in Batches to Shut Down
- Restart BMSs — Select resources in batches and restart them.
- Reinstall OS — Reinstall the system with the original image at no c...

You can start ECSs only after they have been shut down.

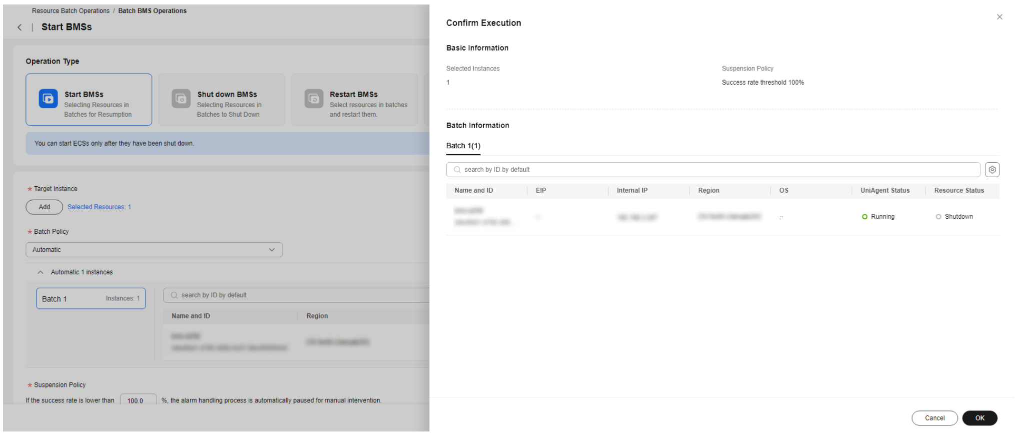
* Target Instance: Add | Selected Resources: 0

* Batch Policy: Select a batch policy.

* Suspension Policy: If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

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

Figure 4-64 Confirming the execution



Resource Batch Operations / Batch BMS Operations

Start BMSs

Operation Type

- Start BMSs: Selecting Resources in Batches for Resumption
- Shut down BMSs: Selecting Resources in Batches to Shut Down
- Restart BMSs: Select resources in batches and restart them.

You can start ECSs only after they have been shut down.

* Target Instance: Add Selected Resources: 1

* Batch Policy: Automatic

Automatic 1 instances

Batch 1 Instances: 1

Name and ID	Region
[illegible]	[illegible]

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

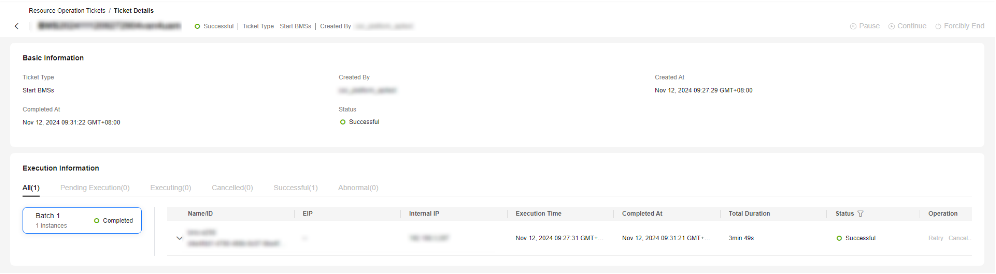
Batch Information

Batch 1(1)

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[illegible]	[illegible]	[illegible]	[illegible]	--	Running	Shutdown

Step 8 View the execution result.

Figure 4-65 Viewing the result



Resource Operation Tickets / Ticket Details

Successful | Ticket Type Start BMSs | Created By [illegible]

Basic Information

Ticket Type: Start BMSs

Created By: [illegible]

Created At: Nov 12, 2024 09:27:29 GMT+08:00

Completed At: Nov 12, 2024 09:31:22 GMT+08:00

Status: Successful

Execution Information

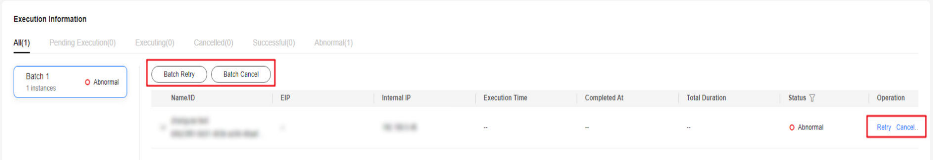
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1 1 instances Completed

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[illegible]	[illegible]	[illegible]	Nov 12, 2024 09:27:31 GMT+...	Nov 12, 2024 09:31:21 GMT+...	3min 49s	Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-66 Canceling or retrying a batch BMS startup task



Execution Information

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

Batch 1 1 instances Abnormal

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[illegible]	[illegible]	[illegible]	--	--	--	Abnormal	Retry Cancel..

----End

4.5.2 Batch Stopping BMSs

Scenarios

Stop BMSs in batches on COC.

Precautions

Stopped instances cannot be selected.

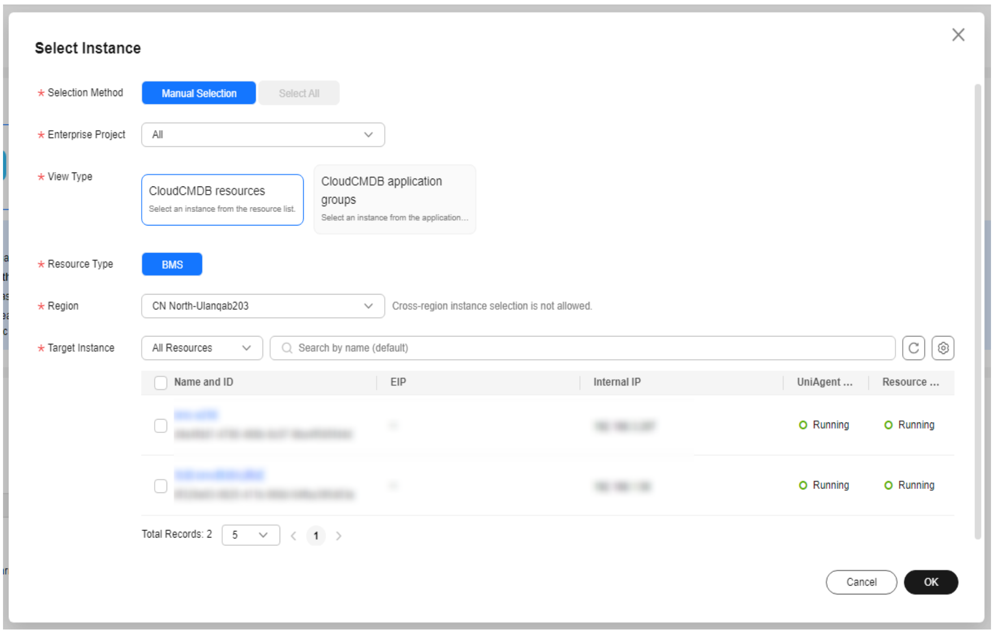
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**. On the displayed page, click the **Bare Metal Server** tab, and then click the **Shut Down BMSs** card on the tab page.

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

Figure 4-67 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application...)

* Resource Type: BMS

* Region: CN North-Ulanqab203 — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

□ Name and ID	EIP	Internal IP	UniAgent ...	Resource ...
□ [redacted]	[redacted]	[redacted]	○ Running	○ Running
□ [redacted]	[redacted]	[redacted]	○ Running	○ Running

Total Records: 2 | 5 | < 1 >

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 target instances are in the same batch.

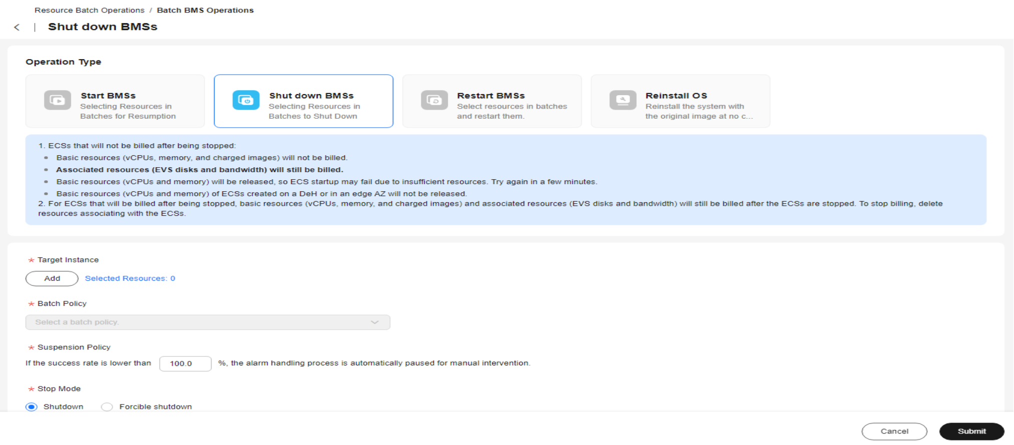
Step 5 Set **Suspension Policy**.

NOTE

- You can set the execution success rate. When the number of failed instances reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
- The value is from 0 to 100 and can be accurate to one decimal place.

Step 6 Click **Submit**.

Figure 4-68 Stopping instances



Resource Batch Operations / Batch BMS Operations

Shut down BMSs

Operation Type

- Start BMSs: Selecting Resources in Batches for Resumption
- Shut down BMSs: Selecting Resources in Batches to Shut Down
- Restart BMSs: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...

1. ECSs that will not be billed after being stopped:
   - Basic resources (vCPUs, memory, and charged images) will not be billed.
   - **Associated resources (EVS disks and bandwidth) will still be billed.**
   - Basic resources (vCPUs and memory) will be released, so ECS startup may fail due to insufficient resources. Try again in a few minutes.
   - Basic resources (vCPUs and memory) of ECSs created on a DeH or in an edge AZ will not be released.
2. For ECSs that will be billed after being stopped, basic resources (vCPUs, memory, and charged images) and associated resources (EVS disks and bandwidth) will still be billed after the ECSs are stopped. To stop billing, delete resources associating with the ECSs.

* Target Instance

Add Selected Resources: 0

* Batch Policy

Select a batch policy.

* Suspension Policy

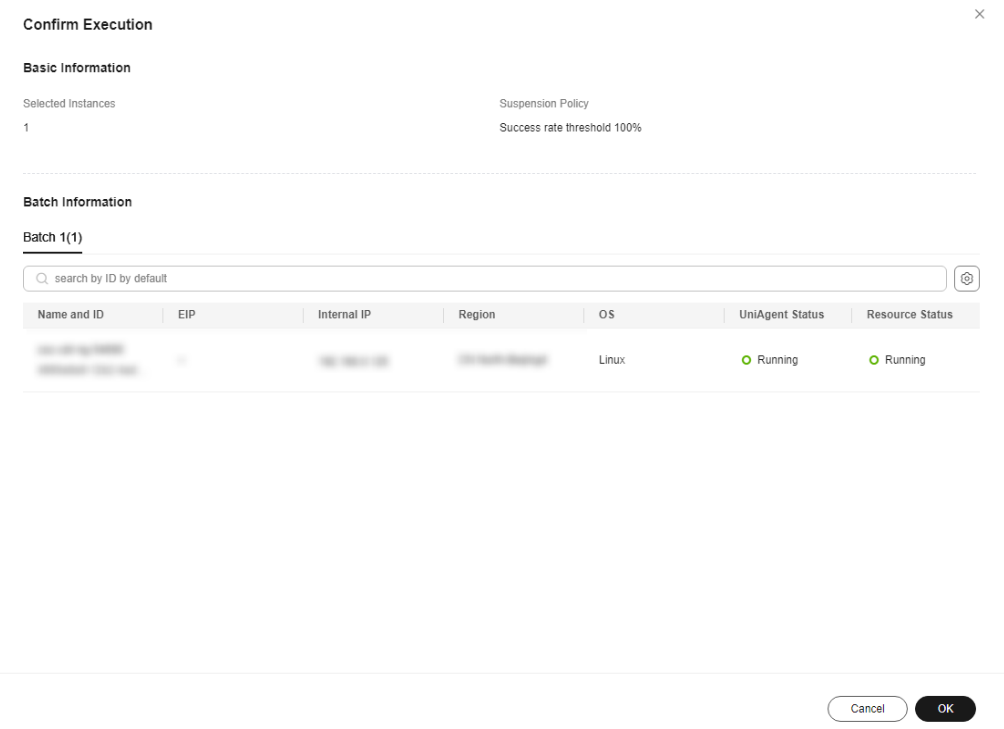
If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

* Stop Mode

● Shutdown ○ Forcible shutdown

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

Figure 4-69 Confirming the execution



Confirm Execution

Basic Information

Selected Instances: 1

Suspension Policy: Success rate threshold 100%

Batch Information

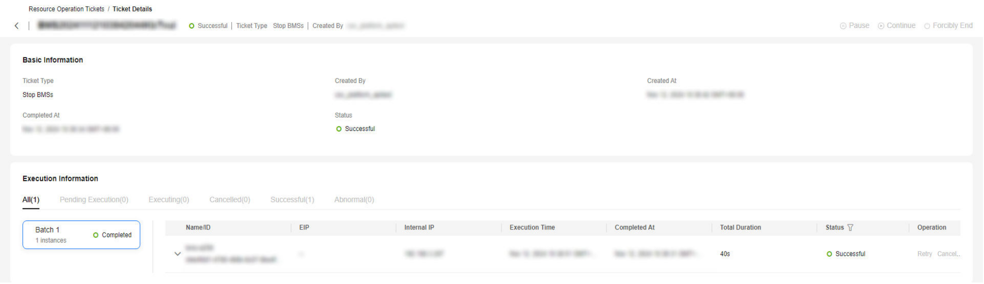
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	○ Running	○ Running

Step 8 View the execution result.

Figure 4-70 Viewing the result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type Stop BMSs | Created By [redacted]

Basic Information

Ticket Type: Stop BMSs
Created By: [redacted]
Created At: [redacted]
Completed At: [redacted]
Status: ○ Successful

Execution Information

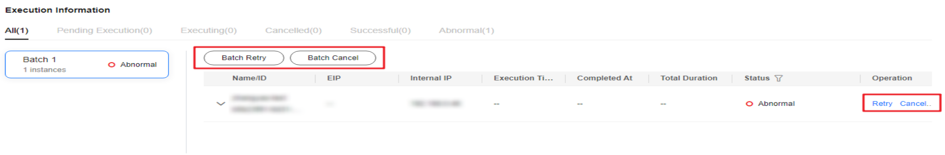
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1
1 instances ○ Completed

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	--	[redacted]	[redacted]	[redacted]	40s	○ Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the **Operation** column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the **Operation** column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-71 Canceling or retrying batch tasks



Execution Information

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

Batch 1
1 instances ○ Abnormal

Name/ID	EIP	Internal IP	Execution Ti...	Completed At	Total Duration	Status	Operation
[redacted]	--	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.5.3 Batch Restarting BMSs

Scenarios

Restart BMS instances in batches on COC.

Precautions

Stopped instances cannot be selected.

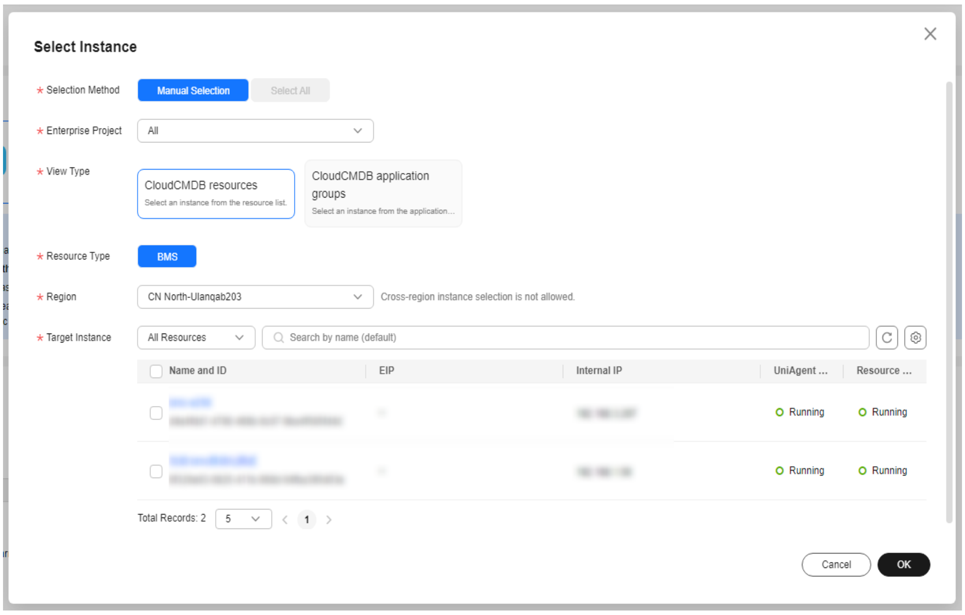
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**. On the displayed page, click the **Bare Metal Server (BMS)** tab, and then click the **Restart BMSs** card on the tab page.

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

Figure 4-72 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application...)

* Resource Type: BMS

* Region: CN North-Ulanqab203 — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

□ Name and ID	EIP	Internal IP	UniAgent ...	Resource ...
□ [redacted]	-	[redacted]	Running	Running
□ [redacted]	-	[redacted]	Running	Running

Total Records: 2 | 5 | < 1 >

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 target instances are in the same batch.

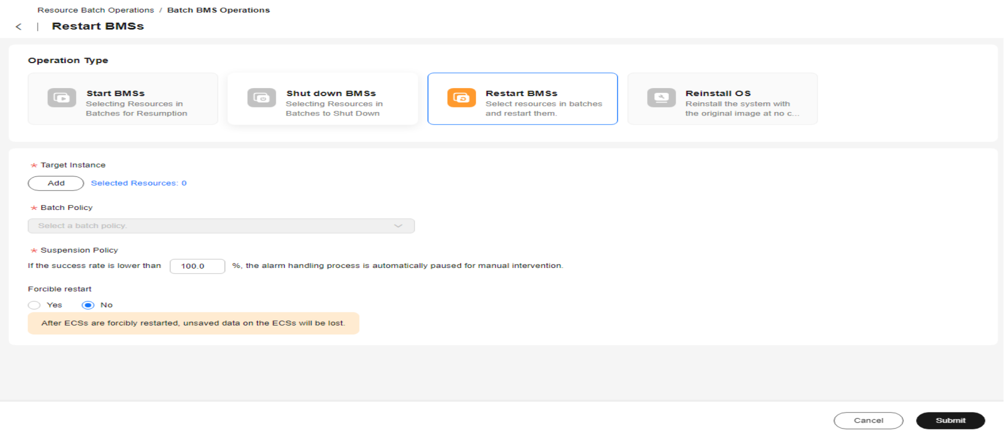
Step 5 Set **Suspension Policy**.

NOTE

- You can set the execution success rate. When the number of failed instances reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
- The value is from 0 to 100 and can be accurate to one decimal place.

Step 6 Click **Submit**.

Figure 4-73 Restarting instances



Resource Batch Operations / Batch BMS Operations

< | Restart BMSs

Operation Type

- Start BMSs: Selecting Resources in Batches for Resumption
- Shut down BMSs: Selecting Resources in Batches to Shut Down
- Restart BMSs: Select resources in batches and restart them.
- Reinstall OS: Reinstall the system with the original image at no c...

* Target Instance: Add | Selected Resources: 0

* Batch Policy: Select a batch policy.

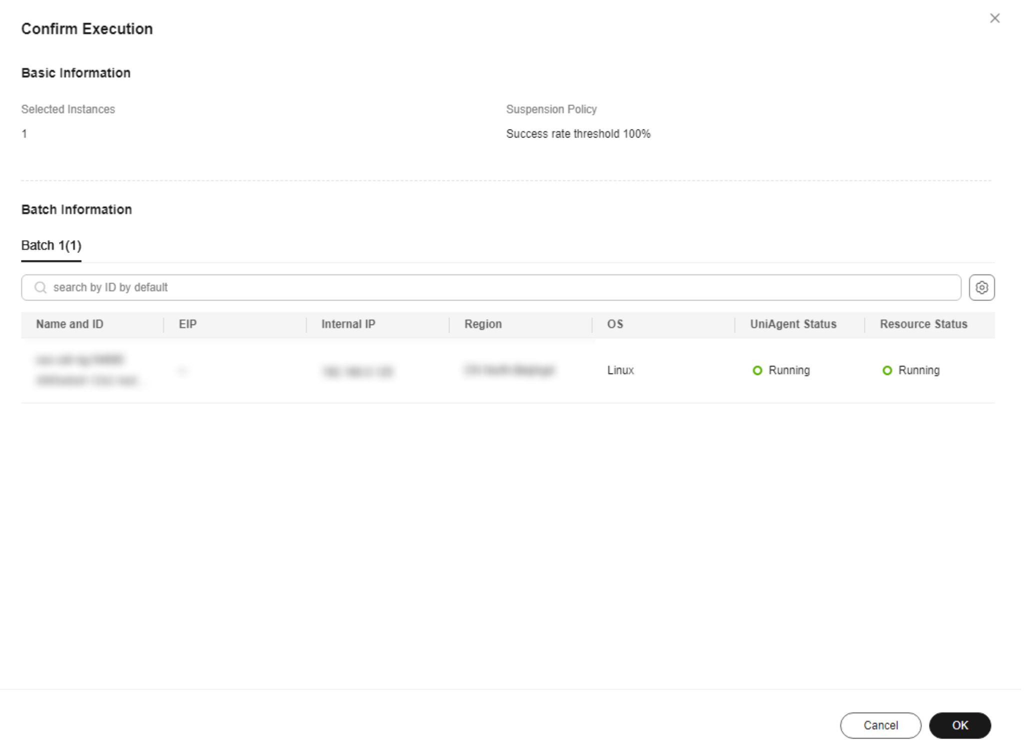
* Suspension Policy: If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Forcible restart: ○ Yes ● No

After ECSs are forcibly restarted, unsaved data on the ECSs will be lost.

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

Figure 4-74 Confirming the execution



Confirm Execution

Basic Information

Selected Instances	Suspension Policy
1	Success rate threshold 100%

Batch Information

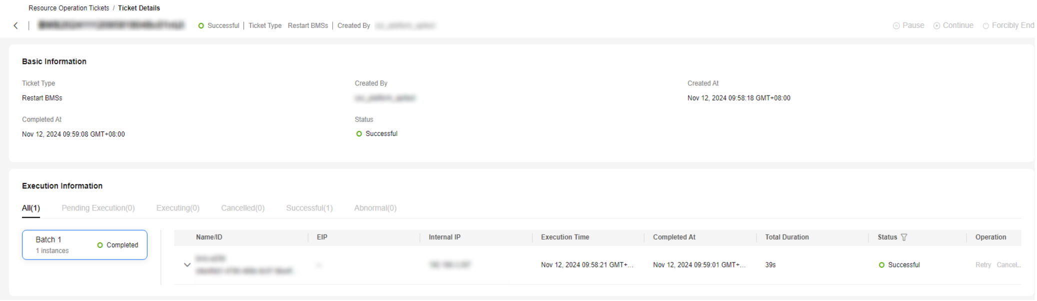
Batch 1(1)

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	[redacted]	[redacted]	[redacted]	Linux	○ Running	○ Running

Step 8 View the execution result.

Figure 4-75 Viewing the result



Resource Operation Tickets / Ticket Details

[redacted] ○ Successful | Ticket Type Restart BMSs | Created By [redacted]

Basic Information

Ticket Type	Created By	Created At
Restart BMSs	[redacted]	Nov 12, 2024 09:58:18 GMT+08:00
Completed At	Status	
Nov 12, 2024 09:59:08 GMT+08:00	○ Successful	

Execution Information

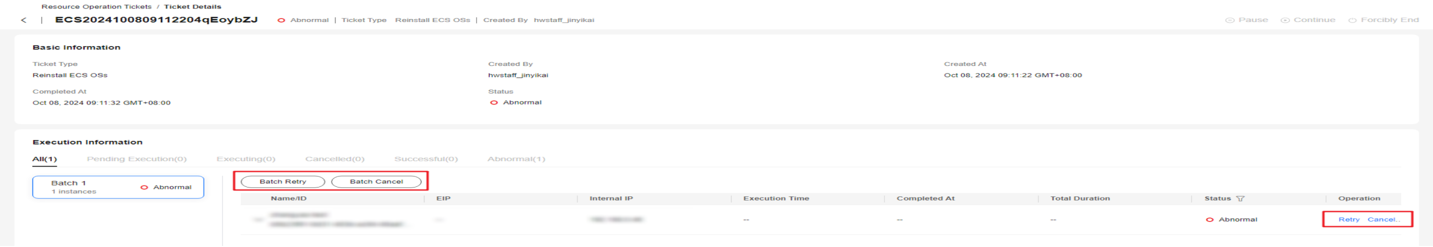
All(1) Pending Execution(0) Executing(0) Cancelled(0) Successful(1) Abnormal(0)

Batch 1 ○ Completed
1 instances

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Nov 12, 2024 09:58:21 GMT+...	Nov 12, 2024 09:59:01 GMT+...	39s	○ Successful	Retry Cancel..

Step 9 If the execution result is abnormal, you can click the **Retry** button in the Operation column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the Operation column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-76 Canceling or retrying a batch BMS startup task



Resource Operation Tickets / Ticket Details

ECS2024100809112204qEoybZJ ○ Abnormal | Ticket Type Reinstall ECS OSs | Created By hwstaff_jinyikai

Pause Continue Forcibly End

Basic Information

Ticket Type: Reinstall ECS OSs
Created By: hwstaff_jinyikai
Created At: Oct 08, 2024 09:11:22 GMT+08:00
Completed At: Oct 08, 2024 09:11:32 GMT+08:00
Status: ○ Abnormal

Execution Information

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

Batch 1 ○ Abnormal
1 instances

Batch Retry Batch Cancel

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	--	[redacted]	--	--	--	○ Abnormal	Retry Cancel..

----End

4.5.4 Batch Reinstalling OSs on BMSs

Scenarios

Reinstall OSs on BMSs in batches on COC.

Precautions

Instances that have been started cannot be selected.

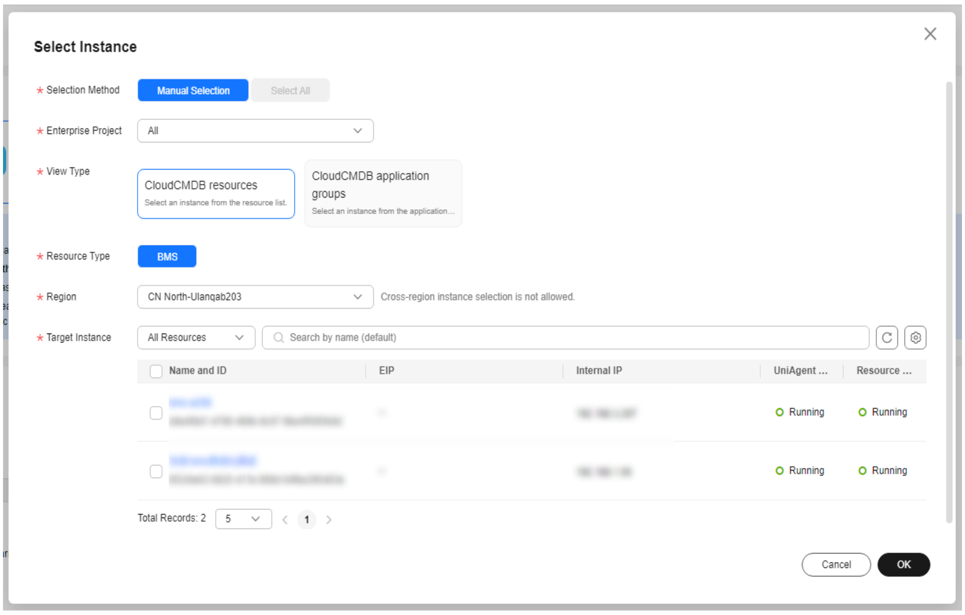
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**. On the displayed page, click the **Bare Metal Server (BMS)** tab, and then click the **Restall OSs** card on the tab page.

Step 3 On the **Reinstall OS** page, click **Add**.

Figure 4-77 Selecting instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application...)

* Resource Type: BMS

* Region: CN North-Ulanqab203 — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

Name and ID	EIP	Internal IP	UniAgent ...	Resource ...
[redacted]	--	[redacted]	○ Running	○ Running
[redacted]	--	[redacted]	○ Running	○ Running

Total Records: 2 | 5 | < 1 >

Cancel OK

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 target instances are in the same batch.

Step 5 Set **Suspension Policy**.

NOTE

- You can set the execution success rate. When the number of failed instances reaches the number failed ones that are calculated based on the execution success rate, the service ticket status becomes abnormal and the service ticket stops being executed.
- The value is from 0 to 100 and can be accurate to one decimal place.

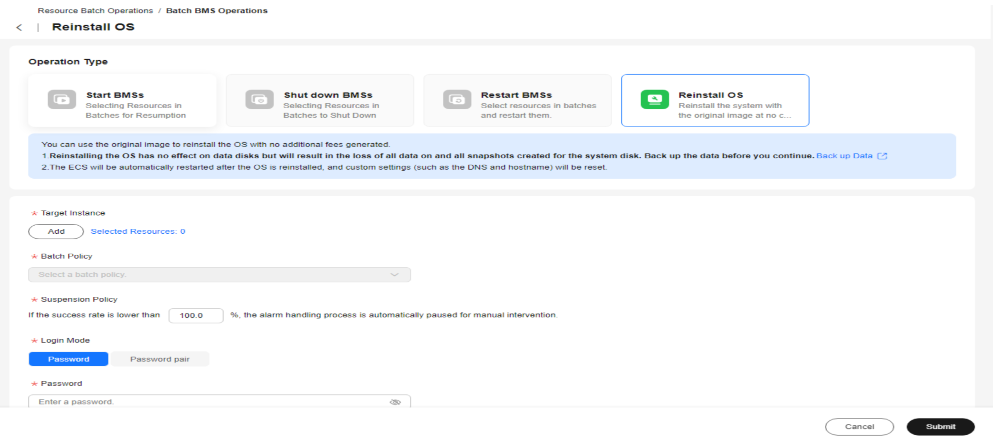
Step 6 Set **Login Mode**.

Login mode:

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

Step 7 Click **Submit**.

Figure 4-78 Reinstalling OSs



Resource Batch Operations / Batch BMS Operations

Reinstall OS

Operation Type

Start BMSs
Selecting Resources in Batches for Resumption

Shut down BMSs
Selecting Resources in Batches to Shut Down

Restart BMSs
Select resources in batches and restart them.

Reinstall OS
Reinstall the system with the original image at no c...

You can use the original image to reinstall the OS with no additional fees generated.
1.Reinstalling the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system disk. Back up the data before you continue. Back up Data
2.The ECS will be automatically restarted after the OS is reinstalled, and custom settings (such as the DNS and hostname) will be reset.

* Target Instance

Add Selected Resources: 0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

* Login Mode

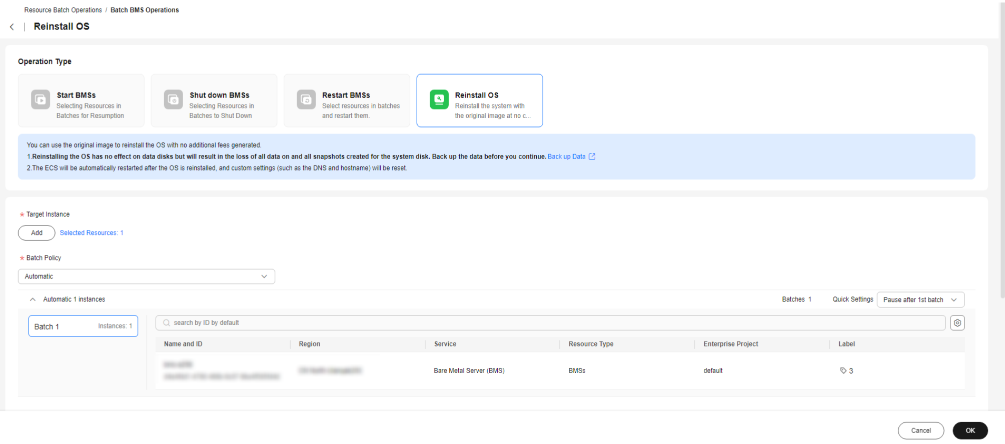
Password | Password pair

* Password

Enter a password.

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

Figure 4-79 Confirming the execution


Resource Batch Operations / Batch BMS Operations
Reinstall OS
Operation Type
Start BMSs
Selecting Resources in Batches for Resumption
Shut down BMSs
Selecting Resources in Batches to Shut Down
Restart BMSs
Select resources in batches and restart them.
Reinstall OS
Reinstall the system with the original image at no c...
Back up Data
Add
Selected Resources: 1
Automatic 1 instances
Batches 1
Quick Settings
Pause after 1st batch
Batch 1
Instances: 1
search by ID by default
Cancel
OK

You can use the original image to reinstall the OS with no additional fees generated.

1.**Reinstalling the OS has no effect on data disks but will result in the loss of all data on and all snapshots created for the system disk. Back up the data before you continue.** Back up Data

2.The ECS will be automatically restarted after the OS is reinstalled, and custom settings (such as the DNS and hostname) will be reset.

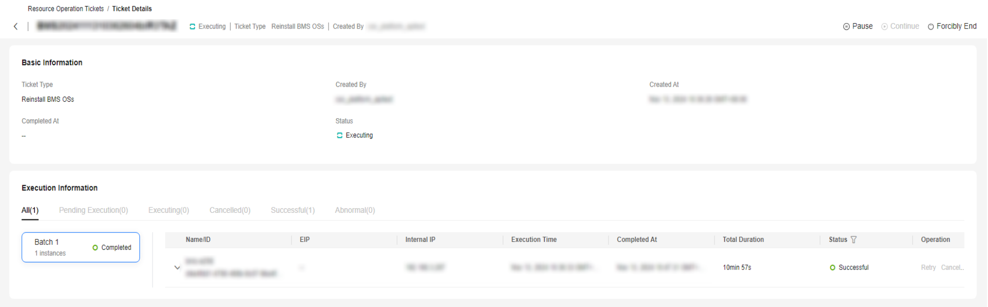
* Target Instance

* Batch Policy: Automatic

Name and ID	Region	Service	Resource Type	Enterprise Project	Label
[redacted]	[redacted]	Bare Metal Server (BMS)	BMSs	default	3

Step 9 View the execution result.

Figure 4-80 Viewing the execution result



[redacted] Executing | Ticket Type Reinstall BMS OSs | Created By [redacted]

Ticket Type: Reinstall BMS OSs

Created By: [redacted]

Created At: [redacted]

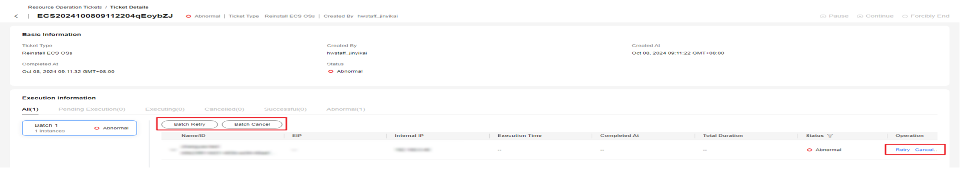
Completed At: --

Status: Executing

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	10min 57s	Successful	Retry Cancel..

Step 10 If the execution result is abnormal, you can click the **Retry** button in the Operation column or the **Batch Retry** button above the list to re-execute the failed one or more tasks. You can also click the **Cancel** button in the Operation column or **Batch Cancel** button above the list to skip one or more abnormal tasks.

Figure 4-81 Canceling or retrying a batch BMS startup task



ECS2024100809112204qEoybZJ Abnormal | Ticket Type Reinstall ECS OSs | Created By hwstaff_jinyikai

Ticket Type: Reinstall ECS OSs

Created By: hwstaff_jinyikai

Created At: Oct 08, 2024 09:11:22 GMT+08:00

Completed At: Oct 08, 2024 09:11:32 GMT+08:00

Status: Abnormal

Name/ID	EIP	Internal IP	Execution Time	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	--	--	--	Abnormal	Retry Cancel..

----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.

⚠ CAUTION

Currently, patch management supports only servers that can access the public network. You can bind an EIP or NAT gateway to implement patch management.

NOTE

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

- **Table 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

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

Table 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, CCE instances, and BMS instances as required.

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

Scenarios

Create a patch baseline on Cloud Operations Center.

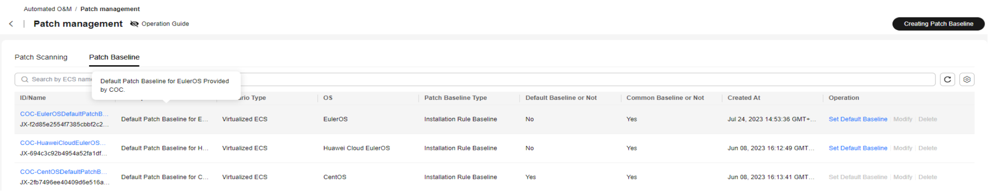
Procedure

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



Automated O&M / Patch management

Patch management   Operation Guide   Creating Patch Baseline

Patch Scanning   Patch Baseline

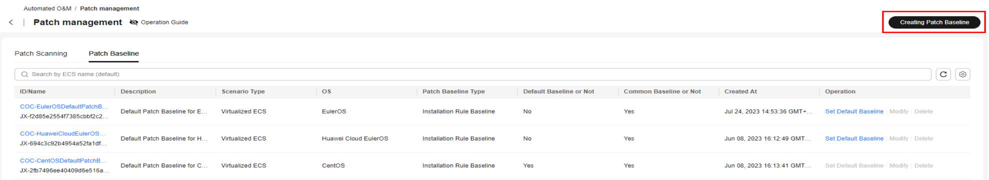
Search by ECS nam

Default Patch Baseline for EulerOS Provided by COC.

ID/Name		rio Type	OS	Patch Baseline Type	Default Baseline or Not	Common Baseline or Not	Created At	Operation
COC-EulerOSDefaultPatchB... JX-f2d85e2554f7385cbbf2c2...	Default Patch Baseline for E...	Virtualized ECS	EulerOS	Installation Rule Baseline	No	Yes	Jul 24, 2023 14:53:36 GMT+...	Set Default Baseline Modify Delete
COC-HuaweiCloudEulerOS... JX-694c3c92b4954a52fa1df...	Default Patch Baseline for H...	Virtualized ECS	Huawei Cloud EulerOS	Installation Rule Baseline	No	Yes	Jun 08, 2023 16:12:49 GMT...	Set Default Baseline Modify Delete
COC-CentOSDefaultPatchB... JX-2fb7496ee40409d6e516a...	Default Patch Baseline for C...	Virtualized ECS	CentOS	Installation Rule Baseline	Yes	Yes	Jun 08, 2023 16:13:41 GMT...	Set Default Baseline Modify Delete

Step 4 Click **Creating Patch Baseline**.

Figure 5-2 Creating a patch baseline



Automated O&M / Patch management

Patch management   Operation Guide   Creating Patch Baseline

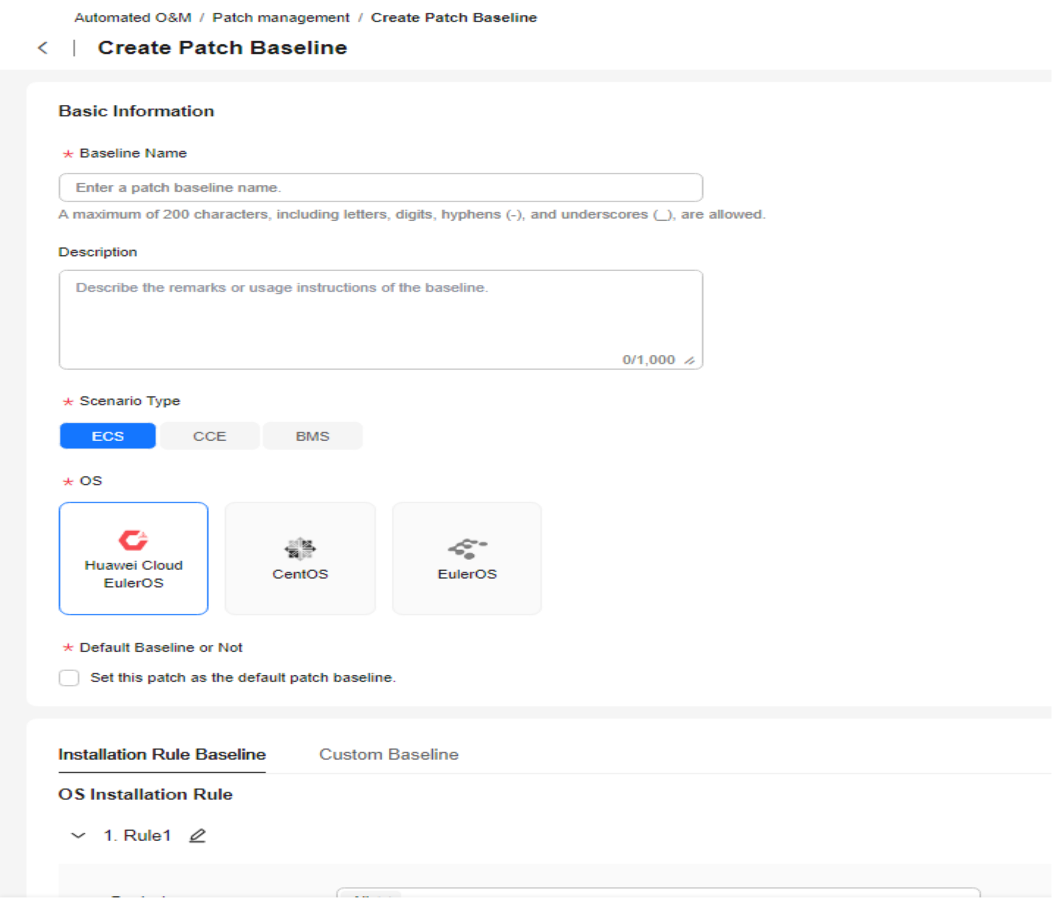
Patch Scanning   Patch Baseline

Search by ECS name (default)

ID/Name	Description	Scenario Type	OS	Patch Baseline Type	Default Baseline or Not	Common Baseline or Not	Created At	Operation
COC-EulerOSDefaultPatchB... JX-f2d85e2554f7385cbbf2c2...	Default Patch Baseline for E...	Virtualized ECS	EulerOS	Installation Rule Baseline	No	Yes	Jul 24, 2023 14:53:36 GMT+...	Set Default Baseline Modify Delete
COC-HuaweiCloudEulerOS... JX-694c3c92b4954a52fa1df...	Default Patch Baseline for H...	Virtualized ECS	Huawei Cloud EulerOS	Installation Rule Baseline	No	Yes	Jun 08, 2023 16:12:49 GMT...	Set Default Baseline Modify Delete
COC-CentOSDefaultPatchB... JX-2fb7496ee40409d6e516a...	Default Patch Baseline for C...	Virtualized ECS	CentOS	Installation Rule Baseline	Yes	Yes	Jun 08, 2023 16:13:41 GMT...	Set Default Baseline Modify Delete

Step 5 Set the patch baseline information as prompted.

Figure 5-3 Setting the patch baseline information



Automated O&M / Patch management / Create Patch Baseline

Create Patch Baseline

Basic Information

* Baseline Name

Enter a patch baseline name.

A maximum of 200 characters, including letters, digits, hyphens (-), and underscores (_), are allowed.

Description

Describe the remarks or usage instructions of the baseline.

0/1,000

* Scenario Type

ECS CCE BMS

* OS

Huawei Cloud EulerOS | CentOS | EulerOS

* Default Baseline or Not

□ Set this patch as the default patch baseline.

Installation Rule Baseline | Custom Baseline

OS Installation Rule

1. Rule1

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**.

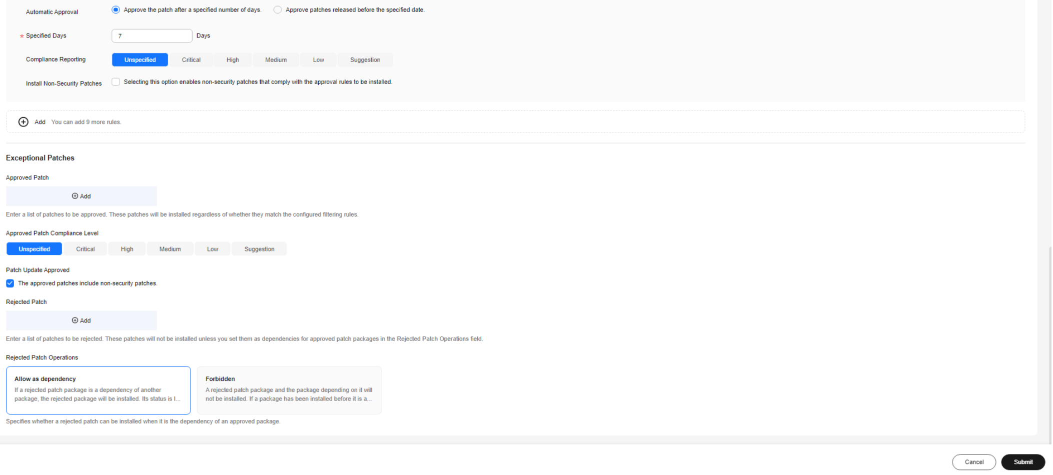
Table 5-4 Customized installation rule

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



Automatic Approval: ● Approve the patch after a specified number of days. ○ Approve patches released before the specified date.

* Specified Days: 7 Days

Compliance Reporting: Unspecified

Install Non-Security Patches: □ Selecting this option enables non-security patches that comply with the approval rules to be installed.

Add You can add 9 more rules.

Exceptional Patches

Approved Patch

Enter a list of patches to be approved. These patches will be installed regardless of whether they match the configured filtering rules.

Approved Patch Compliance Level: Unspecified

Patch Update Approved

☑ The approved patches include non-security patches.

Rejected Patch

Enter a list of patches to be rejected. These patches will not be installed unless you set them as dependencies for approved patch packages in the Rejected Patch Operations field.

Rejected Patch Operations

Allow as dependency
If a rejected patch package is a dependency of another package, the rejected package will be installed. Its status is I...

Forbidden
A rejected patch package and the package depending on it will not be installed. If a package has been installed before it is a...

Specifies whether a rejected patch can be installed when it is the dependency of an approved package.

----End

5.1.2 Scanning a Patch

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

Scenarios

Scan patches on the ECS, CCE, or BMS instances to generate patch compliance reports for analysis using COC.

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 COC patch management feature.
- Whether the instance is shut down.

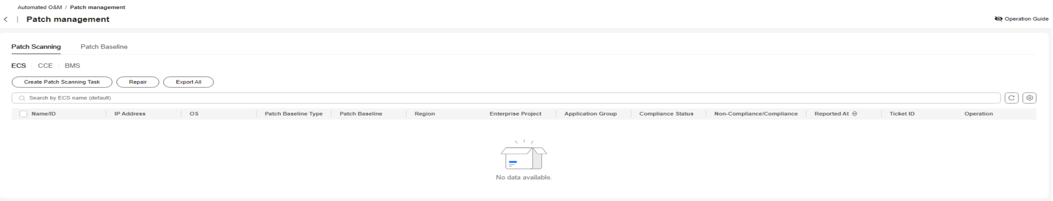
Procedure

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

Figure 5-5 Compliance report list



Automated O&M / Patch management

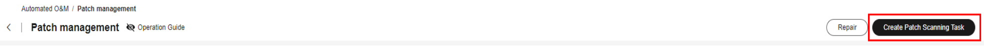
Patch management

□ Name/ID	IP Address	OS	Patch Baseline Type	Patch Baseline	Region	Enterprise Project	Application Group	Compliance Status	Non-Compliance/Compliance	Reported At	Ticket ID	Operation

No data available.

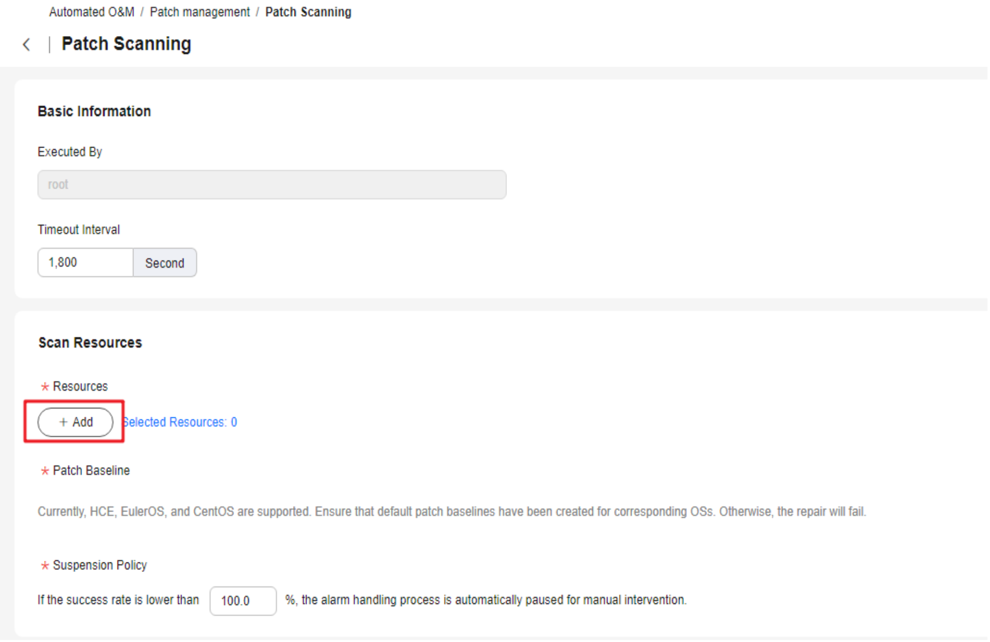
Step 4 Click **Create Patch Scanning Task**.

Figure 5-6 Creating a patch scanning task



Step 5 Click **+ Add**.

Figure 5-7 Selecting instances



Basic Information

Executed By

root

Timeout Interval

1,800 Second

Scan Resources

* Resources

* Patch Baseline

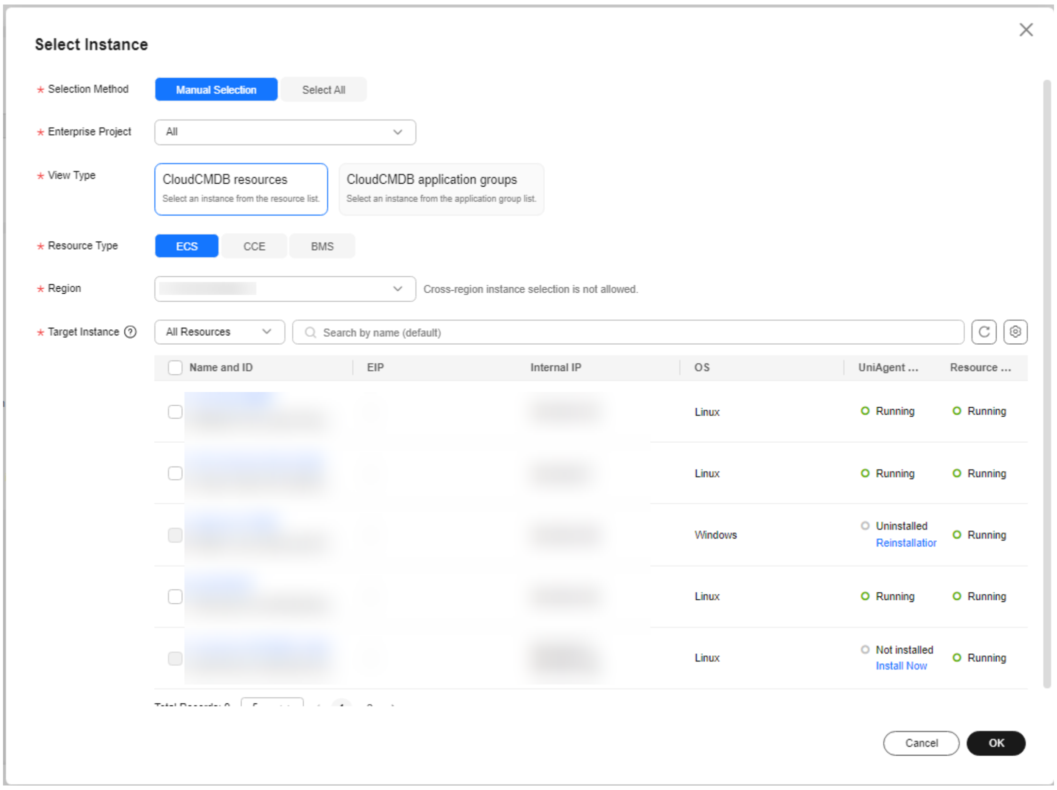
Currently, HCE, EulerOS, and CentOS are supported. Ensure that default patch baselines have been created for corresponding OSs. Otherwise, the repair will fail.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 6 Select the ECS, CCE, or BMS instances to scan.

Figure 5-8 Selecting the target ECS instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

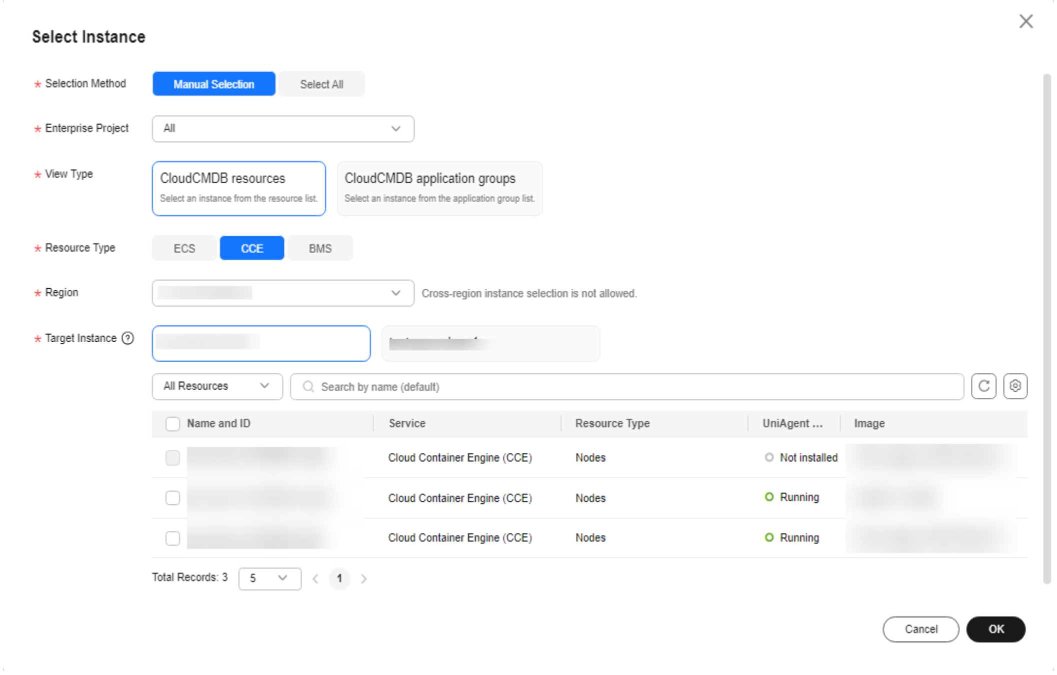
* Resource Type: ECS | CCE | BMS

* Region: [redacted] Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

Name and ID	EIP	Internal IP	OS	UniAgent ...	Resource ...
[redacted]	[redacted]	[redacted]	Linux	Running	Running
[redacted]	[redacted]	[redacted]	Linux	Running	Running
[redacted]	[redacted]	[redacted]	Windows	Uninstalled Reinstallation	Running
[redacted]	[redacted]	[redacted]	Linux	Running	Running
[redacted]	[redacted]	[redacted]	Linux	Not installed Install Now	Running

Figure 5-9 Selecting the target CCE instances



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS | CCE | BMS

* Region: [redacted] Cross-region instance selection is not allowed.

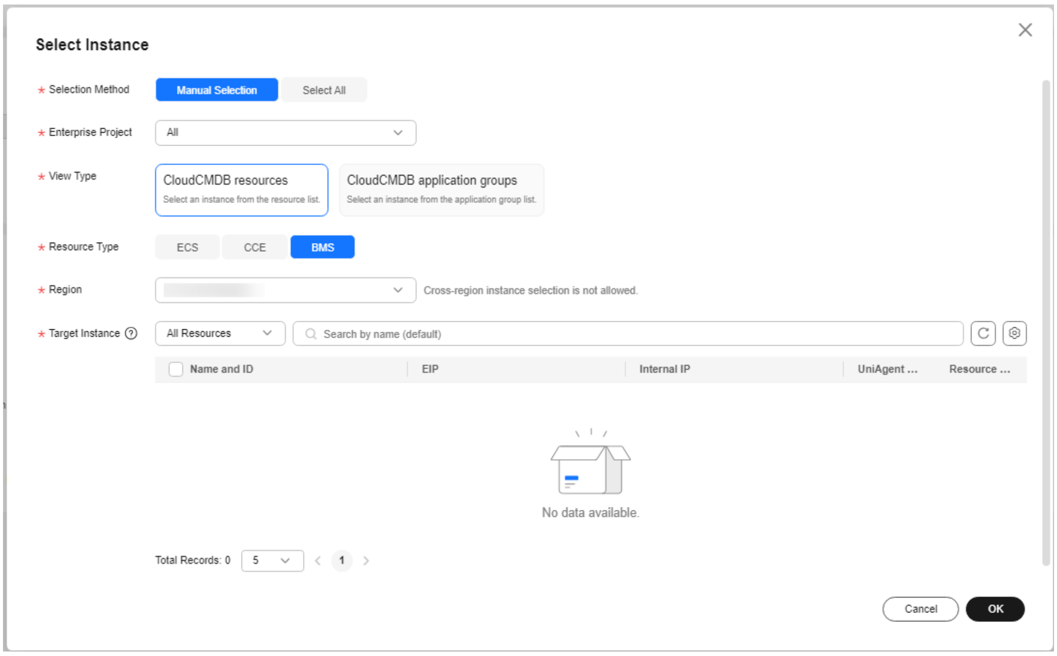
* Target Instance: [redacted] [redacted]

All Resources | Search by name (default)

Name and ID	Service	Resource Type	UniAgent ...	Image
[redacted]	Cloud Container Engine (CCE)	Nodes	Not installed	[redacted]
[redacted]	Cloud Container Engine (CCE)	Nodes	Running	[redacted]
[redacted]	Cloud Container Engine (CCE)	Nodes	Running	[redacted]

Total Records: 3 | 5 | 1

Figure 5-10 Select the target BMS instances.



Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS | CCE | BMS

* Region: Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

Name and ID	EIP	Internal IP	UniAgent ...	Resource ...

No data available.

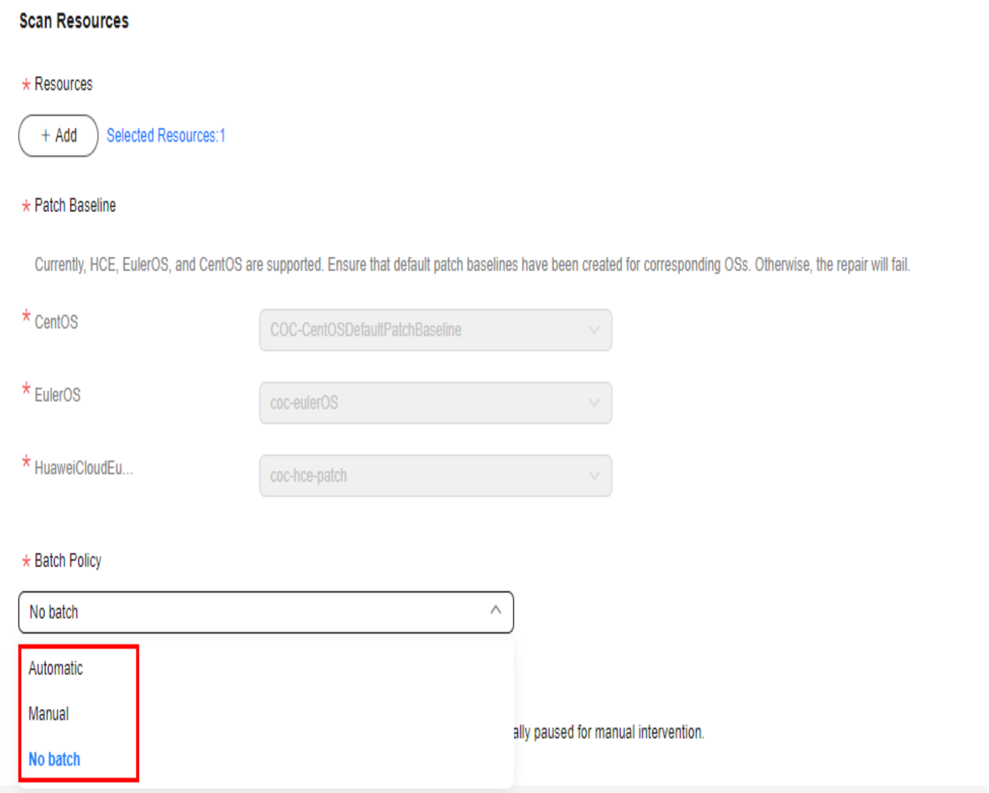
Total Records: 0 | 5 | 1

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 5-11 Selecting batch policies



Scan Resources

* Resources

+ Add Selected Resources:1

* Patch Baseline

Currently, HCE, EulerOS, and CentOS are supported. Ensure that default patch baselines have been created for corresponding OSs. Otherwise, the repair will fail.

* CentOS COC-CentOSDefaultPatchBaseline

* EulerOS coc-eulerOS

* HuaweiCloudEu... coc-hce-patch

* Batch Policy

No batch

Automatic

Manual

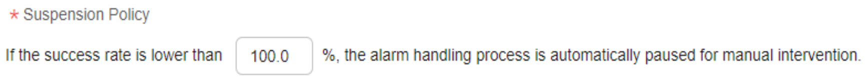
No batch

ally paused for manual intervention.

Step 8 Configure 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 5-12 Suspension policy

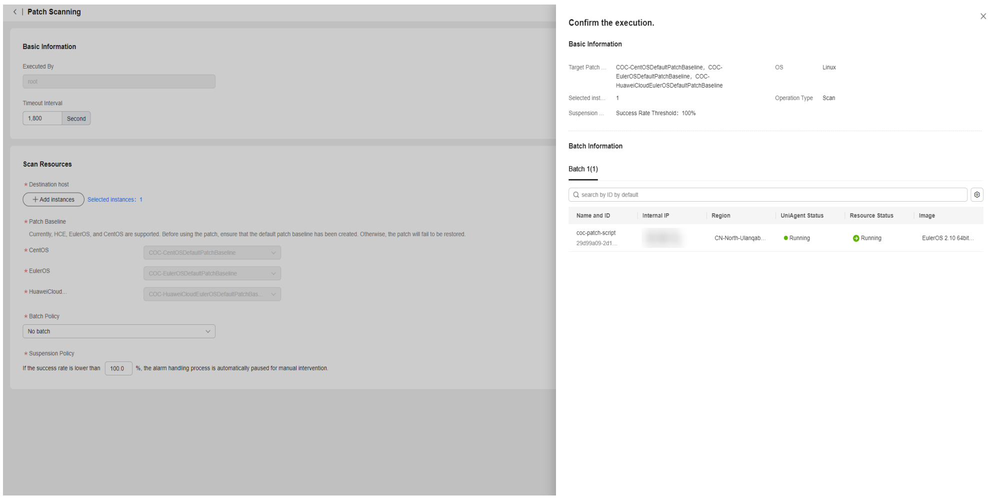


* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 9 Click **Submit**.

Figure 5-13 Execution page after clicking **Submit**



Patch Scanning

Basic Information

Executed By: root

Timeout Interval: 1,800 Second

Scan Resources

* Destination host: + Add instances Selected instances: 1

* Patch Baseline

Currently, HCE, EulerOS, and CentOS are supported. Before using the patch, ensure that the default patch baseline has been created. Otherwise, the patch will fail to be restored.

* CentOS: COC-CentOSDefaultPatchBaseline

* EulerOS: COC-EulerOSDefaultPatchBaseline

* HuaweiCloud...: COC-HuaweiCloudEulerOSDefaultPatchBas...

* Batch Policy: No batch

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Confirm the execution.

Basic Information

Target Patch ...	COC-CentOSDefaultPatchBaseline, COC-EulerOSDefaultPatchBaseline, COC-HuaweiCloudEulerOSDefaultPatchBaseline	OS	Linux
Selected inst...	1	Operation Type	Scan
Suspension ...	Success Rate Threshold: 100%		

Batch Information

Batch 1(1)

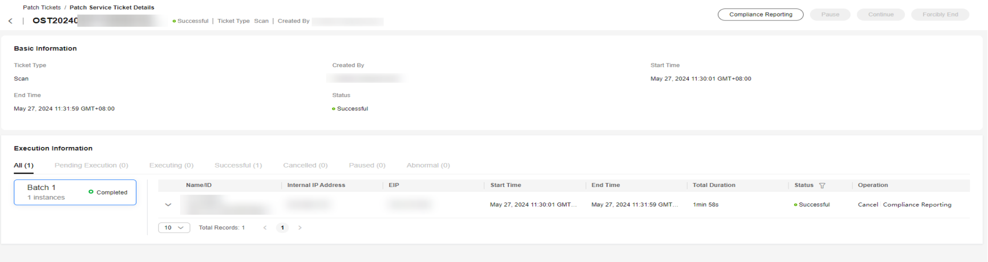
search by ID by default

Name and ID	Internal IP	Region	UniAgent Status	Resource Status	Image
coc-patch-script 29d99a09-2d1...	[redacted]	CN-North-Ulanqab...	● Running	Running	EulerOS 2.10 64bit...

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 5-14 Service ticket details



Patch Tickets / Patch Service Ticket Details

OST2024C[redacted] ● Successful | Ticket Type Scan | Created By [redacted]

Compliance Reporting Pause Continue Forcibly End

Basic Information

Ticket Type Scan	Created By [redacted]	Start Time May 27, 2024 11:30:01 GMT+08:00
End Time May 27, 2024 11:31:59 GMT+08:00	Status ● Successful	

Execution Information

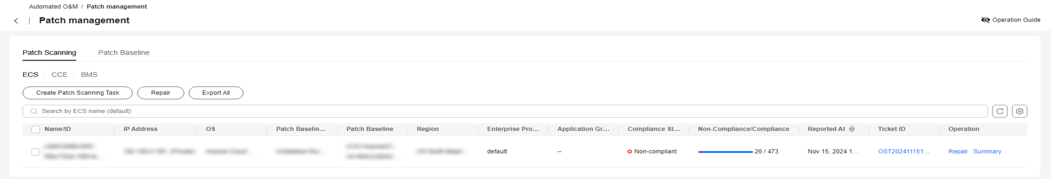
All (1) Pending Execution (0) Executing (0) Successful (1) Cancelled (0) Paused (0) Abnormal (0)

Batch 1 1 instances Completed

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	May 27, 2024 11:30:01 GMT...	May 27, 2024 11:31:59 GMT...	1min 58s	● Successful	Cancel Compliance Reporting

10 Total Records: 1 < 1 >

Figure 5-15 Compliance report list



Automated O&M / Patch management

Patch management

Operation Guide

Patch Scanning Patch Baseline

ECS CCE BMS

Create Patch Scanning Task Repair Export All

Search by ECS name (default)

Name/ID	IP Address	OS	Patch Baselin...	Patch Baseline	Region	Enterprise Pro...	Application Gr...	Compliance St...	Non-Compliance/Compliance	Reported At	Ticket ID	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	default	--	○ Non-compliant	26 / 473	Nov 15, 2024 1...	OST202411151...	Repair Summary

----End

5.1.3 Repairing Patches

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

Scenarios

Repair patches on COC.

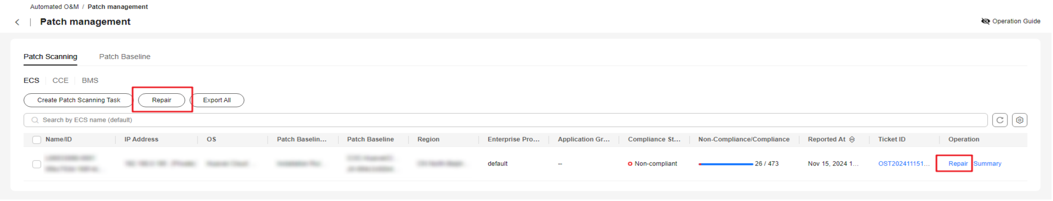
Procedure

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 5-16 Select the target instances


Automated O&M / Patch management
Patch management
Operation Guide
Patch Scanning
Patch Baseline
ECS
CCE
BMS
Create Patch Scanning Task
Repair
Export All
Search by ECS name (default)

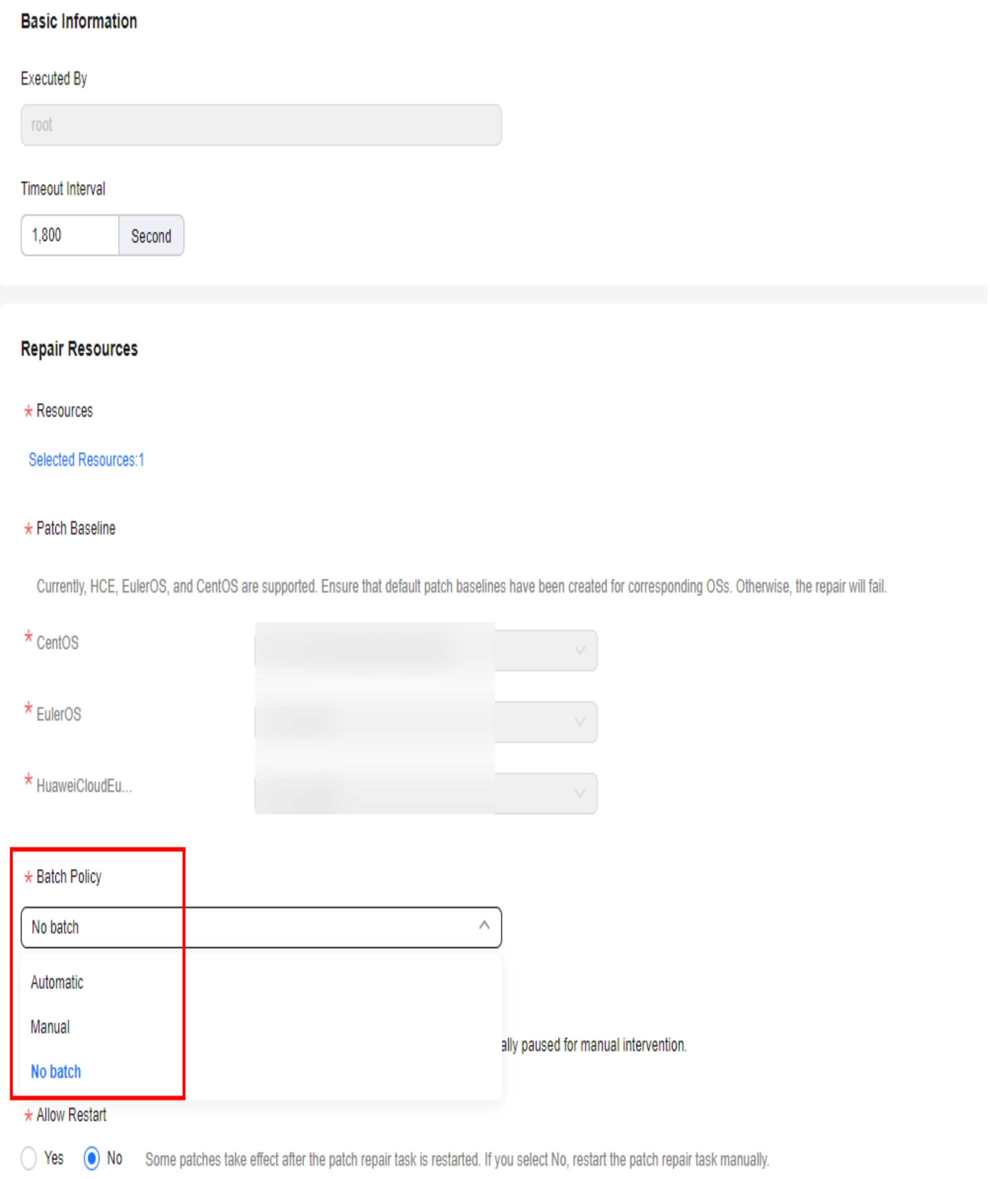
	Name/ID	IP Address	OS	Patch Baselin...	Patch Baseline	Region	Enterprise Pro...	Application Gr...	Compliance St...	Non-Compliance/Compliance	Reported At	Ticket ID	Operation
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	default	--	○ Non-compliant	26 / 473	Nov 15, 2024 1...	OST202411151...	Repair Summary

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 5-17 Selecting the batch policy



Basic Information

Executed By

root

Timeout Interval

1,800 Second

Repair Resources

* Resources

Selected Resources:1

* Patch Baseline

Currently, HCE, EulerOS, and CentOS are supported. Ensure that default patch baselines have been created for corresponding OSs. Otherwise, the repair will fail.

* CentOS

* EulerOS

* HuaweiCloudEu...

* Batch Policy

No batch

Automatic

Manual

No batch

ally paused for manual intervention.

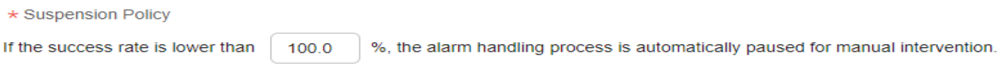
* Allow Restart

○ Yes ● No Some patches take effect after the patch repair task is restarted. If you select No, restart the patch repair task manually.

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 5-18 Suspension policy



* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

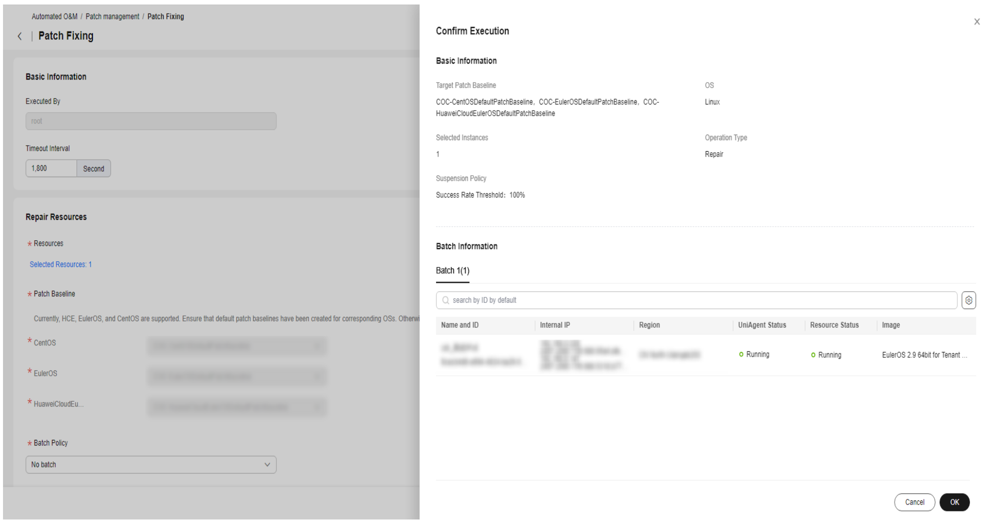
Step 6 Set whether to allow restart.

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 5-19 Execution information page



Automated O&M / Patch management / Patch Fixing

Patch Fixing

Basic Information

Executed By: root

Timeout Interval: 1,800 Second

Repair Resources

* Resources

Selected Resources: 1

* Patch Baseline

Currently, HCE, EulerOS, and CentOS are supported. Ensure that default patch baselines have been created for corresponding OSs. Otherwi

* CentOS [redacted]

* EulerOS [redacted]

* HuaweiCloudEu... [redacted]

* Batch Policy: No batch

Confirm Execution

Basic Information

Target Patch Baseline: COC-CentOSDefaultPatchBaseline，COC-EulerOSDefaultPatchBaseline，COC-HuaweiCloudEulerOSDefaultPatchBaseline

OS: Linux

Selected Instances: 1

Operation Type: Repair

Suspension Policy

Success Rate Threshold：100%

Batch Information

Batch 1(1)

search by ID by default

Name and ID	Internal IP	Region	UniAgent Status	Resource Status	Image
[redacted]	[redacted]	[redacted]	Running	Running	EulerOS 2.9 64bit for Tenant ...

Cancel OK

----End

5.1.4 Viewing the Patch Compliance Report Details

After the patch compliance scan or repair completed, you can view the details of the patch on the instance.

Scenarios

View the patch compliance scanning and patch repairing results on COC.

Precautions

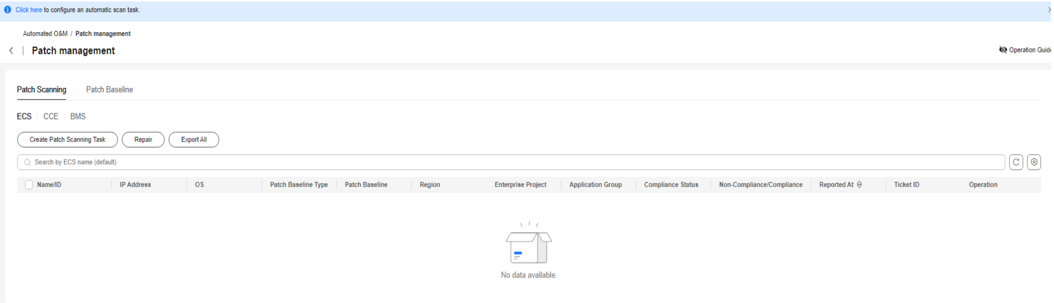
The patch compliance report retains the latest scan or repair record.

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**.

Figure 5-20 Patch management



Click here to configure an automatic scan task.

Automated O&M / Patch management

Patch management

Operation Guide

Patch Scanning | Patch Baseline

ECS | CCE | BMS

Create Patch Scanning Task | Repair | Export All

Search by ECS name (default)

Name/ID	IP Address	OS	Patch Baseline Type	Patch Baseline	Region	Enterprise Project	Application Group	Compliance Status	Non-Compliance/Compliance	Reported At	Ticket ID	Operation

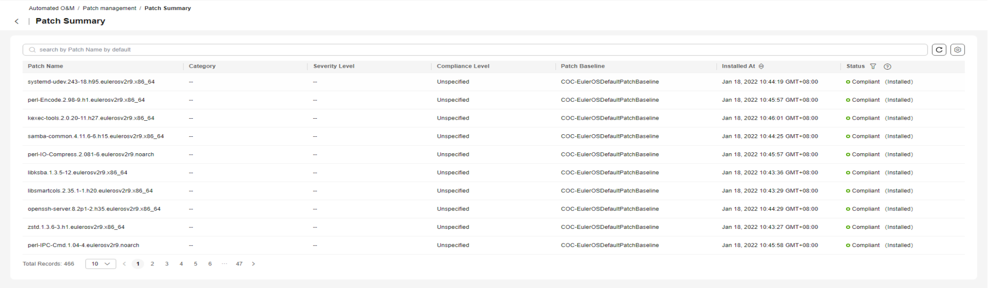
No data available.

Step 3 Locate the row containing the patch compliance report for which you want to check details 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 repair fails.

Figure 5-21 Patch compliance report summary



Automated O&M / Patch management / Patch Summary
Patch Summary
search by Patch Name by default

Patch Name	Category	Severity Level	Compliance Level	Patch Baseline	Installed At	Status
systemd-udev.243-18.h95.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:44:19 GMT+08:00	Compliant (Installed)
perl-Encode.2.98-9.h1.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:45:57 GMT+08:00	Compliant (Installed)
kexec-tools.2.0.20-11.h27.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:46:01 GMT+08:00	Compliant (Installed)
samba-common.4.11.6-6.h15.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:44:25 GMT+08:00	Compliant (Installed)
perl-IO-Compress.2.081-6.eulerosv2r9.noarch	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:45:57 GMT+08:00	Compliant (Installed)
libksba.1.3.5-12.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:43:36 GMT+08:00	Compliant (Installed)
libsmartcols.2.35.1-1.h20.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:43:29 GMT+08:00	Compliant (Installed)
openssh-server.8.2p1-2.h35.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:44:29 GMT+08:00	Compliant (Installed)
zstd.1.3.6-3.h1.eulerosv2r9.x86_64	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:43:27 GMT+08:00	Compliant (Installed)
perl-IPC-Cmd.1.04-4.eulerosv2r9.noarch	--	--	Unspecified	COC-EulerOSDefaultPatchBaseline	Jan 18, 2022 10:45:58 GMT+08:00	Compliant (Installed)

----End

5.1.5 Automatic Patch Operations

You can create automatic tasks for patch scanning or patch repair.

Scenarios

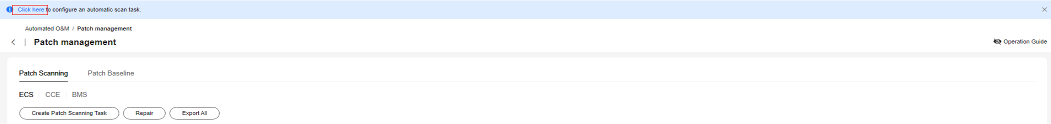
Create automatic patch tasks on COC.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Resource O&M** > **Automation** > **Patch Management**. On the displayed page, click **Click here** in the upper part of the page to configure an automation task.

Figure 5-22 Learn more



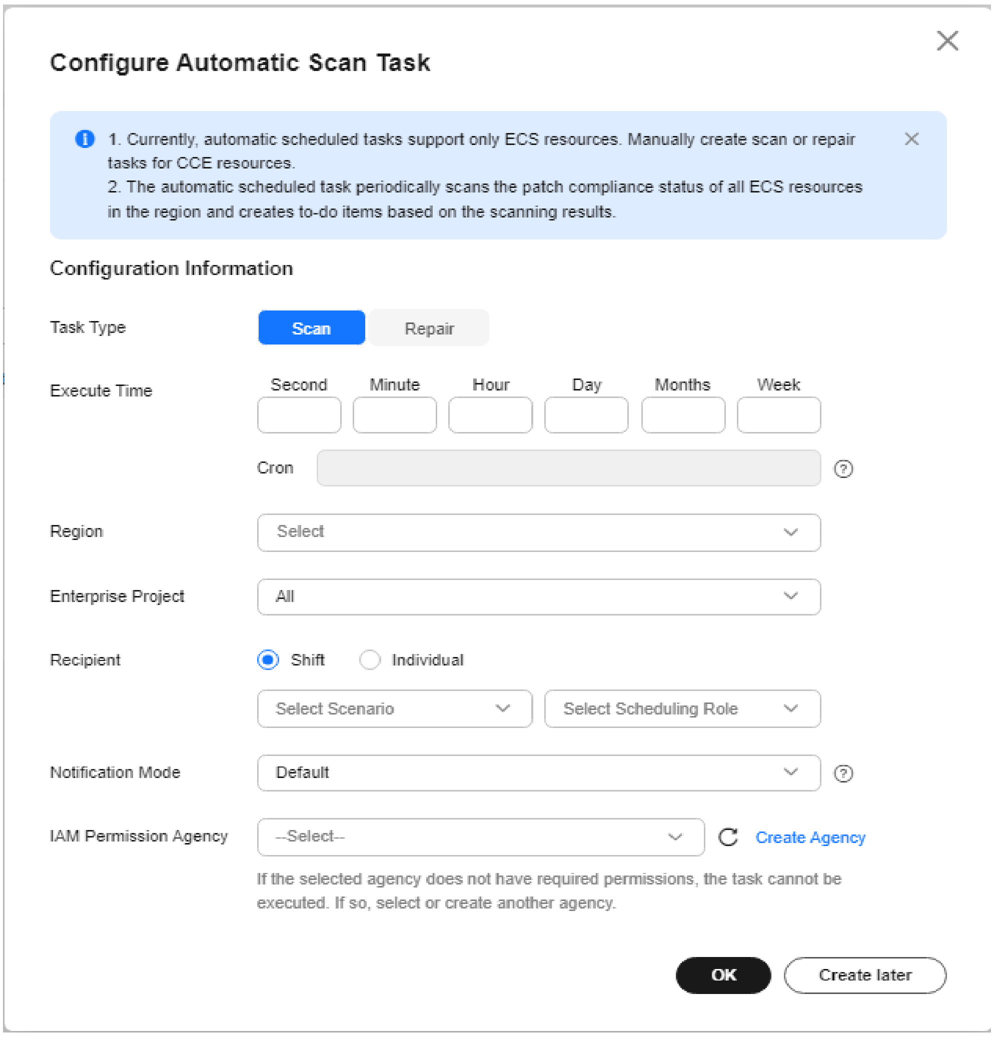
Click here to configure an automatic scan task.

Step 3 Set automation execution parameters and click **OK**.

NOTE

The automatic patch task will be performed periodically on all Linux ECSs where agents are running properly in your selected region. Ensure you understand the impact scope of the task.

Figure 5-23 Scheduled task parameters



Configure Automatic Scan Task

1. Currently, automatic scheduled tasks support only ECS resources. Manually create scan or repair tasks for CCE resources.
2. The automatic scheduled task periodically scans the patch compliance status of all ECS resources in the region and creates to-do items based on the scanning results.

Configuration Information

Task Type: Scan | Repair

Execute Time: Second | Minute | Hour | Day | Months | Week

Cron

Region: Select

Enterprise Project: All

Recipient: ● Shift ○ Individual

Select Scenario | Select Scheduling Role

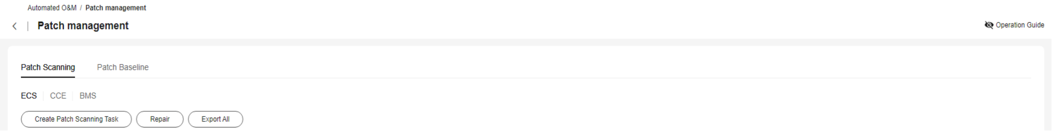
Notification Mode: Default

IAM Permission Agency: --Select-- | Create Agency

If the selected agency does not have required permissions, the task cannot be executed. If so, select or create another agency.

Step 4 Click **OsPatchAutomaticScanning** or **OsPatchAutomaticRepair** in the upper part of the page to view or modify the task.

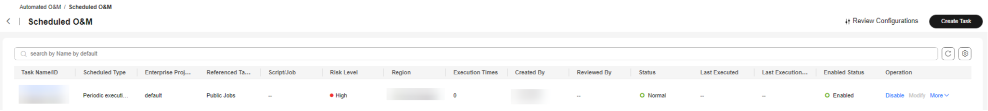
Figure 5-24 Completing configuration



Automated O&M / Patch management

Patch management

Figure 5-25 Viewing the scheduled O&M task



Automated O&M / Scheduled O&M

Scheduled O&M

Task Name/ID	Scheduled Type	Enterprise Proj...	Referenced Ta...	Script/Job	Risk Level	Region	Execution Times	Created By	Reviewed By	Status	Last Executed	Last Execution...	Enabled Status	Operation
[redacted]	Periodic executi...	default	Public Jobs	--	● High	[redacted]	0	[redacted]	--	○ Normal	--	--	○ Enabled	Disable Modify More

----End

5.2 Script Management

You can create, modify, and delete scripts, and execute customized scripts and public scripts on target VMs. With this function, you can use customized scripts or public scripts to perform operations on the target instances.

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

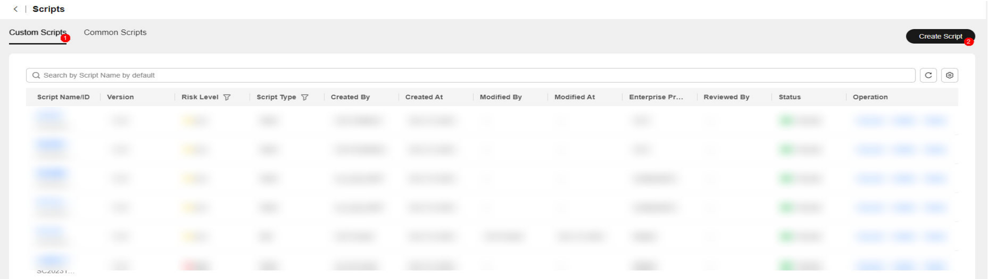
Confirm and complete the risk level of the script content.

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 5-26 Clicking **Create Script**

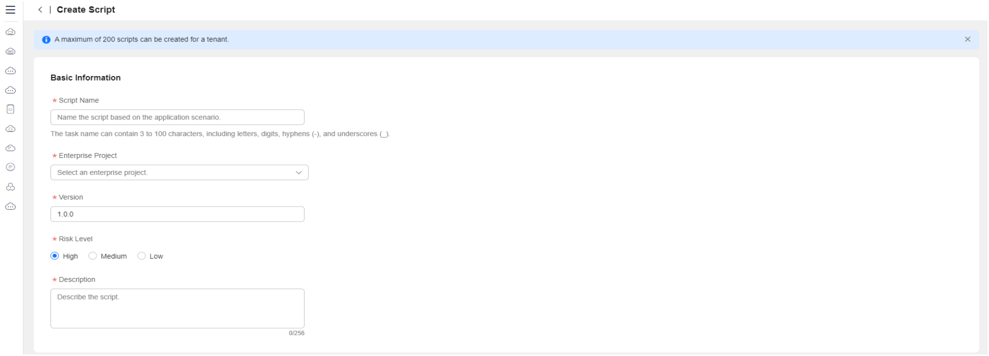


Scripts

Script Name/ID	Version	Risk Level	Script Type	Created By	Created At	Modified By	Modified At	Enterprise Pr...	Reviewed By	Status	Operation

Step 3 Enter the basic script information.

Figure 5-27 Setting parameters



A maximum of 200 scripts can be created for a tenant.

Basic Information

* Script Name

Name the script based on the application scenario.

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

* Enterprise Project

Select an enterprise project.

* Version

1.0.0

* Risk Level

● High ○ Medium ○ Low

* Description

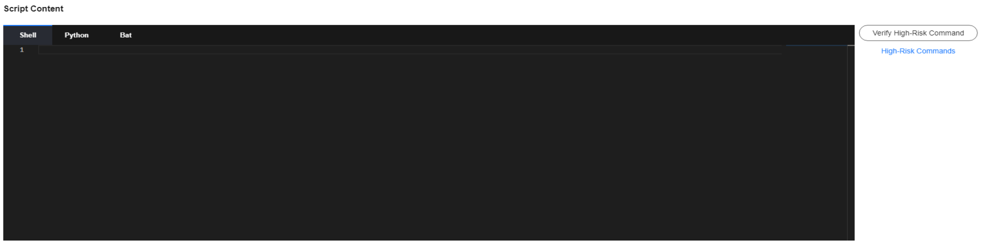
Describe the script.

0/256

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

> NOTE
>
> The interpreter that is automatically added to the first line of the script content, for example, #!/usr/bin/python, requires a Python soft link on your VMs. If the soft link is missing, you need to modify the interpreter to ensure that it can be executed by your VMs.

Figure 5-28 Entering the script content

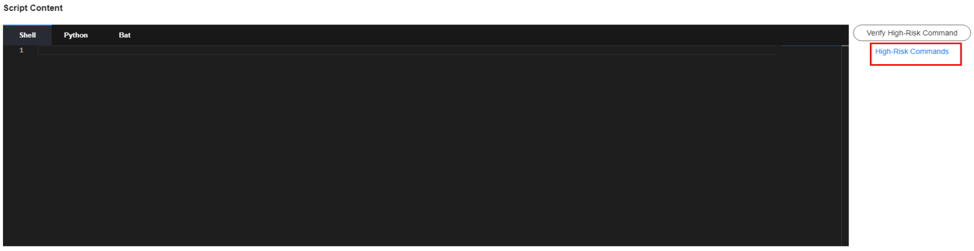


Step 5 Click **Verify High-Risk Command**.

- 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.

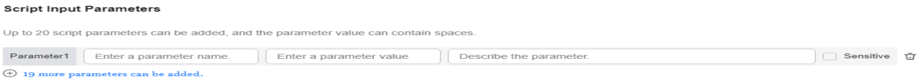
> NOTE
>
> The result of high-risk command verification is used only as a reference for grading the script risk level. The system does not forcibly require the consistency between script risk level and the verification result. Evaluate the risk level based on the actual service impact.

Figure 5-29 Verifying high-risk commands



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

Figure 5-30 Entering script input parameters

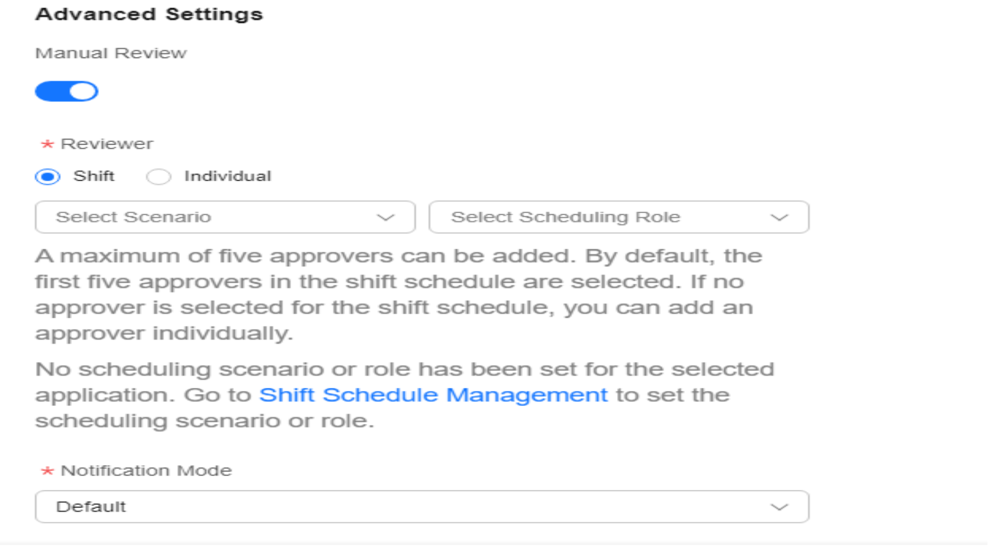


Up to 20 script parameters can be added, and the parameter value can contain spaces.

> **NOTE**
>
> **Sensitive**: parameters are anonymized and encrypted for storage.

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

Figure 5-31 Selecting the reviewer and the notification mode

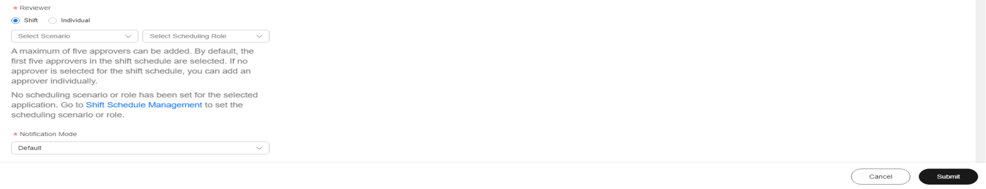


A maximum of five approvers can be added. By default, the first five approvers in the shift schedule are selected. If no approver is selected for the shift schedule, you can add an approver individually.

No scheduling scenario or role has been set for the selected application. Go to Shift Schedule Management to set the scheduling scenario or role.

Step 8 Click **Submit**.

Figure 5-32 Click **Submit**.



* Reviewer

● Shift ○ Individual

Select Scenario | Select Scheduling Role

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

No scheduling scenario or role has been set for the selected application. Go to Shift Schedule Management to set the scheduling scenario or role.

* Notification Mode

Default

----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

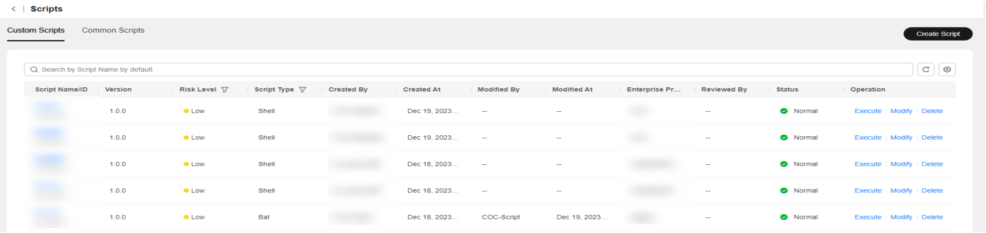
Confirm and complete the risk level of the script content when modifying a script.

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 5-33 Script management

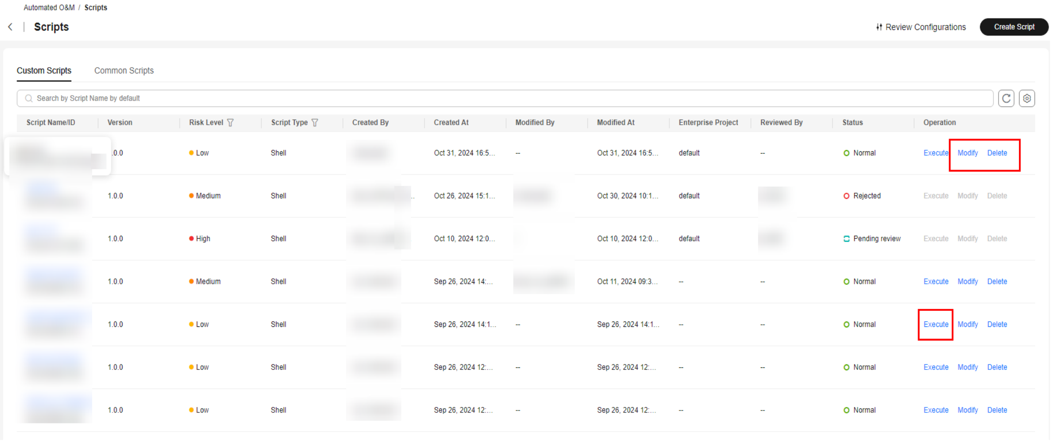


Script Name/ID	Version	Risk Level	Script Type	Created By	Created At	Modified By	Modified At	Enterprise Pr...	Reviewed By	Status	Operation
[redacted]	1.0.0	Low	Shell	[redacted]	Dec 19, 2023...	--	--	[redacted]	--	Normal	Execute | Modify | Delete
[redacted]	1.0.0	Low	Shell	[redacted]	Dec 19, 2023...	--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

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 5-34 Modify, **Delete**, and **Review** buttons



Script Name/ID	Version	Risk Level	Script Type	Created By	Created At	Modified By	Modified At	Enterprise Project	Reviewed By	Status	Operation
[redacted]	.0.0	● Low	Shell	[redacted]	Oct 31, 2024 16:5...	--	Oct 31, 2024 16:5...	default	--	○ Normal	Execute Modify Delete
[redacted]	1.0.0	● Medium	Shell	[redacted]	Oct 26, 2024 15:1...	[redacted]	Oct 30, 2024 10:1...	default	[redacted]	○ Rejected	Execute Modify Delete
[redacted]	1.0.0	● High	Shell	[redacted]	Oct 10, 2024 12:0...	[redacted]	Oct 10, 2024 12:0...	default	[redacted]	Pending review	Execute Modify Delete
[redacted]	1.0.0	● Medium	Shell	[redacted]	Sep 26, 2024 14:...	[redacted]	Oct 11, 2024 09:3...	--	--	○ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Sep 26, 2024 14:1...	--	Sep 26, 2024 14:1...	--	--	○ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Sep 26, 2024 12:...	--	Sep 26, 2024 12:...	--	--	○ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Sep 26, 2024 12:...	--	Sep 26, 2024 12:...	--	--	○ Normal	Execute Modify Delete

----End

5.2.3 Executing Custom Scripts

The custom script execution capability is provided.

Scenarios

Execute a custom script on COC.

Precautions

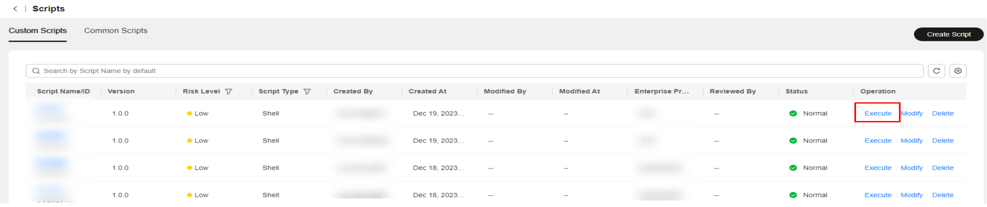
Ensure that you have the permission on the component to which the target VM belongs when executing a script.

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.

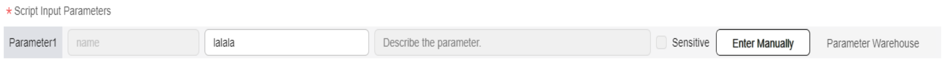
Figure 5-35 Selecting the customized script to be executed



Script Name/ID	Version	Risk Level	Script Type	Created By	Created At	Modified By	Modified At	Enterprise Pr...	Reviewed By	Status	Operation
[redacted]	1.0.0	● Low	Shell	[redacted]	Dec 19, 2023...	--	--	[redacted]	--	✓ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Dec 19, 2023...	--	--	[redacted]	--	✓ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Dec 18, 2023...	--	--	[redacted]	--	✓ Normal	Execute Modify Delete
[redacted]	1.0.0	● Low	Shell	[redacted]	Dec 18, 2023...	--	--	[redacted]	--	✓ Normal	Execute Modify Delete

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.

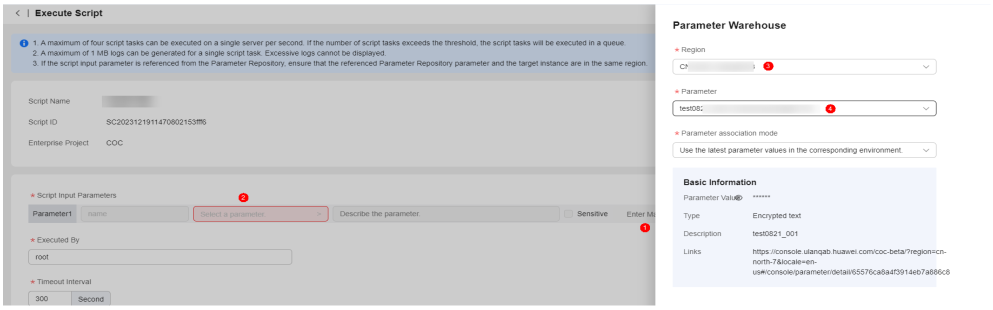
Figure 5-36 Manually entering script parameters



* Script Input Parameters

Parameter1 | name | lalala | Describe the parameter. | □ Sensitive | Enter Manually | Parameter Warehouse

Figure 5-37 Selecting script parameters from the parameter warehouse



< | Execute Script

1. A maximum of four script tasks can be executed on a single server per second. If the number of script tasks exceeds the threshold, the script tasks will be executed in a queue.
2. A maximum of 1 MB logs can be generated for a single script task. Excessive logs cannot be displayed.
3. If the script input parameter is referenced from the Parameter Repository, ensure that the referenced Parameter Repository parameter and the target instance are in the same region.

Script Name [redacted]

Script ID SC20231219114708021 53fff6

Enterprise Project COC

* Script Input Parameters

Parameter1 | name | Select a parameter. > | Describe the parameter. | □ Sensitive | Enter Ma

* Executed By

root

* Timeout Interval

300 Second

Parameter Warehouse

* Region

CN[redacted]

* Parameter

test082[redacted]

* Parameter association mode

Use the latest parameter values in the corresponding environment.

Basic Information

Parameter Value ******

Type Encrypted text

Description test0821_001

Links https://console.ulanqab.huawei.com/coc-beta/?region=cn-north-7&locale=en-us#/console/parameter/detail/65576ca8a4f3914eb7a886c8

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.

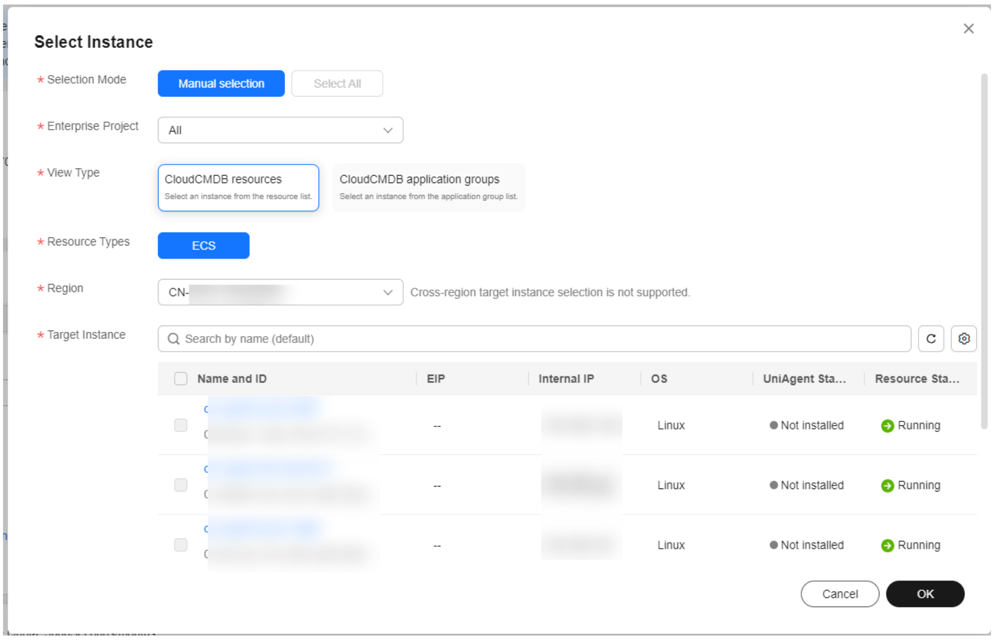
NOTE

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 a single 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 5-38 Selecting target instances



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Types: ECS

* Region: CN-[redacted] Cross-region target instance selection is not supported.

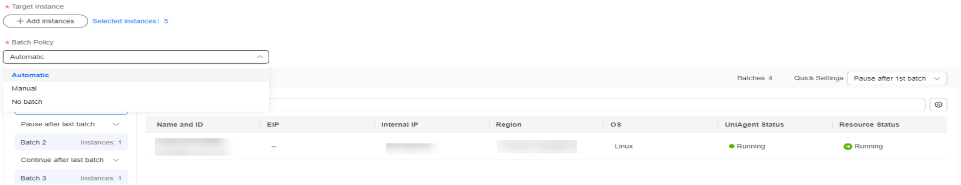
* Target Instance: Search by name (default)

□ Name and ID	EIP	Internal IP	OS	UniAgent Sta...	Resource Sta...
□ [redacted]	--	[redacted]	Linux	● Not installed	Running
□ [redacted]	--	[redacted]	Linux	● Not installed	Running
□ [redacted]	--	[redacted]	Linux	● Not installed	Running

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 5-39 Selecting a batch policy



* Target Instance

+ Add instances Selected instances: 5

* Batch Policy

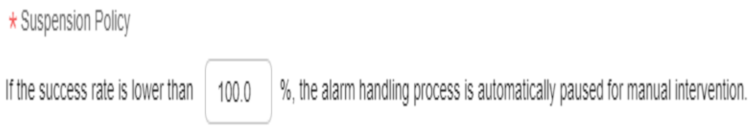
Automatic

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	[redacted]	Linux	● Running	Running

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 5-40 Setting a suspension policy

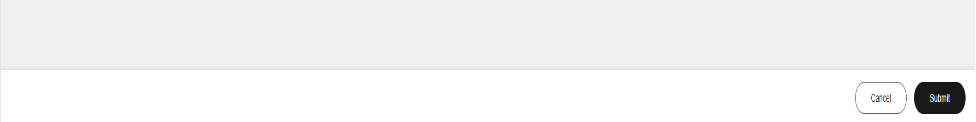


* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 8 Click **Submit**.

Figure 5-41 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 preset in COC. 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

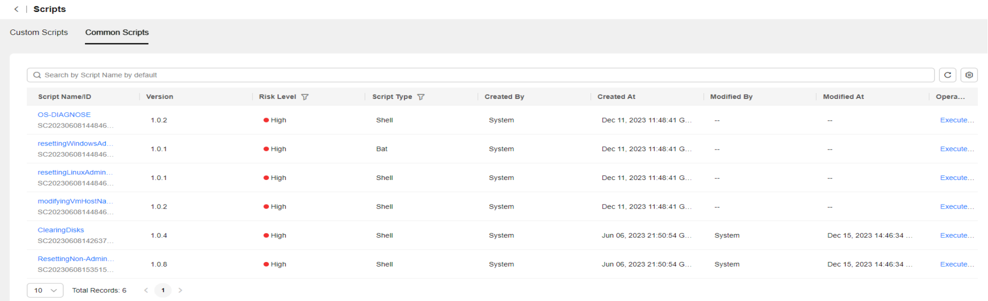
Ensure that you have the permission on the component to which the target VM belongs when executing a script.

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 5-42 Selecting the target common script to be executed

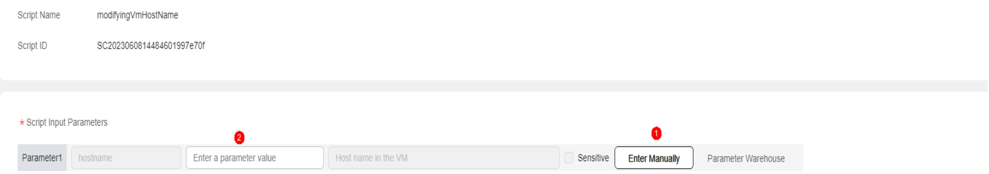


Script Name/ID	Version	Risk Level	Script Type	Created By	Created At	Modified By	Modified At	Opera...
OS-DIAGNOSE SC20230608144846...	1.0.2	● High	Shell	System	Dec 11, 2023 11:48:41 G...	--	--	Execute...
resettingWindowsAd... SC20230608144846...	1.0.1	● High	Bat	System	Dec 11, 2023 11:48:41 G...	--	--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

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

Script parameters can be manually entered or 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 5-43 Manually entering script parameters



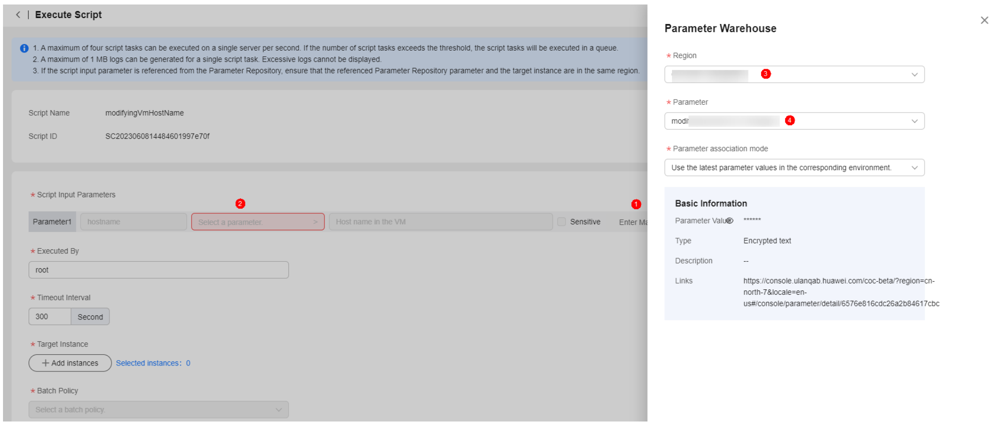
Script Name modifyingVmHostName

Script ID SC2023060814484601997e70f

* Script Input Parameters

Parameter1 | hostname | Enter a parameter value | Host name in the VM | □ Sensitive | Enter Manually | Parameter Warehouse

Figure 5-44 Selecting script parameters from repository



< | Execute Script

1. A maximum of four script tasks can be executed on a single server per second. If the number of script tasks exceeds the threshold, the script tasks will be executed in a queue.
2. A maximum of 1 MB logs can be generated for a single script task. Excessive logs cannot be displayed.
3. If the script input parameter is referenced from the Parameter Repository, ensure that the referenced Parameter Repository parameter and the target instance are in the same region.

Script Name modifyingVmHostName

Script ID SC2023060814484601997e70f

* Script Input Parameters

Parameter1 | hostname | Select a parameter. > | Host name in the VM | □ Sensitive | Enter Ma

* Executed By

root

* Timeout Interval

300 Second

* Target Instance

+ Add instances Selected instances：0

* Batch Policy

Select a batch policy.

Parameter Warehouse

* Region

[redacted]

* Parameter

modi[redacted]

* Parameter association mode

Use the latest parameter values in the corresponding environment.

Basic Information

Parameter Value ******

Type Encrypted text

Description --

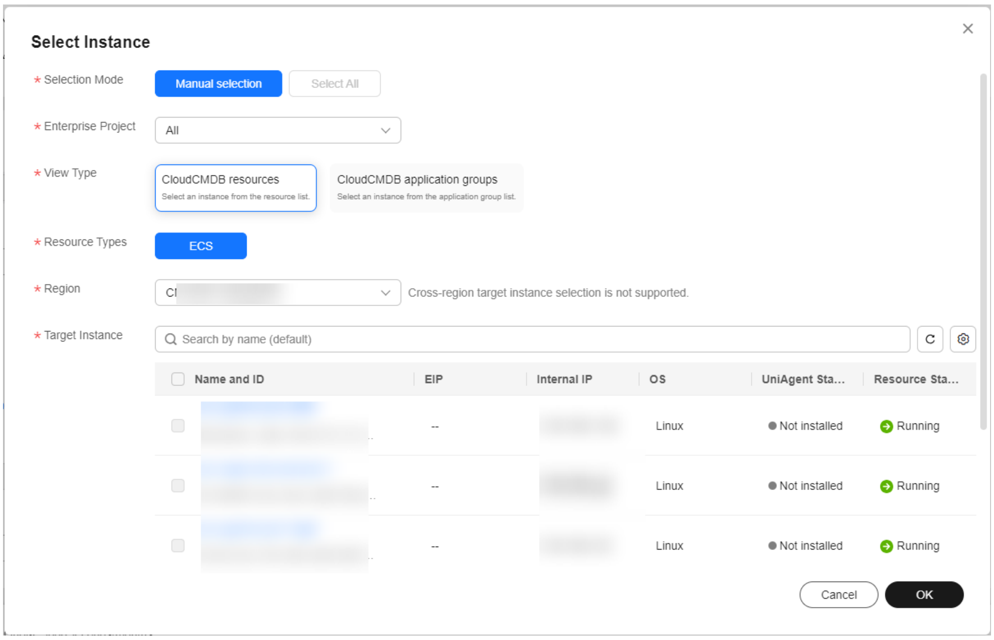
Links https://console.ulanqab.huawei.com/coc-beta/?region=cn-north-7&locale=en-us#/console/parameter/detail/6576e816cdc26a2b84617cbc

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 5-45 Selecting target instances



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Types: ECS

* Region: Cl[redacted] Cross-region target instance selection is not supported.

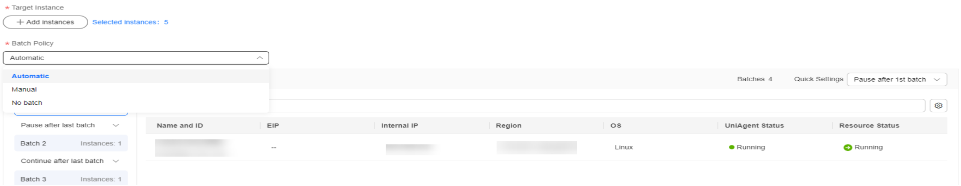
* Target Instance: Search by name (default)

□ Name and ID	EIP	Internal IP	OS	UniAgent Sta...	Resource Sta...
□ [redacted]	--	[redacted]	Linux	● Not installed	● Running
□ [redacted]	--	[redacted]	Linux	● Not installed	● Running
□ [redacted]	--	[redacted]	Linux	● Not installed	● Running

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 5-46 Selecting a batch policy



* Target Instance: + Add instances Selected instances: 5

* Batch Policy: Automatic

Batches 4 Quick Settings: Pause after 1st batch

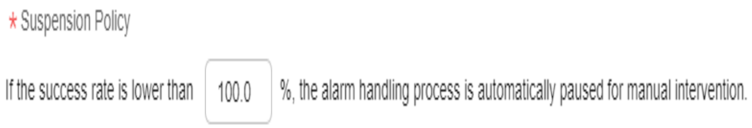
Pause after last batch
Batch 2 Instances: 1
Continue after last batch
Batch 3 Instances: 1

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	[redacted]	Linux	● Running	● Running

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 5-47 Setting a suspension policy

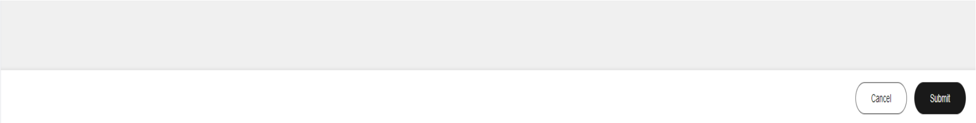


* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 7 Click **Submit**.

Figure 5-48 Submitting the request



----End

5.3 Jobs

A job is a collection of operations (atomic actions). 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 With this function, you can perform specific operations on the target instances.

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 COC.

Precautions

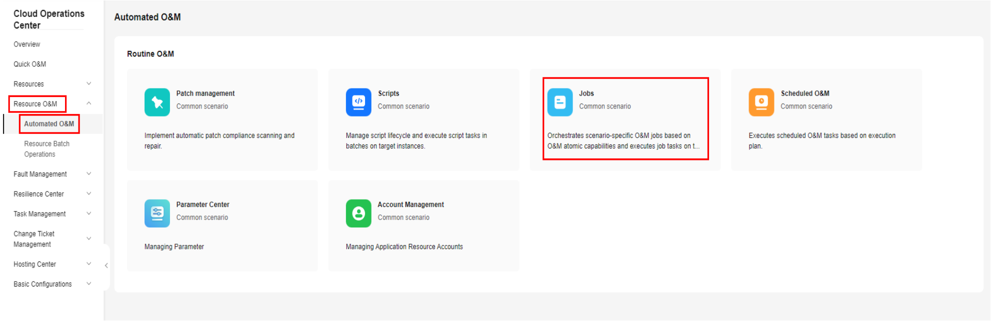
Before executing a common job, ensure that you have the resource permissions of target instances.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-49 Clicking **Jobs**



Implement automatic patch compliance scanning and repair.

Manage script lifecycle and execute script tasks in batches on target instances.

Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on t...

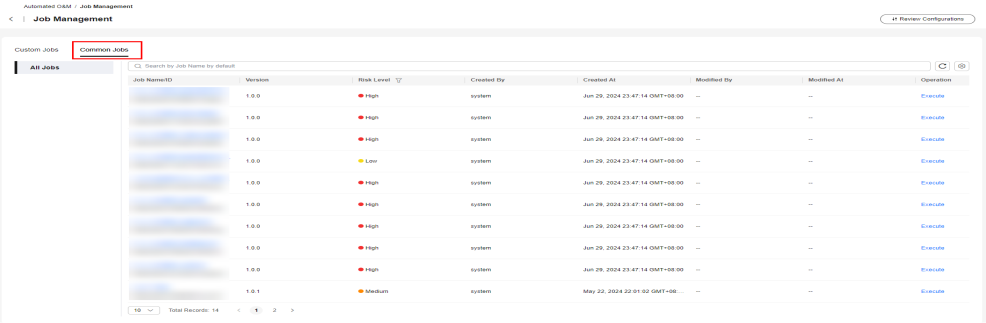
Executes scheduled O&M tasks based on execution plan.

Managing Parameter

Managing Application Resource Accounts

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

Figure 5-50 Selecting and executing a common job



Automated O&M / Job Management

< | Job Management

Review Configurations

Custom Jobs Common Jobs

All Jobs

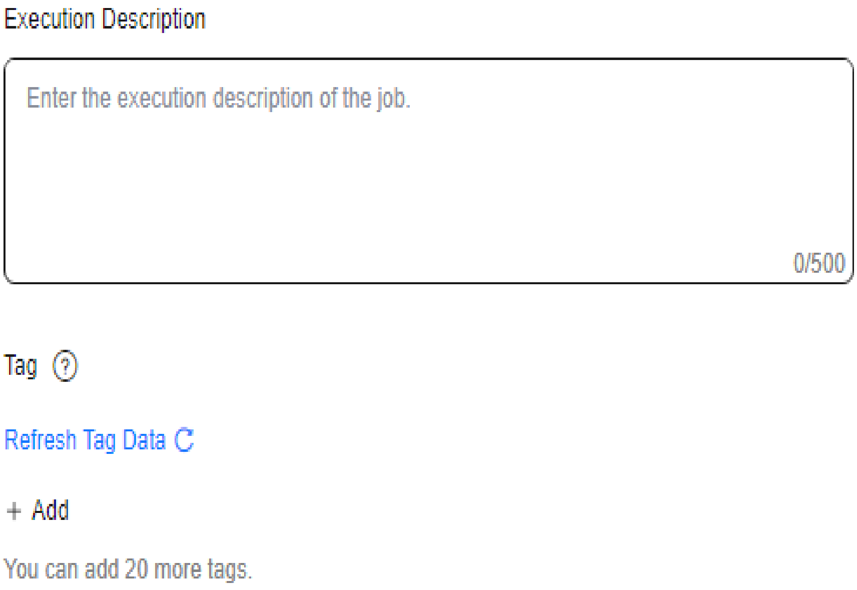
Search by Job Name by default

Job Name/ID	Version	Risk Level	Created By	Created At	Modified By	Modified At	Operation
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● Low	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.0	● High	system	Jun 29, 2024 23:47:14 GMT+08:00	--	--	Execute
[redacted]	1.0.1	● Medium	system	May 22, 2024 22:01:02 GMT+08:...	--	--	Execute

10 Total Records: 14 < 1 2 >

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 5-51 Entering basic execution information



Execution Description

Enter the execution description of the job.

0/500

Tag

Refresh Tag Data

+ Add

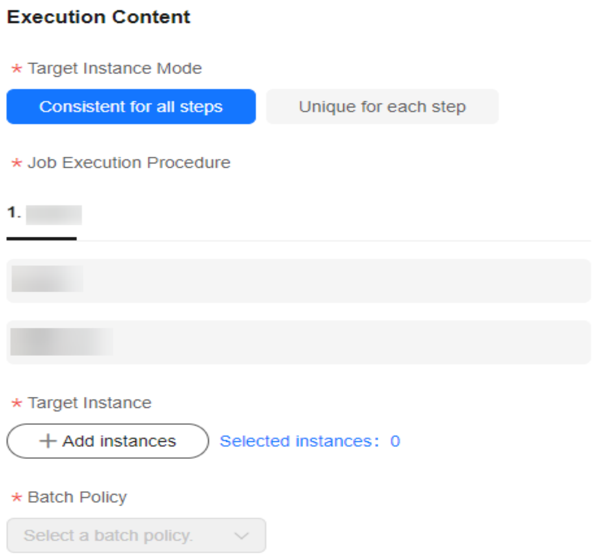
You can add 20 more tags.

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 5-52 Consistent for all steps



Execution Content

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

1.

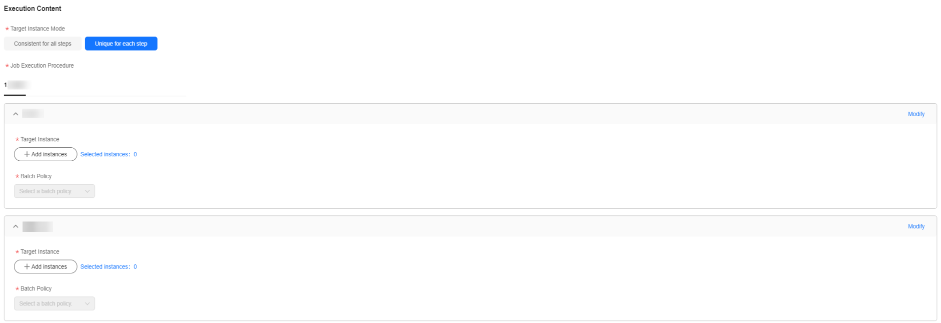
* Target Instance

+ Add instances   Selected instances：0

* Batch Policy

Select a batch policy.

Figure 5-53 Unique for each step



Execution Content

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

1

Modify

* Target Instance

+ Add instances   Selected instances：0

* Batch Policy

Select a batch policy.

Modify

* Target Instance

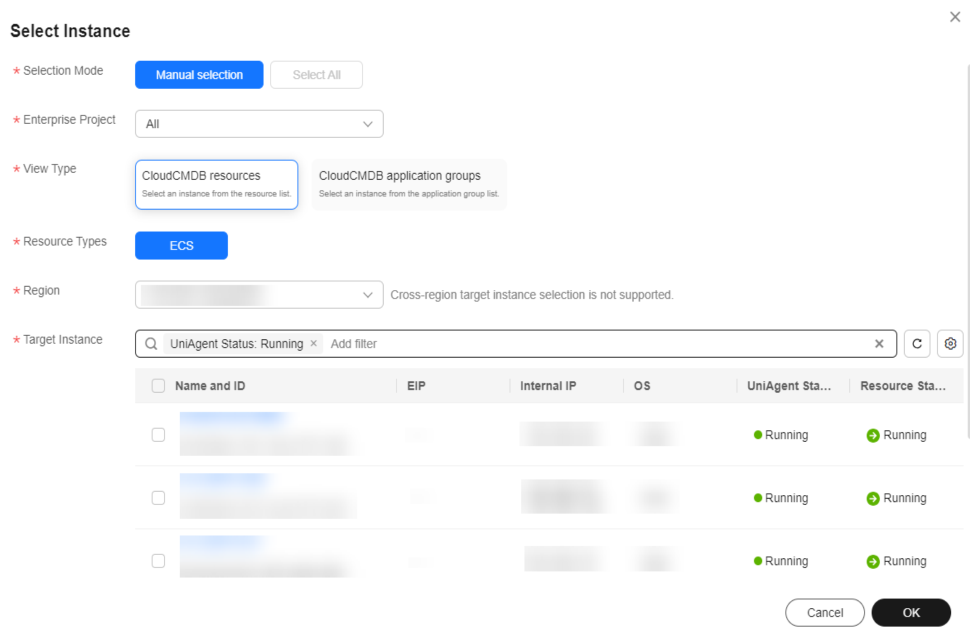
+ Add instances   Selected instances：0

* Batch Policy

Select a batch policy.

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

Figure 5-54 Selecting target instances



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Types: ECS

* Region: Cross-region target instance selection is not supported.

* Target Instance: UniAgent Status: Running × Add filter

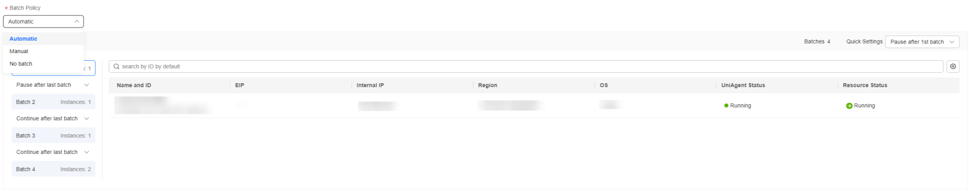
□ Name and ID	EIP	Internal IP	OS	UniAgent Sta...	Resource Sta...
□				● Running	Running
□				● Running	Running
□				● Running	Running

Cancel | OK

Step 7 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 5-55 Selecting a batch policy



* Batch Policy: Automatic

Batches 4 | Quick Settings: Pause after 1st batch

search by ID by default

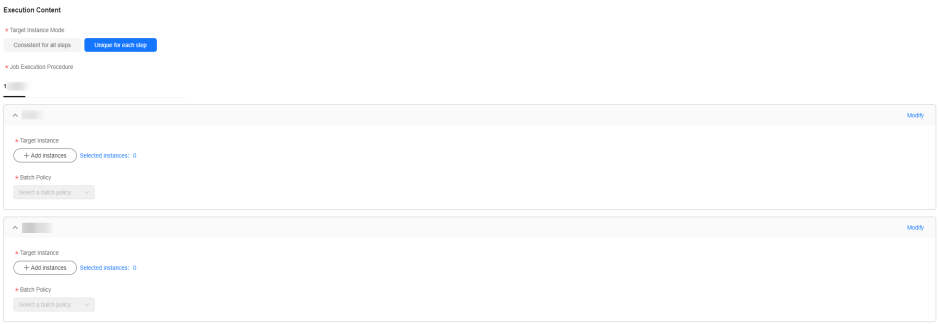
Pause after last batch
Batch 2 Instances: 1
Continue after last batch
Batch 3 Instances: 1
Continue after last batch
Batch 4 Instances: 2

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
					● Running	Running

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 end all tasks of the job.
- Click **End all batches** to end the tasks of all batches in the current step.

Figure 5-56 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 COC.

Precautions

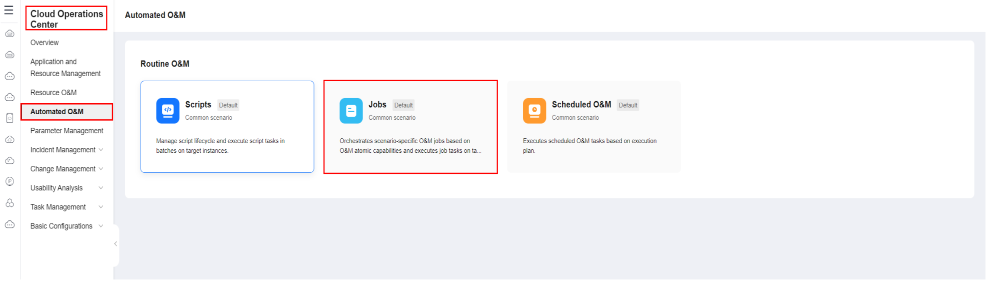
Confirm and fill in the risk level of the operation according to the operation procedure.

Procedure

Step 1 Log in to **COC**.

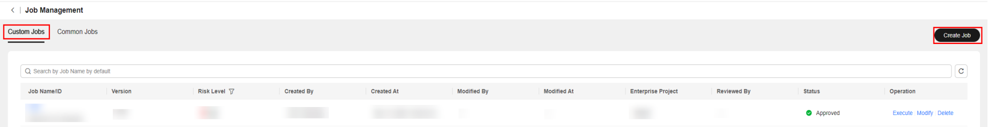
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Jobs**.

Figure 5-57 Job Management page



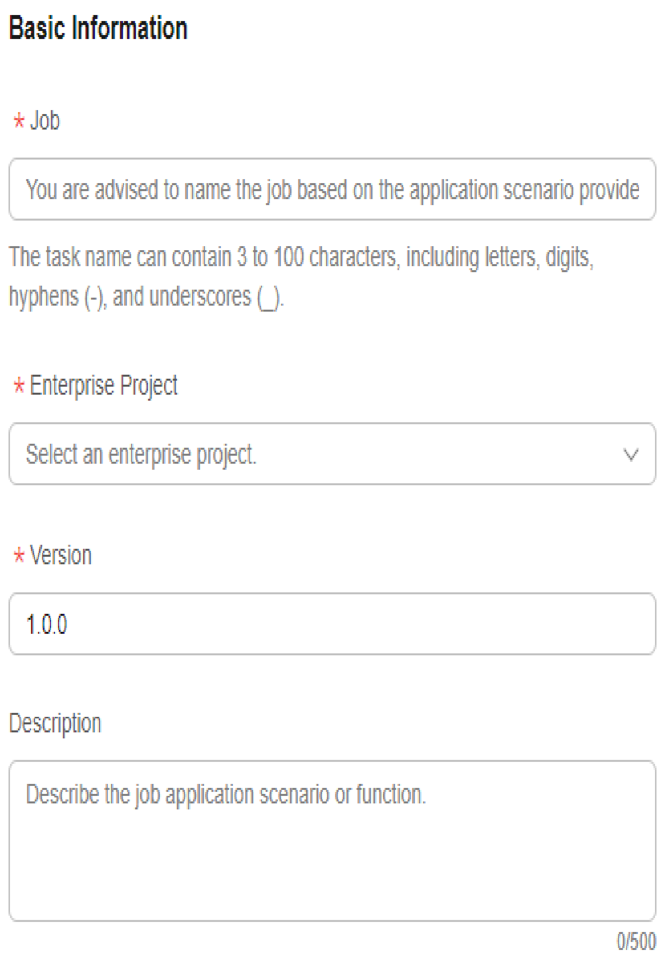
Step 3 Click the **Custom Jobs** tab and click **Create Job**.

Figure 5-58 Clicking **Create Jobs**



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 5-59 Entering basic job information



Basic Information

* Job

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

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

* Enterprise Project

Select an enterprise project.

* Version

1.0.0

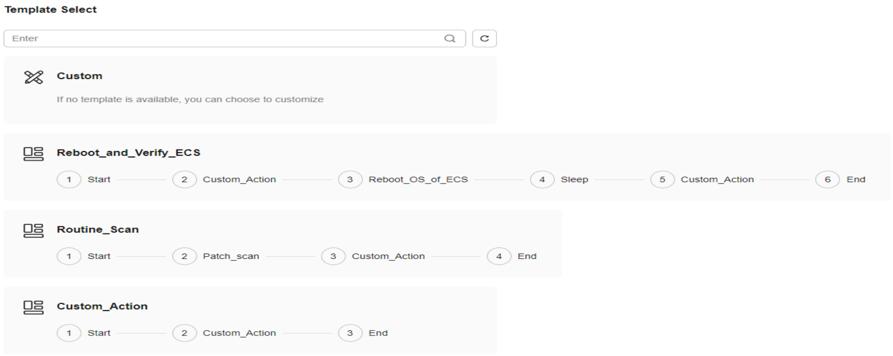
Description

Describe the job application scenario or function.

0/500

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

Figure 5-60 Selecting a job template



Template Select

Enter

Custom

If no template is available, you can choose to customize

Reboot_and_Verify_ECS

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

Routine_Scan

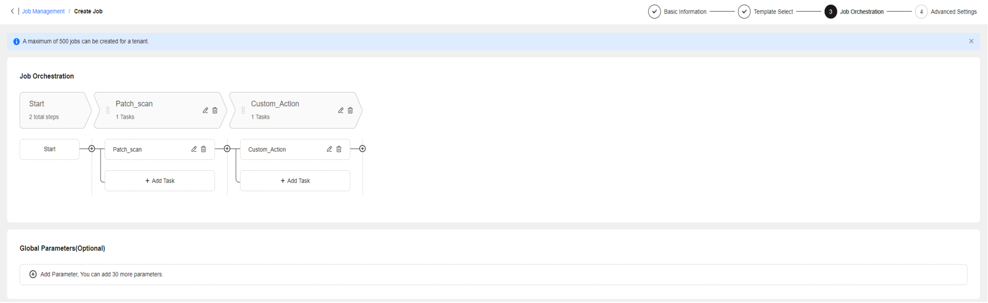
1 Start — 2 Patch_scan — 3 Custom_Action — 4 End

Custom_Action

1 Start — 2 Custom_Action — 3 End

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

Figure 5-61 Orchestrating a job



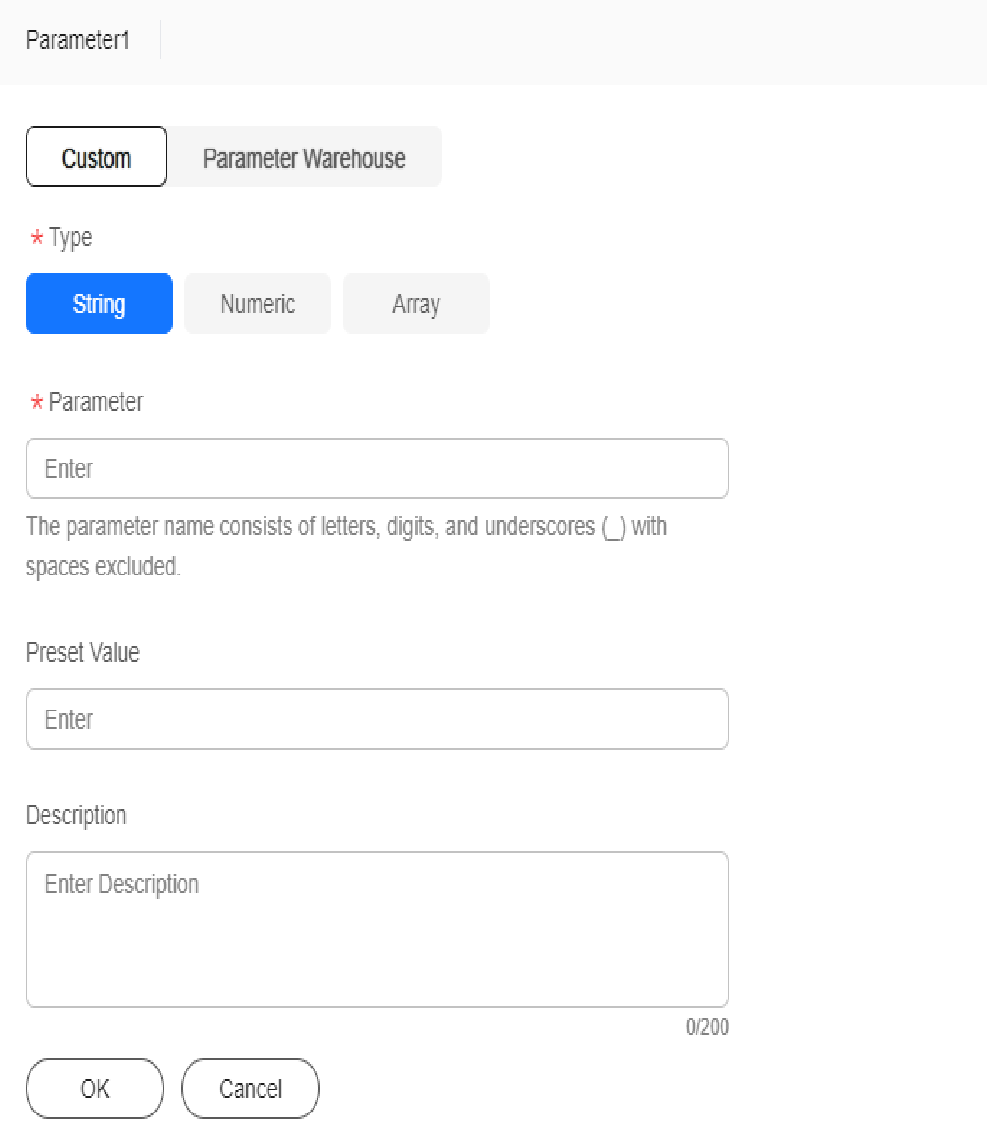
A maximum of 500 jobs can be created for a tenant.

Add Parameter, You can add 30 more parameters.

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 click **Custom**, you need to enter the parameter name, preset value, and parameter description. If you click **Parameter Warehouse**, you need to select the region where the parameter is located, parameter name, and parameter association mode.

Figure 5-62 Selecting **Custom** and adding global parameters



Parameter1

Custom | Parameter Warehouse

* Type

String | Numeric | Array

* Parameter

Enter

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

Preset Value

Enter

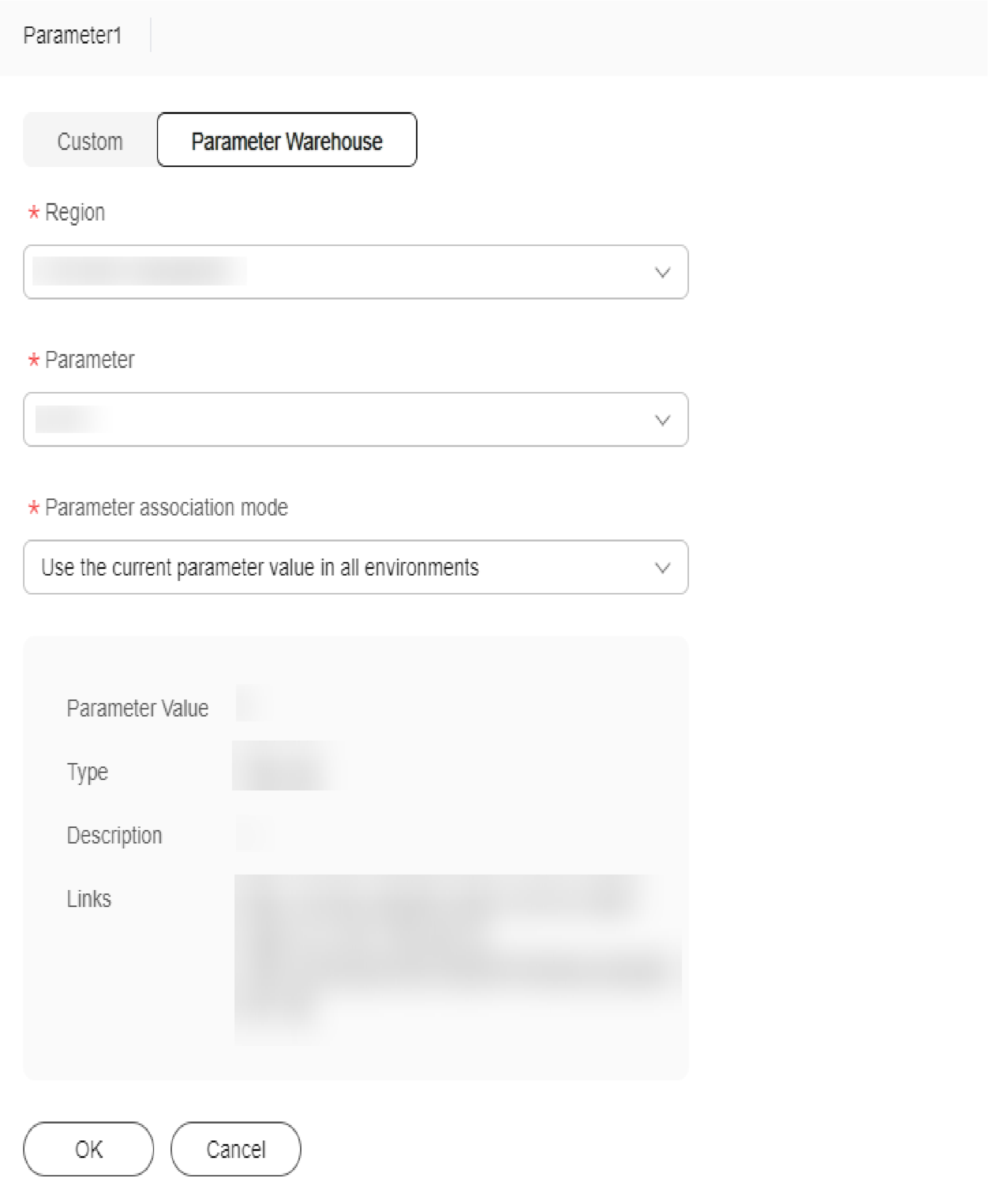
Description

Enter Description

0/200

OK | Cancel

Figure 5-63 Obtaining and adding Global parameters from the parameter warehouse



Parameter association mode: Use the current parameter value in all environments

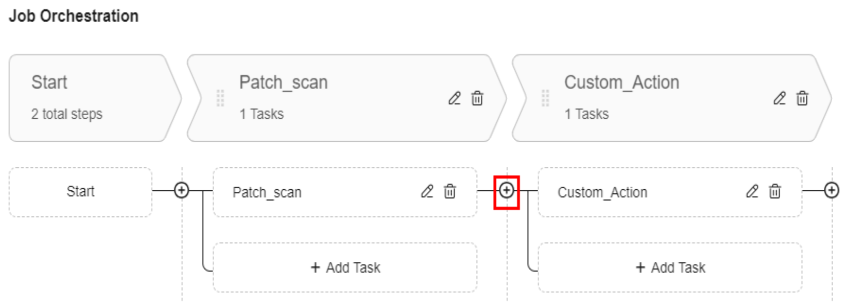
Table 5-8 Parameter association modes

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.

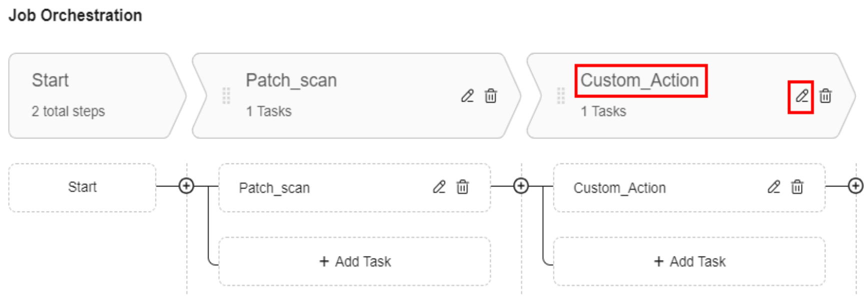
Step 8 Click ⊕ to add a new step.

Figure 5-64 Adding a step



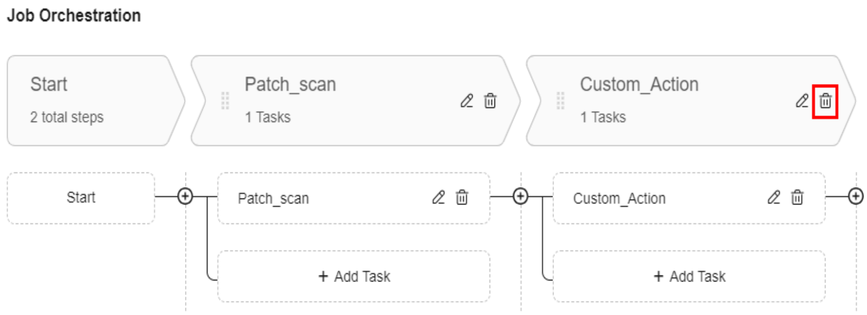
Step 9 Click the step name or ✎ to change the step name.

Figure 5-65 Changing the step name



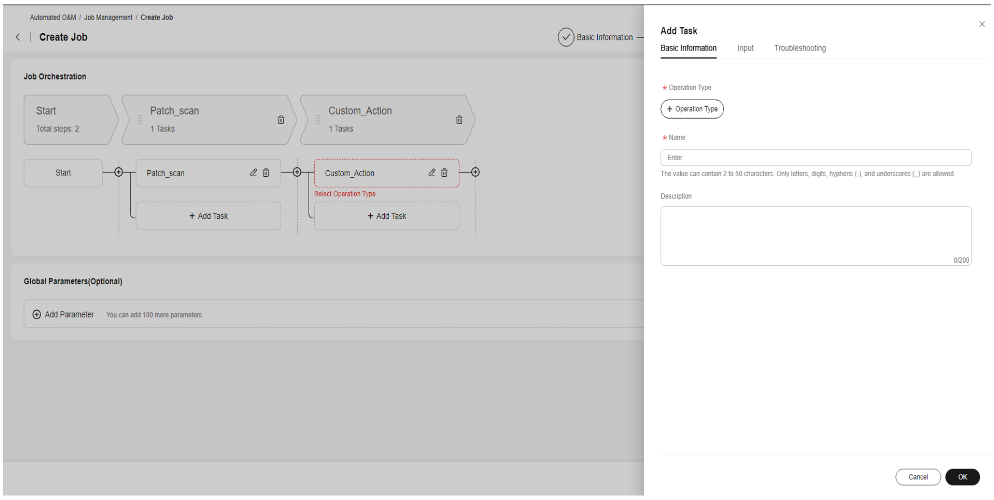
Step 10 If there are unnecessary steps, click 🗑 to delete them.

Figure 5-66 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 5-67 Adding tasks

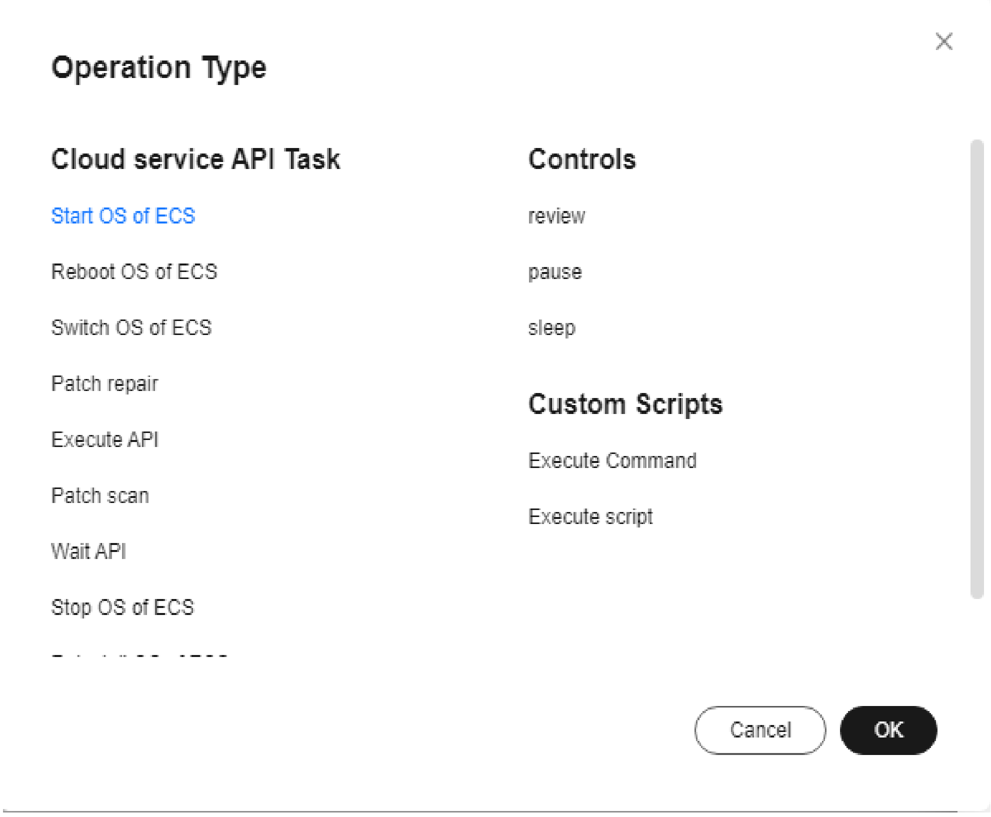


The value can contain 2 to 50 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 12 Click **+ Operation Type** to set the operation type of the current task. The operation type can be **Cloud service API Task**, **Controls**, or **Custom Scripts**.

- **Cloud service API Task**: include ECS-related operation atoms, execution APIs, and **Wait API**. For details about ECS-related operations, see **Batch Operations on ECSs**.
- **Controls**: includes **review**, **pause**, and **sleep**.
- **Custom Scripts**: You can select **Execute script** or **Execute Command**. After a custom script is created, a custom atom record is automatically registered.

Figure 5-68 Selecting an operation type



Operation Type

Cloud service API Task

Start OS of ECS

Reboot OS of ECS

Switch OS of ECS

Patch repair

Execute API

Patch scan

Wait API

Stop OS of ECS

Controls

review

pause

sleep

Custom Scripts

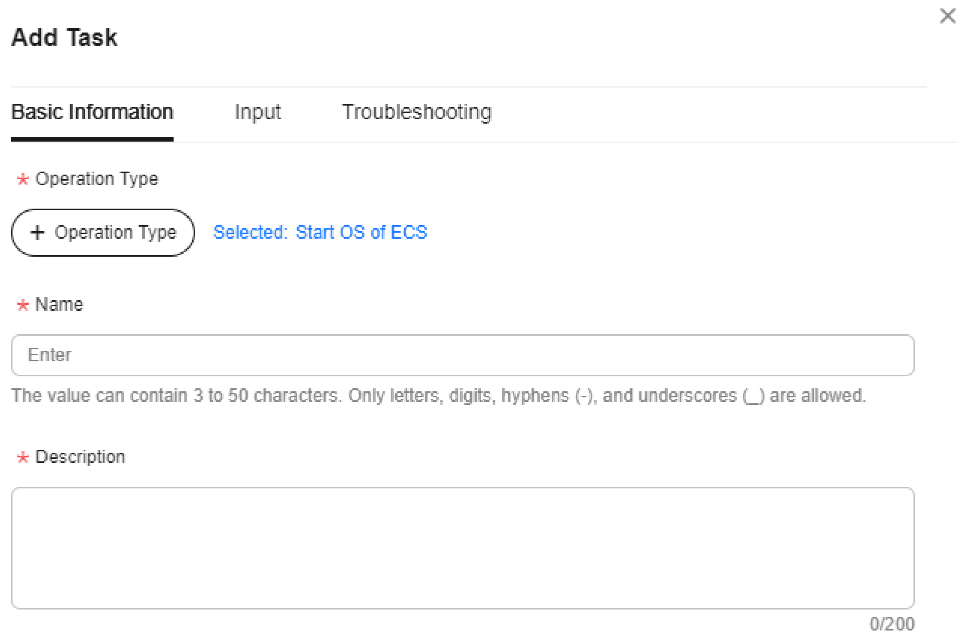
Execute Command

Execute script

Cancel OK

Step 13 Based on the selected operation type, specify basic information such as the name and operation description, parameters, and troubleshooting policy, and click **OK**.

Figure 5-69 Configuring basic information



Add Task

Basic Information Input Troubleshooting

* Operation Type

+ Operation Type Selected: Start OS of ECS

* Name

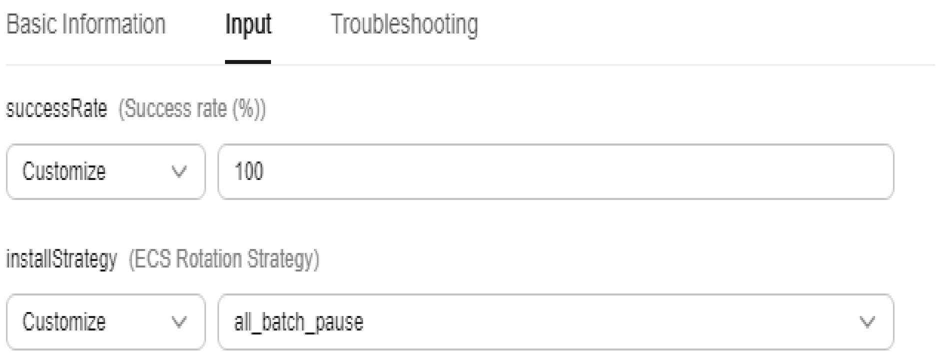
Enter

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

* Description

0/200

Figure 5-70 Set input parameters.



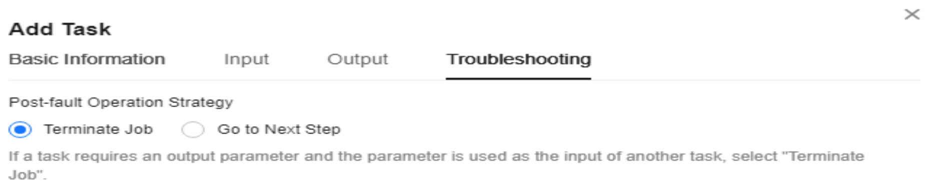
successRate (Success rate (%))

Customize 100

installStrategy (ECS Rotation Strategy)

Customize all_batch_pause

Figure 5-71 Set the troubleshooting policy.



Post-fault Operation Strategy

● Terminate Job ○ Go to Next Step

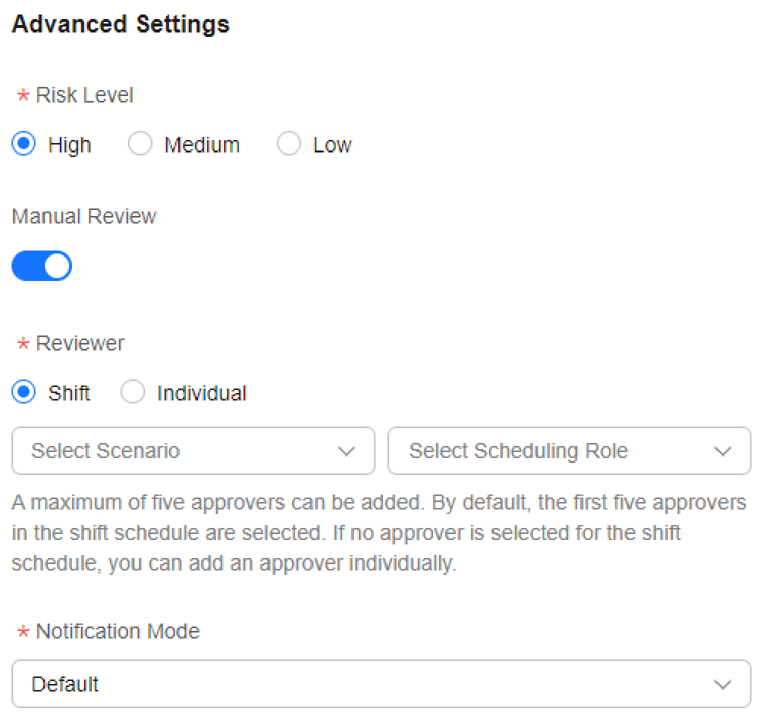
If a task requires an output parameter and the parameter is used as the input of another task, select "Terminate Job".

Step 14 After the job orchestration is complete, set the risk level of the job based on the operation risks, set **Reviewer Notification Mode**, and click **Submit**.

NOTE

- **Manual Review** is enabled by default for jobs whose risk level is **High**.
- If you select **Shift** for **Reviewer**, the users in the current schedule are reviewers. If you select **Individual**, specify some users as reviewers.
- **Notification Mode** specifies in which mode the reviewer will be notified of the review request.

Figure 5-72 Advanced settings



Advanced Settings

* Risk Level

● High ○ Medium ○ Low

Manual Review

* Reviewer

● Shift ○ Individual

Select Scenario | Select Scheduling Role

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

* Notification Mode

Default

----End

5.3.3 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

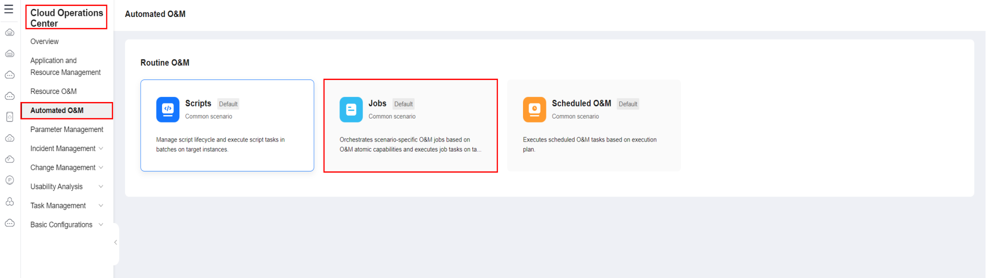
When modifying or cloning a job, determine and fill out the risk level of the job.

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 5-73 Job Management page



Manage script lifecycle and execute script tasks in batches on target instances.

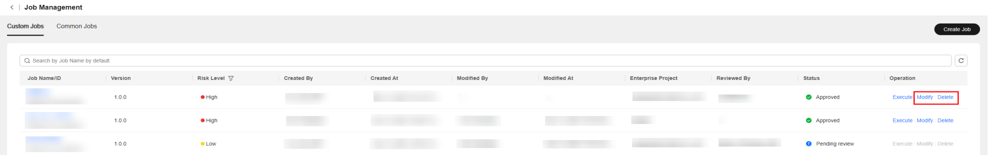
Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on ta...

Executes scheduled O&M tasks based on execution plan.

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 5-74 Performing operations on a job



Job Name/ID	Version	Risk Level	Created By	Created At	Modified By	Modified At	Enterprise Project	Reviewed By	Status	Operation
[redacted]	1.0.0	● High	[redacted]	[redacted]			[redacted]	[redacted]	✓ Approved	Execute Modify Delete
[redacted]	1.0.0	● High	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		✓ Approved	Execute Modify Delete
[redacted]	1.0.0	● Low	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	● Pending review	Execute Modify Delete

----End

5.3.4 Executing a Custom Job

Execute recorded custom jobs.

Scenarios

Execute a custom job on Cloud Operations Center.

Precautions

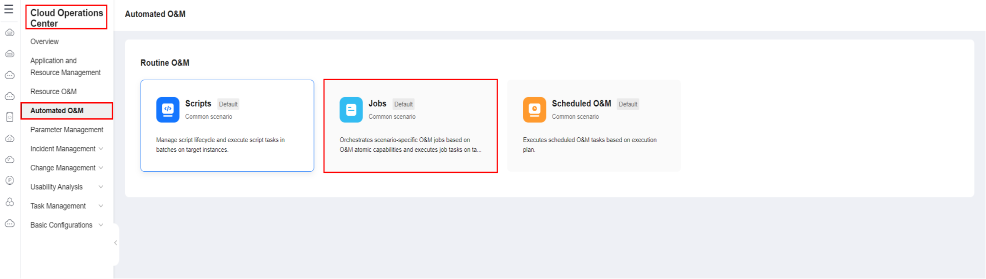
Before executing a job, ensure that you have the resource permissions of target instances.

Procedure

Step 1 Log in to **COC**.

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

Figure 5-75 Job Management page



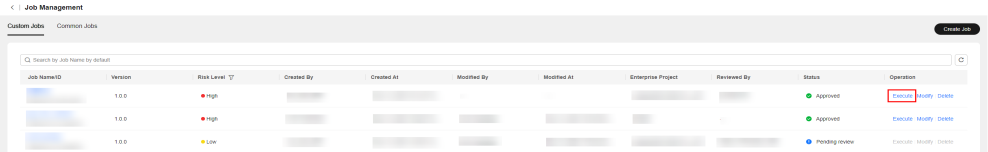
Manage script lifecycle and execute script tasks in batches on target instances.

Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on ta...

Executes scheduled O&M tasks based on execution plan.

Step 3 On the **Job Management** page, click the **Custom Jobs** tab, locate the job to be executed, and click **Execute** in the **Operation** column.

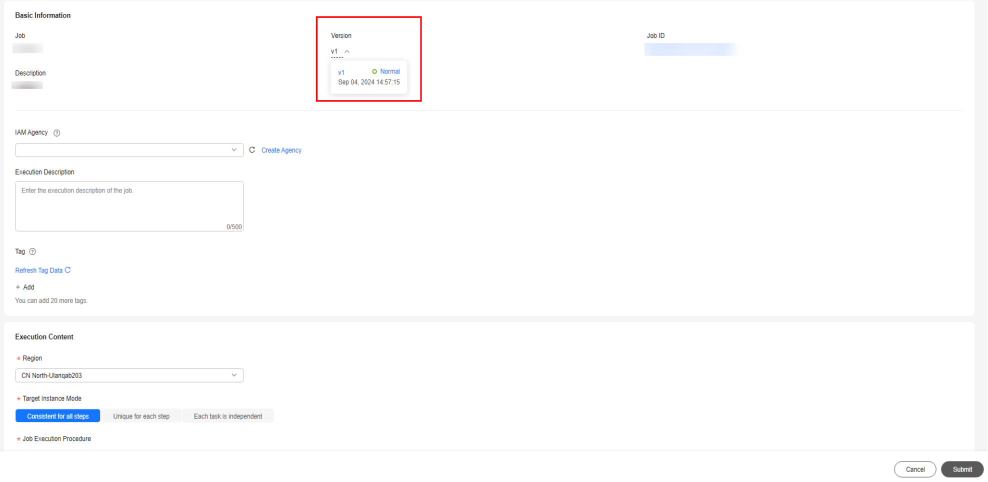
Figure 5-76 Clicking **Execute**



Job Name/ID	Version	Risk Level	Created By	Created At	Modified By	Modified At	Enterprise Project	Reviewed By	Status	Operation
[redacted]	1.0.0	● High	[redacted]	[redacted]			[redacted]	[redacted]	Approved	Execute | Modify | Delete
[redacted]	1.0.0	● High	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		Approved	Execute | Modify | Delete
[redacted]	1.0.0	● Low	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Pending review	Execute | Modify | Delete

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

Figure 5-77 Checking the job steps



Job: [redacted]

Version: v1

v1 Normal Sep 04, 2024 14:57:15

Job ID: [redacted]

Description: [redacted]

IAM Agency

Execution Description: Enter the execution description of the job. 0/500

Tag

You can add 20 more tags.

* Region: CN North-Ulanqab203

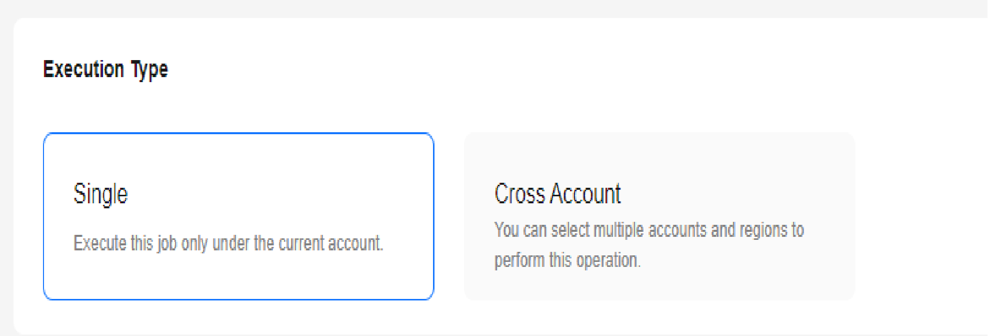
* Target Instance Mode: Consistent for all steps | Unique for each step | Each task is independent

* Job Execution Procedure

Step 5 Select the execution type.

Execution Type includes **Single** and **Cross Account**.

Figure 5-78 Execution Type



Execution Type

Single

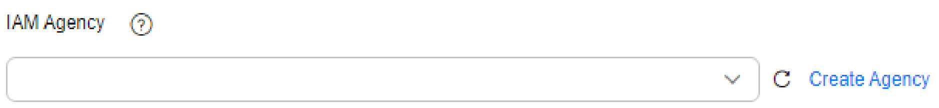
Execute this job only under the current account.

Cross Account

You can select multiple accounts and regions to perform this operation.

Step 6 Select **IAM Agency**. The IAM agency is used to switch the user role during the runbook execution and execute the job.

Figure 5-79 Selecting the IAM agency

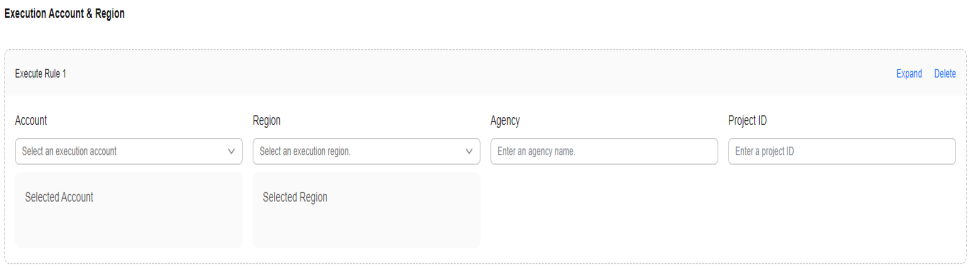


Step 7 If you select **Cross Account**, you need to set the execution rule.

NOTE

- Currently, BMS API call and scripts cannot be executed across accounts.
- To use this function, you need to add the account to the organization, configure the agency permissions, and enter the agency name in advance. For details, see Cross-Account Management.

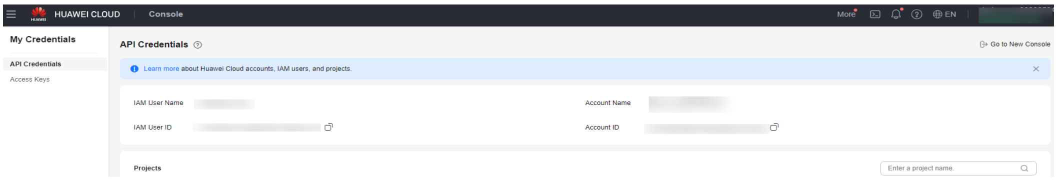
Figure 5-80 Account and Region



Parameter description:

Account: tenant account name, which can be viewed on the **My Credentials** page.

Figure 5-81 Viewing the account name



Learn more about Huawei Cloud accounts, IAM users, and projects.

IAM User Name [redacted]

IAM User ID [redacted]

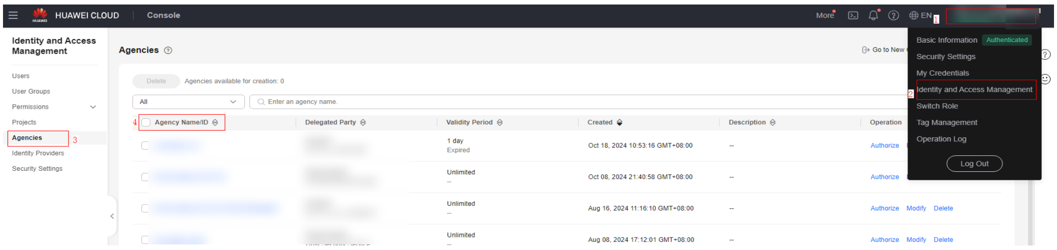
Account Name [redacted]

Account ID [redacted]

Region: region where the target object is located.

Agency: name of the agency in IAM

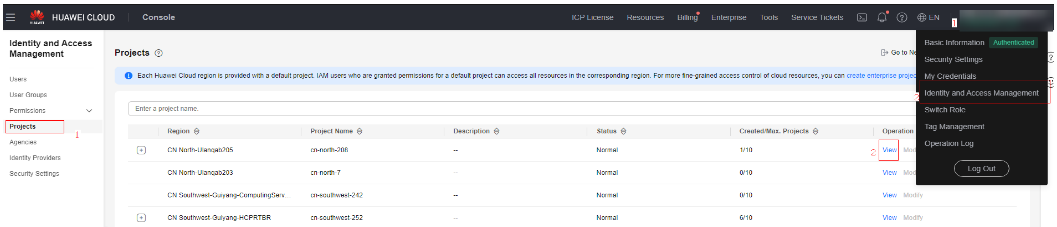
Figure 5-82 Obtaining the agent name



Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
[redacted]	[redacted]	1 day Expired	Oct 18, 2024 10:53:16 GMT+08:00	--	Authorize
[redacted]	[redacted]	Unlimited --	Oct 08, 2024 21:40:58 GMT+08:00	--	Authorize
[redacted]	[redacted]	Unlimited --	Aug 16, 2024 11:16:10 GMT+08:00	--	Authorize Modify Delete
[redacted]	[redacted]	Unlimited --	Aug 08, 2024 17:12:01 GMT+08:00	--	Authorize Modify Delete

Project ID: ID of the project to which the target object belongs.

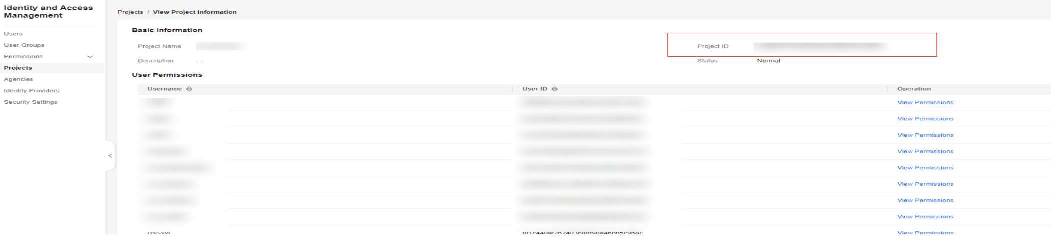
Figure 5-83 Viewing project information



Each Huawei Cloud region is provided with a default project. IAM users who are granted permissions for a default project can access all resources in the corresponding region. For more fine-grained access control of cloud resources, you can create enterprise projec

Region	Project Name	Description	Status	Created/Max. Projects	Operation
CN North-Ulanqab205	cn-north-208	--	Normal	1/10	View Mod
CN North-Ulanqab203	cn-north-7	--	Normal	0/10	View Mod
CN Southwest-Guiyang-ComputingServ...	cn-southwest-242	--	Normal	0/10	View Modify
CN Southwest-Guiyang-HCPRTBR	cn-southwest-252	--	Normal	6/10	View Modify

Figure 5-84 Obtaining a Project ID



Basic Information

Project Name [redacted]

Description --

Project ID [redacted]

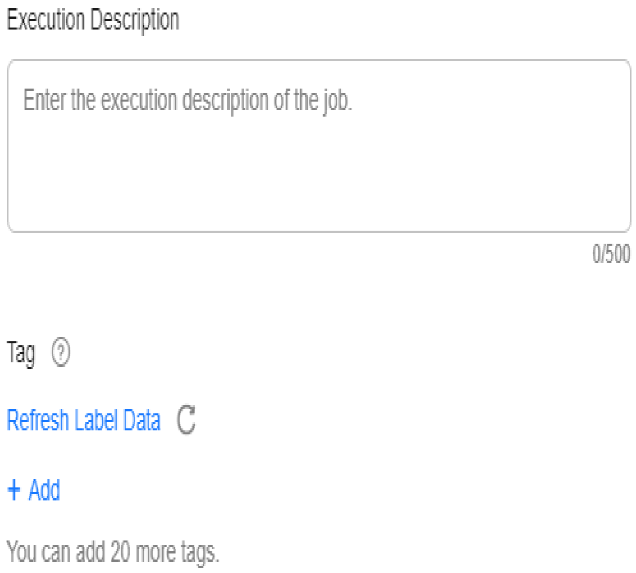
Status Normal

User Permissions

Username	User ID	Operation
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[redacted]	[redacted]	View Permissions
[illegible]	[illegible]	View Permissions

Step 8 Enter basic execution information, including the execution description and tag. You can create tags by following the instructions provided in **Tag Management**.

Figure 5-85 Entering basic execution information



Execution Description

Enter the execution description of the job.

0/500

Tag

Refresh Label Data

+ Add

You can add 20 more tags.

Step 9 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 5-86 Selecting **Consistent for all steps**

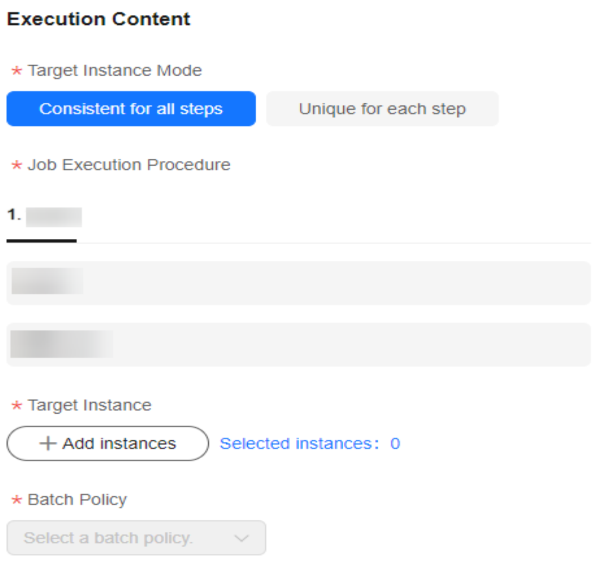
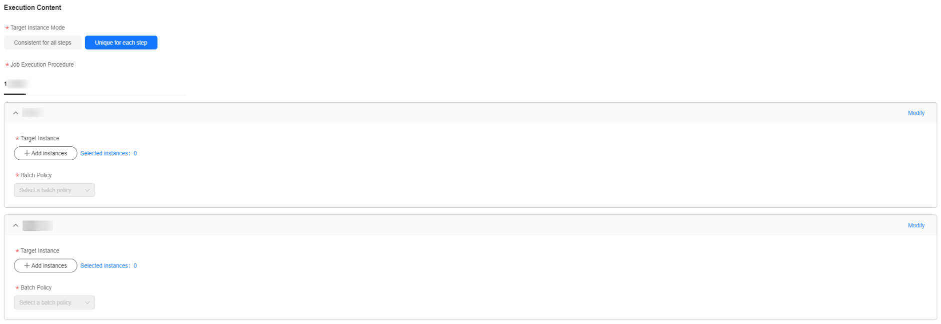
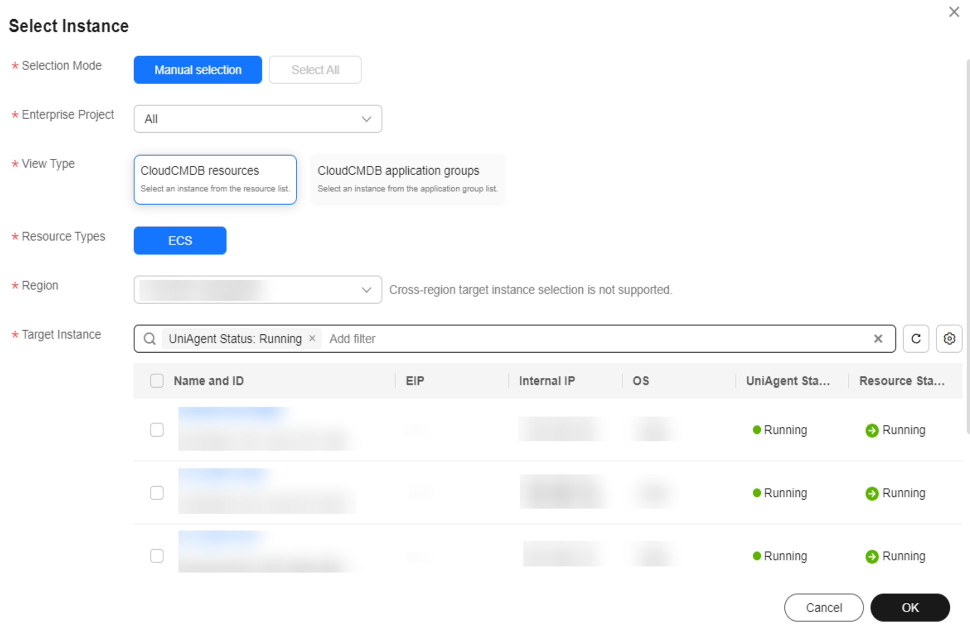


Figure 5-87 Selecting **Unique for each step**



Step 10 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 5-88 Selecting the target instance



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Types: ECS

* Region: Cross-region target instance selection is not supported.

* Target Instance: UniAgent Status: Running × Add filter

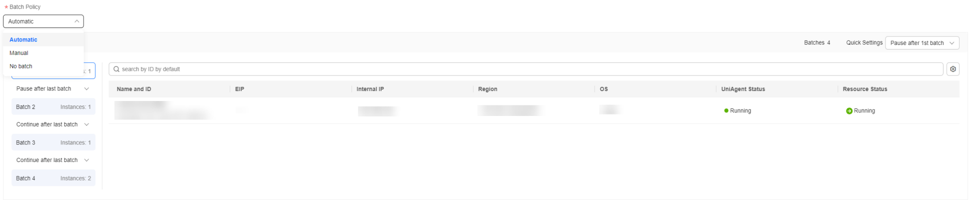
Name and ID	EIP	Internal IP	OS	UniAgent Sta...	Resource Sta...
				Running	Running
				Running	Running
				Running	Running

Cancel | OK

Step 11 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 5-89 Selecting a batch policy



* Batch Policy: Automatic

Automatic | Manual | No batch

Batches 4 Quick Settings: Pause after 1st batch

Pause after last batch
Batch 2 Instances: 1
Continue after last batch
Batch 3 Instances: 1
Continue after last batch
Batch 4 Instances: 2

search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
					Running	Running

Step 12 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.

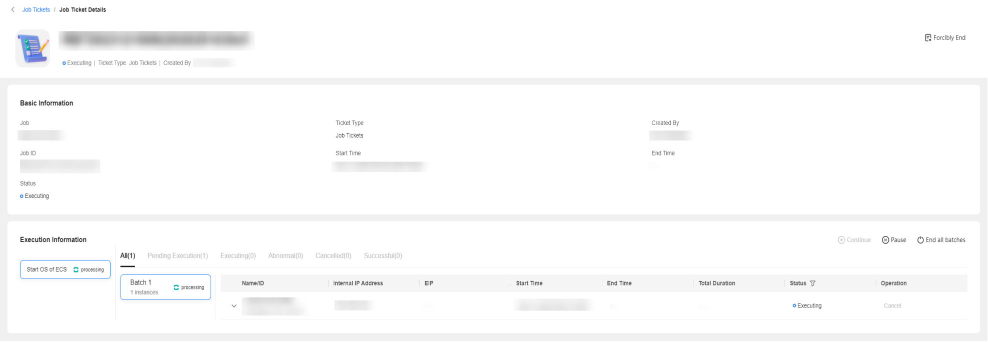
- Click **Forcibly End** to end all tasks of the job. **Currently, the sub-service tickets such as the script service tickets and patch service tickets will not be ended.**.
- Click **Terminate All** to end the tasks of all batches in the current step.

NOTE

– If you click **Terminate All**, the next batch will not be executed. However, the execution of instances in the script will not be terminated.

– If a script is delivered by the UniAgent and is in the running state, it cannot be stopped. You can stop it until the execution is complete.

Figure 5-90 Job ticket details



Job Tickets / Job Ticket Details

[redacted]

Executing | Ticket Type Job Tickets | Created By [redacted]

Forcibly End

Basic Information

Job: [redacted]

Ticket Type: Job Tickets

Created By: [redacted]

Job ID: [redacted]

Start Time: [redacted]

End Time

Status: Executing

Execution Information

Continue | Pause | End all batches

Start OS of ECS processing

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

Batch 1
1 instances processing

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]		[redacted]			Executing	Cancel

----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 Log in to COC.

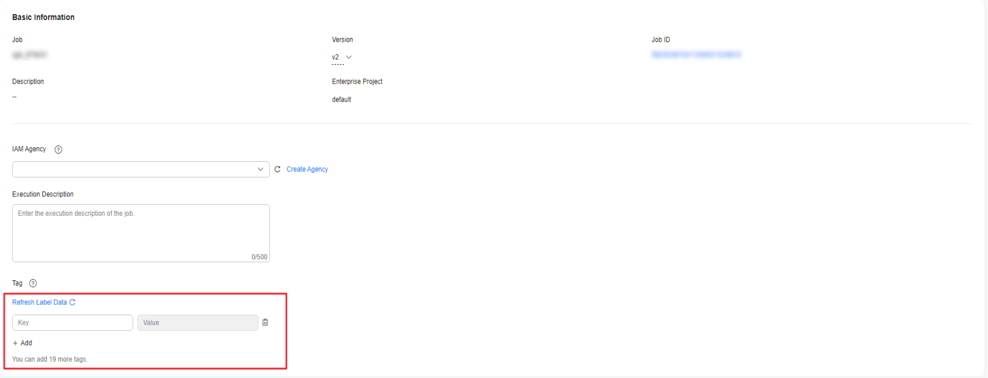
Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **Jobs**.

Step 3 On the **Job Management** page, click the **Custom Jobs** tab, locate the job to be executed, and click **Execute** in the **Operation** column.

Step 4 In the **Basic Information** area, click **+Add** and enter the tag key and value.

Step 5 Click the deletion icon on the right of the added tag to delete the tag.

Figure 5-91 Adding a tag



Basic Information

Job: [redacted]

Version: v2

Job ID: [redacted]

Description: --

Enterprise Project: default

IAM Agency

Create Agency

Execution Description

Enter the execution description of the job.

0/500

Tag

Refresh Label Data

Key | Value

+ Add

You can add 19 more tags.

----End

Editing a Tag

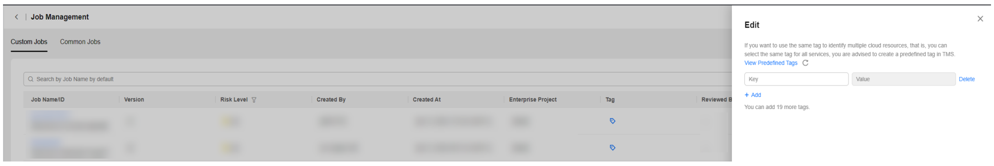
Step 1 Log in to COC.

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

Step 3 On the **Job Management** page, click the **Custom Jobs tab**, click 🏷 in the job list, and click **Edit**.

Step 4 Modify the tag by referring to the steps for adding a tag, and click **OK**.

Figure 5-92 Editing a tag



If you want to use the same tag to identify multiple cloud resources, that is, you can select the same tag for all services, you are advised to create a predefined tag in TMS.

You can add 19 more tags.

----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

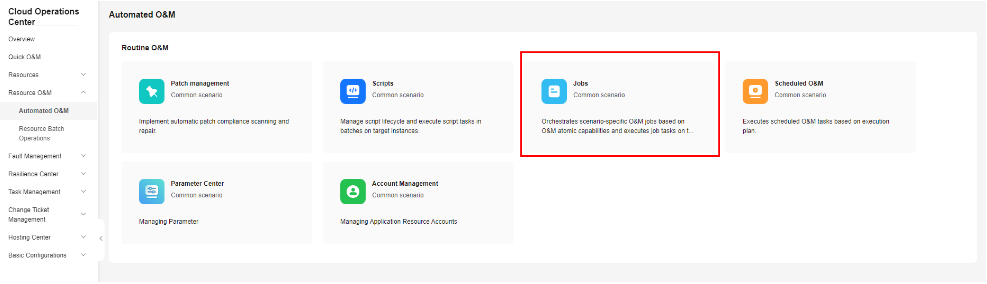
The atomic action can be used to invoke the OpenAPI of a cloud service registered with the API Explorer. If the OpenAPI is an asynchronous call, you can use the atomic action of Wait API to wait for the target object to reach the expected state.

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 5-93 Jobs



Implement automatic patch compliance scanning and repair.

Manage script lifecycle and execute script tasks in batches on target instances.

Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on t...

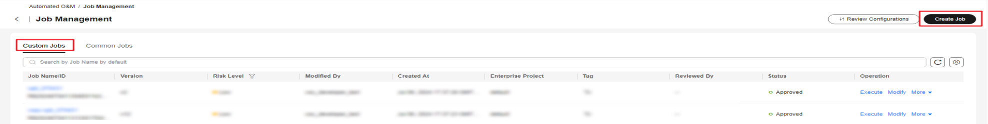
Executes scheduled O&M tasks based on execution plan.

Managing Parameter

Managing Application Resource Accounts

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

Figure 5-94 Clicking **Create Job**



Automated O&M / Job Management

Job Management

Review Configurations | Create Job

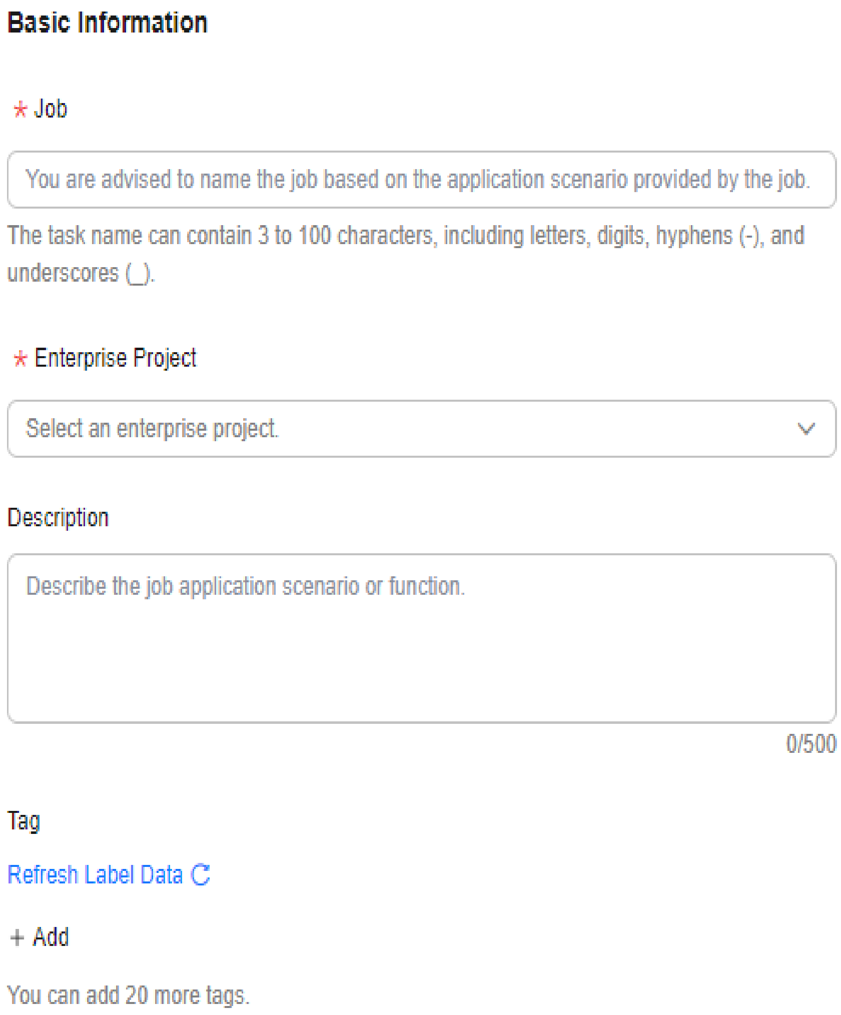
Custom Jobs | Common Jobs

Search by Job Name by default

Job Name/ID	Version	Risk Level	Modified By	Created At	Enterprise Project	Tag	Reviewed By	Status	Operation
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More

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 5-95 Entering basic job information



Basic Information

* Job

You are advised to name the job based on the application scenario provided by the job.

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

* Enterprise Project

Select an enterprise project.

Description

Describe the job application scenario or function.

0/500

Tag

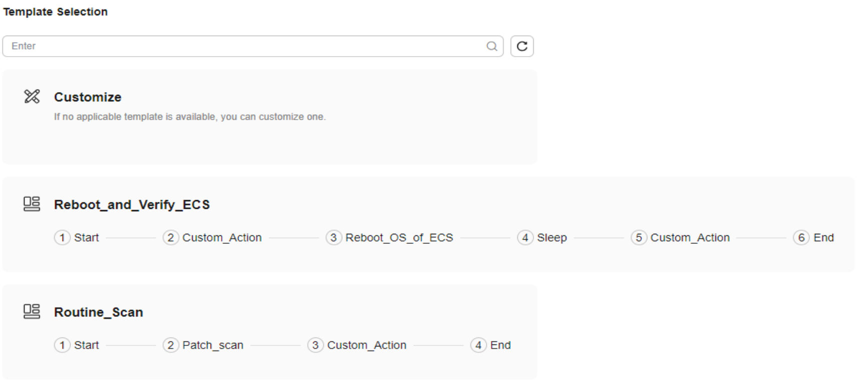
Refresh Label Data

+ Add

You can add 20 more tags.

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

Figure 5-96 Selecting a job template



Template Selection

Enter

Customize

If no applicable template is available, you can customize one.

Reboot_and_Verify_ECS

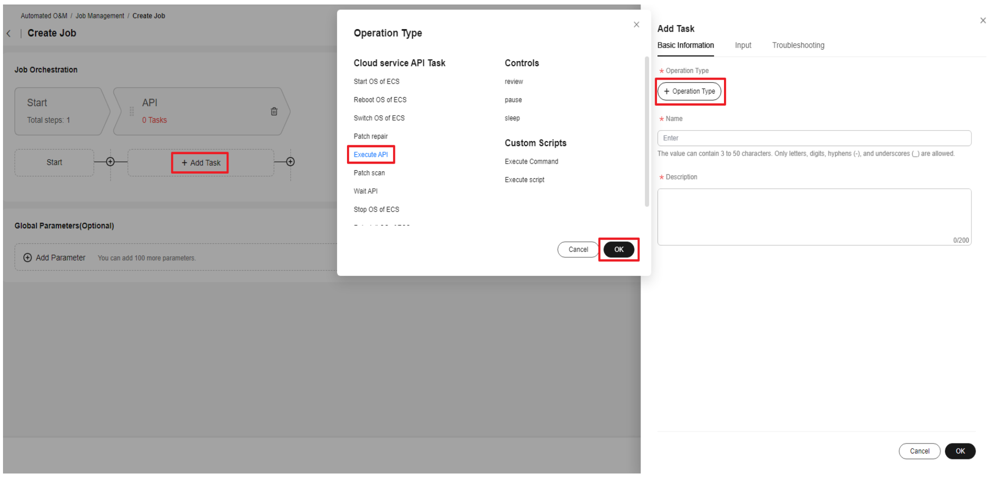
1 Start — 2 Custom_Action — 3 Reboot_OS_of_ECS — 4 Sleep — 5 Custom_Action — 6 End

Routine_Scan

1 Start — 2 Patch_scan — 3 Custom_Action — 4 End

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

Figure 5-97 Adding tasks



Automated O&M / Job Management / Create Job

Create Job

Job Orchestration

Start
Total steps: 1

API
0 Tasks

Start

+ Add Task

Global Parameters(Optional)

Add Parameter You can add 100 more parameters.

Operation Type

Cloud service API Task
- Start OS of ECS
- Reboot OS of ECS
- Switch OS of ECS
- Patch repair
- Execute API
- Patch scan
- Wait API
- Stop OS of ECS

Controls
- review
- pause
- sleep

Custom Scripts
- Execute Command
- Execute script

Cancel OK

Add Task

Basic Information | Input | Troubleshooting

* Operation Type

+ Operation Type

* Name

Enter

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

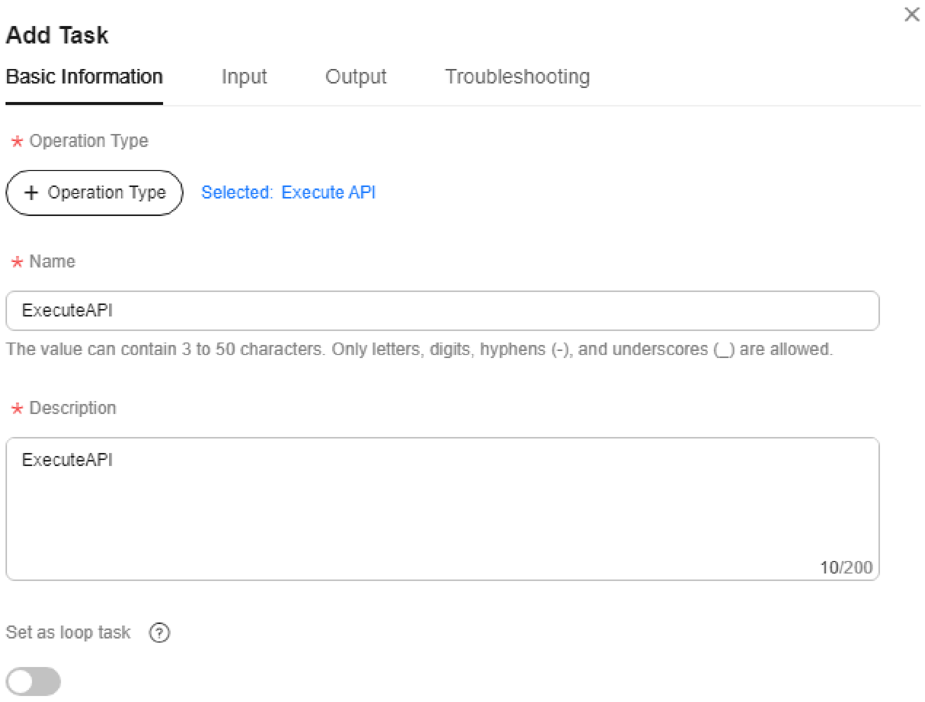
* Description

0/200

Cancel OK

Step 7 Enter the task name and operation description.

Figure 5-98 Configuring basic information



Add Task

* Operation Type

Selected: Execute API

* Name

ExecuteAPI

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

* Description

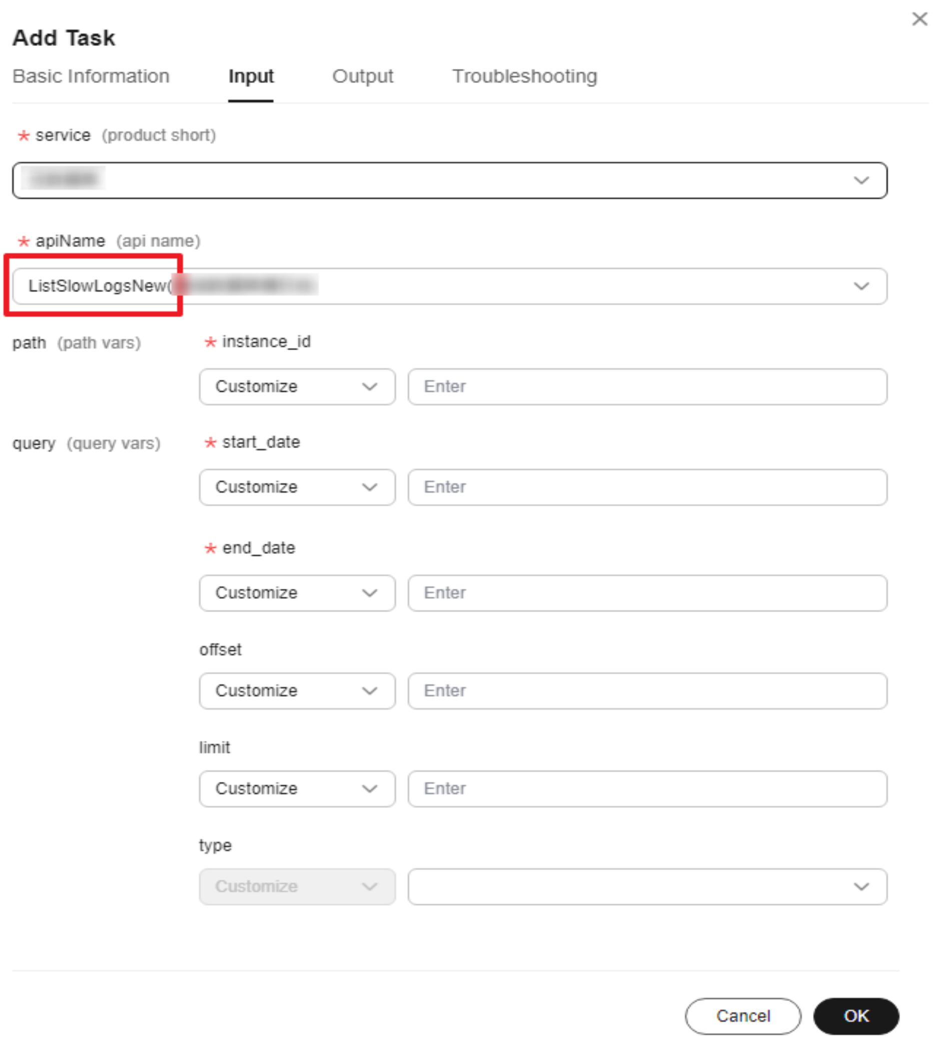
ExecuteAPI

10/200

Set as loop task

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

Figure 5-99 Adding input information



Add Task

Basic Information | **Input** | Output | Troubleshooting

* service (product short)

[redacted]

* apiName (api name)

ListSlowLogsNew([redacted]

path (path vars)

* instance_id: Customize | Enter

query (query vars)

* start_date: Customize | Enter

* end_date: Customize | Enter

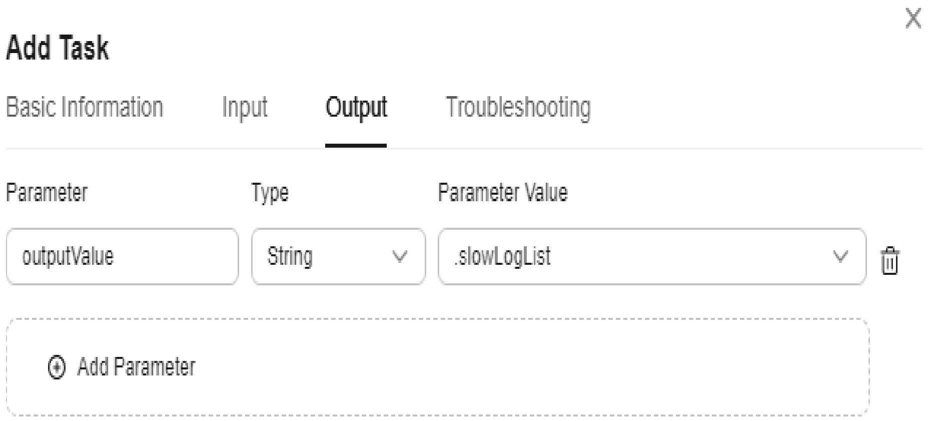
offset: Customize | Enter

limit: Customize | Enter

type: Customize |

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.

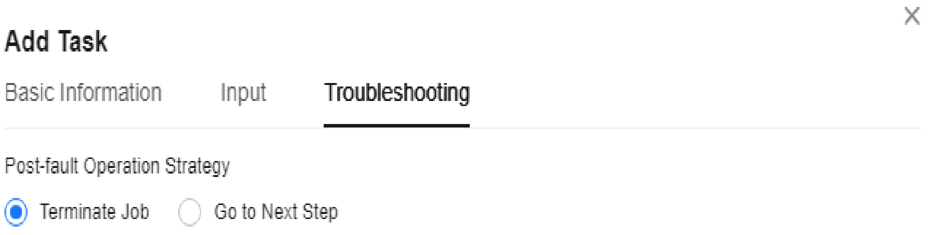
Figure 5-100 Adding output information



Parameter	Type	Parameter Value
outputValue	String	.slowLogList

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

Figure 5-101 Adding troubleshooting policy



Post-fault Operation Strategy

● Terminate Job ○ Go to Next Step

Step 11 Click **OK**.

----End

5.3.6.2 Wait API

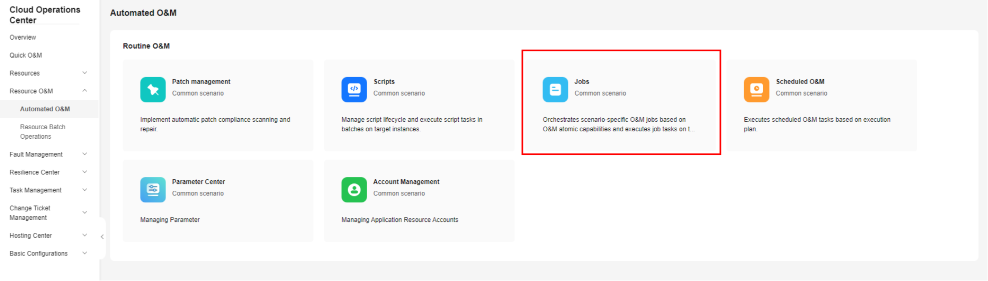
The atomic action can be used to wait for the target object to reach the expected state. For example, after calling the **StartServer** API of the ECS using the Execute API atomic action, call the **ShowServer** API of the ECS using the Wait API atomic action. Wait until the status in the API response 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 5-102 Jobs



Implement automatic patch compliance scanning and repair.

Manage script lifecycle and execute script tasks in batches on target instances.

Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on t...

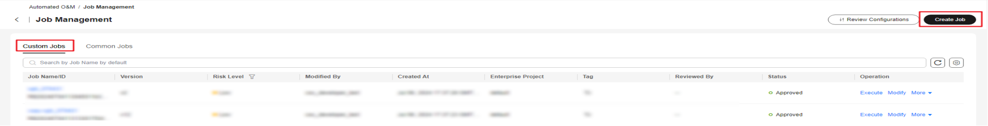
Executes scheduled O&M tasks based on execution plan.

Managing Parameter

Managing Application Resource Accounts

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

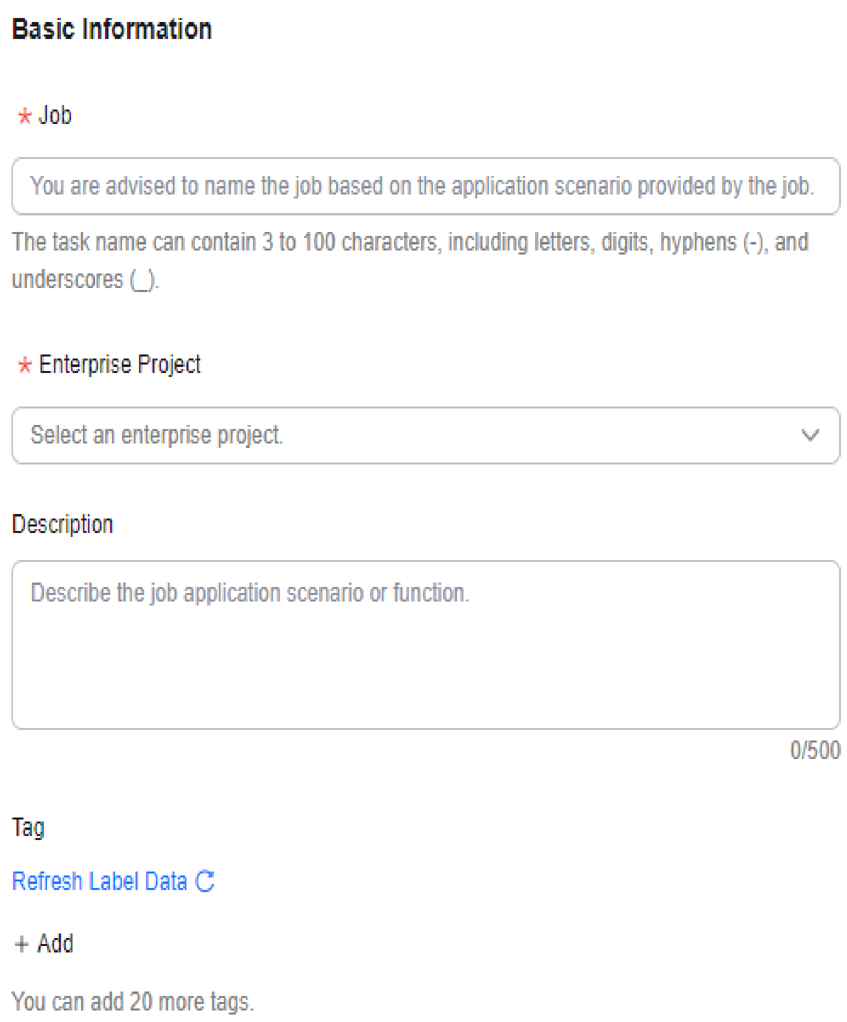
Figure 5-103 Clicking **Create Job**



Job Name/ID	Version	Risk Level	Modified By	Created At	Enterprise Project	Tag	Reviewed By	Status	Operation
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More

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 5-104 Entering basic job information



Basic Information

* Job

You are advised to name the job based on the application scenario provided by the job.

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

* Enterprise Project

Select an enterprise project.

Description

Describe the job application scenario or function.

0/500

Tag

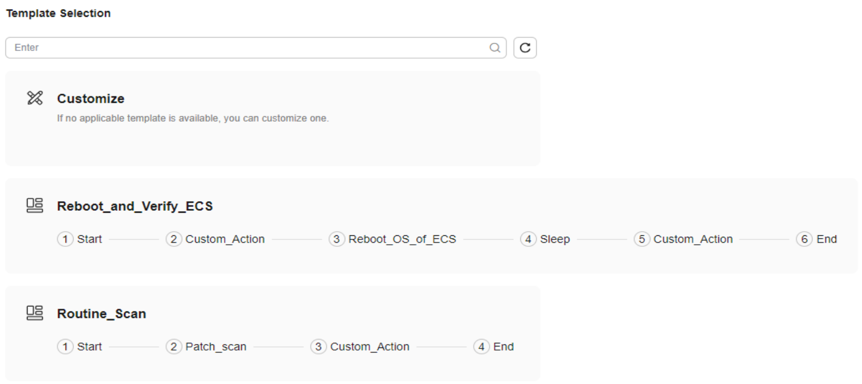
Refresh Label Data

+ Add

You can add 20 more tags.

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

Figure 5-105 Selecting a job template



Template Selection

Enter

Customize

If no applicable template is available, you can customize one.

Reboot_and_Verify_ECS

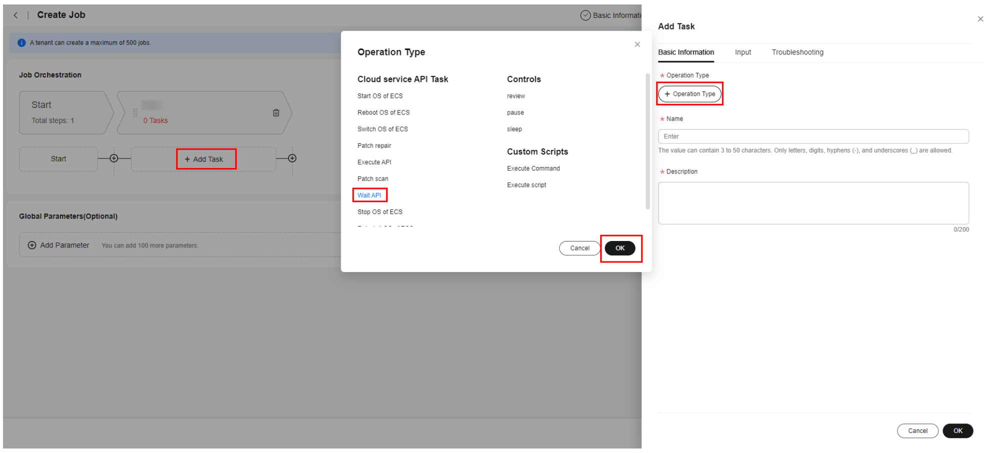
1 Start — 2 Custom_Action — 3 Reboot_OS_of_ECS — 4 Sleep — 5 Custom_Action — 6 End

Routine_Scan

1 Start — 2 Patch_scan — 3 Custom_Action — 4 End

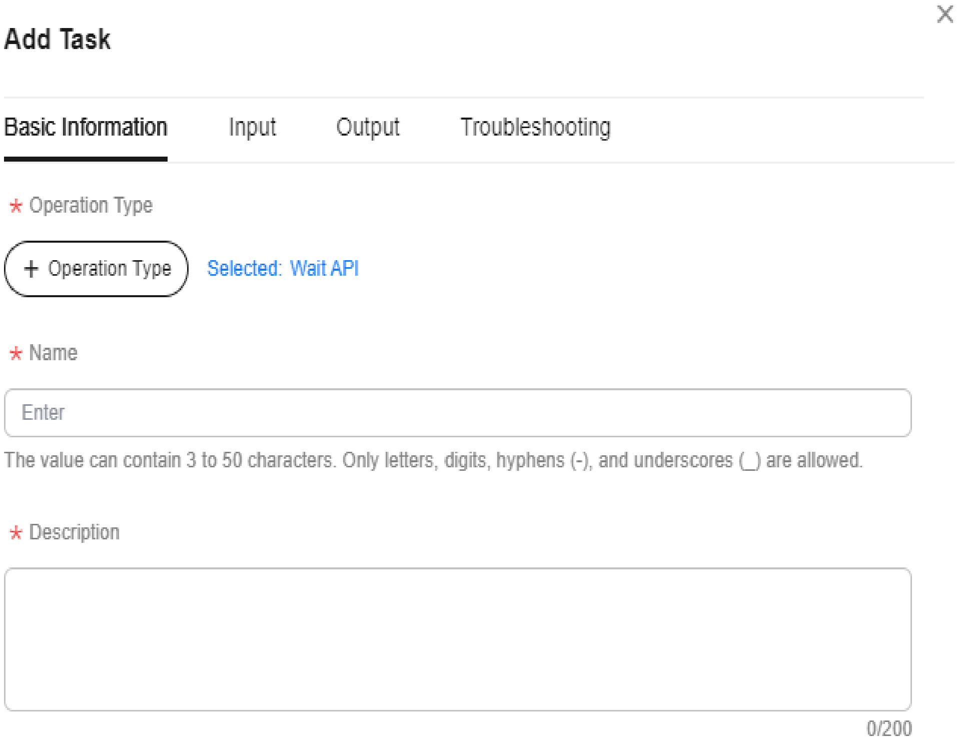
Step 6 Perform job orchestration. Click **+ Add Task**, and click **+ Operation Type**. On the displayed dialog box, click **Wait API**.

Figure 5-106 Adding tasks



Step 7 Enter the task name and operation description.

Figure 5-107 Setting the basic information



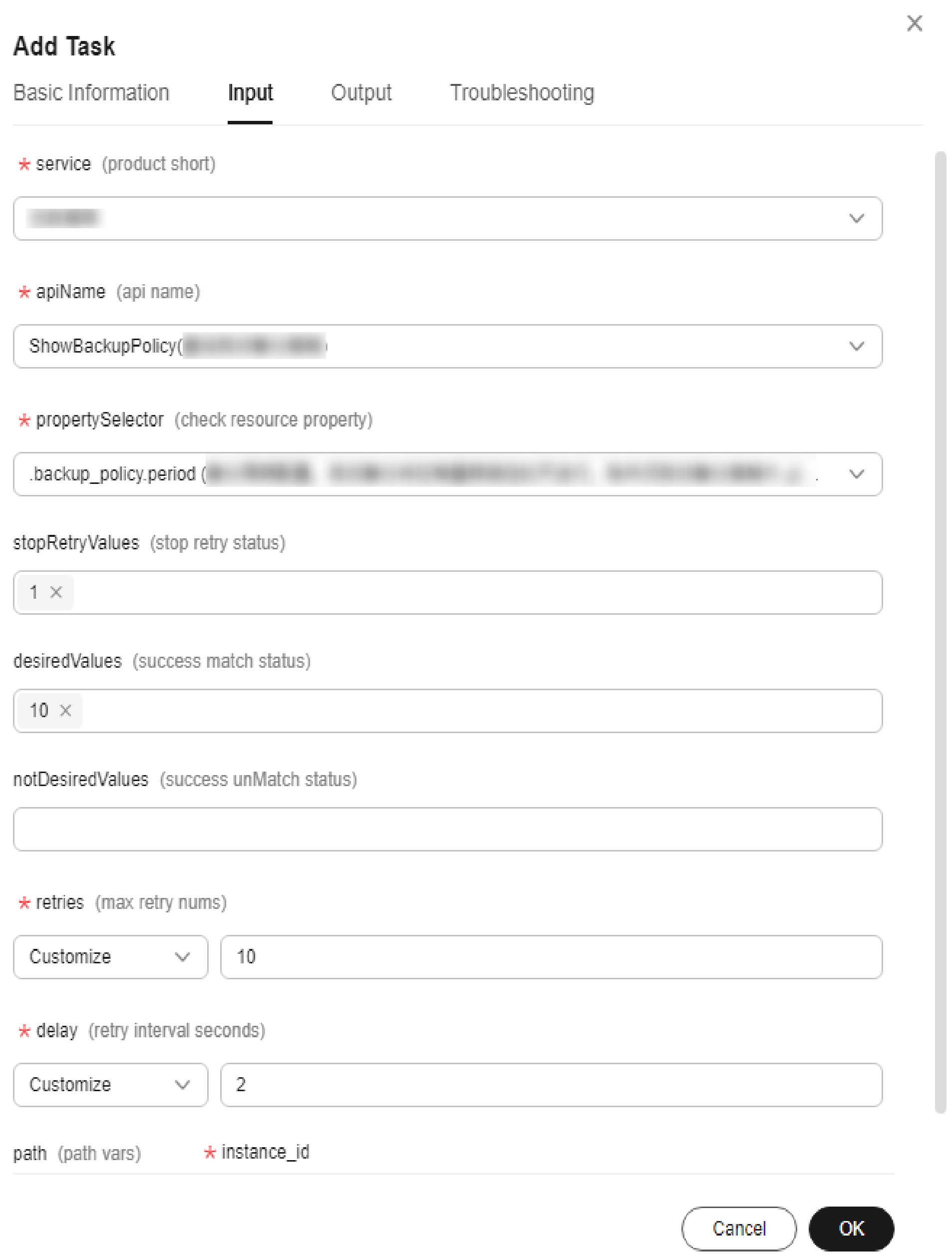
Step 8 Click **Input**, select **service** (product short name), **apiName** (API name),

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 5-108 Adding input information



Add Task

Basic Information | Input | Output | Troubleshooting

* service (product short)

[redacted]

* apiName (api name)

ShowBackupPolicy([redacted]

* propertySelector (check resource property)

.backup_policy.period ([redacted]

stopRetryValues (stop retry status)

1 ×

desiredValues (success match status)

10 ×

notDesiredValues (success unMatch status)

* retries (max retry nums)

Customize | 10

* delay (retry interval seconds)

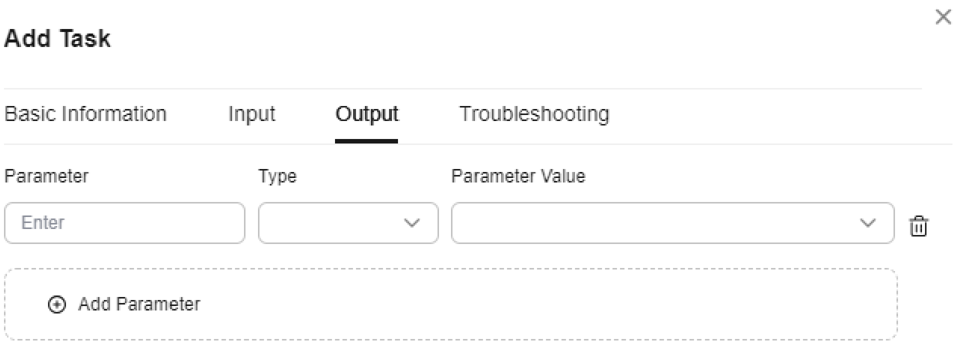
Customize | 2

path (path vars) * instance_id

Cancel | OK

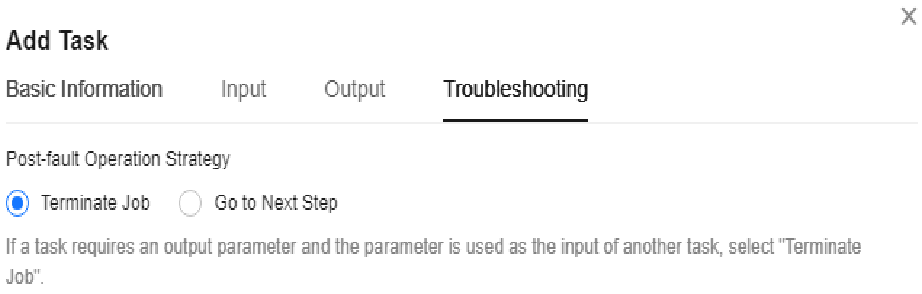
Step 9 Click **Output** and configure the output content as required. For example, you can add **backup_policy** in the API response as the parameter of the string type, and name it **outputValue**. If output parameters are not required, you do not need to add output parameters.

Figure 5-109 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 5-110 Adding troubleshooting policy



● Terminate Job ○ Go to Next Step

If a task requires an output parameter and the parameter is used as the input of another task, select "Terminate Job".

Step 11 Click **OK**.

----End

5.3.6.3 Execute Command

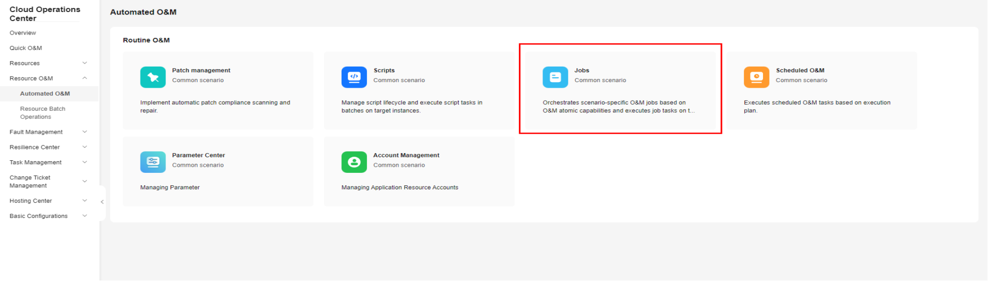
The atomic action can be used to execute a specific command.

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 5-111 Jobs



Patch management: Implement automatic patch compliance scanning and repair.

Scripts: Manage script lifecycle and execute script tasks in batches on target instances.

Jobs: Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on t...

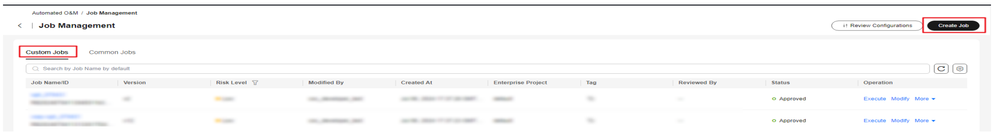
Scheduled O&M: Executes scheduled O&M tasks based on execution plan.

Parameter Center: Managing Parameter

Account Management: Managing Application Resource Accounts

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

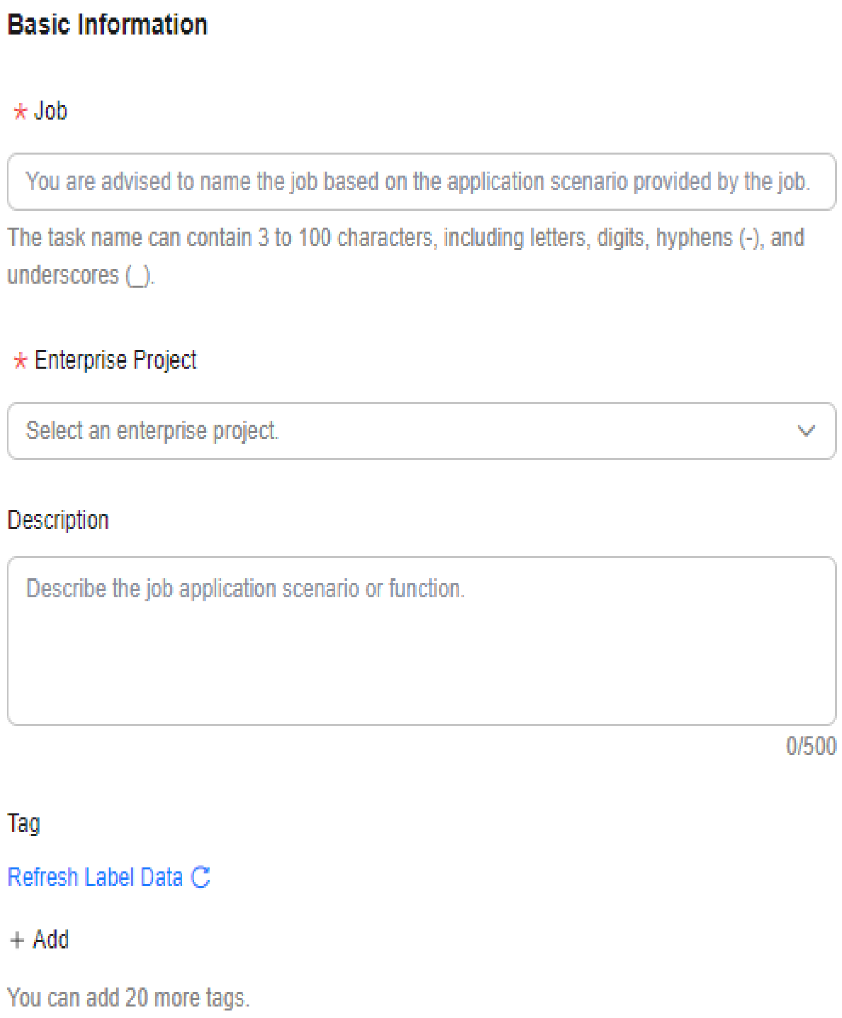
Figure 5-112 Clicking **Create Job**



Job Name/ID	Version	Risk Level	Modified By	Created At	Enterprise Project	Tag	Reviewed By	Status	Operation
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	--	Approved	Execute Modify More

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 5-113 Entering basic job information



Basic Information

* Job

You are advised to name the job based on the application scenario provided by the job.

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

* Enterprise Project

Select an enterprise project.

Description

Describe the job application scenario or function.

0/500

Tag

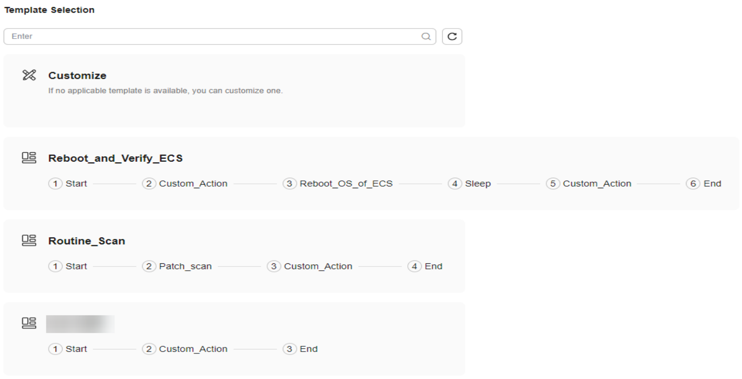
Refresh Label Data

+ Add

You can add 20 more tags.

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

Figure 5-114 Selecting a job template



Template Selection

Enter

Customize

If no applicable template is available, you can customize one.

Reboot_and_Verify_ECS

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

Routine_Scan

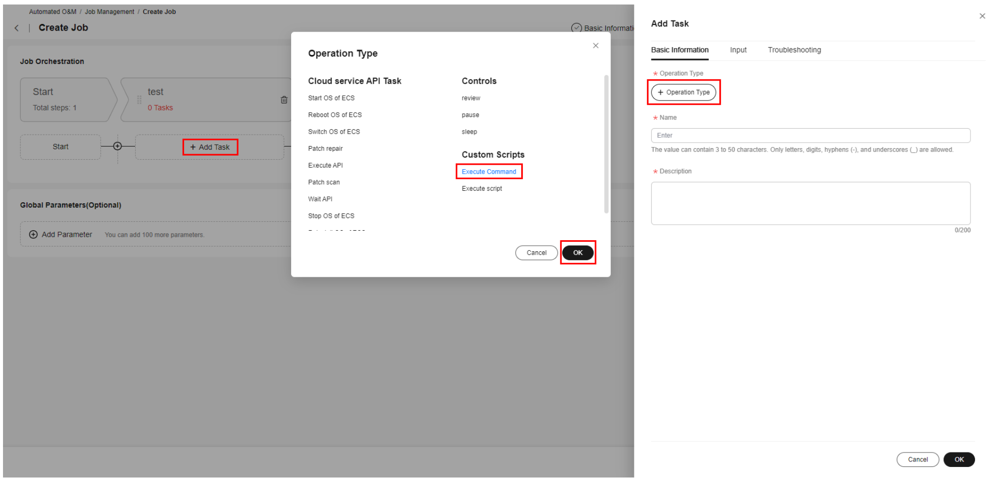
1 Start — 2 Patch_scan — 3 Custom_Action — 4 End

[redacted]

1 Start — 2 Custom_Action — 3 End

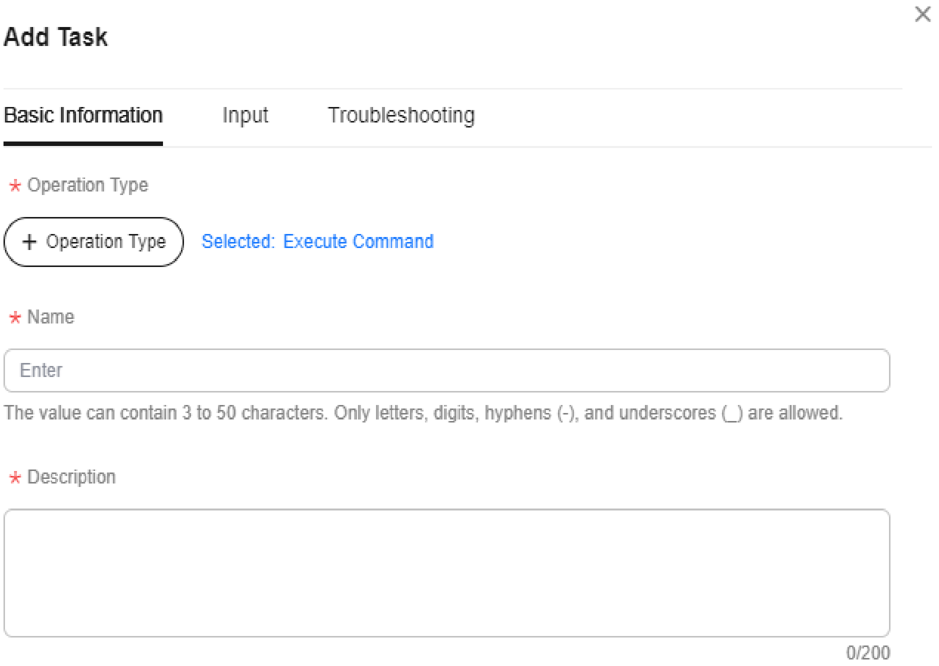
Step 6 Perform job orchestration. Click **+ Add Task**, and click **+ Operation Type**. On the displayed dialog box, click **Execute Command**.

Figure 5-115 Adding tasks



Step 7 Enter the task name and operation description.

Figure 5-116 Setting the basic information


Add Task

Basic Information | Input | Troubleshooting

* Operation Type

+ Operation Type Selected: Execute Command

* Name

Enter

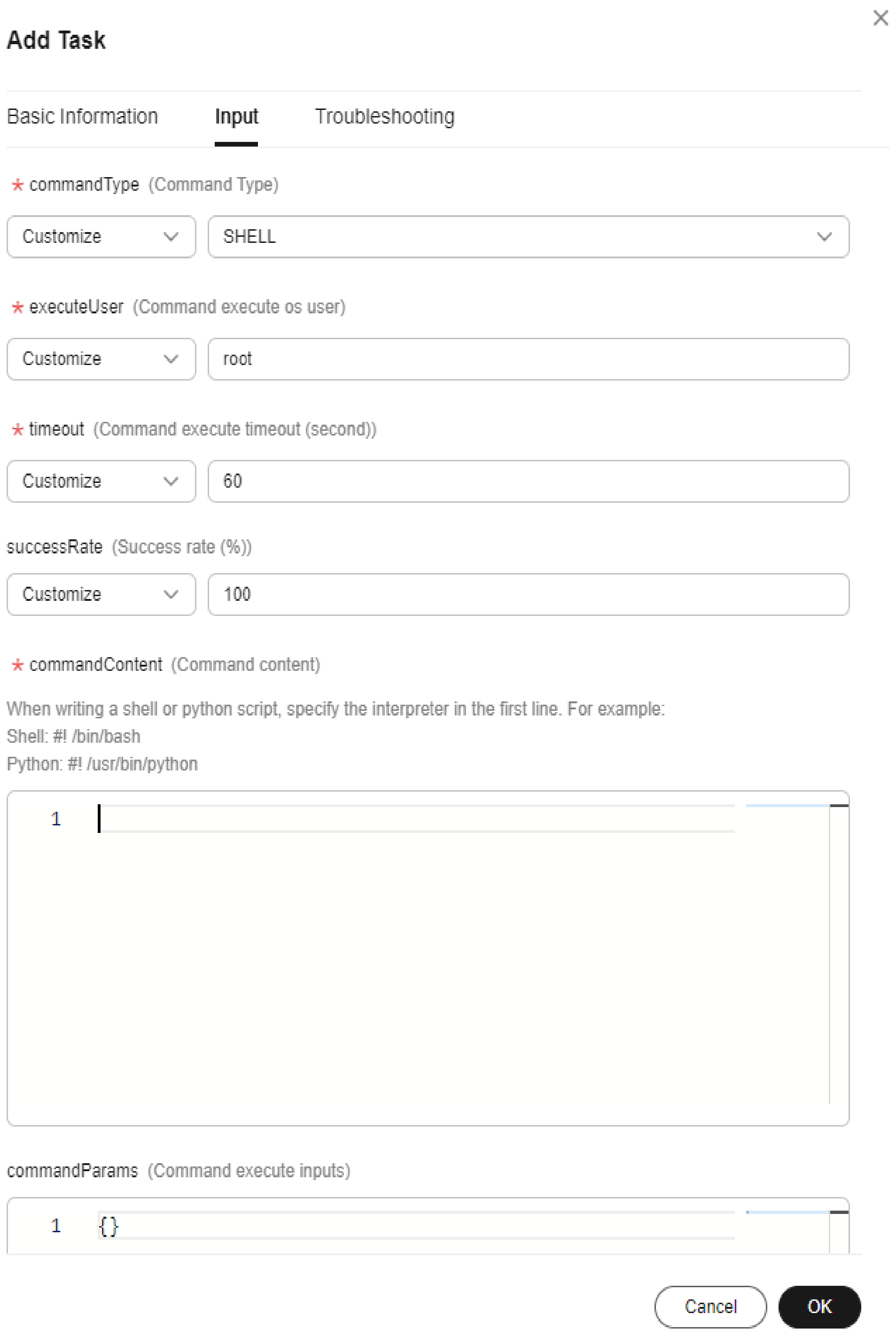
The value can contain 3 to 50 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.

* Description

0/200

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 5-117 Adding input information



Add Task

* commandType (Command Type)
Customize | SHELL

* executeUser (Command execute os user)
Customize | root

* timeout (Command execute timeout (second))
Customize | 60

successRate (Success rate (%))
Customize | 100

* commandContent (Command content)

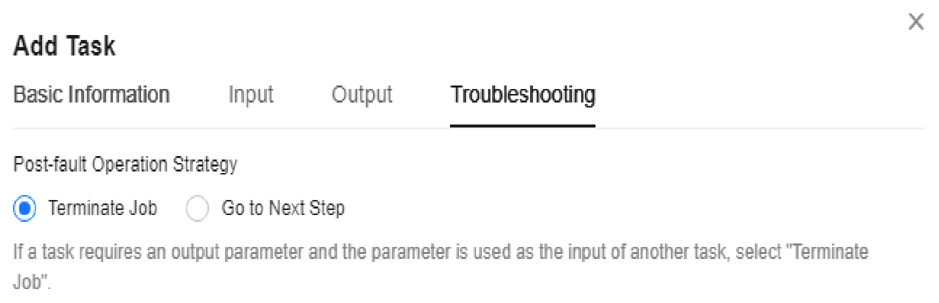
When writing a shell or python script, specify the interpreter in the first line. For example:
Shell: #! /bin/bash
Python: #! /usr/bin/python

commandParams (Command execute inputs)

```
{}
```

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

Figure 5-118 Adding troubleshooting policy



Add Task

Post-fault Operation Strategy

● Terminate Job ○ Go to Next Step

If a task requires an output parameter and the parameter is used as the input of another task, select "Terminate Job".

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.

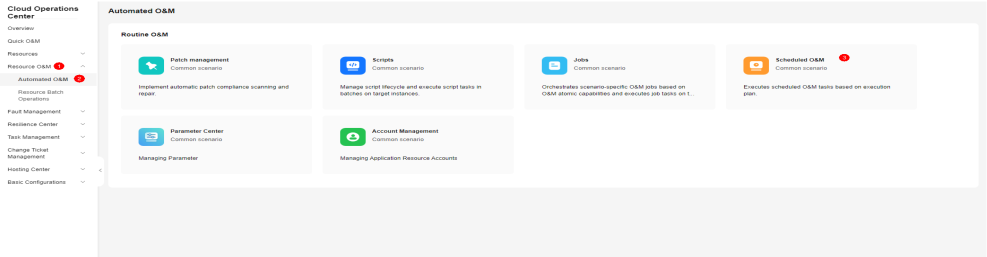
5.4.1 Scheduled Task Management

Creating a Scheduled Task

Step 1 Log in to COC.

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

Figure 5-119 Scheduled O&M



Patch management
Common scenario
Implement automatic patch compliance scanning and repair.

Scripts
Common scenario
Manage script lifecycle and execute script tasks in batches on target instances.

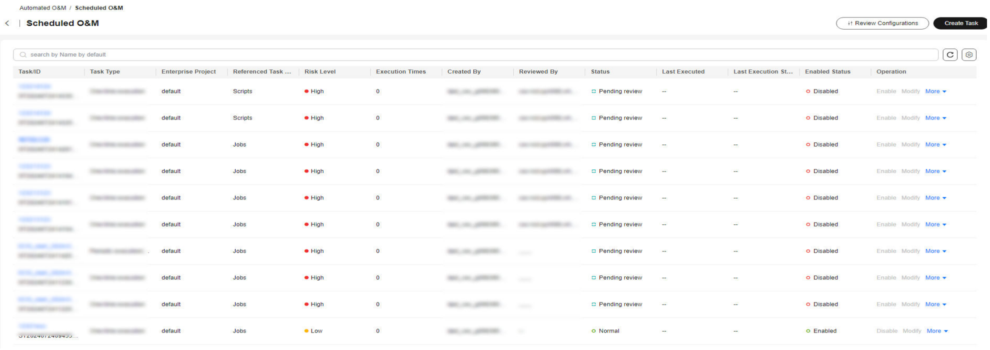
Jobs
Common scenario
Orchestrates scenario-specific O&M jobs based on O&M atomic capabilities and executes job tasks on t...

Scheduled O&M
Common scenario
Executes scheduled O&M tasks based on execution plan.

Parameter Center
Common scenario
Managing Parameter

Account Management
Common scenario
Managing Application Resource Accounts

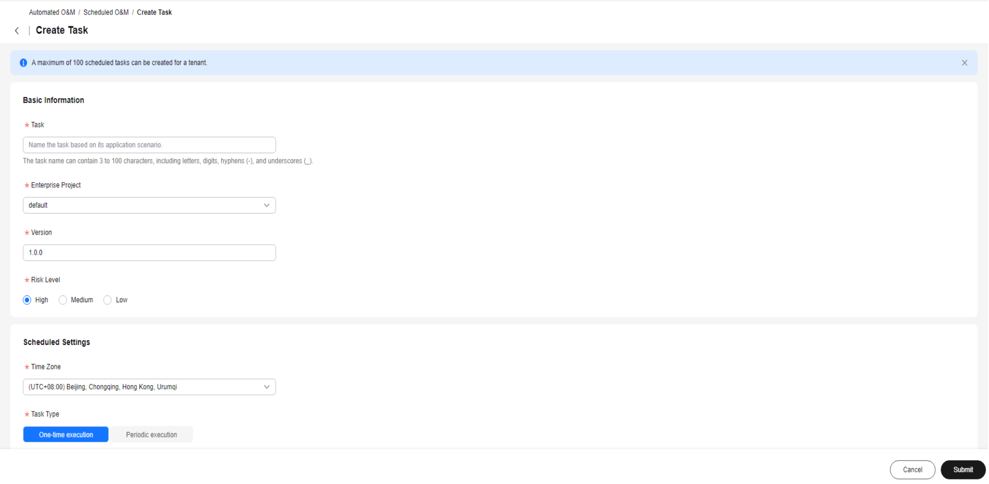
Figure 5-120 Scheduled task list



Task/ID	Task Type	Enterprise Project	Referenced Task ...	Risk Level	Execution Times	Created By	Reviewed By	Status	Last Executed	Last Execution St...	Enabled Status	Operation
[redacted]	[redacted]	default	Scripts	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Scripts	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	[redacted]	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	--	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	--	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● High	0	[redacted]	--	Pending review	--	--	○ Disabled	Enable Modify More ▾
[redacted]	[redacted]	default	Jobs	● Low	0	[redacted]	--	○ Normal	--	--	○ Enabled	Disable Modify More ▾

Step 3 On the **Scheduled O&M** page, click **Create Task** in the upper right corner.

Figure 5-121 Creating a scheduled task



Automated O&M / Scheduled O&M / Create Task

Create Task

A maximum of 100 scheduled tasks can be created for a tenant.

Basic Information

* Task

Name the task based on its application scenario.

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

* Enterprise Project

default

* Version

1.0.0

* Risk Level

● High ○ Medium ○ Low

Scheduled Settings

* Time Zone

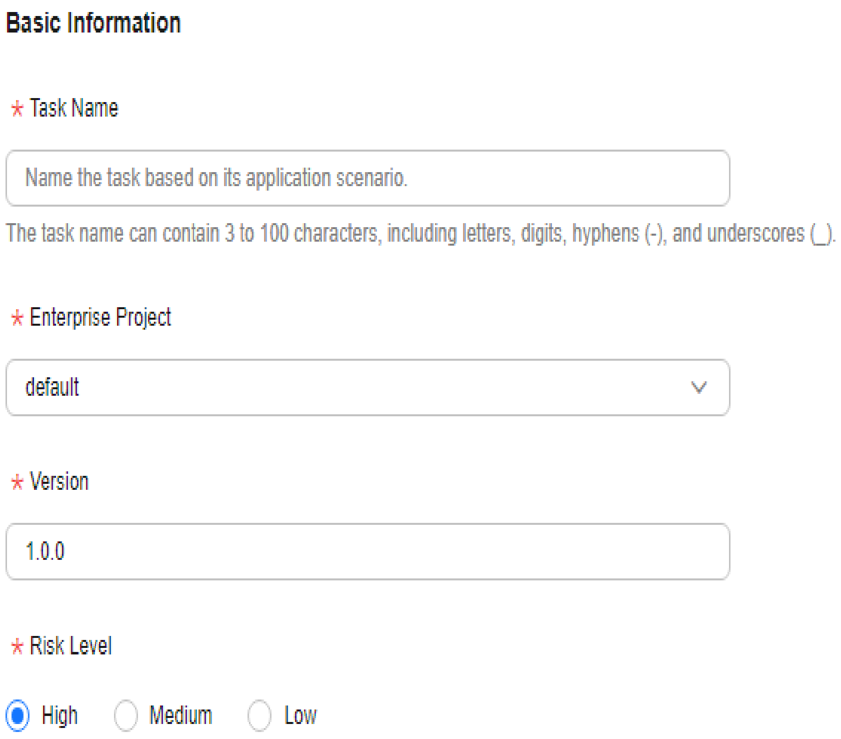
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

* Task Type

[✓ One-time execution] Periodic execution

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

Figure 5-122 Entering basic information



Basic Information

* Task Name

Name the task based on its application scenario.

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

* Enterprise Project

default

* Version

1.0.0

* Risk Level

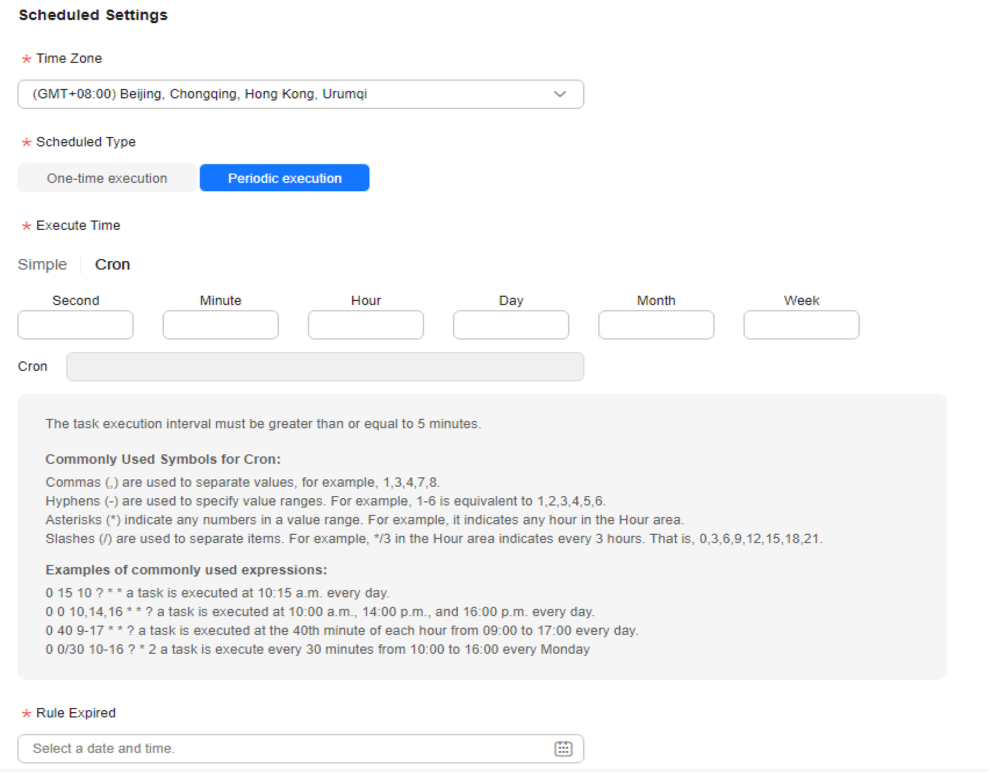
● High ○ Medium ○ Low

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.
IAM Agency	Mandatory. Delegated permission to execute the scheduled task. **NOTE** If the selected task is an ECS startup, ECS shutdown, ECS restart, OS patch scanning, or OS patch repair task in a public job, the system uses the ServiceAgencyForCOC agency by default.
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 5-123 Scheduled Settings



Scheduled Settings

* Time Zone

(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

* Scheduled Type

* Execute Time

The task execution interval must be greater than or equal to 5 minutes.

Commonly Used Symbols for Cron:

Commas (,) are used to separate values, for example, 1,3,4,7,8.
Hyphens (-) are used to specify value ranges. For example, 1-6 is equivalent to 1,2,3,4,5,6.
Asterisks (*) indicate any numbers in a value range. For example, it indicates any hour in the Hour area.
Slashes (/) are used to separate items. For example, */3 in the Hour area indicates every 3 hours. That is, 0,3,6,9,12,15,18,21.

Examples of commonly used expressions:

0 15 10 ? * * a task is executed at 10:15 a.m. every day.
0 0 10,14,16 * * ? a task is executed at 10:00 a.m., 14:00 p.m., and 16:00 p.m. every day.
0 40 9-17 * * ? a task is executed at the 40th minute of each hour from 09:00 to 17:00 every day.
0 0/30 10-16 ? * 2 a task is execute every 30 minutes from 10:00 to 16:00 every Monday

* Rule Expired

Select a date and time.

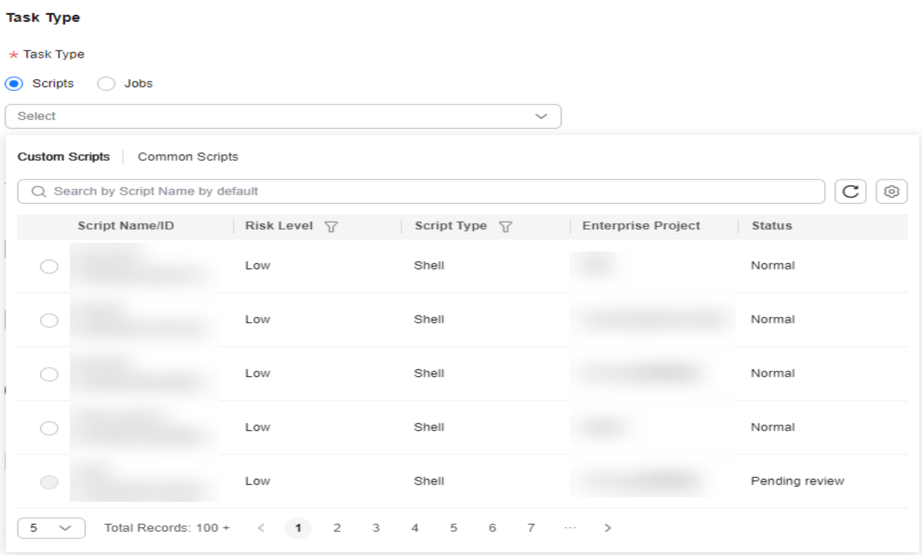
Table 5-11 Parameters

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.

Parameter	Sub-parameter Name	Description
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. Click ○ before **Scripts**.

Figure 5-124 Task Type



Task Type

* Task Type

● Scripts ○ Jobs

Select

Custom Scripts | Common Scripts

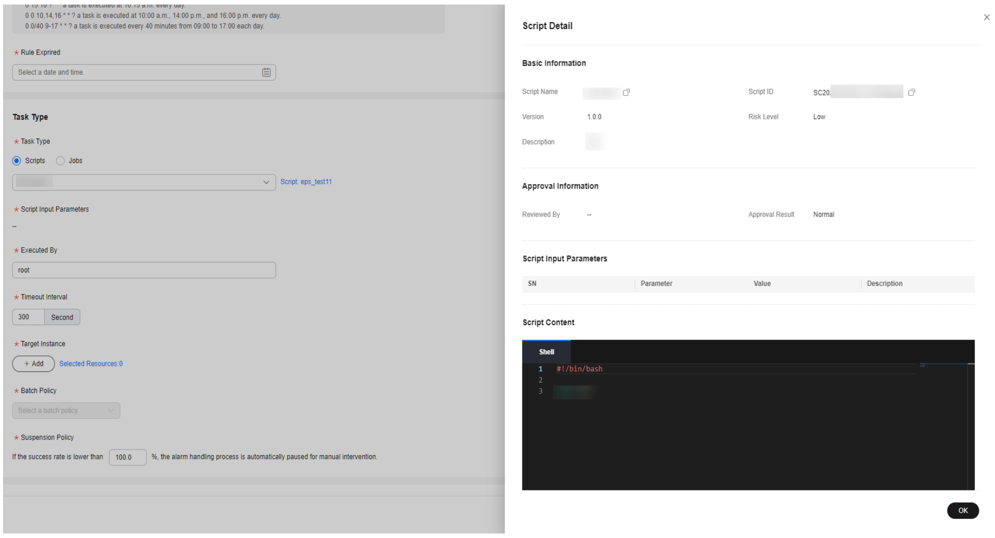
Search by Script Name by default

	Script Name/ID	Risk Level	Script Type	Enterprise Project	Status
○	[redacted]	Low	Shell	[redacted]	Normal
○	[redacted]	Low	Shell	[redacted]	Normal
○	[redacted]	Low	Shell	[redacted]	Normal
○	[redacted]	Low	Shell	[redacted]	Normal
○	[redacted]	Low	Shell	[redacted]	Pending review

5 Total Records: 100 + < 1 2 3 4 5 6 7 ··· >

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

Figure 5-125 Script Details



0 15 10 ? a task is executed at 10:15 a.m. every day.
0 0 10,14,16 * * ? a task is executed at 10:00 a.m., 14:00 p.m., and 16:00 p.m. every day.
0 0/40 9-17 * * ? a task is executed every 40 minutes from 09:00 to 17:00 each day.

* Rule Exprired: Select a date and time.

Task Type

* Task Type: ● Scripts ○ Jobs

[redacted] Script: eps_test11

* Script Input Parameters: --

* Executed By: root

* Timeout Interval: 300 Second

* Target Instance: + Add Selected Resources:0

* Batch Policy: Select a batch policy.

* Suspension Policy: If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Script Detail

Basic Information

Script Name	[redacted]	Script ID	SC20[redacted]
Version	1.0.0	Risk Level	Low
Description	[redacted]		

Approval Information

Reviewed By	--	Approval Result	Normal

Script Input Parameters

SN	Parameter	Value	Description

Script Content

Shell

```
#!/bin/bash

[redacted]
```

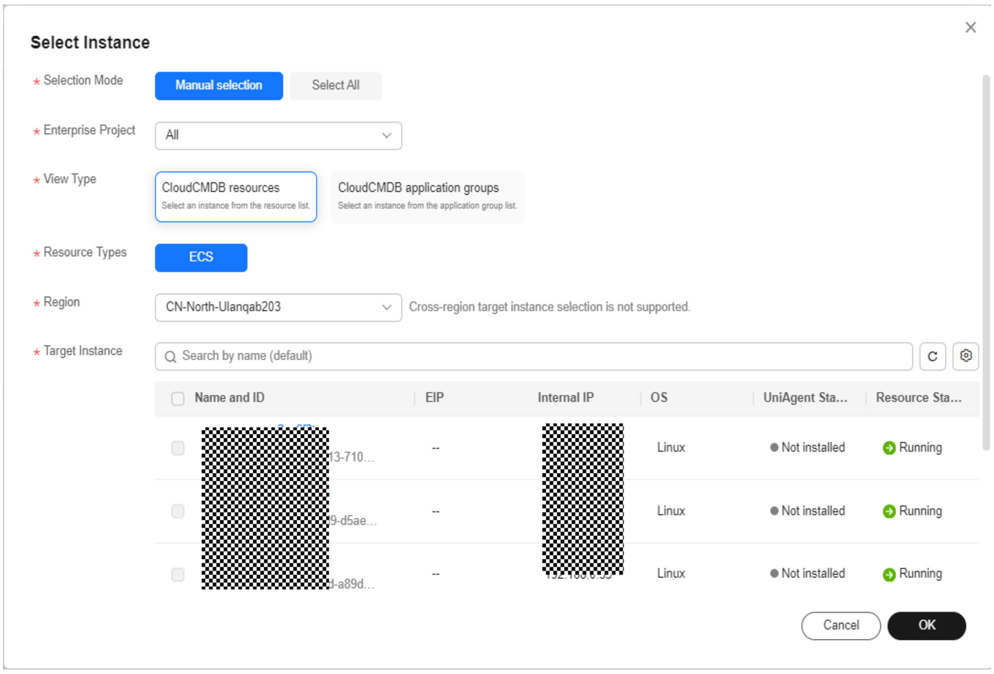
c. Default script parameters are displayed in **Script Input Parameters**. You can select **Sensitive** to determine whether to display the parameters in plaintext. You can click the text box to edit the parameter values.

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**. The **Select Instance** page is displayed. Click **Manual selection**, set **Enterprise Project**, **View Type**, **Resource Type**, and **Region**, and search for the target instances in the search box. Select the check box before the instance list and click **OK**. Only instances whose UniAgent status is **Running** can be selected.

Figure 5-126 Manually selecting instances (CloudCMDB ResourceS)



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

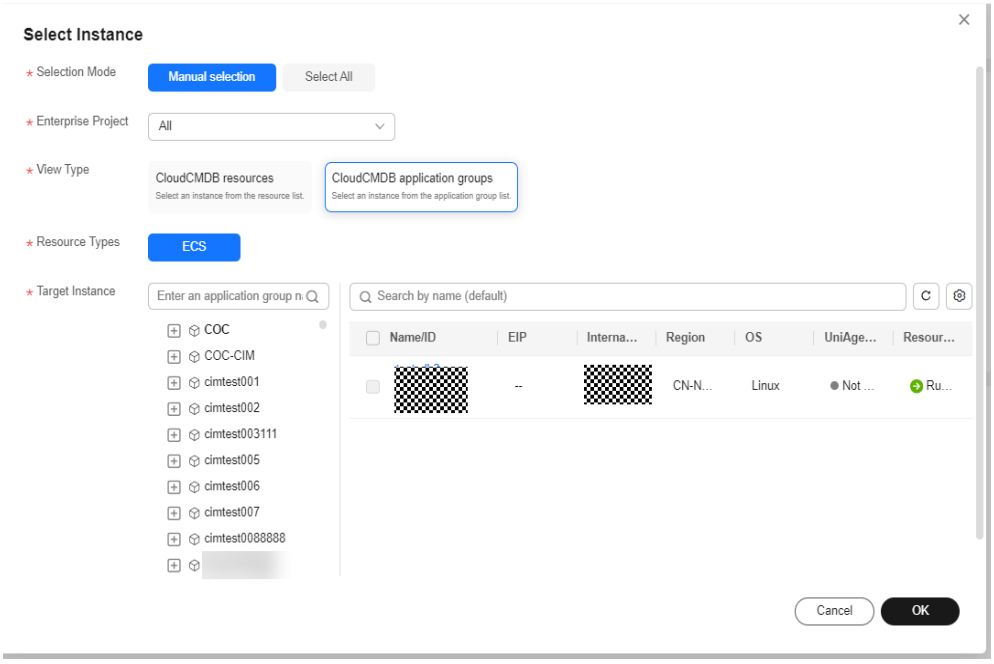
* Resource Types: ECS

* Region: CN-North-Ulanqab203 Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

□	Name and ID	EIP	Internal IP	OS	UniAgent Sta...	Resource Sta...
□	[redacted]13-710...	--	[redacted]	Linux	● Not installed	Running
□	[redacted]9-d5ae...	--	[redacted]	Linux	● Not installed	Running
□	[redacted]-a89d...	--	[redacted]	Linux	● Not installed	Running

Figure 5-127 Manually selecting instances (CloudCMDB application groups)



Select Instance

* Selection Mode: Manual selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Types: ECS

* Target Instance: Enter an application group n | Search by name (default)

- COC
- COC-CIM
- cimtest001
- cimtest002
- cimtest003111
- cimtest005
- cimtest006
- cimtest007
- cimtest0088888

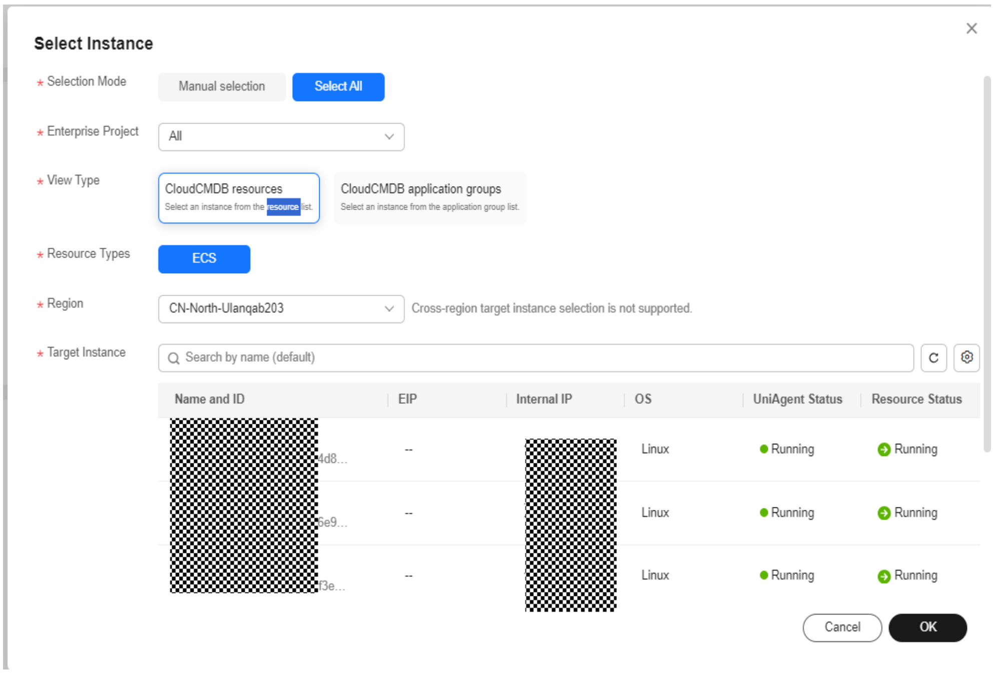
□	Name/ID	EIP	Interna...	Region	OS	UniAge...	Resour...
□	[redacted]	--	[redacted]	CN-N...	Linux	● Not ...	Ru...

Select All: Click **Select All**, set **Enterprise Project**, **View Type**, **Resource Type**, **Region**, and search for target instances on the search box. 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 to execute the task. By default, only instances whose **UniAgent Status** is **Running** are displayed in the list.

NOTE

If you select a task of ECS startup, ECS shutdown, or ECS restart, and select **Select All** for **Selection Method**, a maximum of 500 instances can be selected at a time. If more than 500 instances need to be selected, manually select them.

Figure 5-128 Selecting All (CloudCMDB resources)

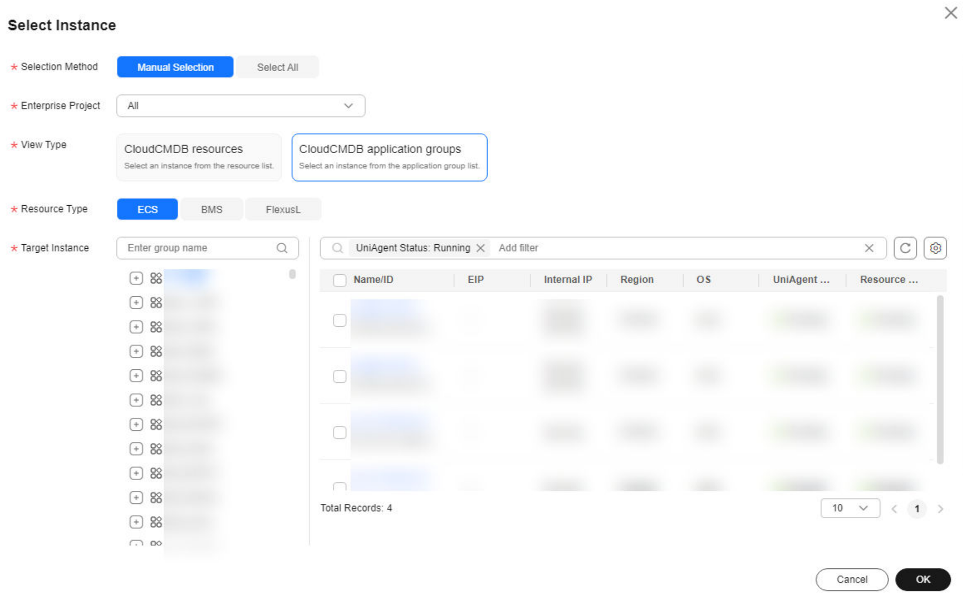


Select Instance

- * Selection Mode: Manual selection | **Select All**
- * Enterprise Project: All
- * View Type: **CloudCMDB resources** (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)
- * Resource Types: ECS
- * Region: CN-North-Ulanqab203 — Cross-region target instance selection is not supported.
- * Target Instance: Search by name (default)

Name and ID	EIP	Internal IP	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	Linux	● Running	Running
[redacted]	--	[redacted]	Linux	● Running	Running
[redacted]	--	[redacted]	Linux	● Running	Running

Figure 5-129 Selecting All (CloudCMDB application groups)



Select Instance

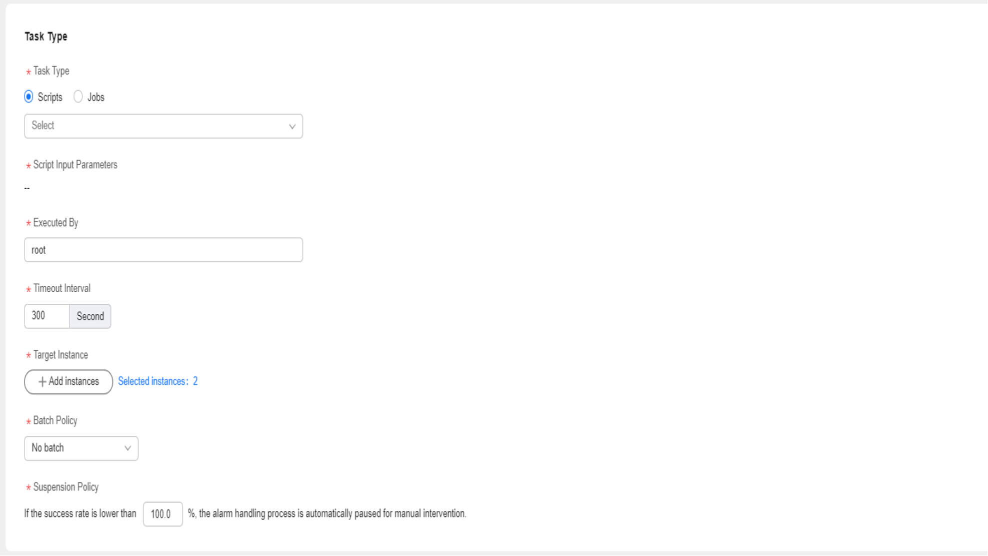
- * Selection Method: **Manual Selection** | Select All
- * Enterprise Project: All
- * View Type: CloudCMDB resources (Select an instance from the resource list.) | **CloudCMDB application groups** (Select an instance from the application group list.)
- * Resource Type: **ECS** | BMS | FlexusL
- * Target Instance: Enter group name; UniAgent Status: Running; Add filter

Name/ID	EIP	Internal IP	Region	OS	UniAgent ...	Resource ...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Total Records: 4

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

Figure 5-130 Page displayed when **Manual selection** is selected



Task Type

* Task Type

● Scripts ○ Jobs

Select

* Script Input Parameters

--

* Executed By

root

* Timeout Interval

300 Second

* Target Instance

+ Add instances Selected instances: 2

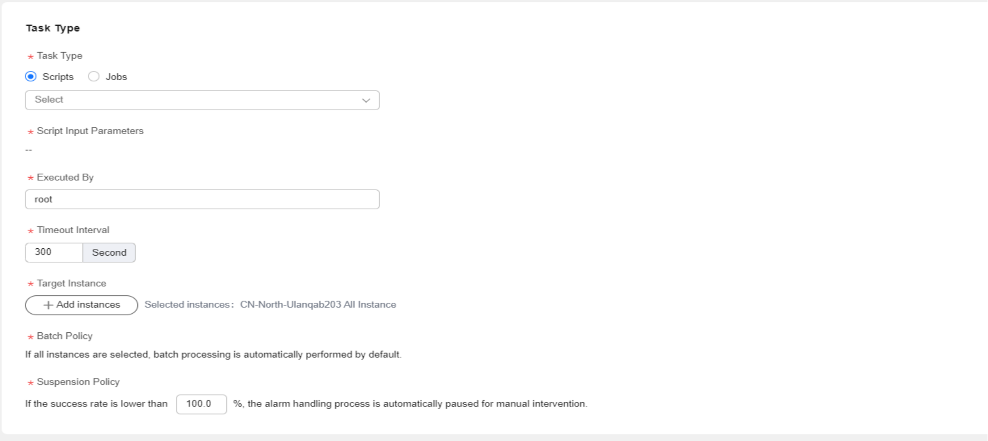
* Batch Policy

No batch

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Figure 5-131 Page displayed when **Select All** is selected



Task Type

* Task Type

● Scripts ○ Jobs

Select

* Script Input Parameters

--

* Executed By

root

* Timeout Interval

300 Second

* Target Instance

+ Add instances Selected instances: CN-North-Ulanqab203 All Instance

* Batch Policy

If all instances are selected, batch processing is automatically performed by default.

* Suspension Policy

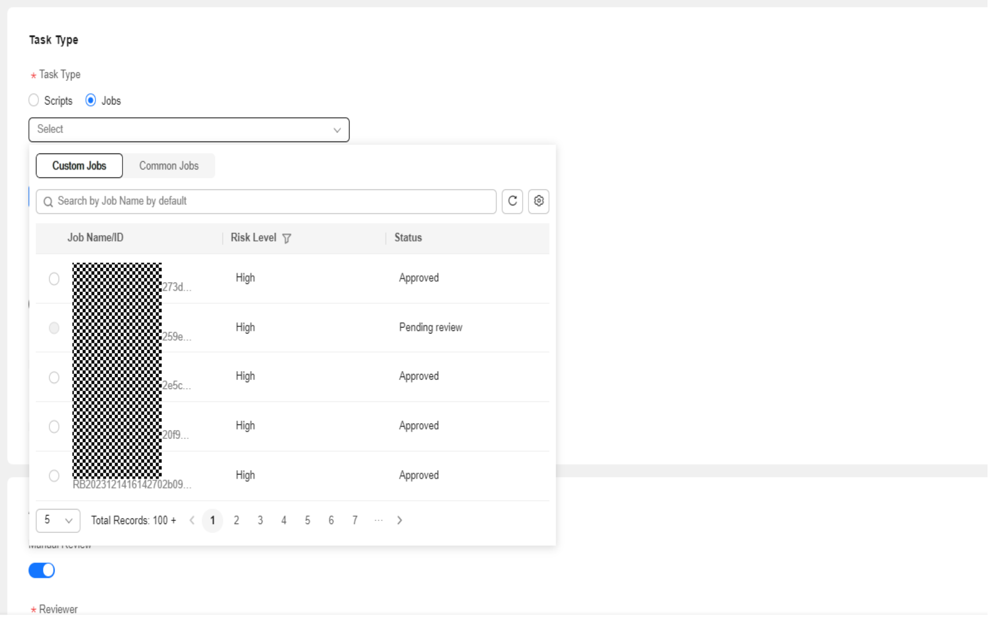
If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Step 7 a. Select the task type. If you select **Jobs**, click the text box, select **Custom Jobs** or **Common Jobs**, and enter the key word in the search box to search for target jobs. Select the desired job.

NOTE

Currently, jobs that reference global parameters and jobs without target instances are not supported.

Figure 5-132 Selecting **Jobs**



Task Type

* Task Type

○ Scripts ● Jobs

Select

Custom Jobs | Common Jobs

Search by Job Name by default

	Job Name/ID	Risk Level	Status
○	[redacted]	High	Approved
○	[redacted]	High	Pending review
○	[redacted]	High	Approved
○	[redacted]	High	Approved
○	[redacted]	High	Approved

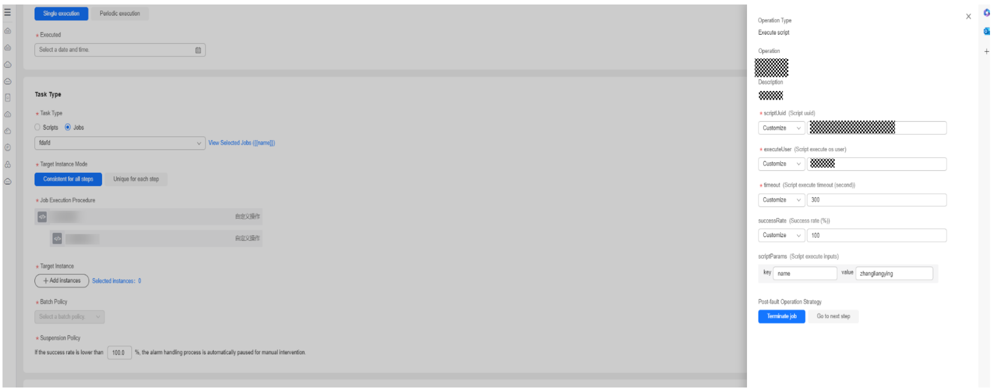
5 Total Records: 100 + < 1 2 3 4 5 6 7 ··· >

Manual Review

* Reviewer

b. Click **View Selected Jobs**. The job details are displayed on the right.

Figure 5-133 Viewing job details



Single execution | Periodic execution

* Executed

Select a date and time.

Task Type

* Task Type

○ Scripts ● Jobs

fdafd View Selected Jobs ({{name}})

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

[redacted] 自定义操作

[redacted] 自定义操作

* Target Instance

+ Add instances Selected instances: 0

* Batch Policy

Select a batch policy.

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Operation Type

Execute script

Operation

[redacted]

Description

[redacted]

* scriptUuid (Script uuid)

Customize [redacted]

* executeUser (Script execute os user)

Customize [redacted]

* timeout (Script execute timeout (second))

Customize 300

successRate (Success rate (%))

Customize 100

scriptParams (Script execute inputs)

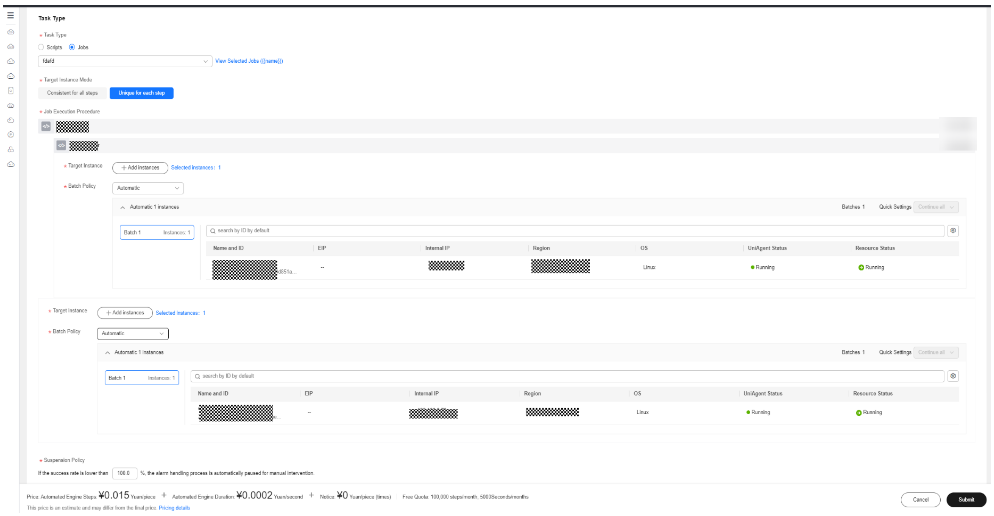
key name value zhangliangying

Post-fault Operation Strategy

Terminate job | Go to next step

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 5-134 Selecting **Unique for each step**



Task Type

* Task Type

○ Scripts ● Jobs

fdafd — View Selected Jobs ({{name}})

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

* Target Instance — Add instances — Selected instances: 1

* Batch Policy — Automatic

Automatic 1 instances — Batches 1 — Quick Settings

Batch 1 Instances: 1 — search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	[redacted]	Linux	Running	Running

* Target Instance — Add instances — Selected instances: 1

* Batch Policy — Automatic

Automatic 1 instances — Batches 1 — Quick Settings

Batch 1 Instances: 1 — search by ID by default

Name and ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	[redacted]	Linux	Running	Running

* Suspension Policy

If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

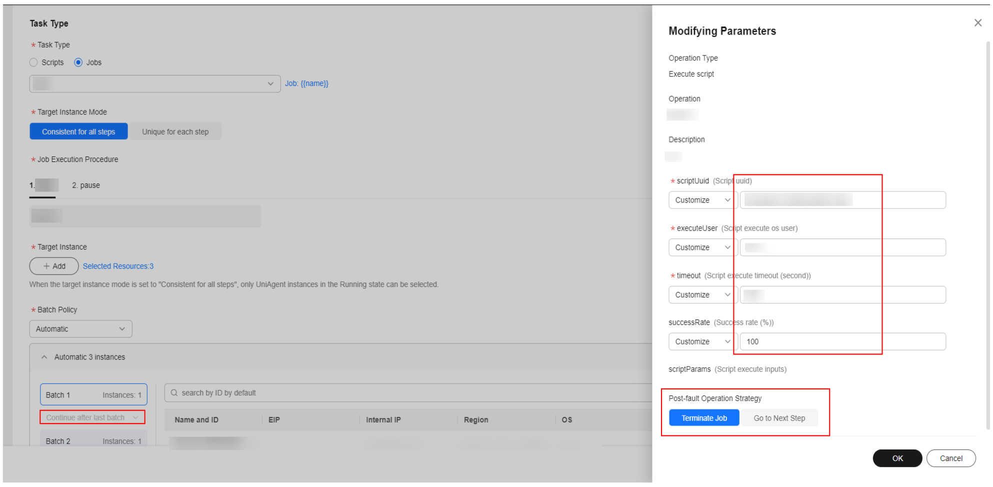
Price: Automated Engine Steps: ¥0.015 Yuan/piece + Automated Engine Duration: ¥0.0002 Yuan/second + Notice: ¥0 Yuan/piece (times) | Free Quota: 100,000 steps/month, 5000Seconds/months

This price is an estimate and may differ from the final price. Pricing details

Cancel | Submit

d. Modify job execution parameters. Click a job step name. The job step details are displayed on the right. Set **successRate** and **InstallStrategy**, select **Post-fault Operation Strategy**, and click **OK**.

Figure 5-135 Modifying job execution parameters



Modifying Parameters

Operation Type

Execute script

Operation

Description

* scriptUuid (Script uuid) — Customize

* executeUser (Script execute os user) — Customize

* timeout (Script execute timeout (second)) — Customize

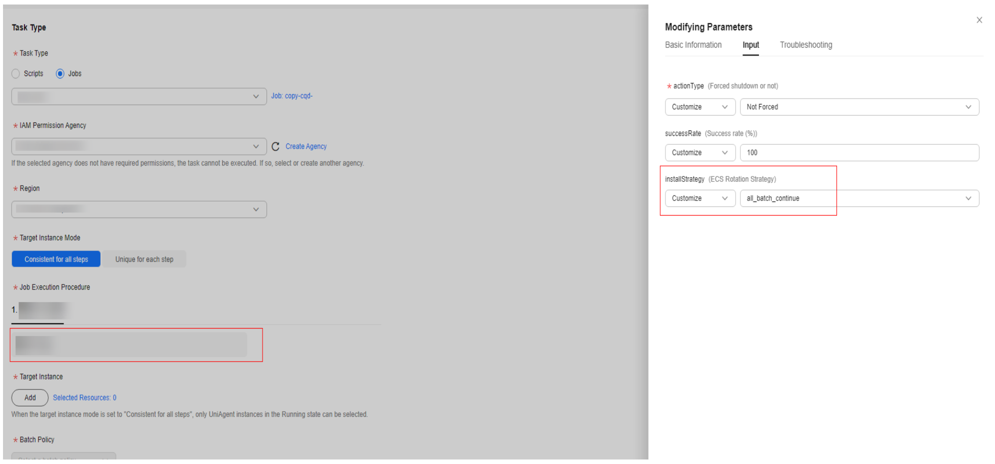
successRate (Success rate (%)) — Customize — 100

scriptParams (Script execute inputs)

Post-fault Operation Strategy: Terminate Job | Go to Next Step

OK | Cancel

Figure 5-136 Configuring a suspension and resumption policy



Task Type

* Task Type

○ Scripts ● Jobs

Job: copy-cqd-

* IAM Permission Agency

Create Agency

If the selected agency does not have required permissions, the task cannot be executed. If so, select or create another agency.

* Region

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

1.

* Target Instance

Add Selected Resources: 0

When the target instance mode is set to "Consistent for all steps", only UniAgent instances in the Running state can be selected.

* Batch Policy

Modifying Parameters

Basic Information | Input | Troubleshooting

* actionType (Forced shutdown or not)

Customize | Not Forced

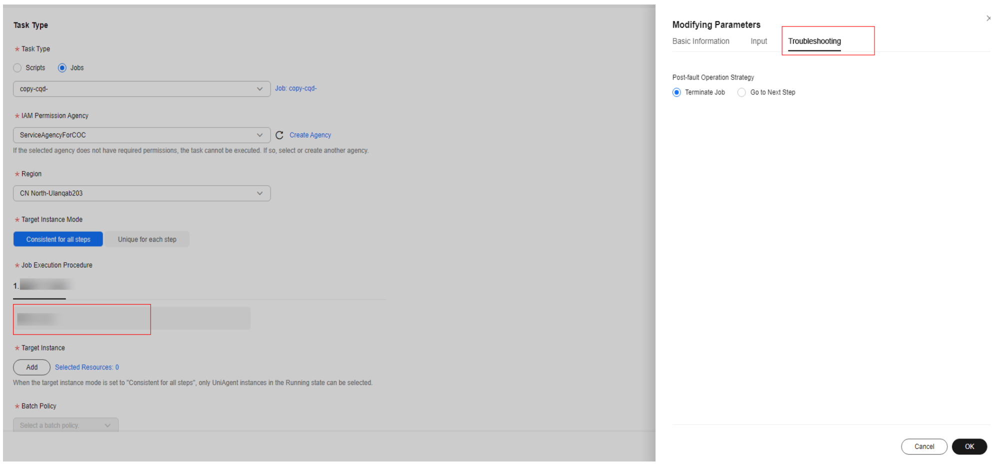
successRate (Success rate (%))

Customize | 100

installStrategy (ECS Rotation Strategy)

Customize | all_batch_continue

Figure 5-137 Troubleshooting policy



Task Type

* Task Type

○ Scripts ● Jobs

copy-cqd- Job: copy-cqd-

* IAM Permission Agency

ServiceAgencyForCOC Create Agency

If the selected agency does not have required permissions, the task cannot be executed. If so, select or create another agency.

* Region

CN North-Ulanqab203

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

1.

* Target Instance

Add Selected Resources: 0

When the target instance mode is set to "Consistent for all steps", only UniAgent instances in the Running state can be selected.

* Batch Policy

Select a batch policy.

Modifying Parameters

Basic Information | Input | Troubleshooting

Post-fault Operation Strategy

● Terminate Job ○ Go to Next Step

Cancel | OK

e. Select instances. You can select instances in either of the following ways:

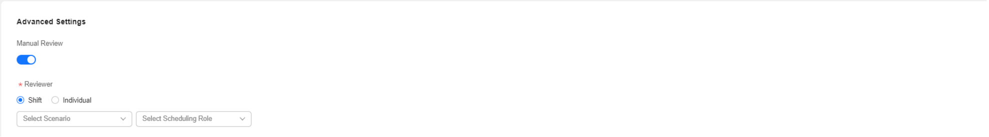
Manual selection: You need to manually select instances.

Select All: Select all instances associated with a single region or application.

f. Set **Batch Policy** and **Suspension Policy**.

Step 8 You can determine whether to enable **Manual Review** based on the service requirements.

Figure 5-138 Setting manual review



Advanced Settings

Manual Review

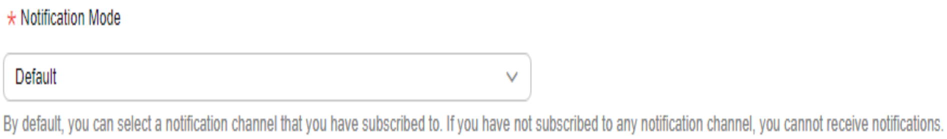
* Reviewer

● Shift ○ Individual

Select Scenario | Select Scheduling Role

Step 9 Determine whether to enable **Send Notification** based on service requirements. If enabled, set **Notification Policy**, **Recipient**, and **Notification Mode**.

Figure 5-139 Setting notifications



* Notification Mode

Default

By default, you can select a notification channel that you have subscribed to. If you have not subscribed to any notification channel, you cannot receive 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.

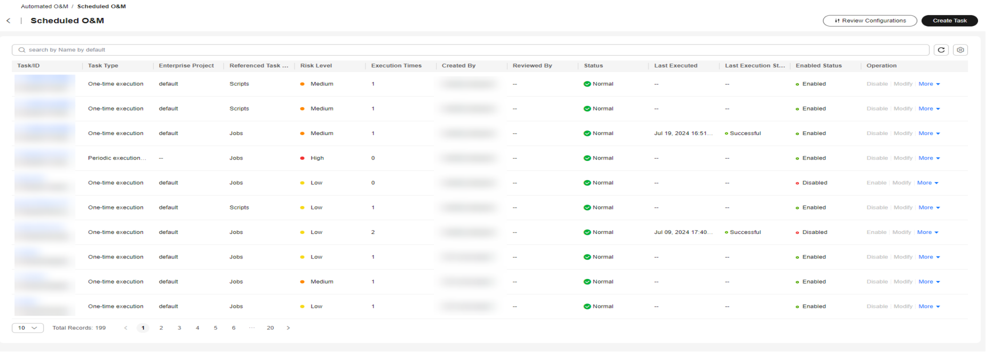
----End

Viewing a Scheduled Task

Step 1 Log in to COC.

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

Figure 5-140 Scheduled tasks



Automated O&M / Scheduled O&M

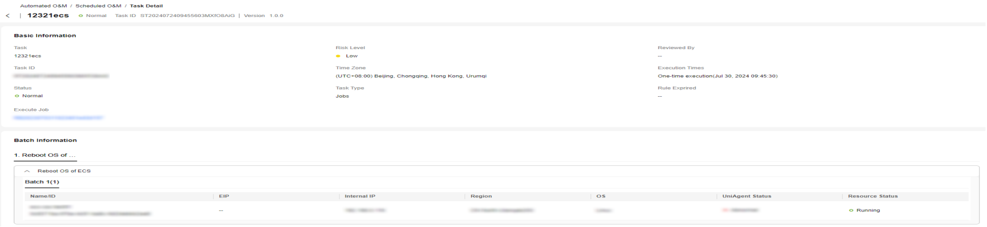
Scheduled O&M

Task/ID	Task Type	Enterprise Project	Referenced Task ...	Risk Level	Execution Times	Created By	Reviewed By	Status	Last Executed	Last Execution St...	Enabled Status	Operation
[redacted]	One-time execution	default	Scripts	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Scripts	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Jobs	Medium	1	[redacted]	--	Normal	Jul 19, 2024 16:51...	Successful	Enabled	Disable | Modify | More
[redacted]	Periodic execution...	--	Jobs	High	0	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Jobs	Low	0	[redacted]	--	Normal	--	--	Disabled	Enable | Modify | More
[redacted]	One-time execution	default	Scripts	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Jobs	Low	2	[redacted]	--	Normal	Jul 09, 2024 17:40...	Successful	Disabled	Enable | Modify | More
[redacted]	One-time execution	default	Jobs	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Jobs	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More
[redacted]	One-time execution	default	Jobs	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable | Modify | More

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

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

Figure 5-141 Viewing task details



Automated O&M / Scheduled O&M / Task Detail

12321ecs Normal Task ID ST2024072409455603MXfO8AiG | Version 1.0.0

Basic Information

Task: 12321ecs

Task ID: [redacted]

Status: Normal

Execute Job: [redacted]

Risk Level: Low

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Task Type: Jobs

Reviewed By: --

Execution Times: One-time execution(Jul 30, 2024 09:45:30)

Rule Exprired: --

Batch Information

1. Reboot OS of ...

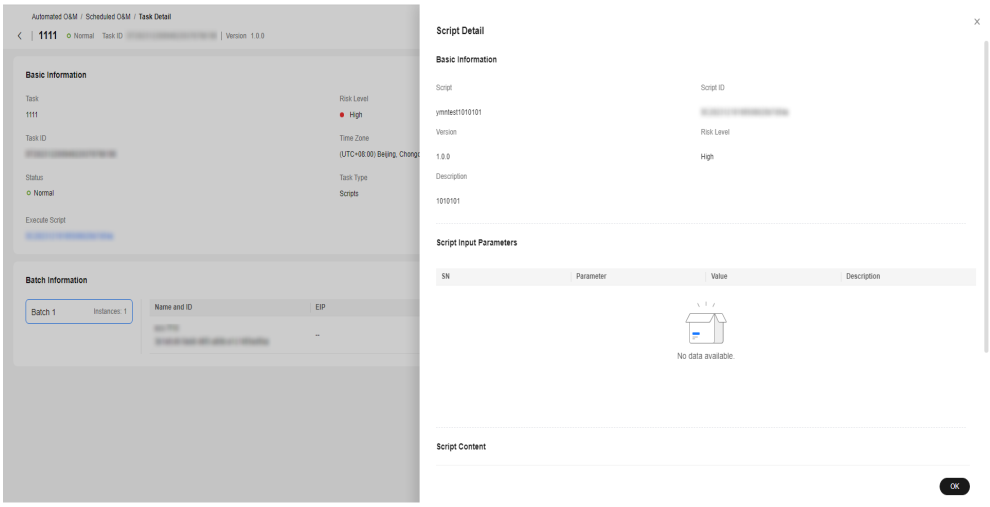
Reboot OS of ECS

Batch 1(1)

Name/ID	EIP	Internal IP	Region	OS	UniAgent Status	Resource Status
[redacted]	--	[redacted]	[redacted]	[redacted]	[redacted]	Running

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 5-142 Script or job details



1111 Normal Task ID [redacted] | Version 1.0.0

Basic Information

Task: 1111

Risk Level: High

Task ID: [redacted]

Time Zone: (UTC+08:00) Beijing, Chongc

Status: Normal

Task Type: Scripts

Execute Script: [redacted]

Batch Information

Batch 1 Instances: 1

Name and ID	EIP
[redacted]	--

Script Detail

Basic Information

Script: ymntest1010101

Script ID: [redacted]

Version: 1.0.0

Risk Level: High

Description: 1010101

Script Input Parameters

SN	Parameter	Value	Description

Script Content

NOTE

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

----End

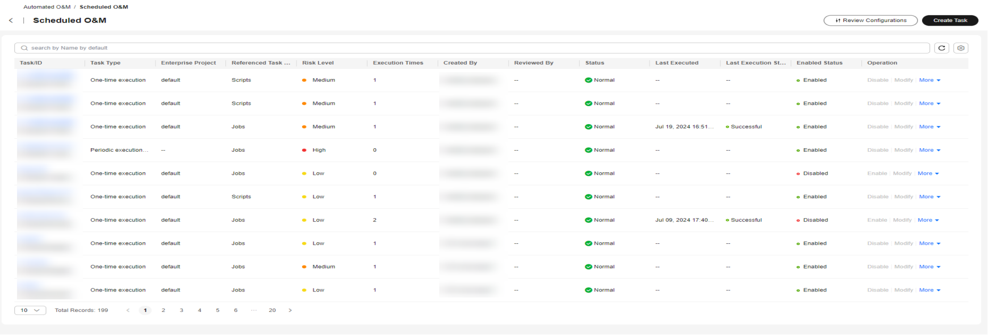
Enabling and Disabling a Scheduled Task

Step 1 Log in to COC.

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

Step 3 Locate a target task, and click **Enable** or **Disable** in the **Operation** column to enable or disable the scheduled task.

Figure 5-143 Viewing task list



Task/ID	Task Type	Enterprise Project	Referenced Task ...	Risk Level	Execution Times	Created By	Reviewed By	Status	Last Executed	Last Execution St...	Enabled Status	Operation
[redacted]	One-time execution	default	Scripts	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Scripts	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Jobs	Medium	1	[redacted]	--	Normal	Jul 19, 2024 16:51...	Successful	Enabled	Disable Modify More
[redacted]	Periodic execution...	--	Jobs	High	0	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Jobs	Low	0	[redacted]	--	Normal	--	--	Disabled	Enable Modify More
[redacted]	One-time execution	default	Scripts	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Jobs	Low	2	[redacted]	--	Normal	Jul 09, 2024 17:40...	Successful	Disabled	Enable Modify More
[redacted]	One-time execution	default	Jobs	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Jobs	Medium	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More
[redacted]	One-time execution	default	Jobs	Low	1	[redacted]	--	Normal	--	--	Enabled	Disable Modify More

10 Total Records: 199 < 1 2 3 4 5 6 ··· 20 >

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

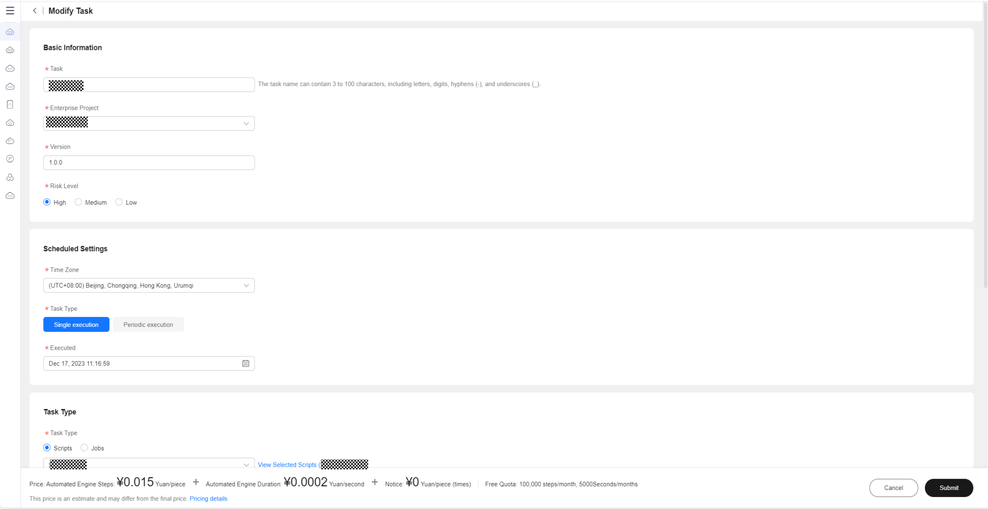
Editing a Scheduled Task

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **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 5-144 Modifying a scheduled task



Modify Task

Basic Information

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

* Enterprise Project
[redacted]

* Version
1.0.0

* Risk Level
● High ○ Medium ○ Low

Scheduled Settings

* Time Zone
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

* Task Type
[✓ Single execution] Periodic execution

* Executed
Dec 17, 2023 11:16:59

Task Type

* Task Type
● Scripts ○ Jobs
[redacted]
View Selected Scripts ([redacted]

Price: Automated Engine Steps: ¥0.015 Yuan/piece + Automated Engine Duration: ¥0.0002 Yuan/second + Notice: ¥0 Yuan/piece (times) | Free Quota: 100,000 steps/month, 5000Seconds/months

This price is an estimate and may differ from the final price. Pricing details

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

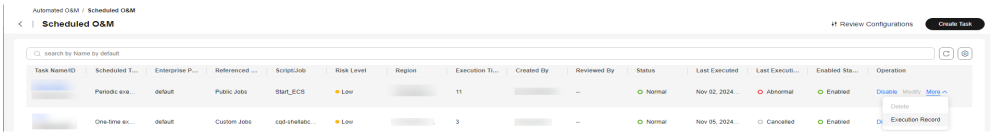
Deleting a Scheduled Task

Step 1 Log in to COC.

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

Step 3 Locate the target task to be deleted, choose **More** > **Delete** in the **Operation** column, and click **OK**.

Figure 5-145 Deleting a scheduled task



Automated O&M / Scheduled O&M

Scheduled O&M

Task Name/ID	Scheduled T...	Enterprise P...	Referenced ...	Script/Job	Risk Level	Region	Execution Ti...	Created By	Reviewed By	Status	Last Executed	Last Executi...	Enabled Sta...	Operation
[redacted]	Periodic exe...	default	Public Jobs	Start_ECS	● Low	[redacted]	11	[redacted]	--	○ Normal	Nov 02, 2024...	○ Abnormal	○ Enabled	Disable Modify More
[redacted]	One-time ex...	default	Custom Jobs	cqd-shellabc...	● Low	[redacted]	3	[redacted]	--	○ Normal	Nov 05, 2024...	○ Cancelled	○ Enabled	Di

NOTE

Only disabled scheduled tasks can be deleted.

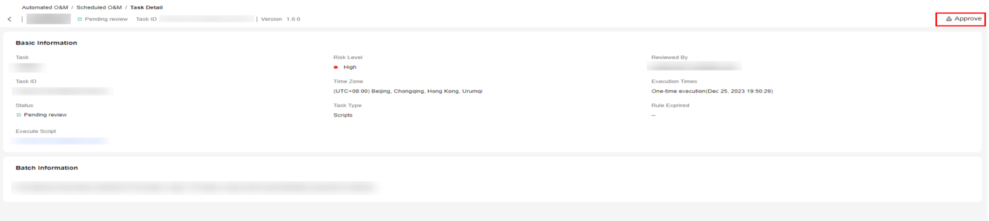
----End

Reviewing Scheduled O&M Tasks

Step 1 Log in to COC.

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

Figure 5-146 Reviewing a scheduled task



Automated O&M / Scheduled O&M / Task Detail

[redacted] Pending review Task ID [redacted] | Version 1.0.0

Basic Information

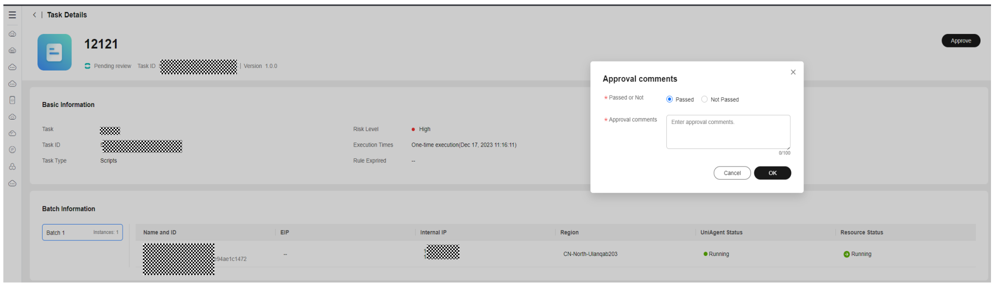
Task: [redacted]
Risk Level: ● High
Reviewed By: [redacted]
Task ID: [redacted]
Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Execution Times: One-time execution(Dec 25, 2023 19:50:29)
Status: Pending review
Task Type: Scripts
Rule Expired: --
Execute Script: [redacted]

Batch Information

[redacted]

Step 3 Click **Approve** in the upper right corner. In the displayed dialog box, select **Passed** or **Not Passed** and enter review comments. Click **OK**.

Figure 5-147 Reviewing a scheduled task



Task Details

12121

Pending review Task ID [redacted] | Version 1.0.0

Basic Information

Task: [redacted]
Task ID: [redacted]
Task Type: Scripts
Risk Level: ● High
Execution Times: One-time execution(Dec 17, 2023 11:16:11)
Rule Expired: --

Approval comments

* Passed or Not: ● Passed ○ Not Passed
* Approval comments: Enter approval comments. 0/100

Batch Information

Batch 1 Instances: 1

Name and ID	EIP	Internal IP	Region	UniAgent Status	Resource Status
[redacted]94ae1c1472	--	[redacted]	CN-North-Ulanqab203	● Running	● Running

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

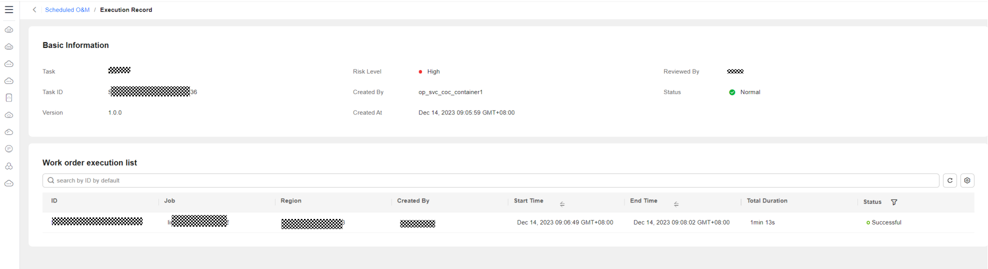
View the execution records of a scheduled task.

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 5-148 Viewing task execution information



Scheduled O&M / Execution Record

Basic Information

Task	[redacted]	Risk Level	● High	Reviewed By	[redacted]
Task ID	[redacted]36	Created By	op_svc_coc_container1	Status	Normal
Version	1.0.0	Created At	Dec 14, 2023 09:05:59 GMT+08:00		

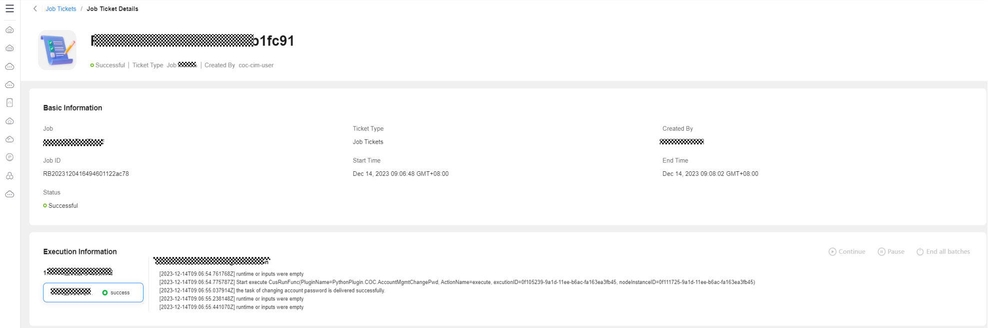
Work order execution list

search by ID by default

ID	Job	Region	Created By	Start Time	End Time	Total Duration	Status
[redacted]	[redacted]	[redacted]	[redacted]	Dec 14, 2023 09:06:49 GMT+08:00	Dec 14, 2023 09:08:02 GMT+08:00	1min 13s	Successful

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 5-149 Job execution details



Job Tickets / Job Ticket Details

[redacted]b1fc91

Successful | Ticket Type Job [redacted] | Created By coc-cim-user

Basic Information

Job [redacted]	Ticket Type Job Tickets	Created By [redacted]
Job ID RB2023120416494601122ac78	Start Time Dec 14, 2023 09:06:48 GMT+08:00	End Time Dec 14, 2023 09:08:02 GMT+08:00
Status Successful		

Execution Information

1[redacted]

[redacted] success

[redacted]

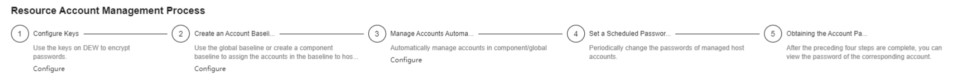
```
[2023-12-14T09:06:54.761768Z] runtime or inputs were empty
[2023-12-14T09:06:54.775787Z] Start execute CusRunFunc(PluginName=PythonPlugin.COC.AccountMgmtChangePwd, ActionName=execute, excutionID=0f105239-9a1d-11ee-b6ac-fa163ea3fb45, nodeInstanceID=0f111725-9a1d-11ee-b6ac-fa163ea3fb45)
[2023-12-14T09:06:55.037914Z] the task of changing account password is delivered successfully.
[2023-12-14T09:06:55.238148Z] runtime or inputs were empty
[2023-12-14T09:06:55.441070Z] runtime or inputs were empty
```

----End

5.5 Account Management

Account Management allows you to centrally manage human-machine accounts of Huawei Cloud ECSs, RDS DB instances, and middleware. Multiple accounts are collected in a unified manner to prevent risks such as forgetting the passwords of multiple resource accounts and leakage of passwords. Users can obtain passwords through **Account Management**.

Figure 5-150 Resource account management process



Resource Account Management Process

1. Configure Keys — Use the keys on DEW to encrypt passwords. Configure
2. Create an Account Baseli... — Use the global baseline or create a component baseline to assign the accounts in the baseline to hos... Configure
3. Manage Accounts Automa... — Automatically manage accounts in component/global Configure
4. Set a Scheduled Passwor... — Periodically change the passwords of managed host accounts.
5. Obtaining the Account Pa... — After the preceding four steps are complete, you can view the password of the corresponding account.

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

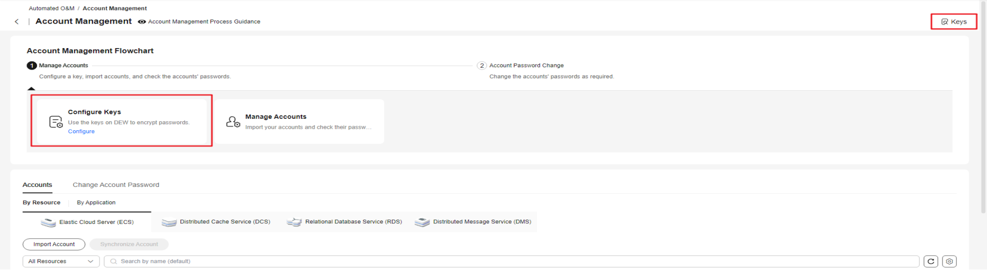
Configuring a Key

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 **Keys** in the upper right corner of the page, or click **Configure** in **Configure Keys** under **Account Management Flowchart**.

Figure 5-151 Configuring keys


Automated O&M / Account Management
Account Management
Account Management Process Guidance
Keys
Account Management Flowchart
1 Manage Accounts
2 Account Password Change
Configure Keys
Configure
Manage Accounts
Accounts
Change Account Password
By Resource
By Application
Elastic Cloud Server (ECS)
Distributed Cache Service (DCS)
Relational Database Service (RDS)
Distributed Message Service (DMS)
Import Account
Synchronize Account
All Resources
Search by name (default)

Configure a key, import accounts, and check the accounts' passwords.

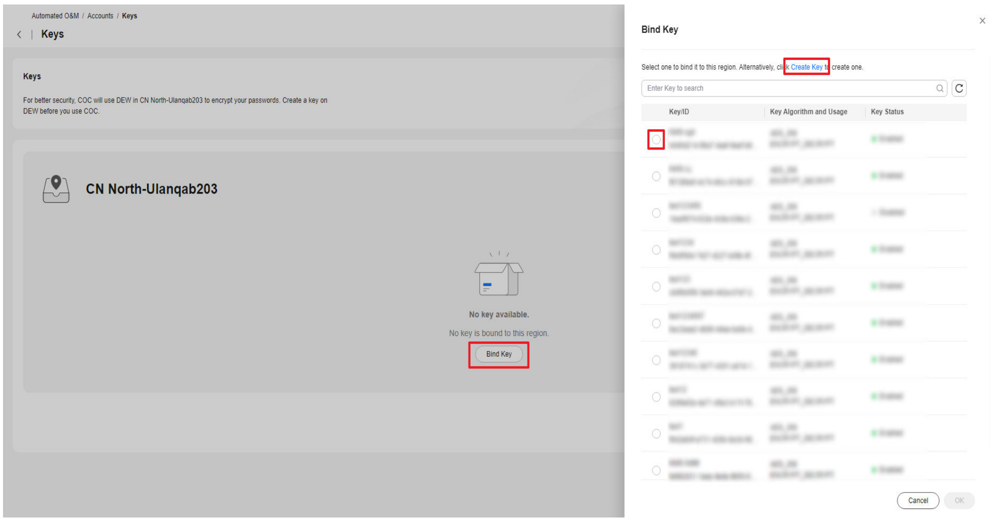
Change the accounts' passwords as required.

Use the keys on DEW to encrypt passwords.

Import your accounts and check their passw...

Step 4 On the **Keys** page, click **Bind Key**. On the displayed Bind Key page, select the key to be bound. If no key is available, click **Create Key** to go to the DEW service to create a key. After creating a key, refresh the list and select it. Click **OK**.

Figure 5-152 Binding a key



For better security, COC will use DEW in CN North-Ulanqab203 to encrypt your passwords. Create a key on DEW before you use COC.

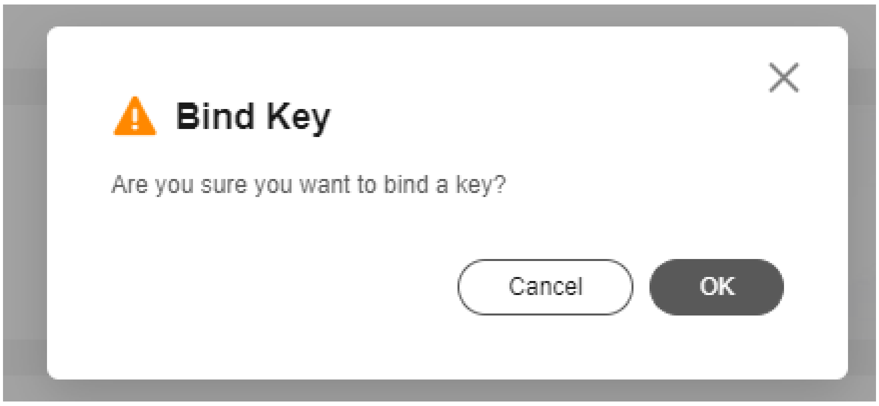
No key available.

No key is bound to this region.

Select one to bind it to this region. Alternatively, click Create Key to create one.

Step 5 In the **Bind Key** confirmation dialog box, a message is displayed, indicating that the bound key cannot be updated once it is used. Click **OK**.

Figure 5-153 Confirming the binding

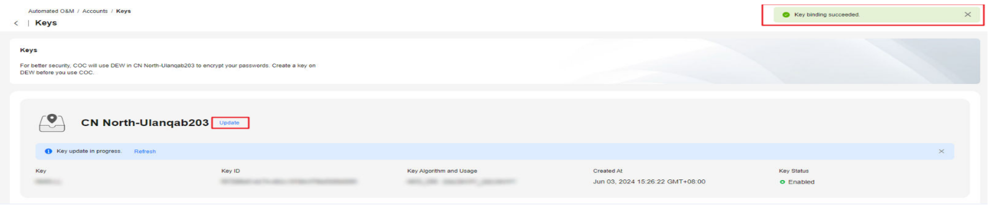


Bind Key

Are you sure you want to bind a key?

Step 6 If you need to update the key, click **Update**.

Figure 5-154 Key binding succeeded



Key binding succeeded.

Keys

For better security, COC will use DEW in CN North-Ulanqab203 to encrypt your passwords. Create a key on DEW before you use COC.

CN North-Ulanqab203

Key update in progress.

Key	Key ID	Key Algorithm and Usage	Created At	Key Status
[redacted]	[redacted]	[redacted]	Jun 03, 2024 15:26:22 GMT+08:00	Enabled

----End

5.5.2 Account Baseline

Creating an Account Baseline

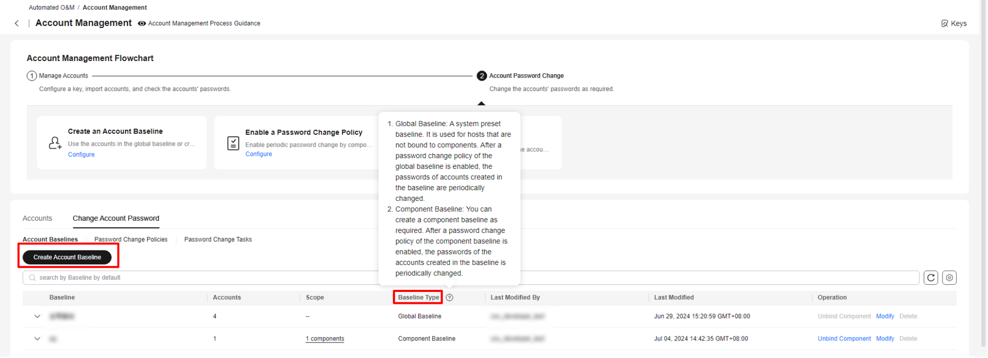
Step 1 Log in to COC.

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

Step 3 Click the **Account Baselines** tab on the **Change Account Password** tab page.

Step 4 For hosts that are not bound to components, the system uses the built-in global baseline to manage host accounts by default. You can also click **Create Account Baseline** (recommended) to define the host accounts to be managed. The prerequisite is that the hosts have been bound to components. For hosts that are not bound to components, you can perform **Creating an Application** and then **Creating a Component** on CloudCMDB.

Figure 5-155 Creating an account baseline



Automated O&M / Account Management

Account Management Account Management Process Guidance Keys

Account Management Flowchart

1 Manage Accounts
Configure a key, import accounts, and check the accounts' passwords.

2 Account Password Change
Change the accounts' passwords as required.

Create an Account Baseline
Use the accounts in the global baseline or cr...
Configure

Enable a Password Change Policy
Enable periodic password change by compo...
Configure

1. Global Baseline: A system preset baseline. It is used for hosts that are not bound to components. After a password change policy of the global baseline is enabled, the passwords of accounts created in the baseline are periodically changed.
2. Component Baseline: You can create a component baseline as required. After a password change policy of the component baseline is enabled, the passwords of the accounts created in the baseline is periodically changed.

Accounts | Change Account Password

Account Baselines | Password Change Policies | Password Change Tasks

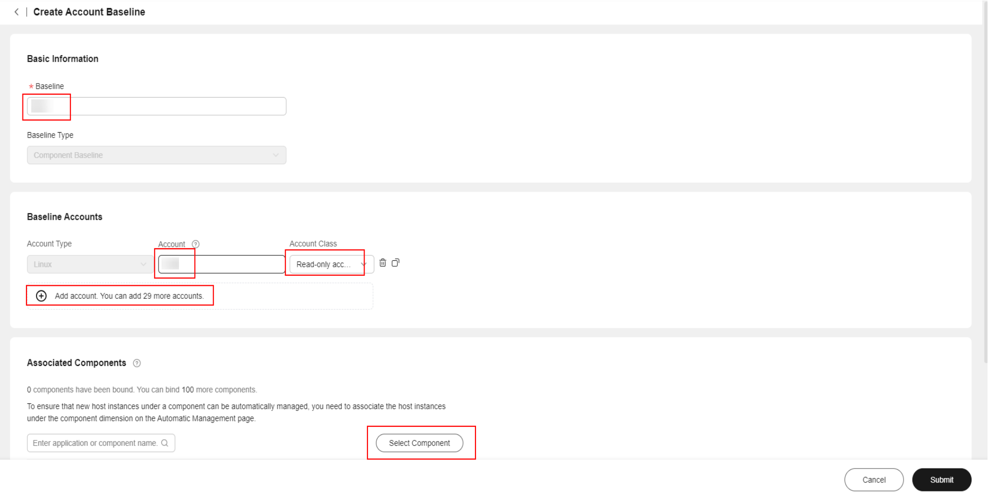
Create Account Baseline

search by Baseline by default

Baseline	Accounts	Scope	Baseline Type	Last Modified By	Last Modified	Operation
[redacted]	4	--	Global Baseline	[redacted]	Jun 29, 2024 15:20:59 GMT+08:00	Unbind Component Modify Delete
[redacted]	1	1 components	Component Baseline	[redacted]	Jul 04, 2024 14:42:35 GMT+08:00	Unbind Component Modify Delete

Step 5 Set the baseline name, and add baseline accounts based on service requirements. For example, set **Account** 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 5-156 Baseline information



Create Account Baseline

Basic Information

* Baseline: [redacted]

Baseline Type: Component Baseline

Baseline Accounts

Account Type	Account	Account Class
Linux	[redacted]	Read-only acc...

Add account. You can add 29 more accounts.

Associated Components

0 components have been bound. You can bind 100 more components.

To ensure that new host instances under a component can be automatically managed, you need to associate the host instances under the component dimension on the Automatic Management page.

Enter application or component name.

Select Component

Cancel Submit

NOTE

The prerequisites for an account to be successfully managed are as follows:

1. The UniAgent has been installed and is in the running state.

2. The host is in the running state.

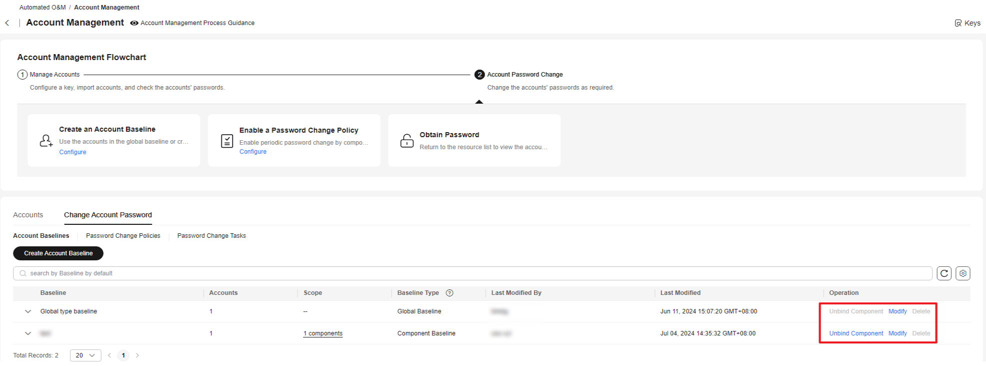
3. The account configured in the baseline exists on the host and can be used to log in to the host.

CAUTION

To ensure that incremental host instances of a component can be automatically managed, you need to enable **Password Change Policy for Component Baseline** in **Component Baseline Dimension** on the **Change Account Password** > **Password Change Policies** tab page.

Step 6 Click **Delete** or **Modify** in the **Operation** column to modify or delete the baseline as needed.

Figure 5-157 Deleting and modifying a baseline



Automated O&M / Account Management

Account Management · Account Management Process Guidance · Keys

Account Management Flowchart

1 Manage Accounts — Configure a key, import accounts, and check the accounts' passwords.

2 Account Password Change — Change the accounts' passwords as required.

Create an Account Baseline — Use the accounts in the global baseline or cr... — Configure

Enable a Password Change Policy — Enable periodic password change by compo... — Configure

Obtain Password — Return to the resource list to view the accou...

Accounts | Change Account Password

Account Baselines | Password Change Policies | Password Change Tasks

Create Account Baseline

search by Baseline by default

Baseline	Accounts	Scope	Baseline Type	Last Modified By	Last Modified	Operation
Global type baseline	1	--	Global Baseline	[redacted]	Jun 11, 2024 15:07:20 GMT+08:00	Unbind Component Modify Delete
[redacted]	1	1 components	Component Baseline	[redacted]	Jul 04, 2024 14:35:32 GMT+08:00	Unbind Component Modify Delete

Total Records: 2 · 20 · 1

⚠ CAUTION

Before deleting a baseline, you need to unbind all associated components.

----End

5.5.3 Password Change Policies

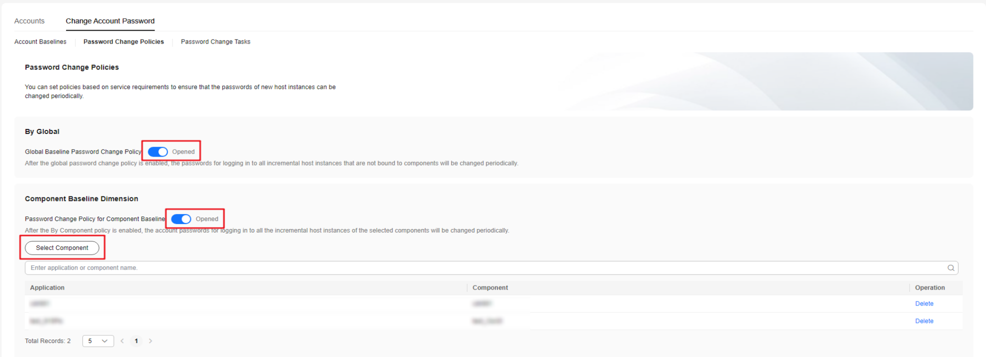
Enabling the Password Change Policy

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 5-158 Enabling the password change policy



Accounts | Change Account Password

Account Baselines | Password Change Policies | Password Change Tasks

Password Change Policies

You can set policies based on service requirements to ensure that the passwords of new host instances can be changed periodically.

By Global

Global Baseline Password Change Policy: Opened

After the global password change policy is enabled, the passwords for logging in to all incremental host instances that are not bound to components will be changed periodically.

Component Baseline Dimension

Password Change Policy for Component Baseline: Opened

After the By Component policy is enabled, the account passwords for logging in to all the incremental host instances of the selected components will be changed periodically.

Select Component

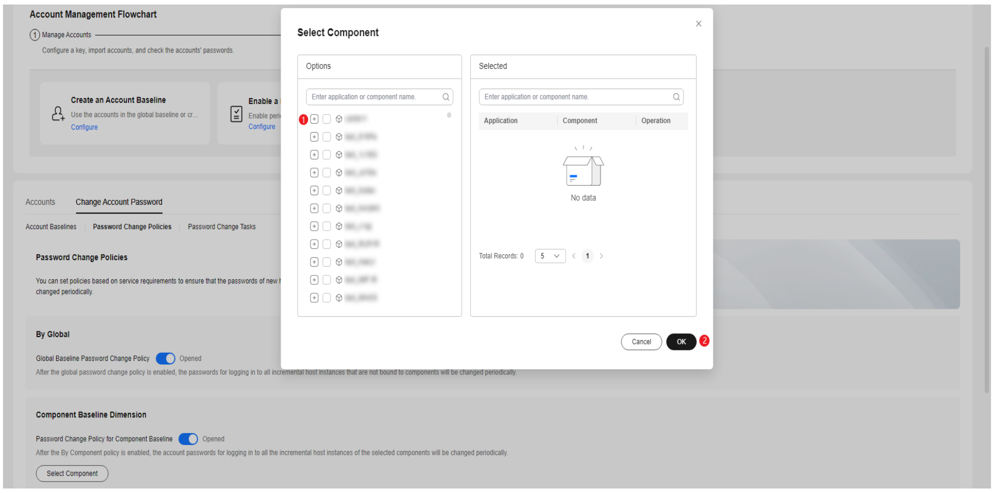
Enter application or component name.

Application	Component	Operation
[redacted]	[redacted]	Delete
[redacted]	[redacted]	Delete

Total Records: 2 · 5 · 1

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 5-159 Selecting a desired component



Configure a key, import accounts, and check the accounts' passwords.

You can set policies based on service requirements to ensure that the passwords of new h changed periodically.

Global Baseline Password Change Policy: Opened

After the global password change policy is enabled, the passwords for logging in to all incremental host instances that are not bound to components will be changed periodically.

Password Change Policy for Component Baseline: Opened

After the By Component policy is enabled, the account passwords for logging in to all the incremental host instances of the selected components will be changed periodically.

----End

5.5.4 Password Change Tasks

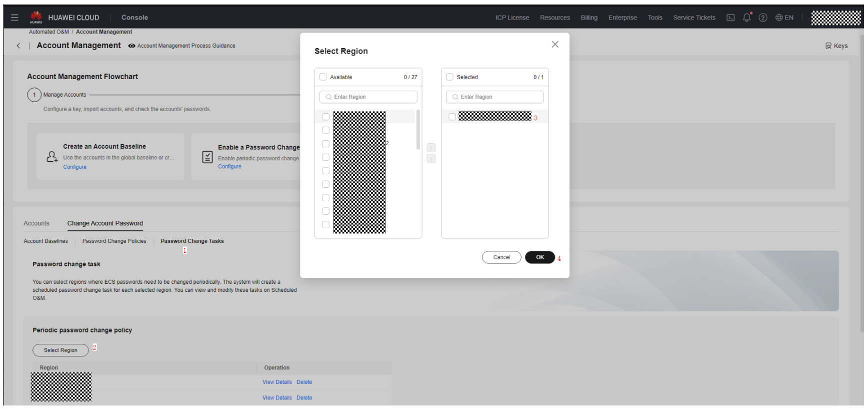
Configuring Password Change Regions

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **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 then **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 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 5-160 Configuring regions



[redacted]

[redacted]

[redacted]

[redacted]

Configure a key, import accounts, and check the accounts' passwords.

You can select regions where ECS passwords need to be changed periodically. The system will create a scheduled password change task for each selected region. You can view and modify these tasks on Scheduled O&M.

Step 4 You can obtain host passwords on the **Accounts** tab page as needed.

----End

5.5.5 Querying the Account Password

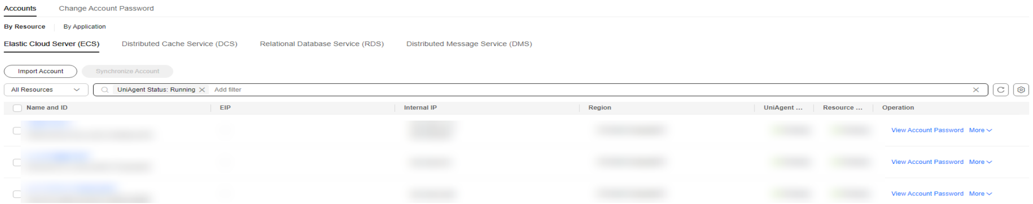
Obtaining Account Passwords

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**.

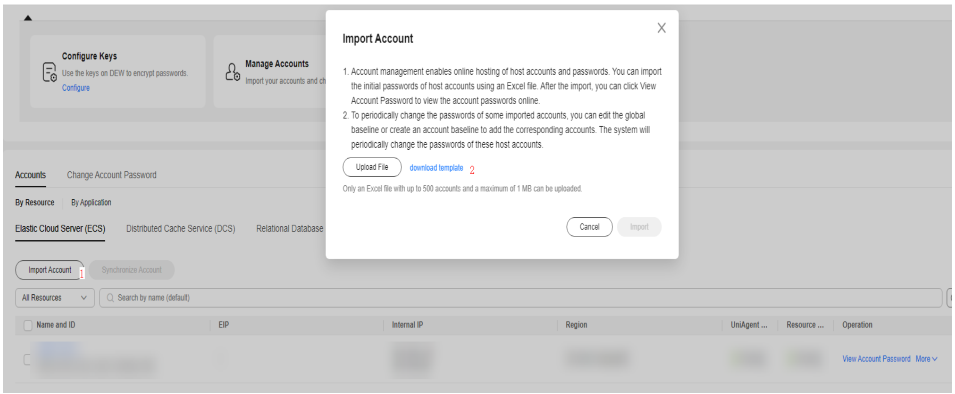
Step 3 Click the **Accounts** tab. **By Resource** is used to manage all purchased host instances, and **By Application** is used to manage purchased hosts that are bound to applications.

Figure 5-161 Accounts



Step 4 To save accounts (only save the accounts and do not change their passwords), click **Import Account**, download the Excel template, enter the host information, confirm the information, and upload the template.

Figure 5-162 Importing accounts



Import Account

1. Account management enables online hosting of host accounts and passwords. You can import the initial passwords of host accounts using an Excel file. After the import, you can click View Account Password to view the account passwords online.
2. To periodically change the passwords of some imported accounts, you can edit the global baseline or create an account baseline to add the corresponding accounts. The system will periodically change the passwords of these host accounts.

Only an Excel file with up to 500 accounts and a maximum of 1 MB can be uploaded.

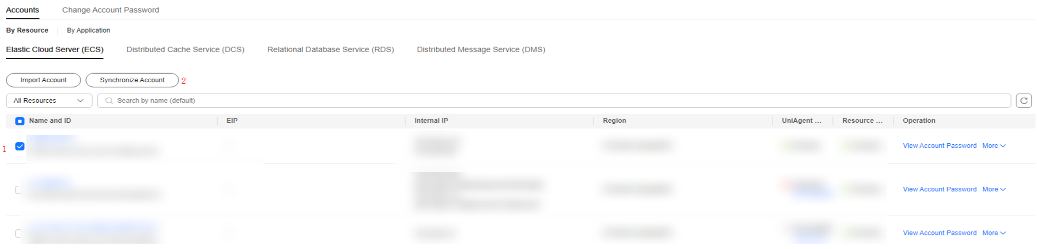
CAUTION

1. The imported host accounts are not managed. If you want to automatically manage the imported accounts, you can modify the global baseline or create an account baseline to add these accounts. Then, the system will immediately manage these host accounts.

2. DCS, RDS, and DMS host accounts that are imported cannot be managed, that is, their passwords cannot be automatically changed.

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

Figure 5-163 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 password 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.

Conditions for changing the password of an ECS host:

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.

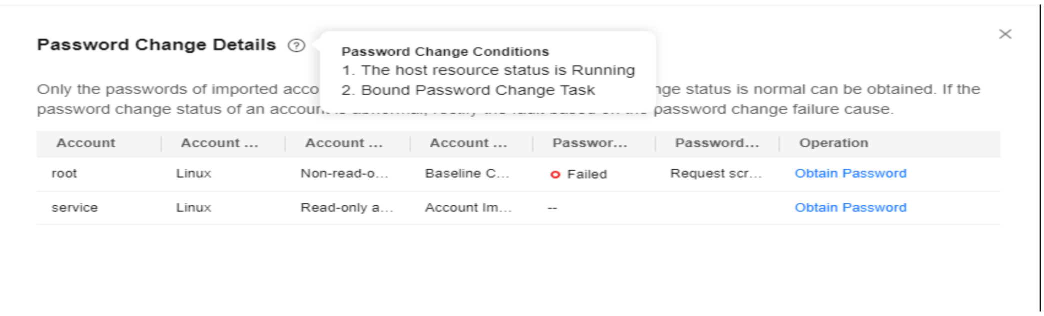
Conditions for changing the passwords of an incremental ECS:

4. The password change policy has been enabled.

Conditions for periodically changing the password of a managed host:

1. A password change task has been bound.

Figure 5-164 Password Change Details



Password Change Details

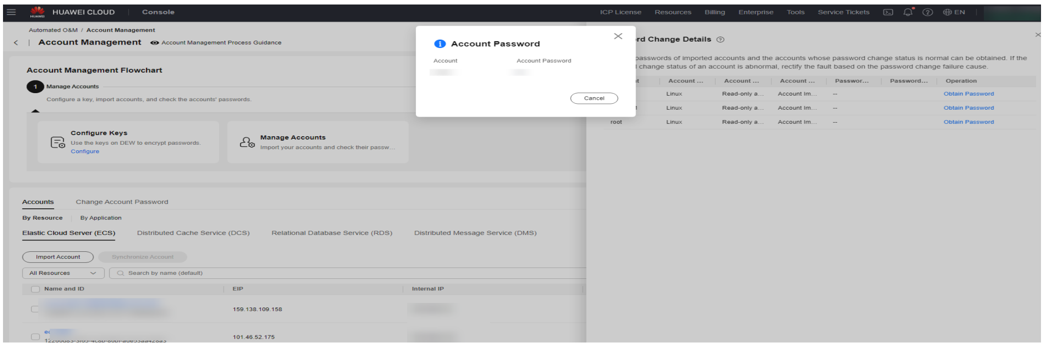
Password Change Conditions
1. The host resource status is Running
2. Bound Password Change Task

Only the passwords of imported acco... ...nge status is normal can be obtained. If the password change status of an accoun... ...password change failure cause.

Account	Account ...	Account ...	Account ...	Passwor...	Password...	Operation
root	Linux	Non-read-o...	Baseline C...	○ Failed	Request scr...	Obtain Password
service	Linux	Read-only a...	Account Im...	--		Obtain Password

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

Figure 5-165 Obtaining account passwords



HUAWEI CLOUD
Console
ICP License
Resources
Billing
Enterprise
Tools
Service Tickets
EN
Automated O&M / Account Management
Account Management
Account Management Process Guidance
Account Management Flowchart
1 Manage Accounts
Configure a key, import accounts, and check the accounts' passwords.
Configure Keys
Use the keys on DEW to encrypt passwords.
Configure
Manage Accounts
Import your accounts and check their passw...
Accounts
Change Account Password
By Resource
By Application
Elastic Cloud Server (ECS)
Distributed Cache Service (DCS)
Relational Database Service (RDS)
Distributed Message Service (DMS)
Import Account
Synchronize Account
All Resources
Search by name (default)
Cancel

Account Password

Account	Account Password

Name and ID	EIP	Internal IP
	159.138.109.158	
	101.46.52.175	

...rd Change Details

...passwords of imported accounts and the accounts whose password change status is normal can be obtained. If the ...change status of an account is abnormal, rectify the fault based on the password change failure cause.

...t	Account ...	Account ...	Account ...	Passwor...	Password...	Operation
	Linux	Read-only a...	Account Im...	--		Obtain Password
	Linux	Read-only a...	Account Im...	--		Obtain Password
root	Linux	Read-only a...	Account Im...	--		Obtain Password

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

----End

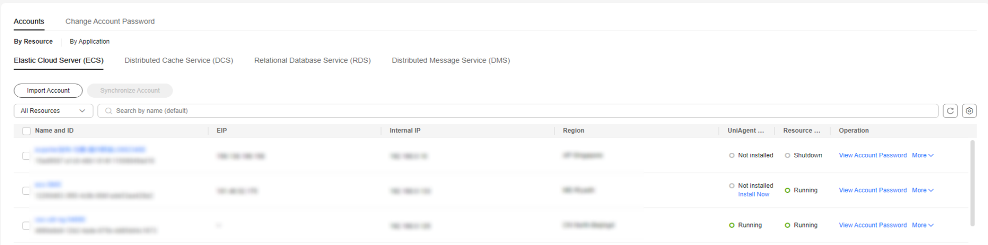
5.5.6 Logging In to a Host Without Any Passwords

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**. In the **Routine O&M** area, click **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 5-166 Accounts



Accounts | Change Account Password

By Resource | By Application

Elastic Cloud Server (ECS) | Distributed Cache Service (DCS) | Relational Database Service (RDS) | Distributed Message Service (DMS)

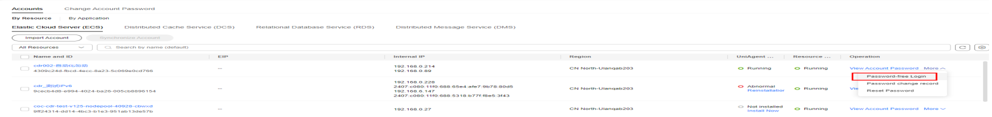
Import Account | Synchronize Account

All Resources | Search by name (default)

Name and ID	EIP	Internal IP	Region	UniAgent ...	Resource ...	Operation
[illegible]	[illegible]	[illegible]	[illegible]	○ Not installed	○ Shutdown	View Account Password More
[illegible]	[illegible]	[illegible]	[illegible]	○ Not installed Install Now	○ Running	View Account Password More
[illegible]	--	[illegible]	[illegible]	○ Running	○ Running	View Account Password More

Step 4 You can search for the host resource to be remotely logged in to from the resource or application perspective and click **Password-free Login** in the **Operation** column to remotely log in to the host.

Figure 5-167 Remotely logging in to a cloud server



Accounts | Change Account Password

By Resource | By Application

Elastic Cloud Server (ECS) | Distributed Cache Service (DCS) | Relational Database Service (RDS) | Distributed Message Service (DMS)

Import Account | Synchronize Account

All Resources | Search by name (default)

Name and ID	EIP	Internal IP	Region	UniAgent ...	Resource ...	Operation
cdr002-自动化勿动 4309c24d-fbcd-4ecc-8a23-5c069e0cd766	--	192.168.0.214 192.168.0.89	CN North-Ulanqab203	○ Running	○ Running	View Account Password More Password-free Login Password change record Reset Password
cdr_测试IPv6 9cecb4d8-e994-4024-ba26-005cb8896154	--	192.168.0.228 2407:c080:11f0:688:65e4:afe7:9b78:80d5 192.168.6.147 2407:c080:11f0:688:5318:b77f:f8e5:3f43	CN North-Ulanqab203	○ Abnormal Reinstallation	○ Running	Vie
coc-cdr-test-v125-nodepool-40928-cbwxd 9ff24314-dd14-4bc3-b1e3-951ab13de57b	--	192.168.0.27	CN North-Ulanqab203	○ Not installed Install Now	○ Running	View Account Password More

NOTE

There are three prerequisites for a successful remote login to a host:

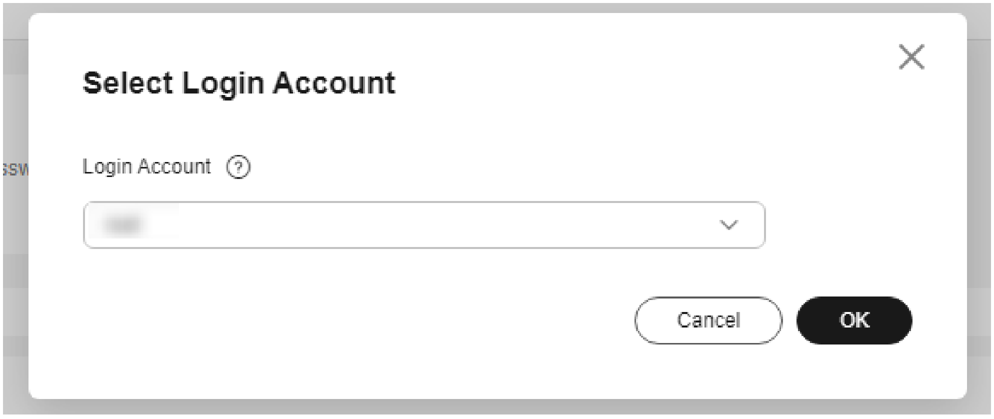
1. A UniAgent has been installed and is running on the target host. The UniAgent version must be later than 1.1.3.8.

2. The host is in the running state.

3. The account configured in the baseline exists on the host and can be used to log in to the host.

Step 5 In the **Select Login Account** dialog box, select the account with which you want to log in to the host from the **Login Account** drop-down list and click **OK**.

Figure 5-168 Selecting the account you want to use for login



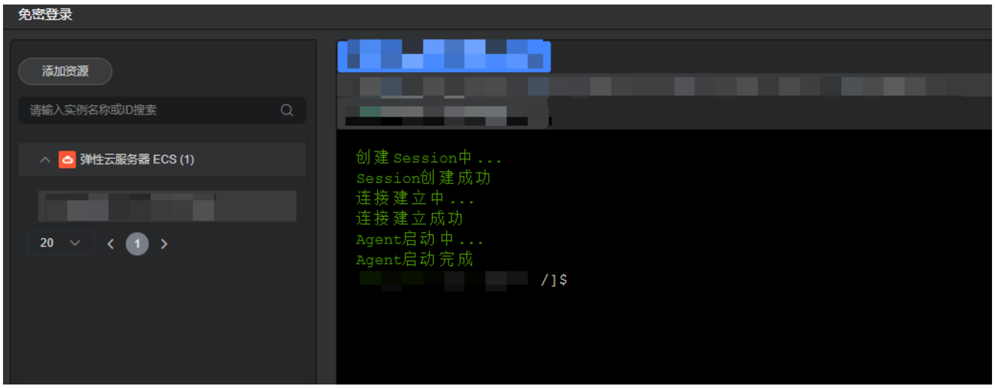
Select Login Account

Login Account ⓘ

[illegible]

Cancel | OK

Figure 5-169 The black screen command page is displayed.



[redacted]

```
创建Session中...
Session创建成功
连接建立中...
连接建立成功
Agent启动中...
Agent启动完成
[redacted] /]$
```

----End

5.6 Parameter Management

5.6.1 Parameter Center

5.6.1.1 Creating a Parameter

Scenarios

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

Precautions

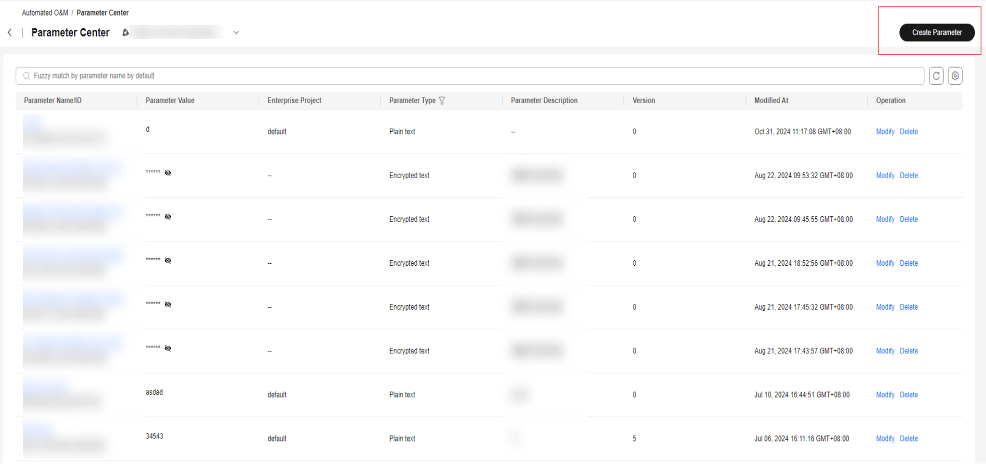
Parameter policies may delete parameters. Exercise caution when configuring parameter policies.

Procedure

Step 1 Log in to COC.

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

Figure 5-170 Creating a parameter



Automated O&M / Parameter Center

Parameter Center [redacted]

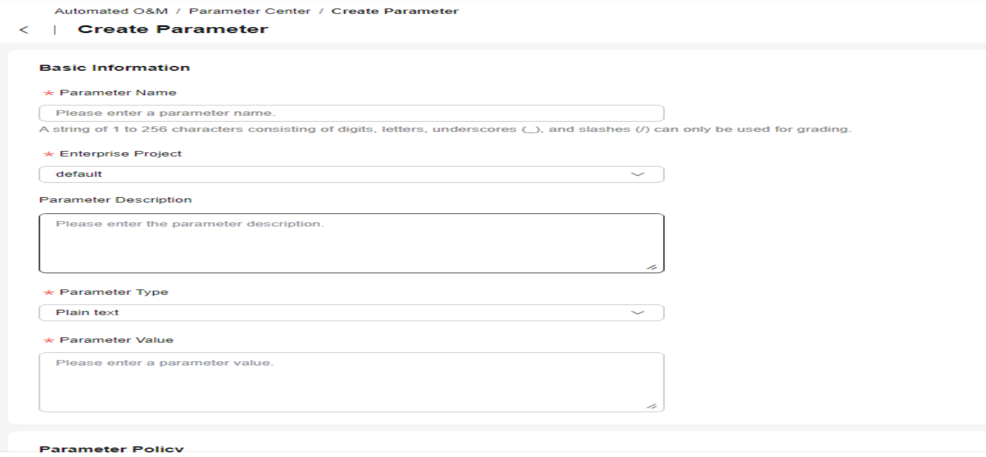
Create Parameter

Fuzzy match by parameter name by default

Parameter Name/ID	Parameter Value	Enterprise Project	Parameter Type	Parameter Description	Version	Modified At	Operation
[redacted]	d	default	Plain text	--	0	Oct 31, 2024 11:17:08 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 22, 2024 09:53:32 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 22, 2024 09:45:55 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 18:52:56 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 17:45:32 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 17:43:57 GMT+08:00	Modify Delete
[redacted]	asdad	default	Plain text	[redacted]	0	Jul 10, 2024 16:44:51 GMT+08:00	Modify Delete
[redacted]	34543	default	Plain text	[redacted]	5	Jul 06, 2024 16:11:16 GMT+08:00	Modify Delete

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

Figure 5-171 Basic information



Automated O&M / Parameter Center / Create Parameter

< | Create Parameter

Basic Information

* Parameter Name

Please enter a parameter name.

A string of 1 to 256 characters consisting of digits, letters, underscores (_), and slashes (/) can only be used for grading.

* Enterprise Project

default

Parameter Description

Please enter the parameter description.

* Parameter Type

Plain text

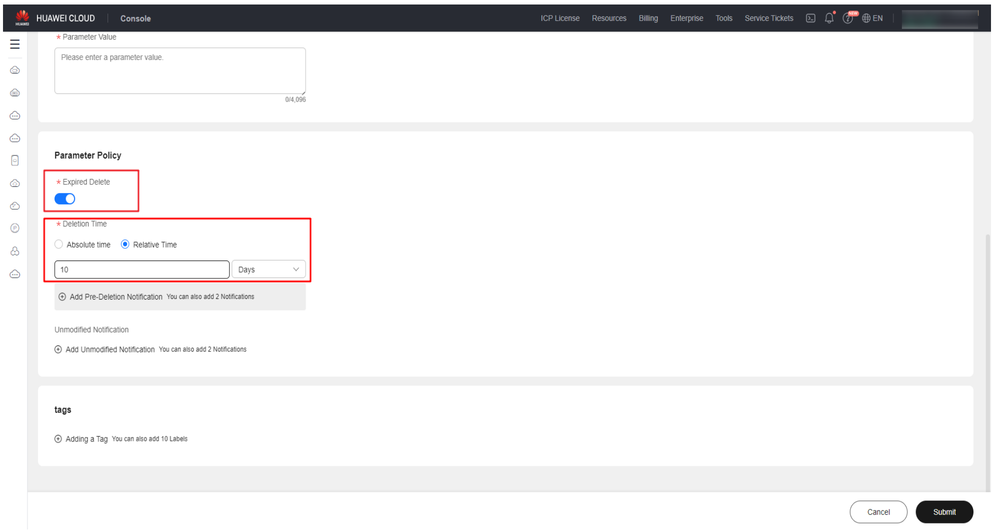
* Parameter Value

Please enter a parameter value.

Parameter Policy

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 **Step 5** and **Step 6**.

Figure 5-172 Policy for deleting the parameter upon expiration



* Parameter Value

Please enter a parameter value.

0/4,096

Parameter Policy

* Expired Delete

* Deletion Time

○ Absolute time ● Relative Time

10 Days

Add Pre-Deletion Notification You can also add 2 Notifications

Unmodified Notification

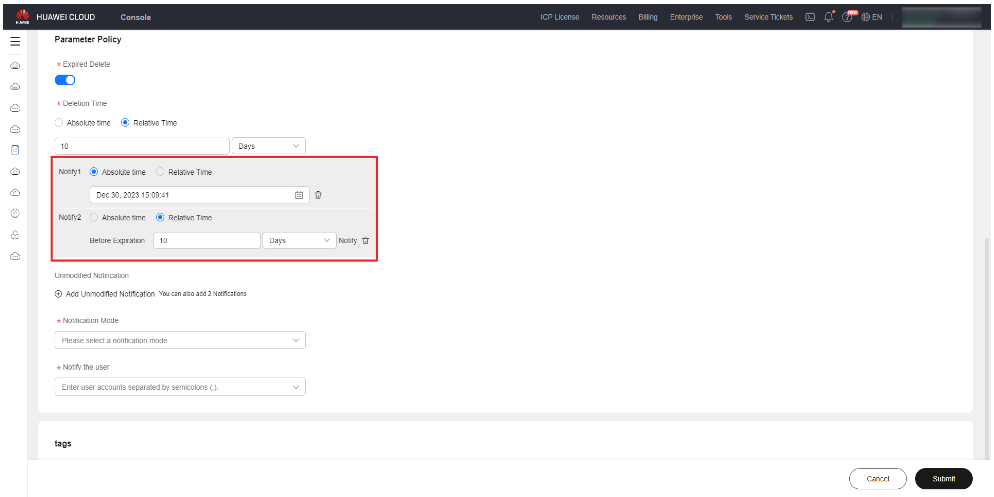
Add Unmodified Notification You can also add 2 Notifications

tags

Adding a Tag You can also add 10 Labels

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 5-173 Adding pre-deletion notifications



Parameter Policy

* Expired Delete

* Deletion Time

○ Absolute time ● Relative Time

10 Days

Notify1 ● Absolute time ○ Relative Time

Dec 30, 2023 15:09:41

Notify2 ○ Absolute time ● Relative Time

Before Expiration 10 Days Notify

Unmodified Notification

Add Unmodified Notification You can also add 2 Notifications

* Notification Mode

Please select a notification mode.

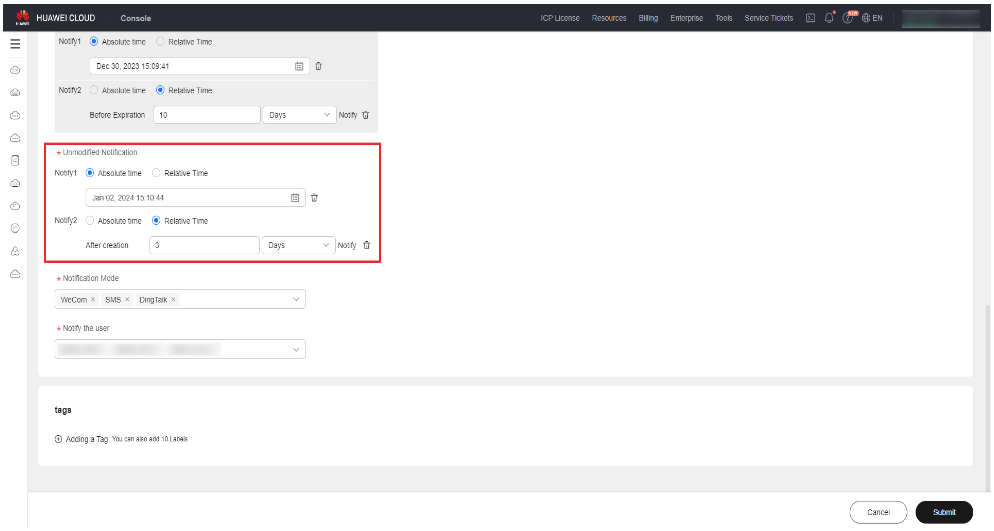
* Notify the user

Enter user accounts separated by semicolons (;).

tags

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 5-174 Adding unmodified notifications



Notify1 ● Absolute time ○ Relative Time

Dec 30, 2023 15:09:41

Notify2 ○ Absolute time ● Relative Time

Before Expiration 10 Days Notify

* Unmodified Notification

Notify1 ● Absolute time ○ Relative Time

Jan 02, 2024 15:10:44

Notify2 ○ Absolute time ● Relative Time

After creation 3 Days Notify

* Notification Mode

WeCom × SMS × DingTalk ×

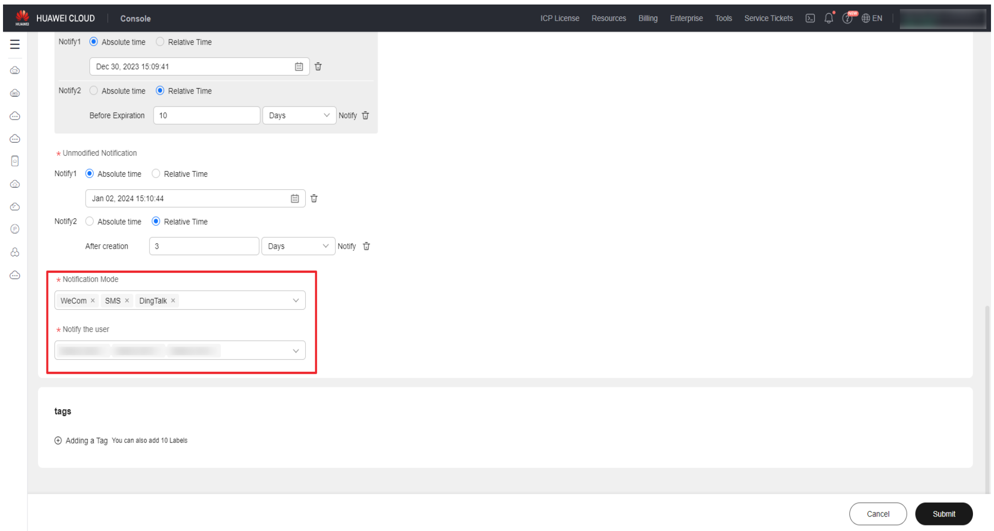
* Notify the user

tags

Adding a Tag You can also add 10 Labels

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

Figure 5-175 Setting Notification Mode and Notify the user



Notify1 ● Absolute time ○ Relative Time

Dec 30, 2023 15:09:41

Notify2 ○ Absolute time ● Relative Time

Before Expiration 10 Days Notify

* Unmodified Notification

Notify1 ● Absolute time ○ Relative Time

Jan 02, 2024 15:10:44

Notify2 ○ Absolute time ● Relative Time

After creation 3 Days Notify

* Notification Mode

WeCom × SMS × DingTalk ×

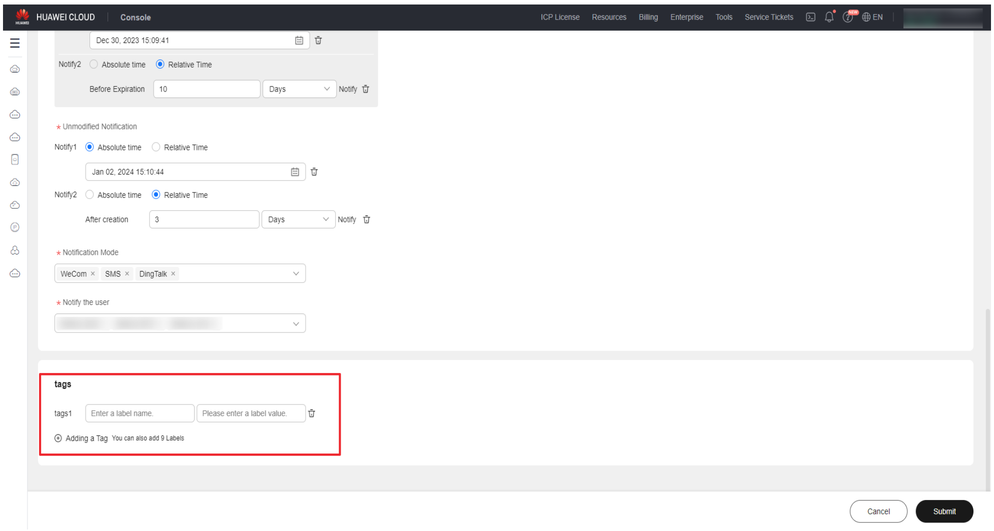
* Notify the user

tags

Adding a Tag You can also add 10 Labels

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

Figure 5-176 Adding parameter tags



Dec 30, 2023 15:09:41

Notify2 ○ Absolute time ● Relative Time

Before Expiration 10 Days Notify

* Unmodified Notification

Notify1 ● Absolute time ○ Relative Time

Jan 02, 2024 15:10:44

Notify2 ○ Absolute time ● Relative Time

After creation 3 Days Notify

* Notification Mode

WeCom × SMS × DingTalk ×

* Notify the user

[redacted]

tags

tags1 Enter a label name. Please enter a label value.

⊕ Adding a Tag You can also add 9 Labels

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

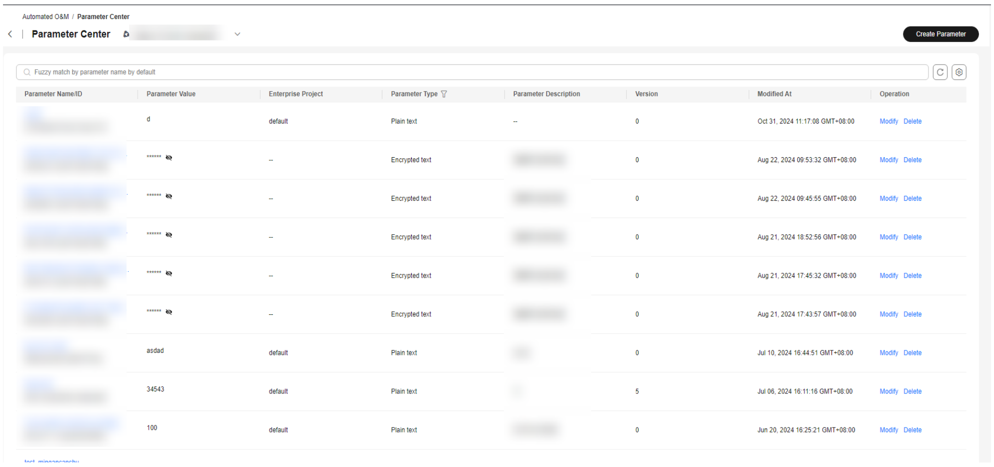
----End

5.6.1.2 Modifying a Parameter

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resource O&M** > **Automatic O&M** and click **Parameter Center**. Locate the target parameter record, and click **Modify** in the **Operation** column.

Figure 5-177 Parameter list



Automated O&M / Parameter Center

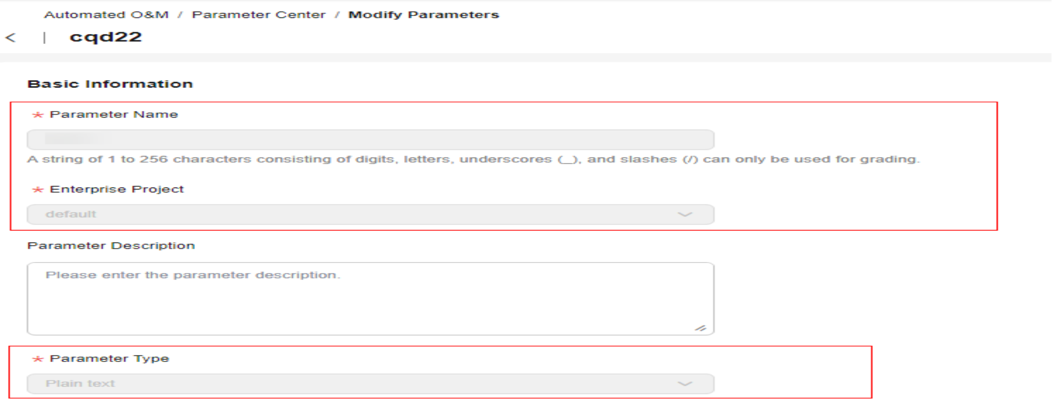
Parameter Center [redacted]

Fuzzy match by parameter name by default

Parameter Name/ID	Parameter Value	Enterprise Project	Parameter Type	Parameter Description	Version	Modified At	Operation
[redacted]	d	default	Plain text	--	0	Oct 31, 2024 11:17:08 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 22, 2024 09:53:32 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 22, 2024 09:45:55 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 18:52:56 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 17:45:32 GMT+08:00	Modify Delete
[redacted]	******	--	Encrypted text	[redacted]	0	Aug 21, 2024 17:43:57 GMT+08:00	Modify Delete
[redacted]	asdad	default	Plain text	[redacted]	0	Jul 10, 2024 16:44:51 GMT+08:00	Modify Delete
[redacted]	34543	default	Plain text	[redacted]	5	Jul 06, 2024 16:11:16 GMT+08:00	Modify Delete
[redacted]	100	default	Plain text	[redacted]	0	Jun 20, 2024 16:25:21 GMT+08:00	Modify Delete

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

Figure 5-178 Parameter details



Automated O&M / Parameter Center / Modify Parameters

< | cqd22

Basic Information

* Parameter Name

[redacted]

A string of 1 to 256 characters consisting of digits, letters, underscores (_), and slashes (/) can only be used for grading.

* Enterprise Project

default

Parameter Description

Please enter the parameter description.

* Parameter Type

Plain text

Step 4 Modify the parameters as required and click **Submit**.

CAUTION

If the notification time is a relative time, note the following:

1. For unmodified notifications: If you click the modification button, the notification time will change immediately.
2. For pre-deletion notifications: If you change the deletion time, the pre-deletion notification time will also change.

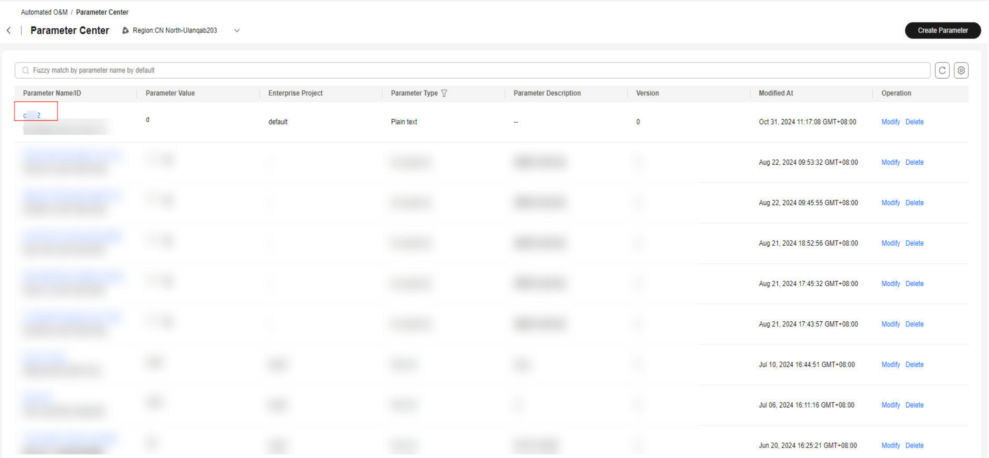
----End

5.6.1.3 Viewing Parameter Details

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Resource O&M** > **Automatic O&M** and click **Parameter Center**. Click the name of a parameter to go to the details page. You can view the parameter details and version history.

Figure 5-179 Parameter list



Automated O&M / Parameter Center

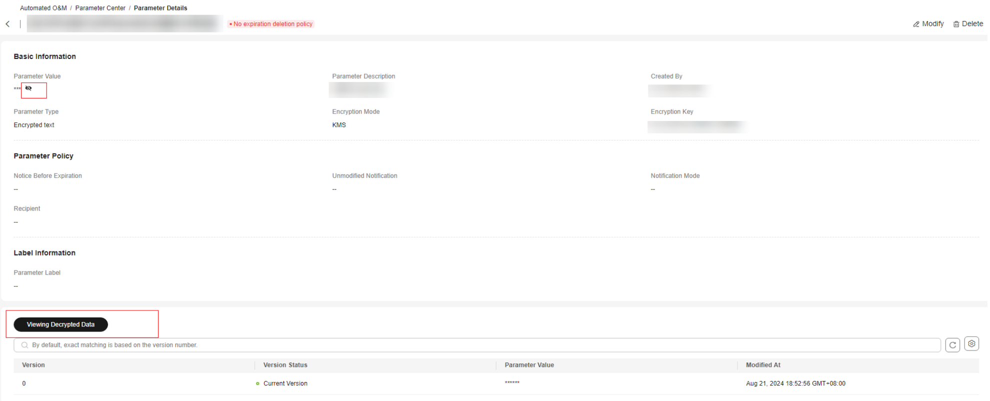
< | Parameter Center Region:CN North-Ulanqab203

Fuzzy match by parameter name by default

Parameter Name/ID	Parameter Value	Enterprise Project	Parameter Type	Parameter Description	Version	Modified At	Operation
c[redacted]2 [redacted]	d	default	Plain text	--	0	Oct 31, 2024 11:17:08 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Aug 22, 2024 09:53:32 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Aug 22, 2024 09:45:55 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Aug 21, 2024 18:52:56 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Aug 21, 2024 17:45:32 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Aug 21, 2024 17:43:57 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Jul 10, 2024 16:44:51 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Jul 06, 2024 16:11:16 GMT+08:00	Modify Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Jun 20, 2024 16:25:21 GMT+08:00	Modify Delete

Step 3 On the **Parameter Details** page, click next to the parameter value to view the value of the sensitive parameter, click **Collapse** to expand the tag list, and click **Viewing Decrypted Data** to view the values of all parameter versions.

Figure 5-180 Parameter details



Automated O&M / Parameter Center / Parameter Details

[redacted] • No expiration deletion policy

Modify Delete

Basic Information

Parameter Value: ***

Parameter Description: [redacted]

Created By: [redacted]

Parameter Type: Encrypted text

Encryption Mode: KMS

Encryption Key: [redacted]

Parameter Policy

Notice Before Expiration: --

Unmodified Notification: --

Notification Mode: --

Recipient: --

Label Information

Parameter Label: --

Viewing Decrypted Data

By default, exact matching is based on the version number.

Version	Version Status	Parameter Value	Modified At
0	Current Version	******	Aug 21, 2024 18:52:56 GMT+08:00

----End

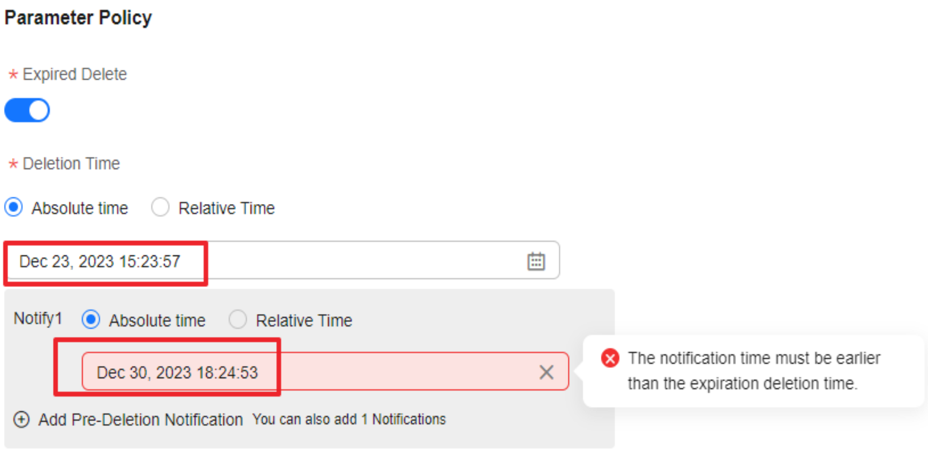
5.6.2 Notification Rules

The parameter notifications are influenced by the time of deletion upon expiration and modification operations. When modifying a parameter, you need to pay attention to the notification rule (configured in the **Parameter Policy** module).

5.6.2.1 Expiration Notification

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

Figure 5-181 If the expiration notification time is later than the time of deletion upon expiration



Parameter Policy

* Expired Delete

* Deletion Time

● Absolute time ○ Relative Time

Dec 23, 2023 15:23:57

Notify1 ● Absolute time ○ Relative Time

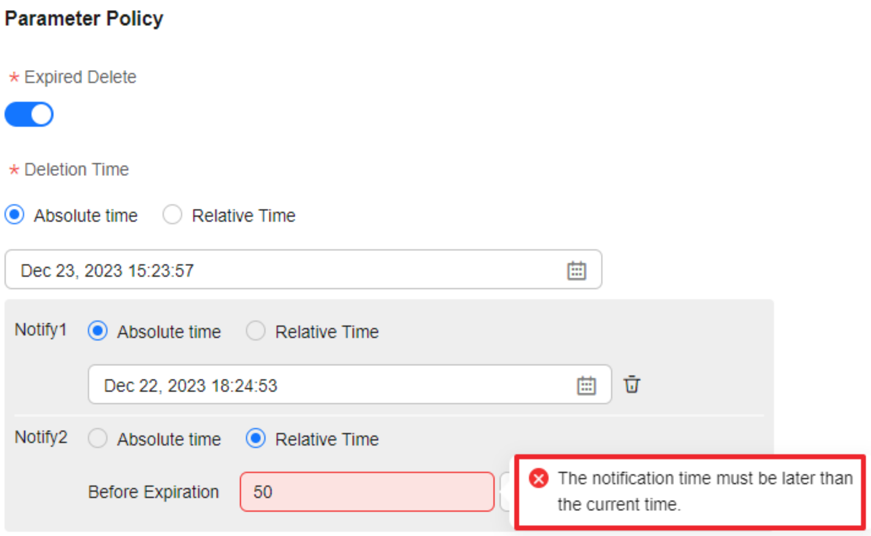
Dec 30, 2023 18:24:53

The notification time must be earlier than the expiration deletion time.

⊕ Add Pre-Deletion Notification You can also add 1 Notifications

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

Figure 5-182 If the expiration notification time is earlier than the system time



Parameter Policy

* Expired Delete

* Deletion Time

● Absolute time ○ Relative Time

Dec 23, 2023 15:23:57

Notify1 ● Absolute time ○ Relative Time

Dec 22, 2023 18:24:53

Notify2 ○ Absolute time ● Relative Time

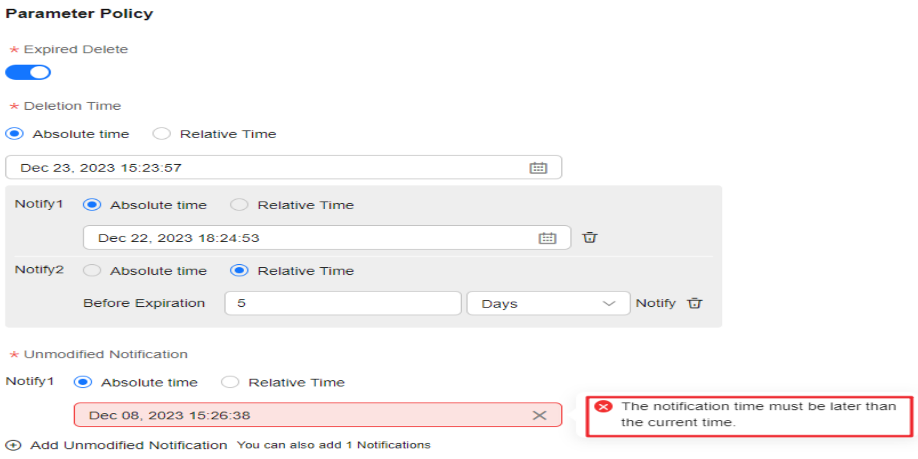
Before Expiration 50

The notification time must be later than the current time.

5.6.2.2 Unmodified Notifications

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

Figure 5-183 If the notification time is earlier than the system time



Parameter Policy

* Expired Delete

* Deletion Time

● Absolute time ○ Relative Time

Dec 23, 2023 15:23:57

Notify1 ● Absolute time ○ Relative Time

Dec 22, 2023 18:24:53

Notify2 ○ Absolute time ● Relative Time

Before Expiration 5 Days Notify

* Unmodified Notification

Notify1 ● Absolute time ○ Relative Time

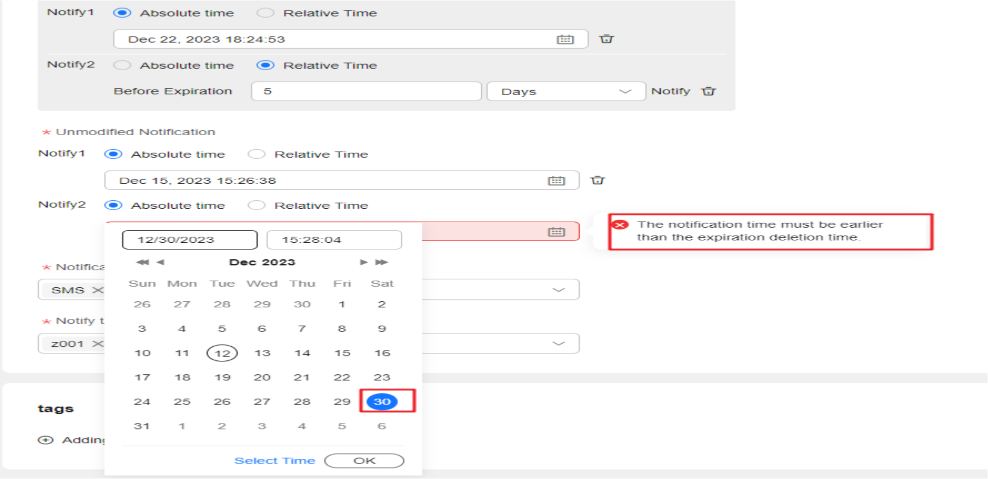
Dec 08, 2023 15:26:38

The notification time must be later than the current time.

⊕ Add Unmodified Notification You can also add 1 Notifications

- 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 5-184 If the unmodified notification time is later than the time of deletion upon expiration



Notify1 ● Absolute time ○ Relative Time

Dec 22, 2023 18:24:53

Notify2 ○ Absolute time ● Relative Time

Before Expiration 5 Days Notify

* Unmodified Notification

Notify1 ● Absolute time ○ Relative Time

Dec 15, 2023 15:26:38

Notify2 ● Absolute time ○ Relative Time

12/30/2023 15:28:04

The notification time must be earlier than the expiration deletion time.

6 Faults

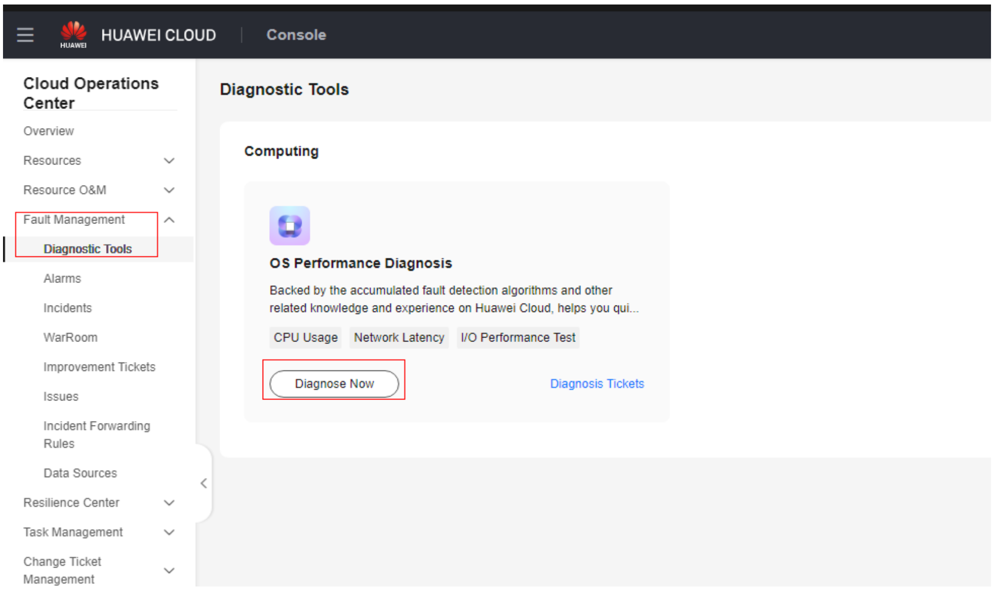
6.1 Diagnosis Tools

6.1.1 Diagnosing OS Faults

Step 1 Log in to **COC**.

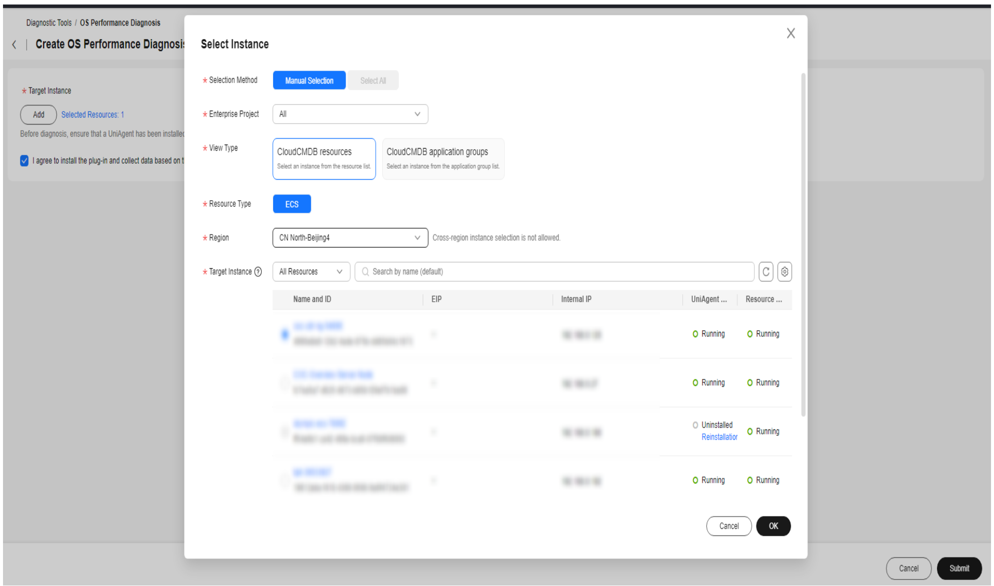
Step 2 In the navigation pane, choose **Fault Management > Diagnostic Tools**. On the displayed page, in the **OS Performance Diagnosis** area, click **Diagnose Now**. The **Create OS Performance Diagnosis Task** page is displayed.

Figure 6-1 OS diagnosis entry



Step 3 On the **Create OS Performance Diagnosis Task** page, click **Add**. Ensure that you have installed a **UniAgent** in advance, and the image and specifications must meet the OS diagnosis requirements.

Figure 6-2 Selecting instances



Diagnostic Tools / OS Performance Diagnosis

Create OS Performance Diagnosis

Select Instance

* Selection Method: Manual Selection | Select All

* Enterprise Project: All

* View Type: CloudCMDB resources (Select an instance from the resource list.) | CloudCMDB application groups (Select an instance from the application group list.)

* Resource Type: ECS

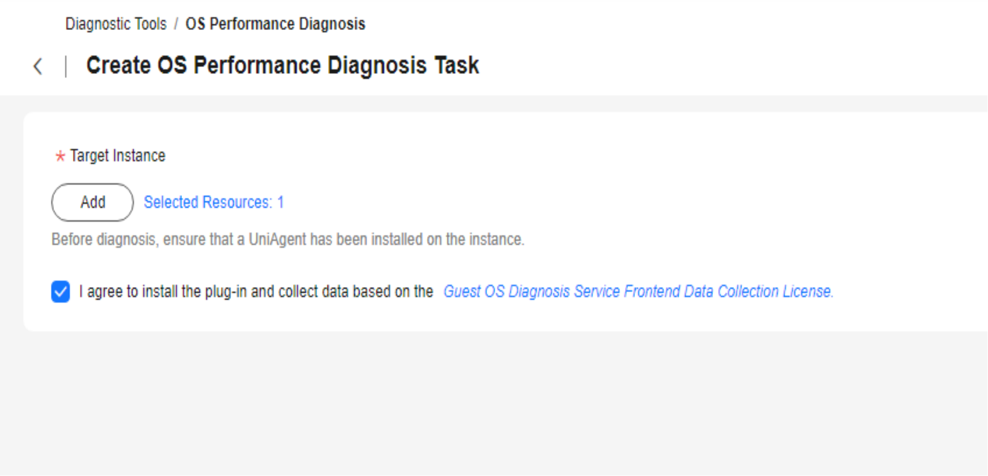
* Region: CN North-Beijing4 — Cross-region instance selection is not allowed.

* Target Instance: All Resources | Search by name (default)

Name and ID	EIP	Internal IP	UniAgent ...	Resource ...
[redacted]	-	[redacted]	Running	Running
[redacted]	-	[redacted]	Running	Running
[redacted]	-	[redacted]	Uninstalled Reinstallation	Running
[redacted]	-	[redacted]	Running	Running

Step 4 On the **Create OS Performance Diagnosis** page, select **I agree to install the plug-in and collect data based on the Guest OS Diagnosis Service Frontend Data Collection License**, and click **Submit**.

Figure 6-3 Agreeing to the authorization agreement and submitting for diagnosis



Diagnostic Tools / OS Performance Diagnosis

Create OS Performance Diagnosis Task

* Target Instance

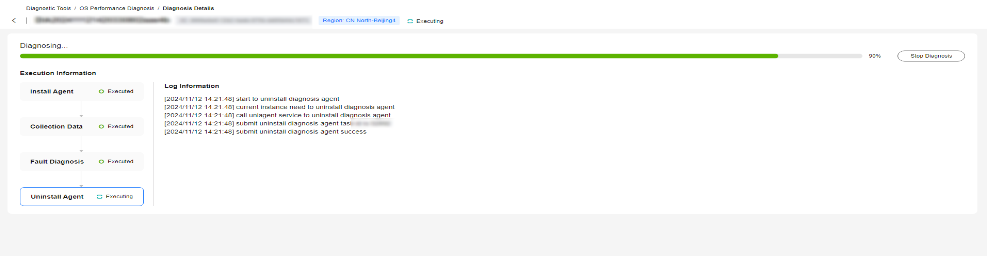
Add | Selected Resources: 1

Before diagnosis, ensure that a UniAgent has been installed on the instance.

☑ I agree to install the plug-in and collect data based on the *Guest OS Diagnosis Service Frontend Data Collection License*.

Step 5 Check the diagnosis step by step. progress bar.

Figure 6-4 Diagnosis in progress



Diagnostic Tools / OS Performance Diagnosis / Diagnosis Details

[redacted] Region: CN North-Beijing4 Executing

Diagnosing...

90%

Execution Information

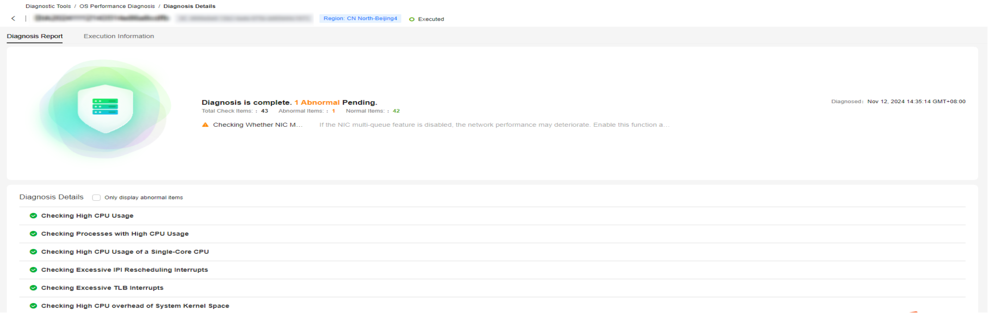
- Install Agent — Executed
- Collection Data — Executed
- Fault Diagnosis — Executed
- Uninstall Agent — Executing

Log Information

```
[2024/11/12 14:21:48] start to uninstall diagnosis agent
[2024/11/12 14:21:48] current instance need to uninstall diagnosis agent
[2024/11/12 14:21:48] call uniagent service to uninstall diagnosis agent
[2024/11/12 14:21:48] submit uninstall diagnosis agent tasl[redacted]
[2024/11/12 14:21:48] submit uninstall diagnosis agent success
```

Step 6 After the diagnosis is complete, view the diagnosis report.

Figure 6-5 Viewing the fiagnosis report



Diagnostic Tools / OS Performance Diagnosis / Diagnosis Details

[redacted] [redacted] Region: CN North-Beijing4 ○ Executed

Diagnosis Report | Execution Information

Diagnosis is complete. 1 Abnormal Pending.
Total Check Items: : 43 Abnormal Items: : 1 Normal Items: : 42

Diagnosed: Nov 12, 2024 14:35:14 GMT+08:00

Checking Whether NIC M... If the NIC multi-queue feature is disabled, the network performance may deteriorate. Enable this function a...

Diagnosis Details □ Only display abnormal items

- Checking High CPU Usage
- Checking Processes with High CPU Usage
- Checking High CPU Usage of a Single-Core CPU
- Checking Excessive IPI Rescheduling Interrupts
- Checking Excessive TLB Interrupts
- Checking High CPU overhead of System Kernel Space

----End

6.2 Alarms

6.2.1 Aggregated Alarms

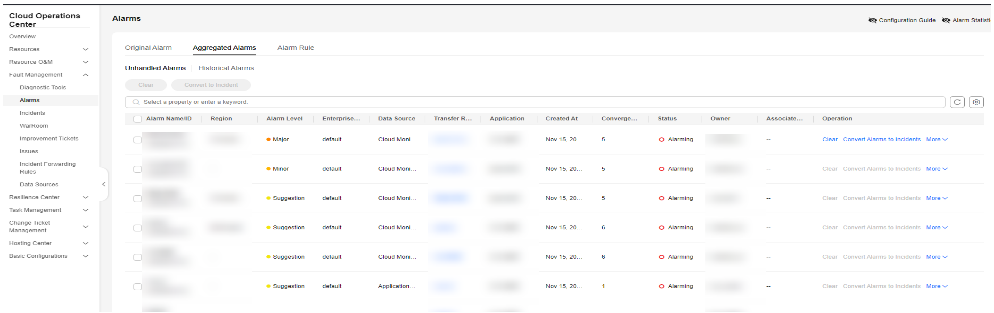
Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Alarms** to view the aggregated alarms and original alarms.

Step 3 On the **Aggregated Alarms** page, search for the alarms by alarm ticket No. or alarm name.

Step 4 Aggregated alarms include current alarms and historical alarms.

Figure 6-6 Alarm list



Alarms

Alarm Name/ID	Region	Alarm Level	Enterprise...	Data Source	Transfer R...	Application	Created At	Converge...	Status	Owner	Associate...	Operation
[redacted]	[redacted]	Major	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
[redacted]		Minor	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
[redacted]	[redacted]	Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
[redacted]	[redacted]	Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	6	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
[redacted]		Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	6	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
[redacted]		Suggestion	default	Application...	[redacted]	[redacted]	Nov 15, 20...	1	Alarming	[redacted]	--	Clear Convert Alarms to Incidents More

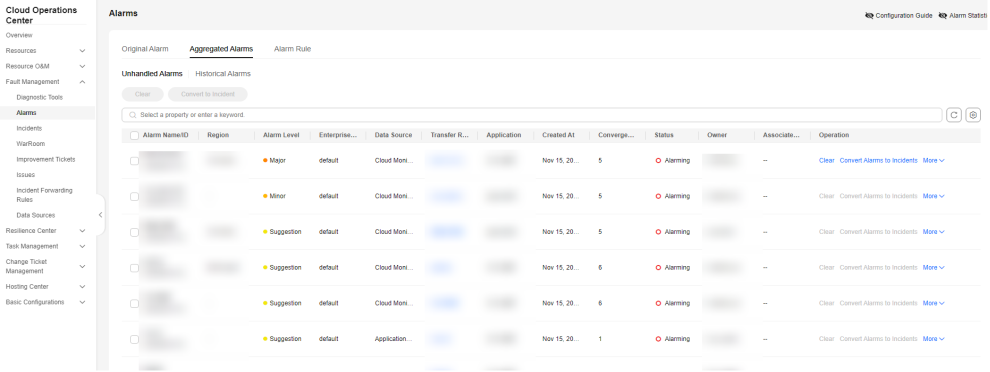
----End

6.2.1.1 Handling Alarms

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Alarms**. On the displayed page, click **Aggregated alarm** > **Unhandled Alarms** tabs. Locate the target alarm record, choose **More** > **handle** in the **Operation** column.

Figure 6-7 Handling alarms



Cloud Operations Center

- Overview
- Resources
- Resource O&M
- Fault Management
  - Diagnostic Tools
  - Alarms
  - Incidents
  - WarRoom
  - Improvement Tickets
  - Issues
  - Incident Forwarding Rules
  - Data Sources
- Resilience Center
- Task Management
- Change Ticket Management
- Hosting Center
- Basic Configurations

Alarms

Configuration Guide Alarm Statisti

Original Alarm | Aggregated Alarms | Alarm Rule

Unhandled Alarms | Historical Alarms

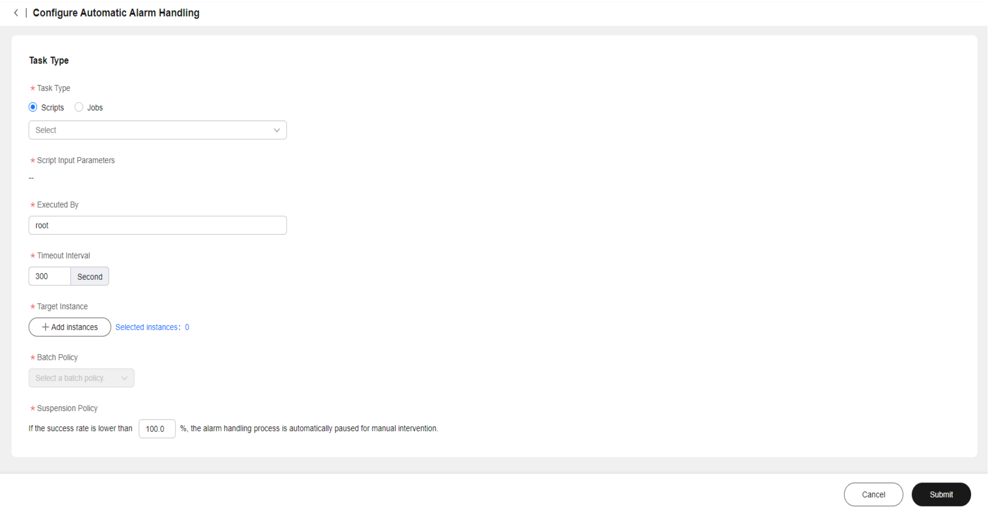
Clear | Convert to Incident

Select a property or enter a keyword.

□	Alarm Name/ID	Region	Alarm Level	Enterprise...	Data Source	Transfer R...	Application	Created At	Converge...	Status	Owner	Associate...	Operation
□	[redacted]	[redacted]	● Major	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
□	[redacted]		● Minor	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
□	[redacted]	[redacted]	● Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	5	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
□	[redacted]	[redacted]	● Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	6	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
□	[redacted]		● Suggestion	default	Cloud Moni...	[redacted]	[redacted]	Nov 15, 20...	6	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More
□	[redacted]		● Suggestion	default	Application...	[redacted]	[redacted]	Nov 15, 20...	1	○ Alarming	[redacted]	--	Clear Convert Alarms to Incidents More

Step 3 On the displayed page, configure the parameters and click **Submit**.

Figure 6-8 Handling an alarm



Configure Automatic Alarm Handling

Task Type

* Task Type
● Scripts ○ Jobs
Select

* Script Input Parameters
--

* Executed By
root

* Timeout Interval
300 Second

* Target Instance
Add instances Selected instances: 0

* Batch Policy
Select a batch policy.

* Suspension Policy
If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

Cancel Submit

NOTE

- If you select **Scripts**, configure the parameters by referring to **Executing Custom Scripts** and **Executing Common Scripts**.
- If you select **Jobs**, configure the parameters by referring to **Executing a Custom Job** and **Executing a Common Job**.

----End

6.2.1.2 Converting an Alarm to an Incident

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Alarms**. On the displayed page, click **Aggregated alarm** > **Unhandled Alarms** tabs.

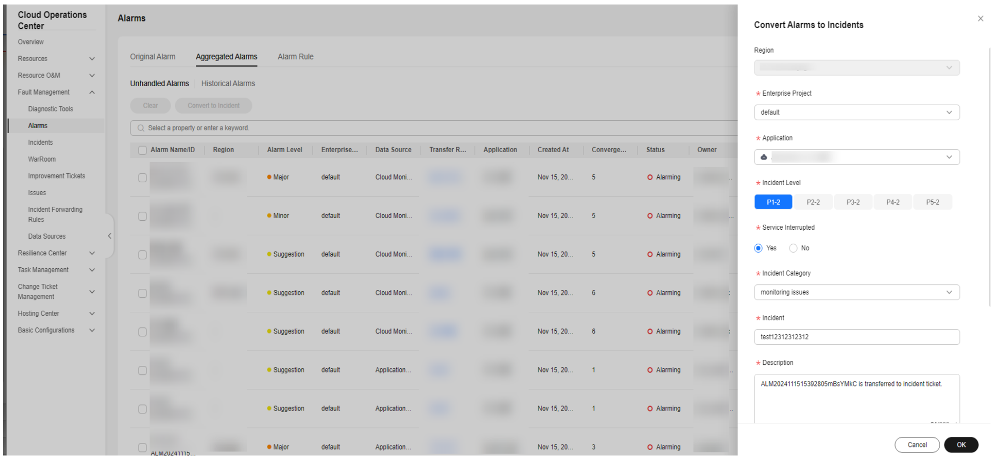
Step 3 Locate the target alarms and click **Convert Alarms to Incidents**.

NOTE

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

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

Figure 6-9 Converting alarms to incidents



Convert Alarms to Incidents

Region

* Enterprise Project: default

* Application

* Incident Level: P1-2 (selected) P2-2 P3-2 P4-2 P5-2

* Service Interrupted: ● Yes ○ No

* Incident Category: monitoring issues

* Incident: test12312312312

* Description: ALM2024111515392805mBsYMkC is transferred to incident ticket.

Cancel OK

NOTE

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

----End

6.2.1.3 Clearing Alarms

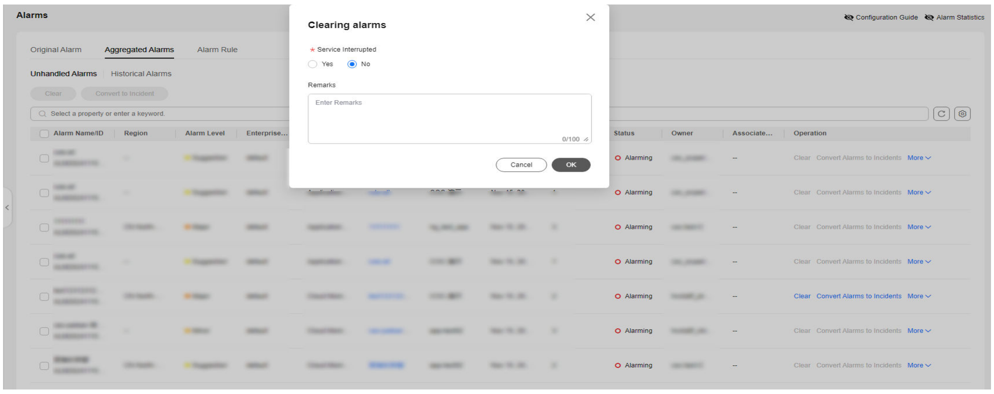
Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Alarms**. On the displayed page, click **Aggregated alarm** > **Unhandled Alarms** tabs.

Step 3 Select the alarms to be deleted and click **Clear** in the **Operation** column or above the alarm list.

Step 4 Set **Service interrupted**. If you select **No**, go to step 5. If you select **Yes**, you must set **Fault occurrence time** and **Fault recovery time**. The service interruption time is included in the SLO interruption record of the corresponding application.

Figure 6-10 Clearing Alarms - Service Interruption



Clearing alarms

* Service Interrupted: ○ Yes ● No

Remarks: Enter Remarks 0/100

Cancel OK

NOTE

To generate an SLO interruption record, you need to set the corresponding SLA rule and SLO rule, and the alarm has the corresponding SLA record.

Step 5 Enter the remarks and click **OK** to clear the alarms.

NOTE

The remarks can contain at most 100 characters, including letters, digits, and special characters.

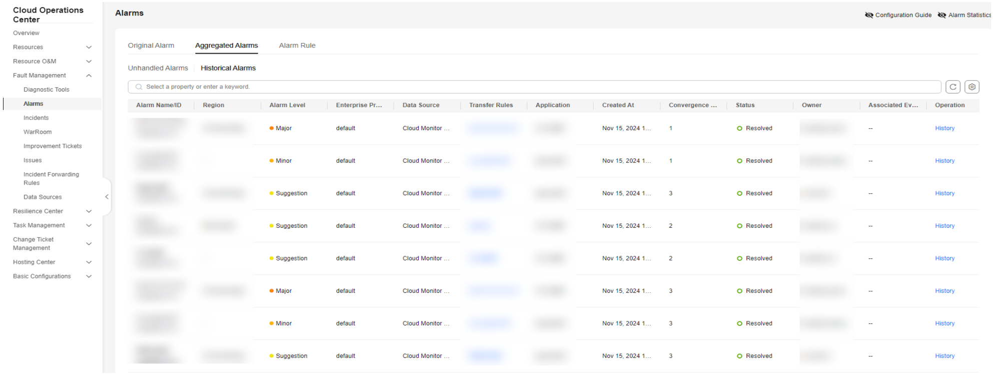
----End

6.2.1.4 Historical Alarms

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Alarms**. On the displayed page, click **Aggregated alarm** > **Unhandled Alarms** tabs.

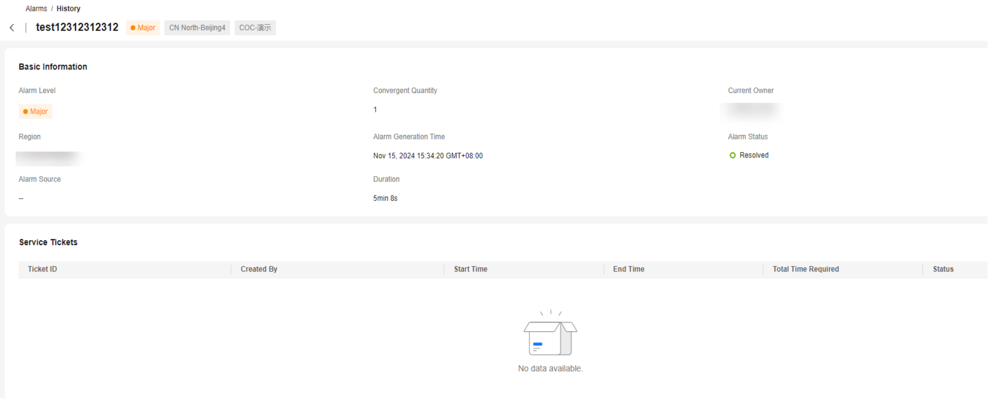
Figure 6-11 Historical alarm list



Alarm Name/ID	Region	Alarm Level	Enterprise Pr...	Data Source	Transfer Rules	Application	Created At	Convergence ...	Status	Owner	Associated Ev...	Operation
[redacted]	[redacted]	● Major	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	1	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Minor	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	1	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Suggestion	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	3	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Suggestion	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	2	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Suggestion	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	2	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Major	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	3	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Minor	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	3	○ Resolved	[redacted]	--	History
[redacted]	[redacted]	● Suggestion	default	Cloud Monitor ...	[redacted]	[redacted]	Nov 15, 2024 1...	3	○ Resolved	[redacted]	--	History

Step 3 Locate the target alarm, and click **More** > **History** in the **Operation** column to view the historical records.

Figure 6-12 Historical records of an alarm



Basic Information

Alarm Level: ● Major

Convergent Quantity: 1

Current Owner: [redacted]

Region: [redacted]

Alarm Generation Time: Nov 15, 2024 15:34:20 GMT+08:00

Alarm Status: ○ Resolved

Alarm Source: --

Duration: 5min 8s

Service Tickets

Ticket ID	Created By	Start Time	End Time	Total Time Required	Status

No data available.

----End

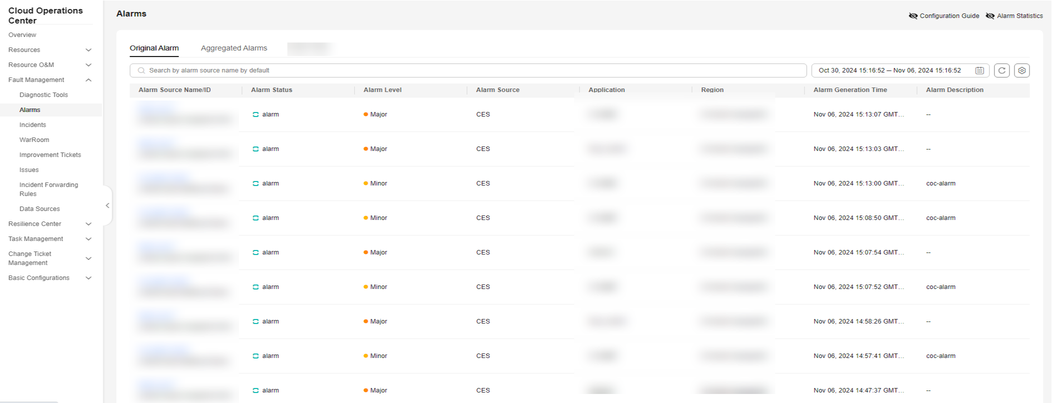
6.2.2 Original Alarms

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Alarms**. On the displayed page, click **Original alarm**.

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

Figure 6-13 Original alarms



Alarm Source Name/ID	Alarm Status	Alarm Level	Alarm Source	Application	Region	Alarm Generation Time	Alarm Description
[redacted]	alarm	● Major	CES	[redacted]	[redacted]	Nov 06, 2024 15:13:07 GMT...	--
[redacted]	alarm	● Major	CES	[redacted]	[redacted]	Nov 06, 2024 15:13:03 GMT...	--
[redacted]	alarm	● Minor	CES	[redacted]	[redacted]	Nov 06, 2024 15:13:00 GMT...	coc-alarm
[redacted]	alarm	● Minor	CES	[redacted]	[redacted]	Nov 06, 2024 15:08:50 GMT...	coc-alarm
[redacted]	alarm	● Major	CES	[redacted]	[redacted]	Nov 06, 2024 15:07:54 GMT...	--
[redacted]	alarm	● Minor	CES	[redacted]	[redacted]	Nov 06, 2024 15:07:52 GMT...	coc-alarm
[redacted]	alarm	● Major	CES	[redacted]	[redacted]	Nov 06, 2024 14:58:26 GMT...	--
[redacted]	alarm	● Minor	CES	[redacted]	[redacted]	Nov 06, 2024 14:57:41 GMT...	coc-alarm
[redacted]	alarm	● Major	CES	[redacted]	[redacted]	Nov 06, 2024 14:47:37 GMT...	--

----End

6.3 Incident Management

Incidents manage all incidents of applications, including incident acceptance and rejection, ticket transfer, processing, and closing. Incidents can be generated based on transfer rules, or created by users or based on alarms.

You can also configure SLA rules. For details about how to configure SLA rules, see **SLA Management**.

6.3.1 Incidents

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

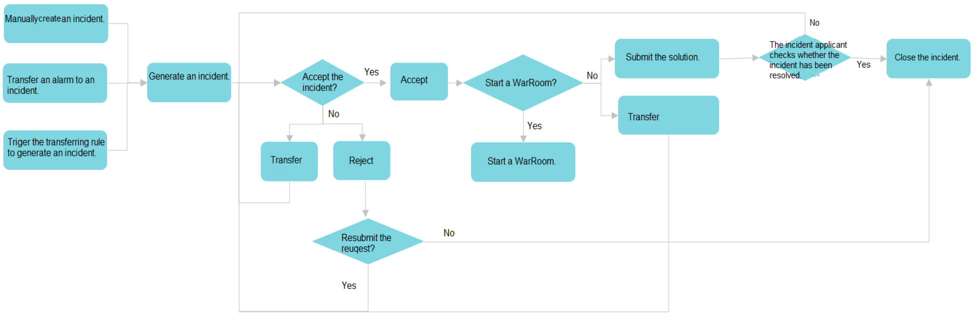
After an incident ticket is rejected, it becomes the rejected state. The creator can close the incident or update the incident information and submit it again.

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.

For details about how to add the incident-level suspension function, see **Reviewing an Incident**.

Figure 6-14 Incident flowchart


Manuallycreatean incident.
Transfer an alarm to an incident.
Triger the transferring rule to generate an incident.
Generate an incident.
Accept the incident?
Yes
Accept
Start a WarRoom?
No
Submit the solution.
Transfer
Yes
Start a WarRoom.
No
The incident applicant checks whether the incident has been resolved.
Yes
Close the incident.
No
Transfer
Reject
Resubmit the reuqest?
No
Yes

6.3.2 Creating an Incident

Scenarios

Create an incident ticket using Cloud Operations Center.

Prerequisites

You have created an application by referring to **Application Management**.

Precautions

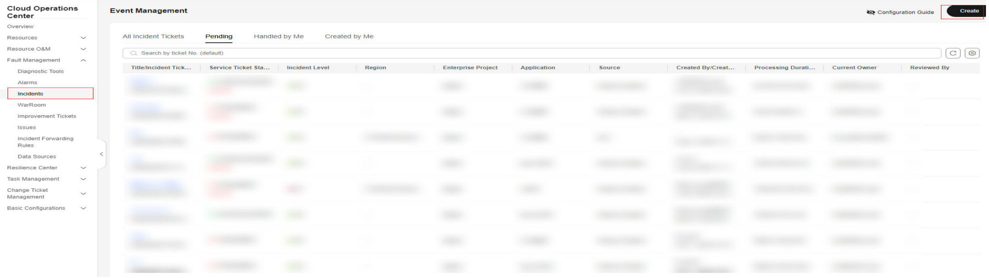
Create an incident service ticket.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**. On the displayed page, click **Create**.

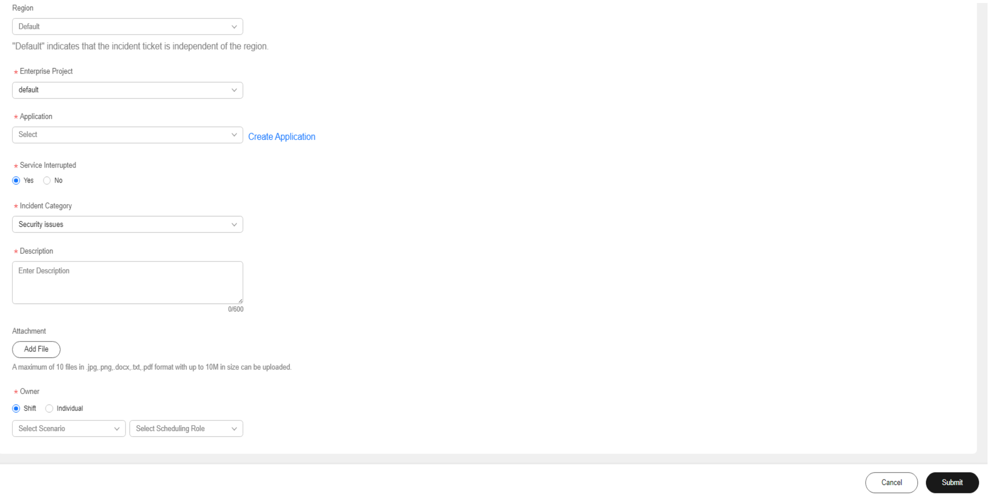
Figure 6-15 Incident ticket list



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

If no shift is available for the owner, create a schedule in **Overview**.

Figure 6-16 Creating an incident service ticket



Region: Default

"Default" indicates that the incident ticket is independent of the region.

* Enterprise Project: default

* Application: Select

* Service Interrupted: ● Yes ○ No

* Incident Category: Security issues

* Description: Enter Description 0/600

Attachment

A maximum of 10 files in .jpg,.png,.docx,.txt,.pdf format with up to 10M in size can be uploaded.

* Owner: ● Shift ○ Individual

Select Scenario

Select Scheduling Role

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

6.3.3 Handling an Incident

6.3.3.1 Rejecting an Incident

Scenarios

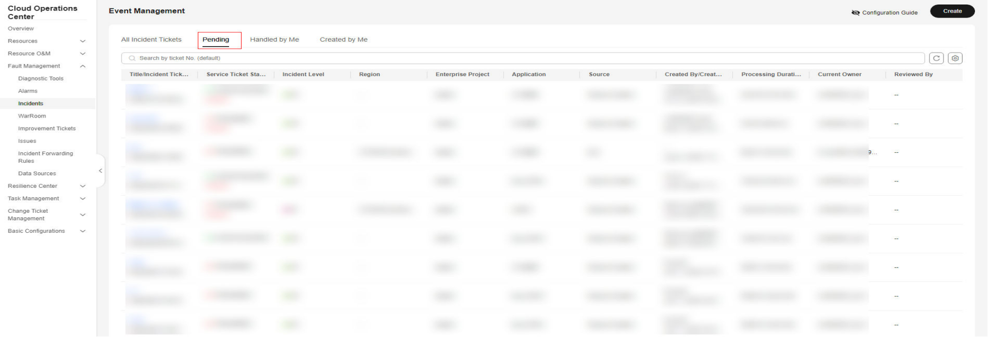
If an incident is unreasonable, the incident handler can reject the incident.

Procedure

Step 1 Log in to **COC**.

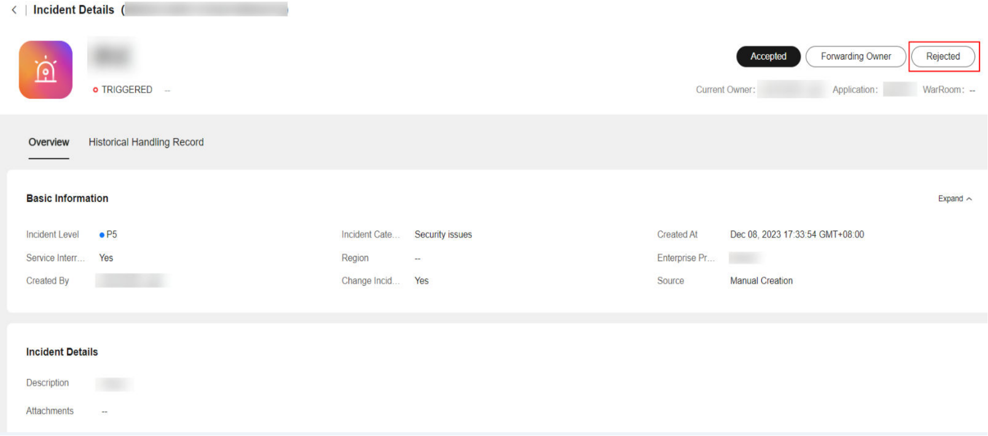
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-17 List of incidents to be handled



Step 3 Click **Rejected**.

Figure 6-18 Rejecting an incident



Incident Level ● P5

Incident Cate... Security issues

Created At Dec 08, 2023 17:33:54 GMT+08:00

Service Interr... Yes

Region --

Enterprise Pr...

Created By

Change Incid... Yes

Source Manual Creation

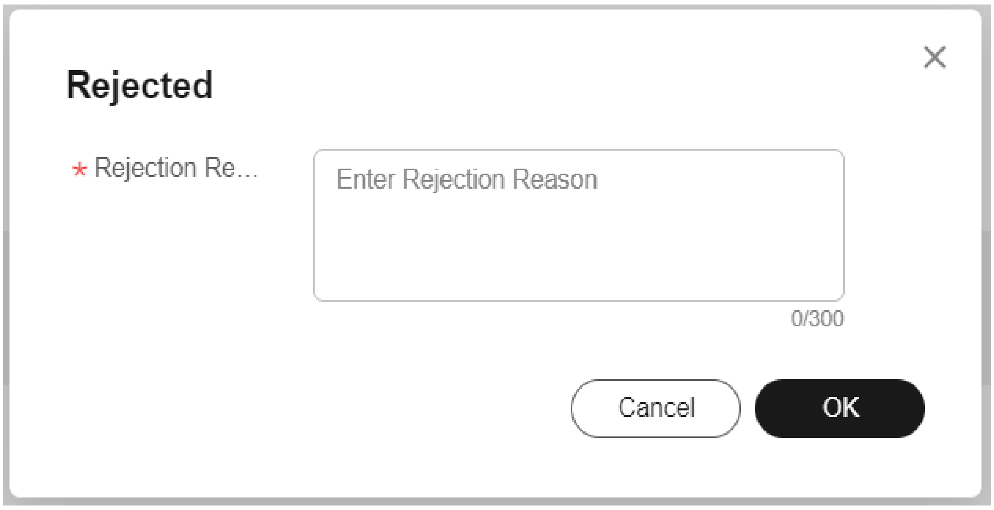
Incident Details

Description

Attachments --

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

Figure 6-19 Entering a reason for rejection



----End

6.3.3.2 Resubmitting an Incident After Rejection

Scenarios

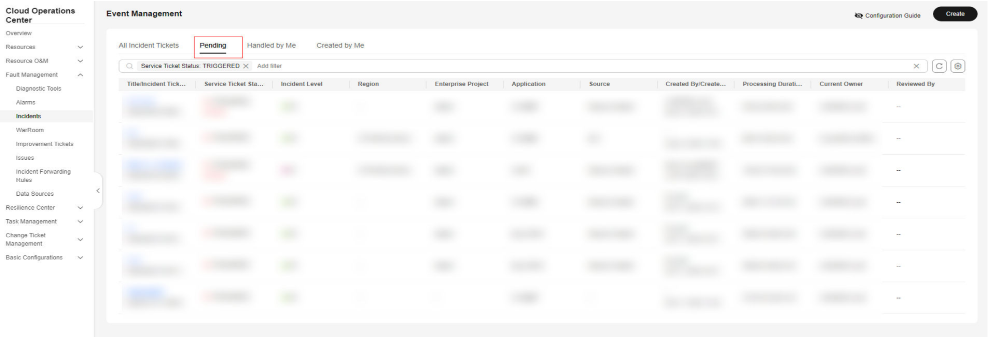
After an incident ticket is rejected, modify the incident ticket content.

Procedure

Step 1 Log in to **COC**.

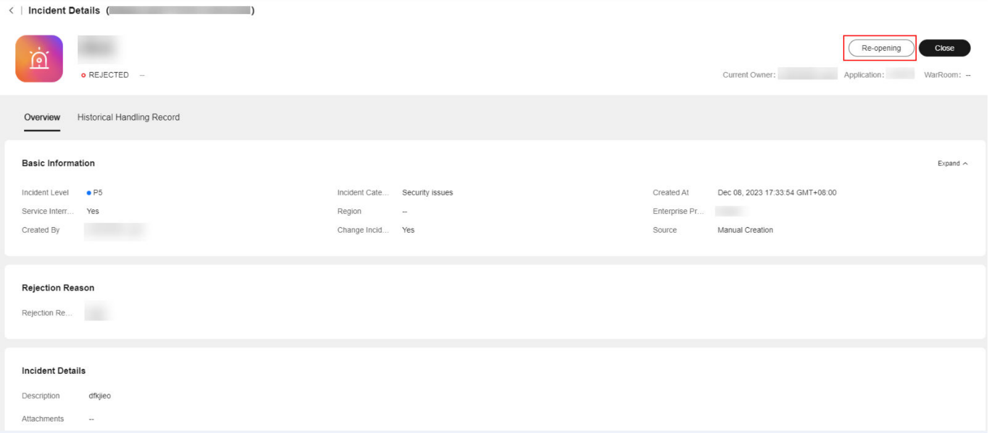
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-20 Incident details



Step 3 Click **Re-opening**.

Figure 6-21 Restarting an incident



Basic Information

Incident Level ● P5
Incident Cate... Security issues
Created At Dec 08, 2023 17:33:54 GMT+08:00
Service Interr... Yes
Region --
Enterprise Pr...
Created By
Change Incid... Yes
Source Manual Creation

Rejection Reason

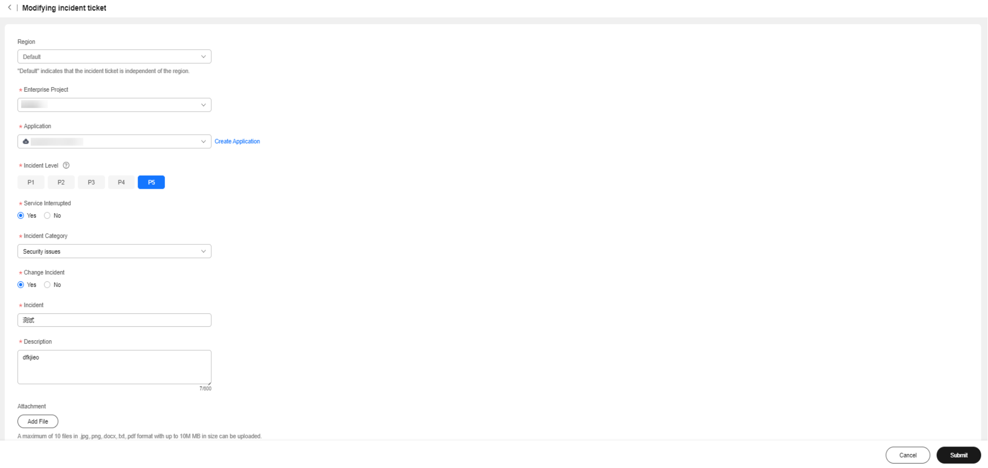
Rejection Re...

Incident Details

Description dfkjieo
Attachments --

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

Figure 6-22 Modifying the content of an incident ticket



Region: Default

"Default" indicates that the incident ticket is independent of the region.

* Enterprise Project

* Application

* Incident Level: P1 P2 P3 P4 [✓ P5]

* Service Interrupted: ● Yes ○ No

* Incident Category: Security issues

* Change Incident: ● Yes ○ No

* Incident: 测试

* Description: dfkjieo

7/800

Attachment

A maximum of 10 files in .jpg,.png,.docx,.txt,.pdf format with up to 10M MB in size can be uploaded.

----End

6.3.3.3 Forwarding Incidents

Scenarios

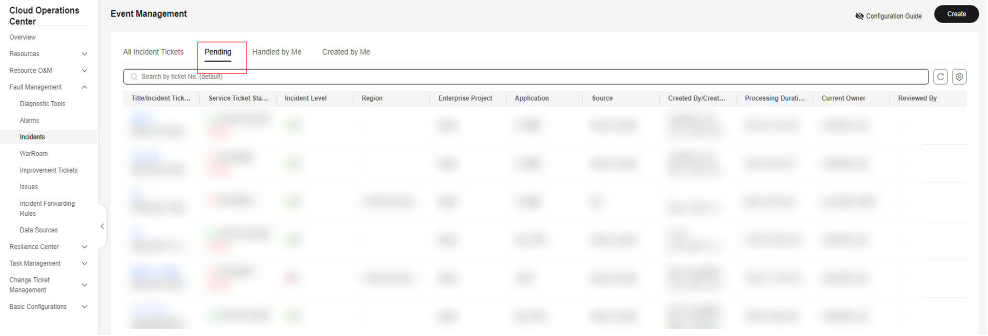
Forward the incident ticket to another person for processing.

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.

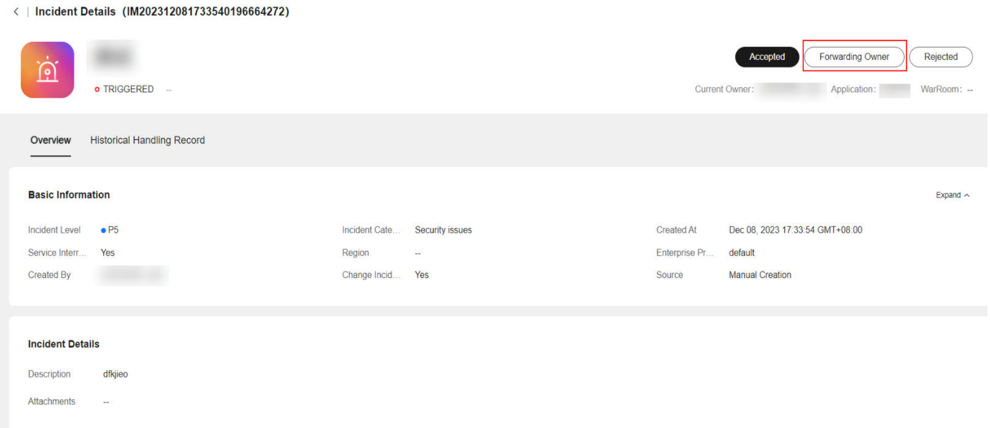
Figure 6-23 Incident details



Title/Incident Tick...	Service Ticket Sta...	Incident Level	Region	Enterprise Project	Application	Source	Created By/Creat...	Processing Durati...	Current Owner	Reviewed By

Step 3 Click **Forwarding Owner**.

Figure 6-24 Transferring the owner



Incident Details (IM20231208173354019664272)

[redacted]

TRIGGERED --

Accepted | Forwarding Owner | Rejected

Current Owner: [redacted] Application: [redacted] WarRoom: --

Overview | Historical Handling Record

Basic Information Expand ^

Incident Level	● P5	Incident Cate...	Security issues	Created At	Dec 08, 2023 17:33:54 GMT+08:00
Service Interr...	Yes	Region	--	Enterprise Pr...	default
Created By	[redacted]	Change Incid...	Yes	Source	Manual Creation

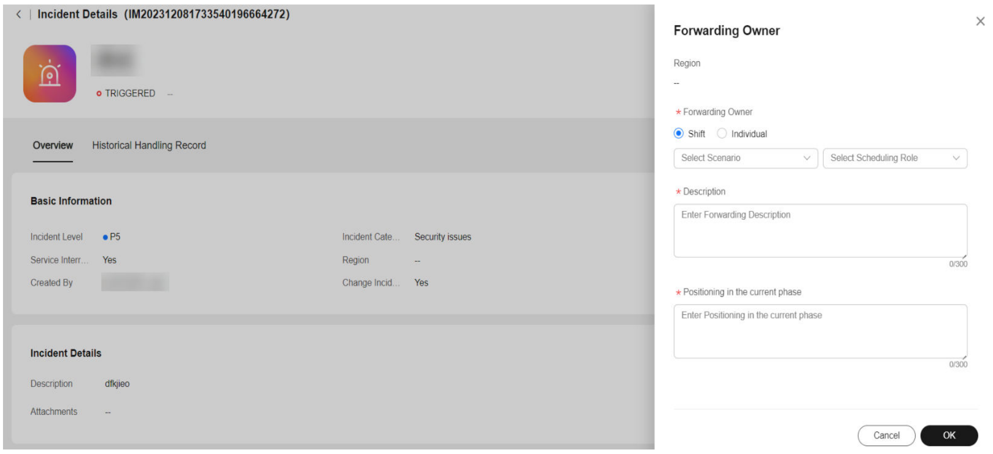
Incident Details

Description dfkjieo

Attachments --

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

Figure 6-25 Entering forwarding information



Incident Details (IM20231208173354019664272)

[redacted]

TRIGGERED --

Overview | Historical Handling Record

Basic Information

Incident Level	● P5	Incident Cate...	Security issues
Service Interr...	Yes	Region	--
Created By	[redacted]	Change Incid...	Yes

Incident Details

Description dfkjieo

Attachments --

Forwarding Owner

Region

--

* Forwarding Owner

● Shift ○ Individual

Select Scenario | Select Scheduling Role

* Description

Enter Forwarding Description

0/300

* Positioning in the current phase

Enter Positioning in the current phase

0/300

Cancel | OK

----End

6.3.3.4 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.

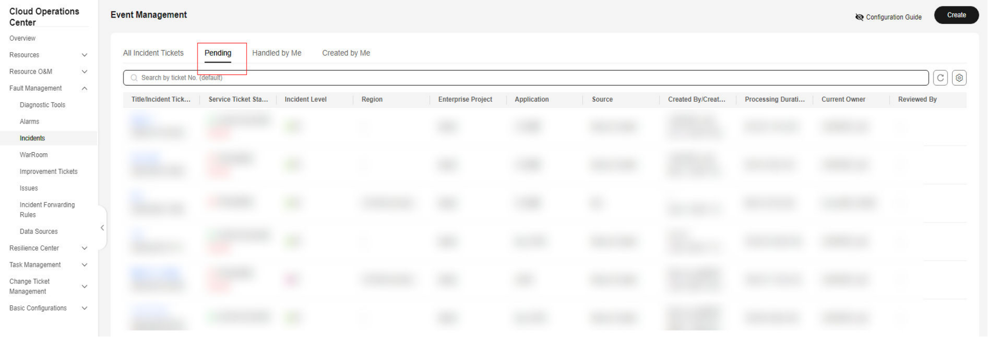
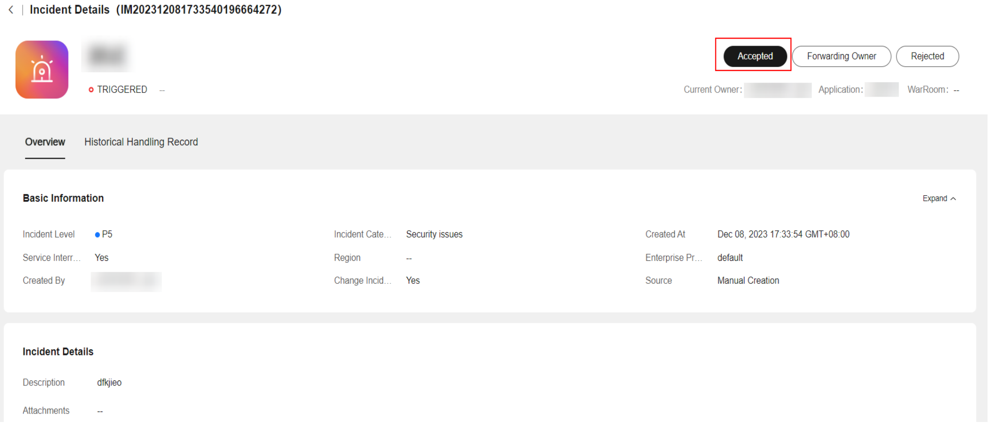


Figure 6-26 Incident details

Step 3 Click **Accepted**.



Incident Details (IM202312081733540196664272)

TRIGGERED --

Current Owner:
Application:
WarRoom: --

Basic Information

Incident Level ● P5
Service Interr... Yes
Created By
Incident Cate... Security issues
Region --
Change Incid... Yes
Created At Dec 08, 2023 17:33:54 GMT+08:00
Enterprise Pr... default
Source Manual Creation

Incident Details

Description dfkjieo
Attachments --

Figure 6-27 Handling an incident

----End

6.3.3.5 Upgrading/Downgrading an Incident

Scenarios

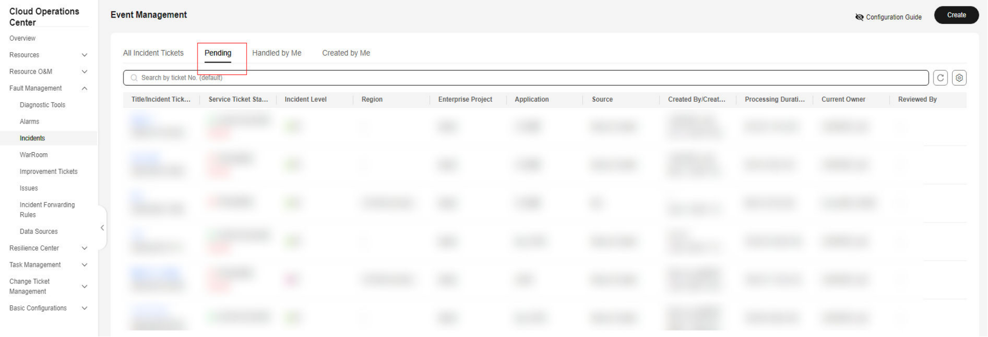
The incident ticket level is inconsistent with the actual situation. The incident level can be modified only after the incident is accepted.

Procedure

Step 1 Log in to **COC**.

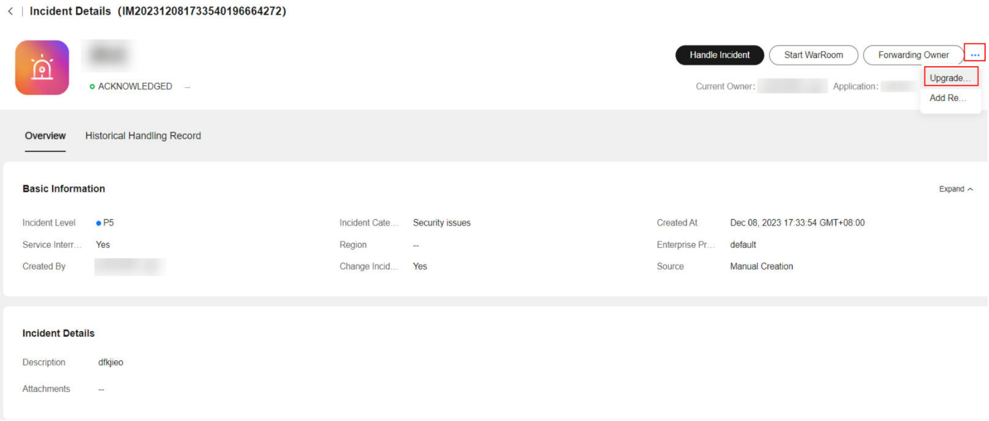
Step 2 In the navigation pane on the left, choose **Fault Management** > **Incidents**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-28 Incident details



Step 3 Click the **...** icon and choose **Upgrade/Downgrade**.

Figure 6-29 Upgrading/downgrading an incident



Incident Details (IM20231208173354019666 4272)

ACKNOWLEDGED --

Current Owner:

Application:

Basic Information

Incident Level ● P5

Incident Cate... Security issues

Created At Dec 08, 2023 17:33:54 GMT+08:00

Service Interr... Yes

Region --

Enterprise Pr... default

Created By

Change Incid... Yes

Source Manual Creation

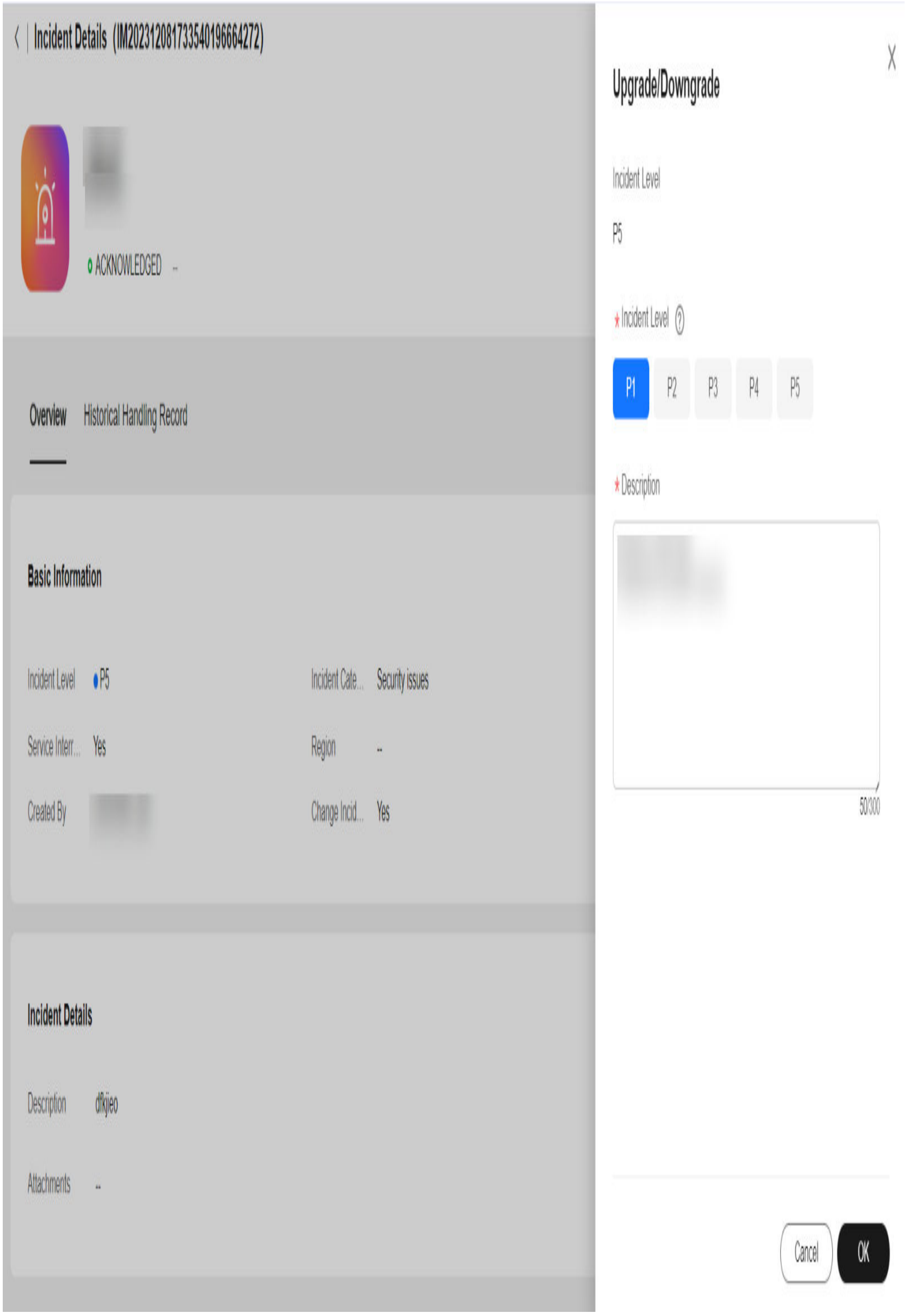
Incident Details

Description dfkjieo

Attachments --

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

Figure 6-30 Entering upgrade and downgrade information



----End

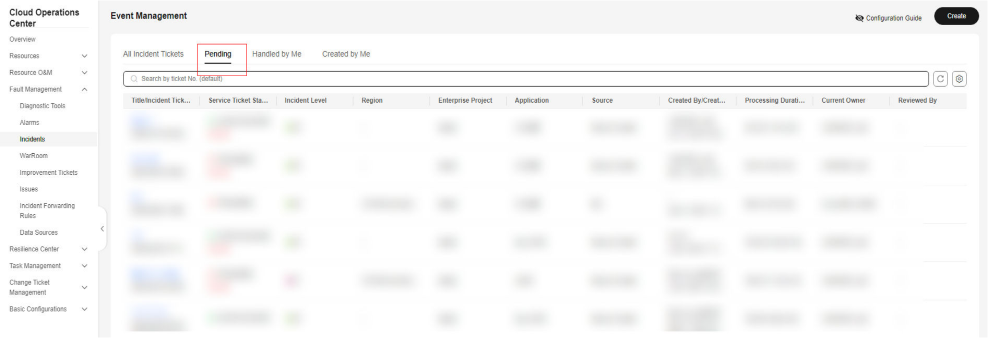
6.3.3.6 Adding Remarks

Procedure

Step 1 Log in to **COC**.

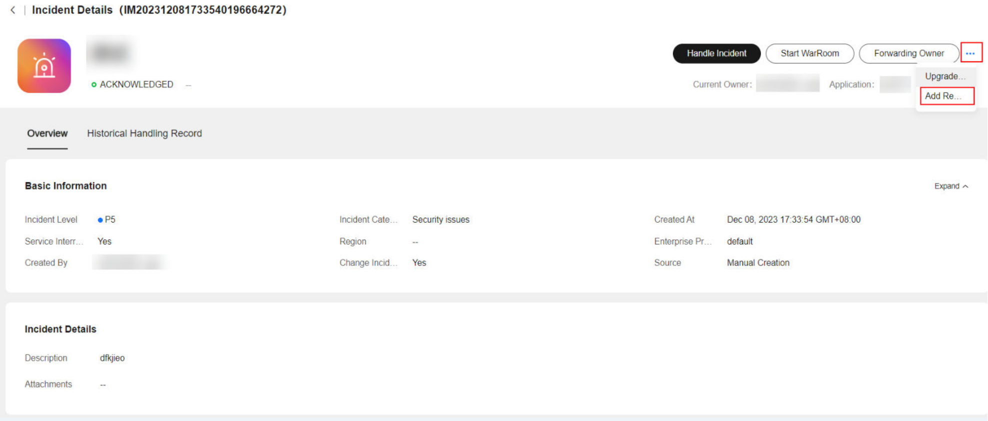
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-31 Incident details



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

Figure 6-32 Adding remarks



Basic Information

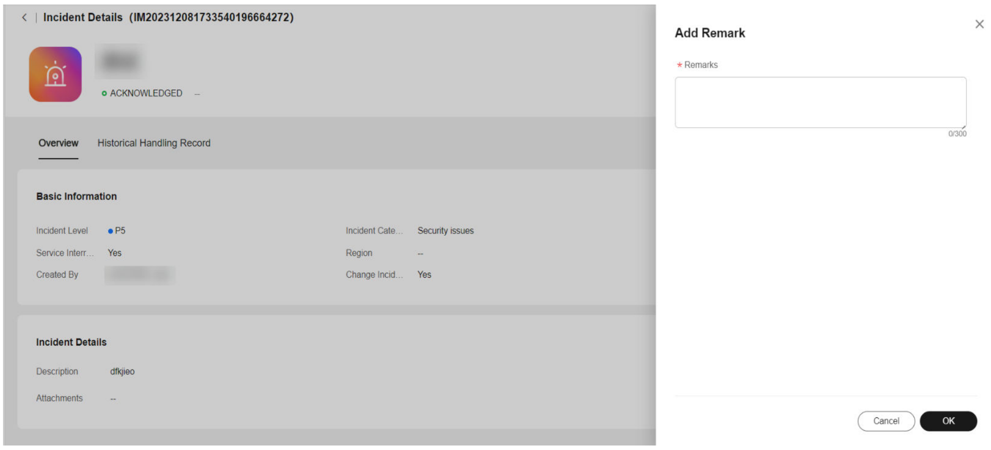
Incident Level ● P5
Incident Cate... Security issues
Created At Dec 08, 2023 17:33:54 GMT+08:00
Service Interr... Yes
Region --
Enterprise Pr... default
Created By
Change Incid... Yes
Source Manual Creation

Incident Details

Description dfkjieo
Attachments --

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

Figure 6-33 Entering remarks information


Incident Details (IM202312081733540196664272)
ACKNOWLEDGED
Overview
Historical Handling Record
Add Remark
* Remarks
0/300
Cancel
OK

Basic Information

Incident Level ● P5
Incident Cate... Security issues
Service Interr... Yes
Region --
Created By
Change Incid... Yes

Incident Details

Description dfkjieo
Attachments --

----End

6.3.3.7 Starting a War Room

Scenarios

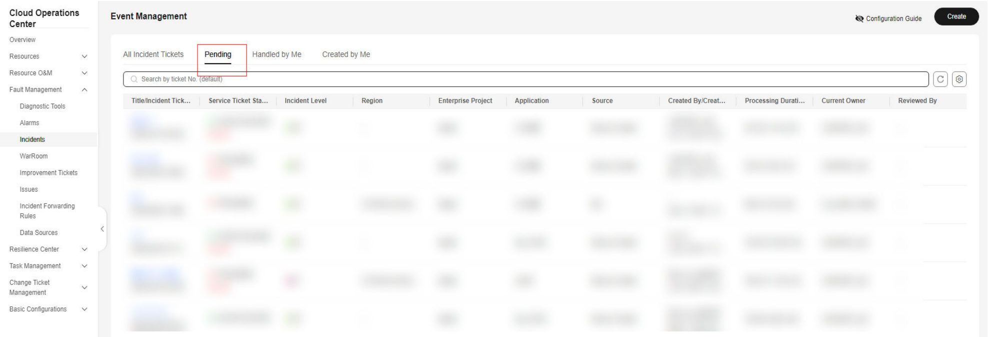
Start a war room for critical incident to recovery the incident quickly.

Procedure

Step 1 Log in to COC.

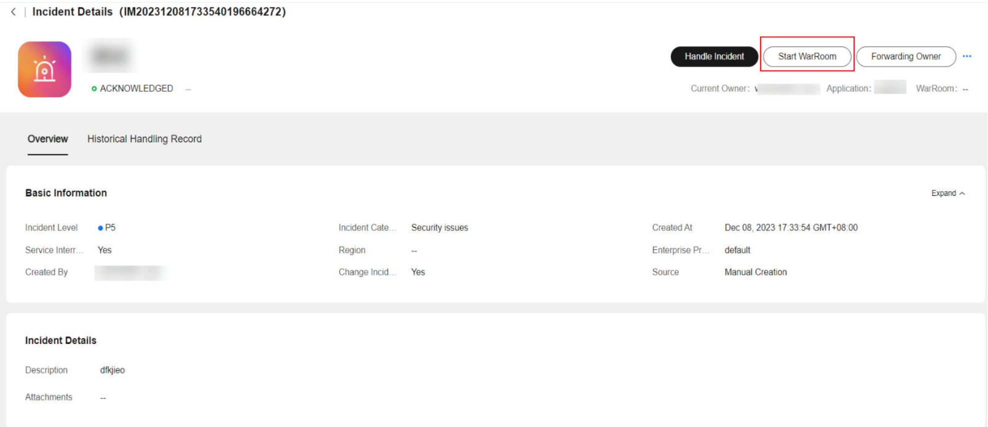
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-34 Incident ticket details



Step 3 Click **Start WarRoom**.

Figure 6-35 Starting a war room



Incident Details (IM202312081733540196664272)

ACKNOWLEDGED --

Current Owner: v

Application:

WarRoom: --

Basic Information

Incident Level	● P5	Incident Cate...	Security issues	Created At	Dec 08, 2023 17:33:54 GMT+08:00
Service Interr...	Yes	Region	--	Enterprise Pr...	default
Created By		Change Incid...	Yes	Source	Manual Creation

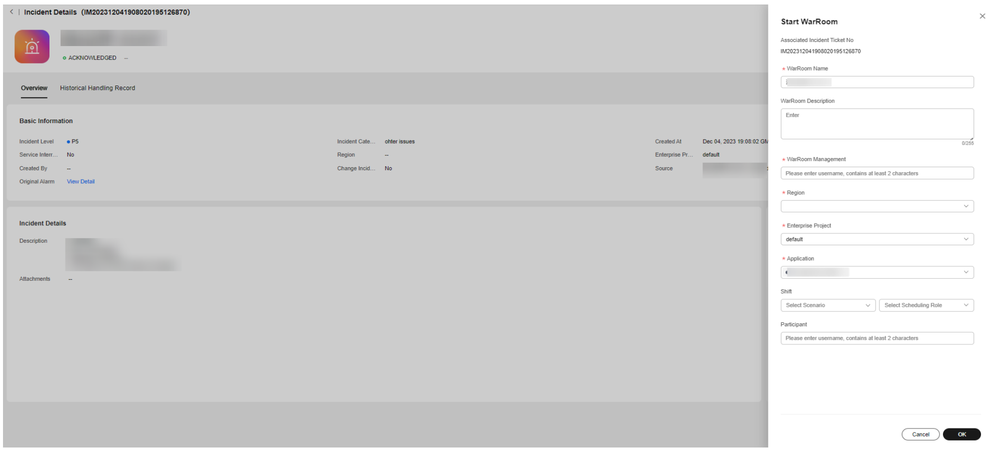
Incident Details

Description dfkjieo

Attachments --

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

Figure 6-36 Entering war room information



< | Incident Details (IM202312041908020195126870)

ACKNOWLEDGED --

Overview | Historical Handling Record

Basic Information

Incident Level	P5	Incident Cate...	ohter issues	Created At	Dec 04, 2023 19:08:02 GM
Service Interr...	No	Region	--	Enterprise Pr...	default
Created By	--	Change Incid...	No	Source	
Original Alarm	View Detail				

Incident Details

Description

Attachments --

Start WarRoom

Associated Incident Ticket No
IM202312041908020195126870

* WarRoom Name

WarRoom Description
Enter
0/255

* WarRoom Management
Please enter username, contains at least 2 characters

* Region

* Enterprise Project
default

* Application

Shift
Select Scenario | Select Scheduling Role

Participant
Please enter username, contains at least 2 characters

Cancel | OK

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 App 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

6.3.3.8 Handling an Incident

Scenarios

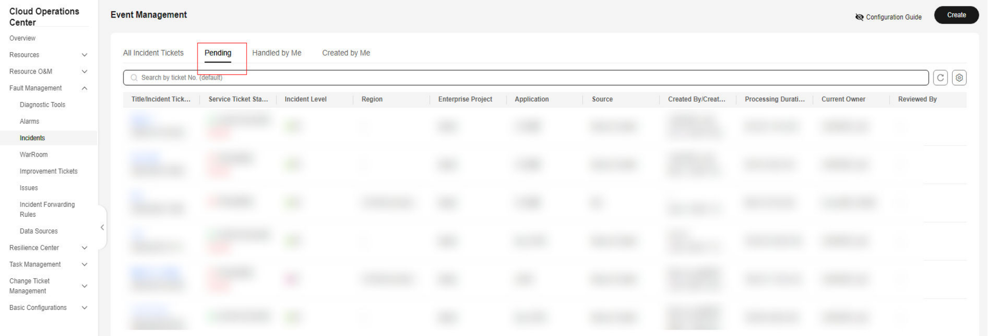
Handle the incident ticket after accepting the incident.

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.

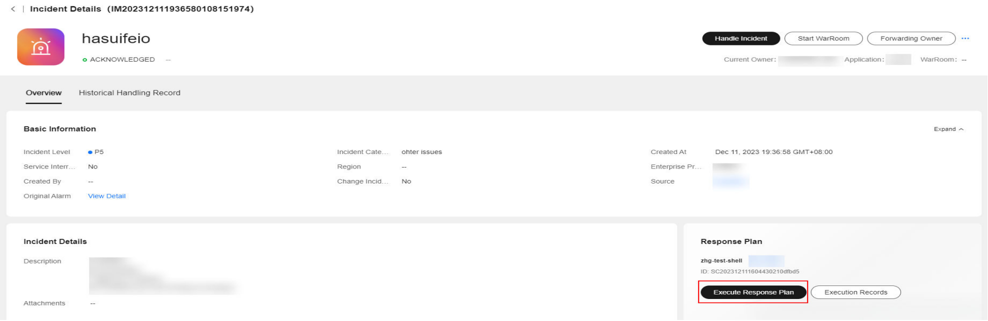
Figure 6-37 Incident details



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 6-38 Executing the response plan



< | Incident Details (IM202312111936580108151974)

hasuifeio

ACKNOWLEDGED --

Current Owner: Application: WarRoom: --

Basic Information

Incident Level: P5
Service Interr...: No
Created By: --
Original Alarm: View Detail
Incident Cate...: ohter issues
Region: --
Change Incid...: No
Created At: Dec 11, 2023 19:36:58 GMT+08:00
Enterprise Pr...:
Source:

Incident Details

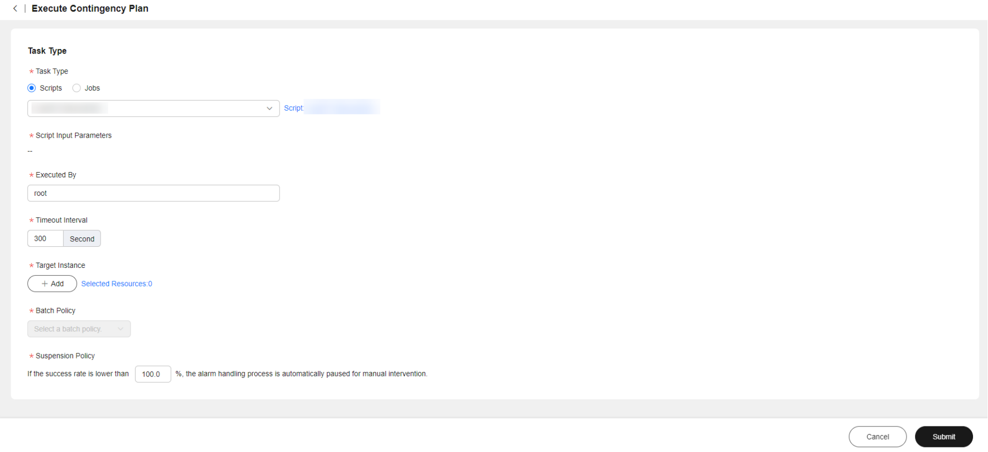
Description:
Attachments: --

Response Plan

zhg-test-shell
ID: SC202312111604430210dfbd5

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

Figure 6-39 Page for executing a job or script



< | Execute Contingency Plan

Task Type

* Task Type
● Scripts ○ Jobs
Script:

* Script Input Parameters
--

* Executed By
root

* Timeout Interval
300 Second

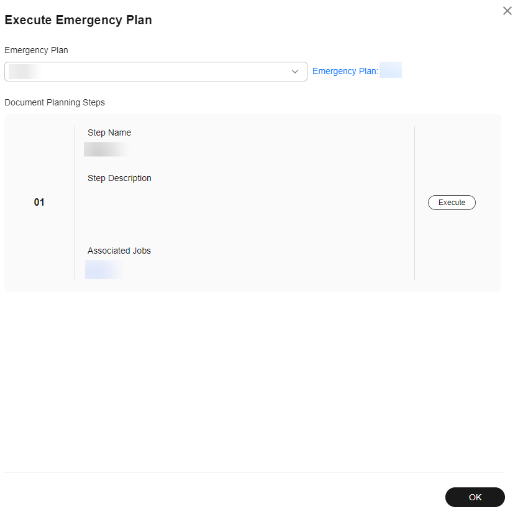
* Target Instance
+ Add Selected Resources:0

* Batch Policy
Select a batch policy.

* Suspension Policy
If the success rate is lower than 100.0 %, the alarm handling process is automatically paused for manual intervention.

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 6-40 Executing a contingency plan



Execute Emergency Plan

Emergency Plan

Emergency Plan:

Document Planning Steps

01

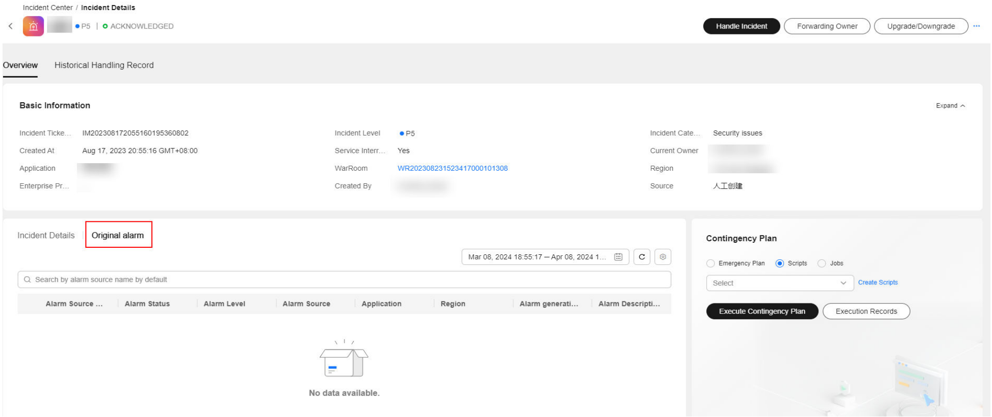
Step Name

Step Description

Associated Jobs

Step 5 View the original alarms associated with the incident.

Figure 6-41 Viewing the alarm associated with an incident



Incident Center / Incident Details

● P5 | ACKNOWLEDGED

Overview | Historical Handling Record

Basic Information

Incident Ticke...	IM20230817205516019536080 2	Incident Level	● P5	Incident Cate...	Security issues
Created At	Aug 17, 2023 20:55:16 GMT+08:00	Service Interr...	Yes	Current Owner	
Application		WarRoom	WR20230823152341700010130 8	Region	
Enterprise Pr...		Created By		Source	人工创建

Incident Details | Original alarm

Mar 08, 2024 18:55:17 – Apr 08, 2024 1...

Search by alarm source name by default

Alarm Source ...	Alarm Status	Alarm Level	Alarm Source	Application	Region	Alarm generati...	Alarm Descripti...

No data available.

Contingency Plan

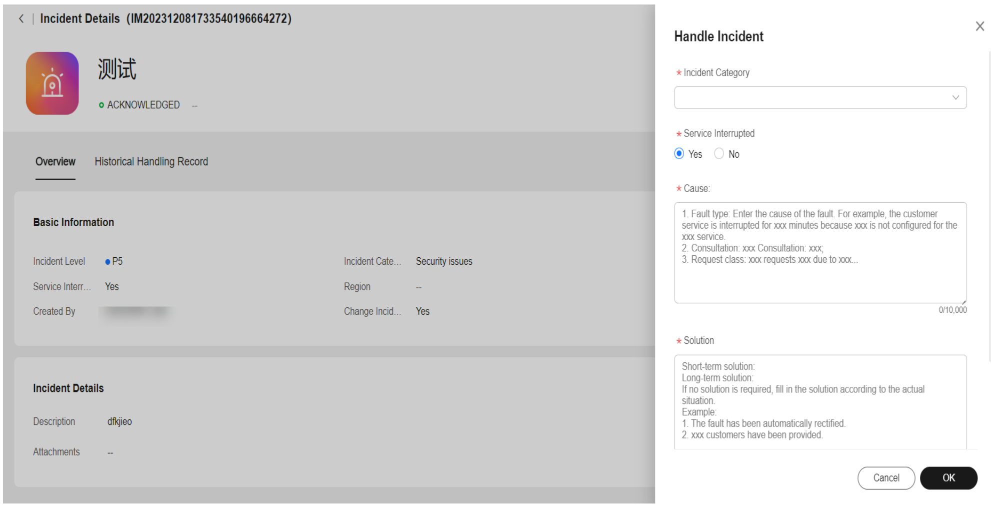
○ Emergency Plan ● Scripts ○ Jobs

Select

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

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

Figure 6-42 Incident handling



< | Incident Details (IM202312081733540196664272)

测试

ACKNOWLEDGED --

Overview | Historical Handling Record

Basic Information

Incident Level	P5	Incident Cate...	Security issues
Service Interr...	Yes	Region	--
Created By	[redacted]	Change Incid...	Yes

Incident Details

Description: dfkjieo

Attachments: --

Handle Incident

* Incident Category

* Service Interrupted

● Yes ○ No

* Cause:

1. Fault type: Enter the cause of the fault. For example, the customer service is interrupted for xxx minutes because xxx is not configured for the xxx service.
2. Consultation: xxx Consultation: xxx;
3. Request class: xxx requests xxx due to xxx...

0/10,000

* Solution

Short-term solution:
Long-term solution:
If no solution is required, fill in the solution according to the actual situation.
Example:
1. The fault has been automatically rectified.
2. xxx customers have been provided.

Cancel | OK

----End

6.3.3.9 Verifying Incident

Scenarios

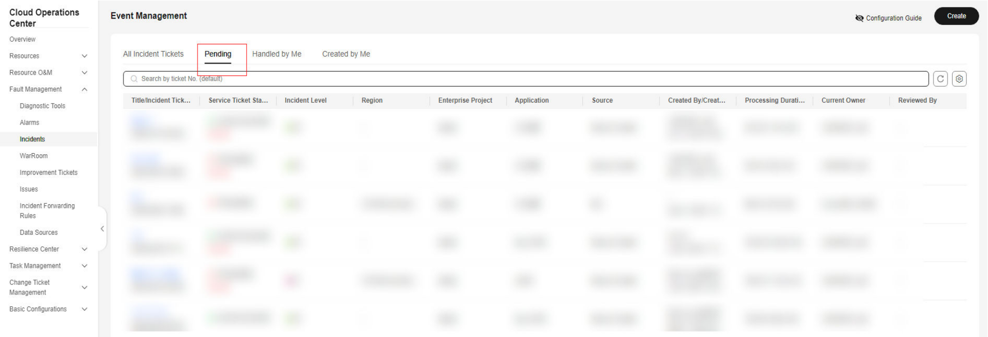
After the incident ticket is processed, verify whether the incident processing is completed.

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.

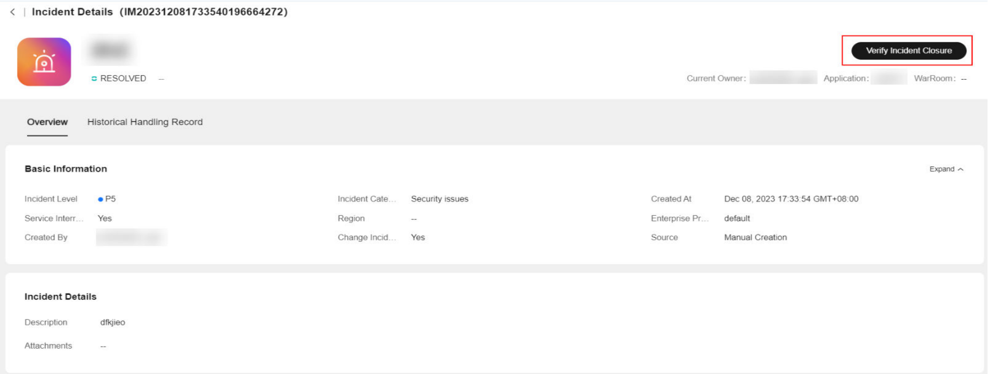
Figure 6-43 Incident details



Title/Incident Tick...	Service Ticket Sta...	Incident Level	Region	Enterprise Project	Application	Source	Created By/Creat...	Processing Durati...	Current Owner	Reviewed By

Step 3 Click **Verify Incident Closure**.

Figure 6-44 Verifying whether the incident is closed



< | Incident Details (IM202312081733540196664272)

[redacted]

RESOLVED --

Verify Incident Closure

Current Owner: [redacted] Application: [redacted] WarRoom: --

Overview | Historical Handling Record

Basic Information Expand

Incident Level	● P5	Incident Cate...	Security issues	Created At	Dec 08, 2023 17:33:54 GMT+08:00
Service Interr...	Yes	Region	--	Enterprise Pr...	default
Created By	[redacted]	Change Incid...	Yes	Source	Manual Creation

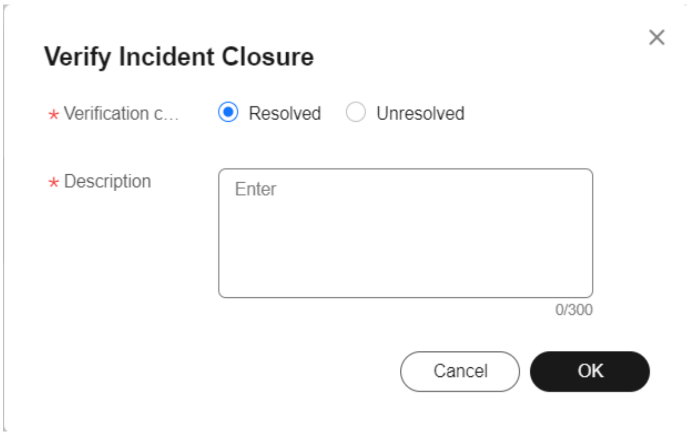
Incident Details

Description dfkjieo

Attachments --

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

Figure 6-45 Verifying close page



Verify Incident Closure

* Verification c... ● Resolved ○ Unresolved

* Description Enter

0/300

Cancel OK

----End

6.3.3.10 Creating an Improvement Ticket For An Incident

Scenarios

If an improvement item is found during the handling of an incident ticket, you can create an improvement ticket to follow up the handling.

Prerequisites

An improvement ticket can be created only after the incident is accepted.

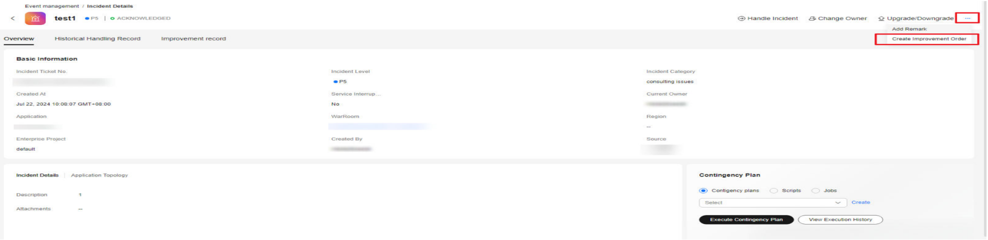
Procedure

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.

Step 3 On the right of the page, click ··· and choose **Create Improvement Order**. On the displayed page, enter improvement information and click **OK**.

Figure 6-46 Creating an improvement ticket



Event management / Incident Details

< test1 ● P5 | ○ ACKNOWLEDGED

Handle Incident | Change Owner | Upgrade/Downgrade | ···

Add Remark

Create Improvement Order

Overview | Historical Handling Record | Improvement record

Basic Information

Incident Ticket No. [redacted]	Incident Level ● P5	Incident Category consulting issues
Created At Jul 22, 2024 10:08:07 GMT+08:00	Service Interrup... No	Current Owner [redacted]
Application [redacted]	WarRoom [redacted]	Region --
Enterprise Project default	Created By [redacted]	Source [redacted]

Incident Details | Application Topology

Description 1

Attachments --

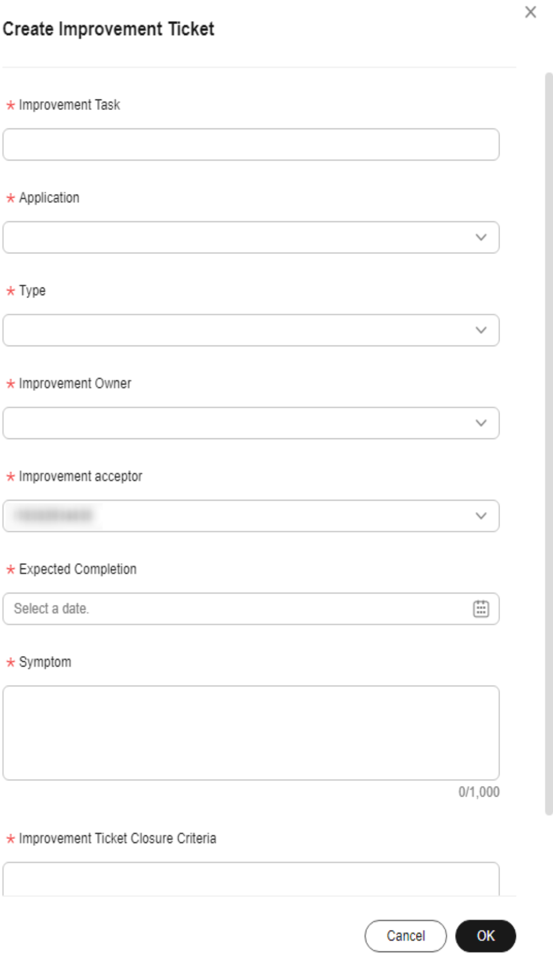
Contingency Plan

● Contigency plans ○ Scripts ○ Jobs

Select Create

Execute Contingency Plan | View Execution History

Figure 6-47 Entering improvement ticket information



Create Improvement Ticket ×

* Improvement Task

* Application

* Type

* Improvement Owner

* Improvement acceptor

[redacted]

* Expected Completion

Select a date.

* Symptom

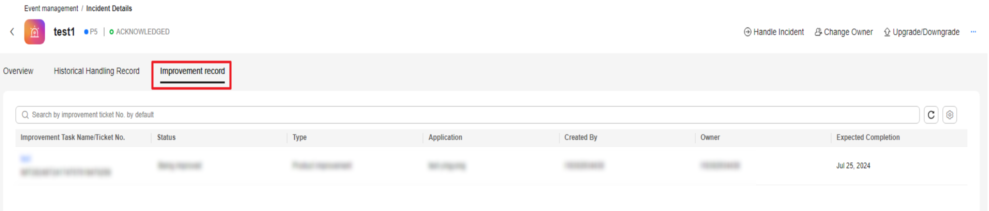
0/1,000

* Improvement Ticket Closure Criteria

Cancel | OK

Step 4 View the improvement ticket status and current owner on the **improvement record** page. You can also click the improvement task name to go to the improvement management page to handle the improvement ticket.

Figure 6-48 Viewing improvement record


Event management / Incident Details
test1
P5
ACKNOWLEDGED
Handle Incident
Change Owner
Upgrade/Downgrade
Overview
Historical Handling Record
Improvement record
Search by improvement ticket No. by default

Improvement Task Name/Ticket No.	Status	Type	Application	Created By	Owner	Expected Completion
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Jul 25, 2024

----End

6.3.3.11 Full-Link Fault Diagnosis

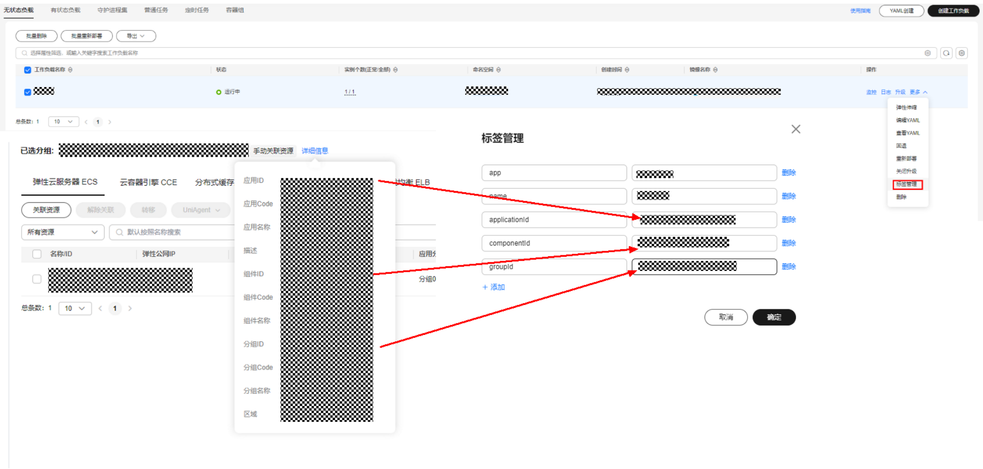
Scenarios

After an incident is created, you can use the full-link fault diagnosis function to quickly locate the root cause of the fault. We provide the relationship topology of the application layer, component layer, and resource layer for customer applications, implement exception coloring based on resource and application alarms, and provide the capabilities of viewing core resource metrics and diagnosing instances.

Prerequisites

- You have performed the operations described in **Creating an Application**, **Manually Associating Resources with a Group**, and **Editing an Application Topology** on CloudCMDB.
- CES has been connected. You can configure CES monitoring by referring to **Integration Management**.
- An incident ticket has been created.
- To display workload and POD information in a CCE cluster, you need to add label to workloads in CCE. (Only one CCE cluster resource can be added to each group. Otherwise, workload information is not displayed.)

Figure 6-49 Configuring CCE workload label



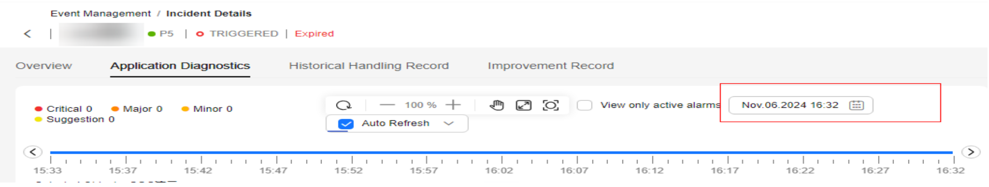
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Fault Management** > **Incidents**, click the **All Incident Tickets** tab, click an incident name to go to the **Incident Details** page, and click the **Application Diagnostics** tab.

Step 3 Select a fault time range to color the alarms generated in this time range. You can enter the end time in the time box. The start time is one hour earlier than the end time. The time axis can be automatically refreshed. After **Auto Refresh** is selected, the end time is automatically refreshed to the latest time based on the refresh frequency.

Figure 6-50 Selecting fault time range



Event Management / Incident Details

[redacted] ● P5 | ○ TRIGGERED | Expired

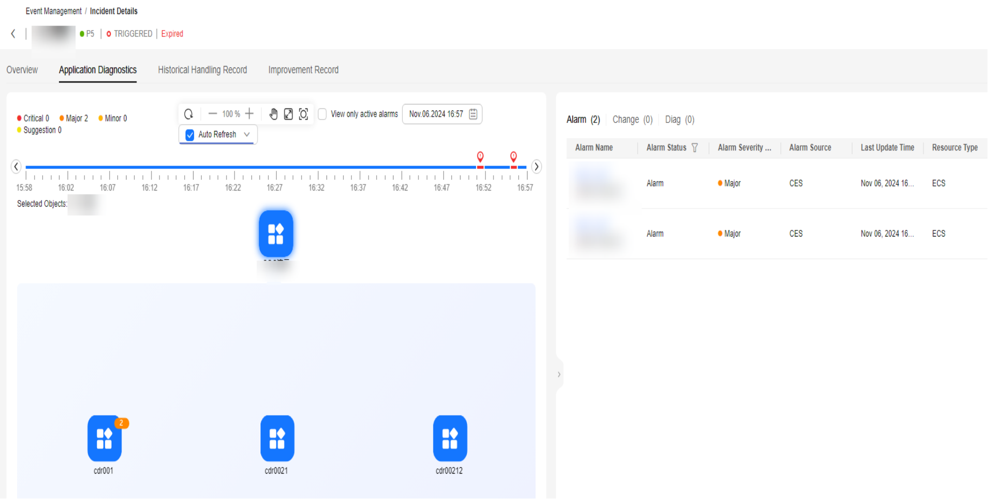
Overview | Application Diagnostics | Historical Handling Record | Improvement Record

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

100 % ☑ Auto Refresh □ View only active alarms Nov.06.2024 16:32

Step 4 By default, all sub-applications of the current application are displayed on the application topology screen.

Figure 6-51 Application topology (application layer)



Event Management / Incident Details

[redacted] ● P5 | ○ TRIGGERED | Expired

Overview | Application Diagnostics | Historical Handling Record | Improvement Record

● Critical 0 ● Major 2 ● Minor 0 ● Suggestion 0

100 % ☑ Auto Refresh □ View only active alarms Nov.06.2024 16:57

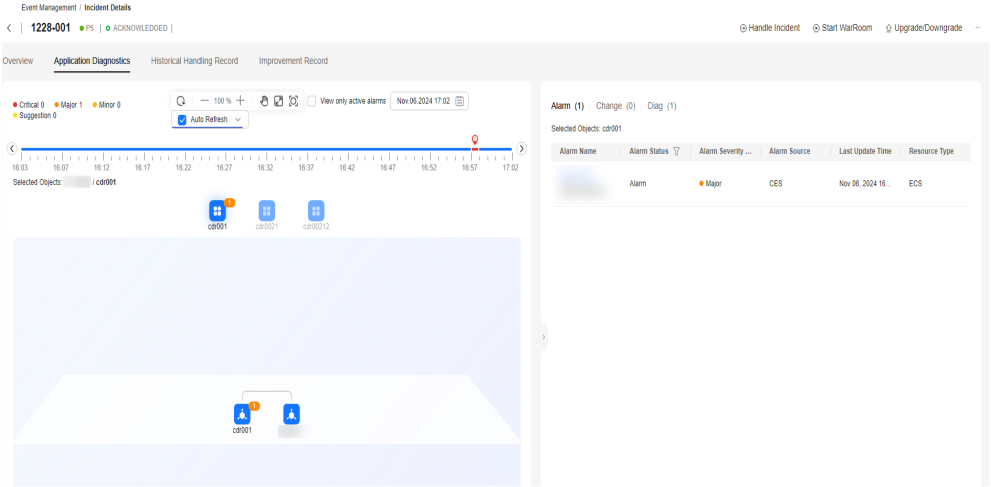
Selected Objects: [redacted]

Alarm (2) | Change (0) | Diag (0)

Alarm Name	Alarm Status	Alarm Severity ...	Alarm Source	Last Update Time	Resource Type
[redacted]	Alarm	● Major	CES	Nov 06, 2024 16...	ECS
[redacted]	Alarm	● Major	CES	Nov 06, 2024 16...	ECS

Step 5 Click a sub-application in the topology to view the component layer. All components of the sub-application are displayed. You can switch to other sub-applications on the top to view their components.

Figure 6-52 Application topology (component layer)



Nov.06.2024 17:02

☑ Auto Refresh

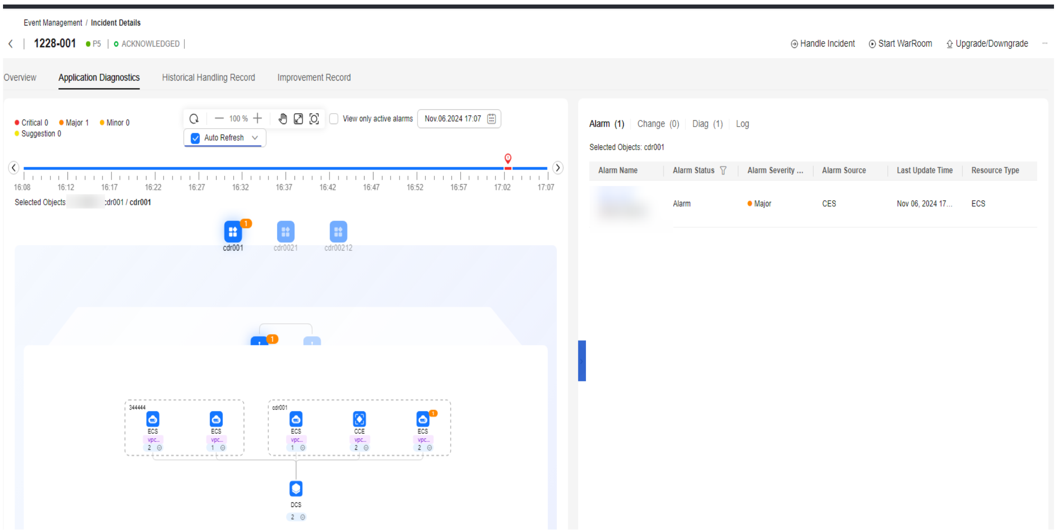
Selected Objects: [redacted] / cdr001

Selected Objects: cdr001

Alarm Name	Alarm Status	Alarm Severity ...	Alarm Source	Last Update Time	Resource Type
[redacted]	Alarm	● Major	CES	Nov 06, 2024 16...	ECS

Step 6 Click a component to view the resource layer. All resources under the component are displayed, and metrics of core cloud services are displayed. If APM is associated in application management, you can also view link-related metrics.

Figure 6-53 Application topology (resource layer)



Nov.06.2024 17:07

☑ Auto Refresh

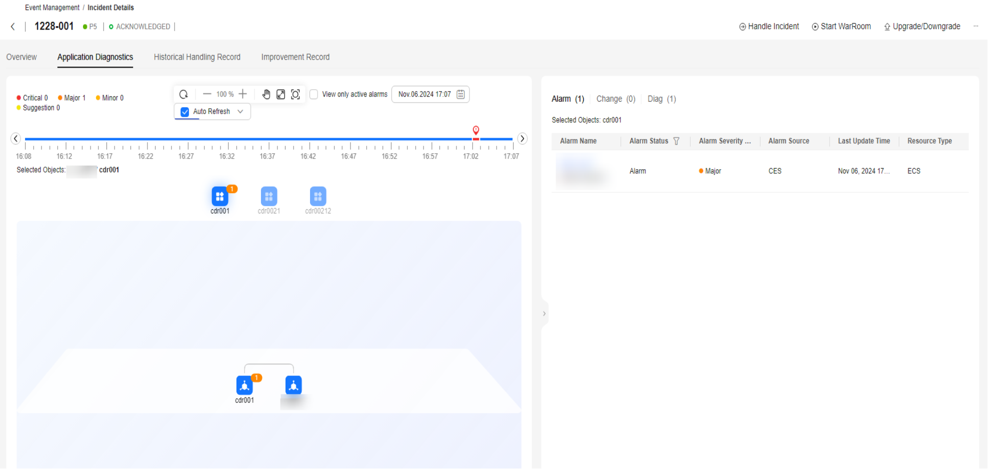
Selected Objects [redacted] :dr001 / cdr001

Selected Objects: cdr001

Alarm Name	Alarm Status	Alarm Severity ...	Alarm Source	Last Update Time	Resource Type
[redacted]	Alarm	● Major	CES	Nov 06, 2024 17...	ECS

Step 7 Click the **Alarm** tab to view application alarms. The list displays the alarms generated within the time range. After a topology object is selected on the left, the alarm information of the selected object is automatically filtered out.

Figure 6-54 Alarm list

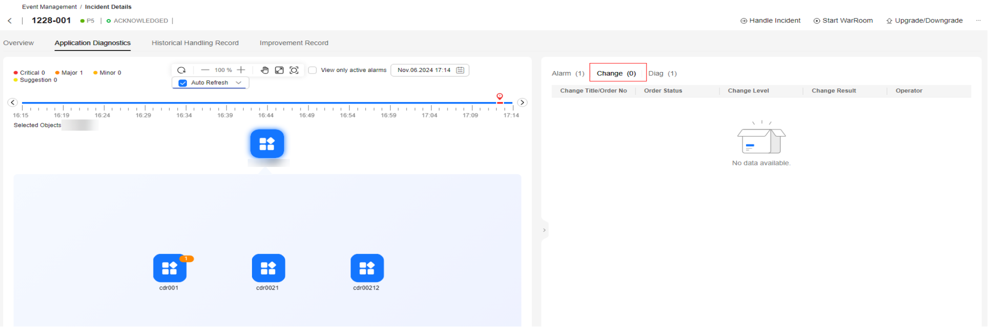


Selected Objects: cdr001

Alarm Name	Alarm Status	Alarm Severity ...	Alarm Source	Last Update Time	Resource Type
[redacted]	Alarm	● Major	CES	Nov 06, 2024 17...	ECS

Step 8 Click the **Change** tab to view application changes. The list displays the changes within the time range.

Figure 6-55 Changes

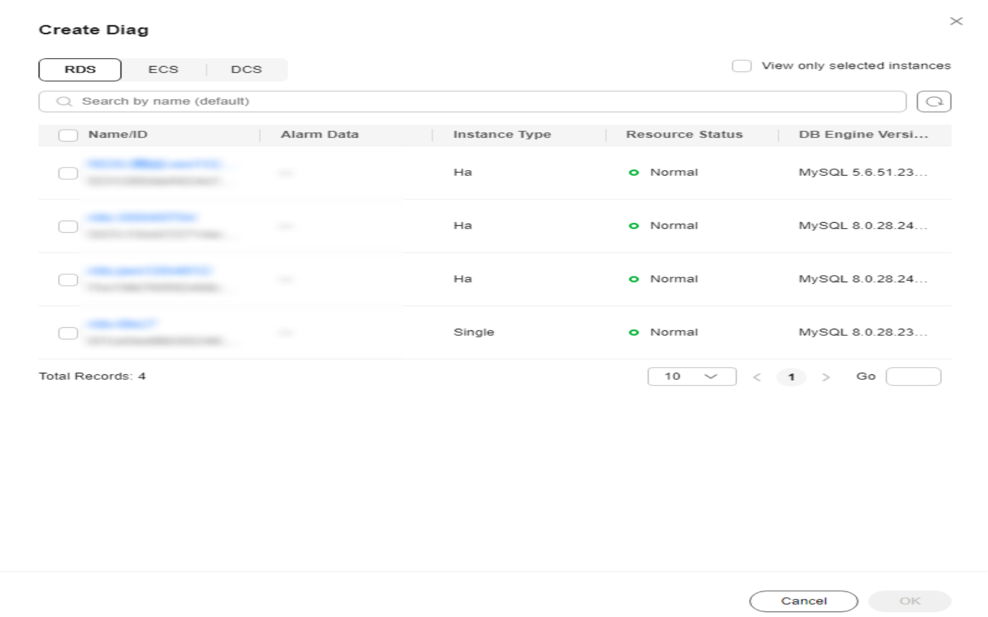


Change Title/Order No	Order Status	Change Level	Change Result	Operator

No data available.

Step 9 Click the **Diag** tab and click **Create Diag** to diagnose DCS, RDS, and DMS resources of an application. After a topology object is selected on the left, the diagnosis information of the selected object is automatically filtered out.

Figure 6-56 Creating a diagnosis task



Create Diag

RDS | ECS | DCS

□ View only selected instances

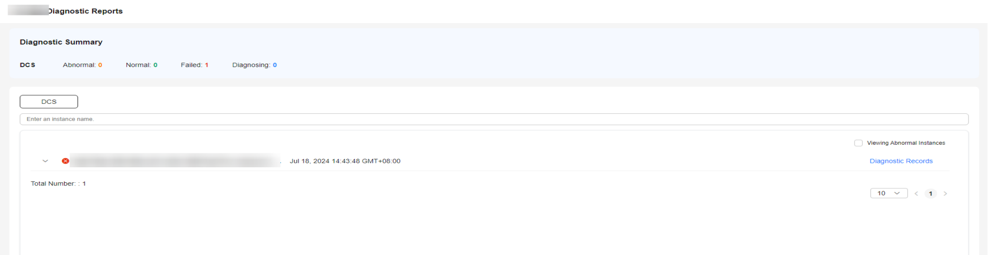
Search by name (default)

□ Name/ID	Alarm Data	Instance Type	Resource Status	DB Engine Versi...
□ [redacted]	--	Ha	○ Normal	MySQL 5.6.51.23...
□ [redacted]	--	Ha	○ Normal	MySQL 8.0.28.24...
□ [redacted]	--	Ha	○ Normal	MySQL 8.0.28.24...
□ [redacted]	--	Single	○ Normal	MySQL 8.0.28.23...

Total Records: 4

Step 10 After the diagnosis is complete, click **View Details** in the diagnosis result list to view the diagnosis report.

Figure 6-57 Diagnosis report



[redacted]Diagnostic Reports

Diagnostic Summary

DCS Abnormal: 0 Normal: 0 Failed: 1 Diagnosing: 0

DCS

Enter an instance name.

□ Viewing Abnormal Instances

[redacted] Jul 18, 2024 14:43:48 GMT+08:00 Diagnostic Records

Total Number: : 1

----End

6.3.4 Incident History

Scenarios

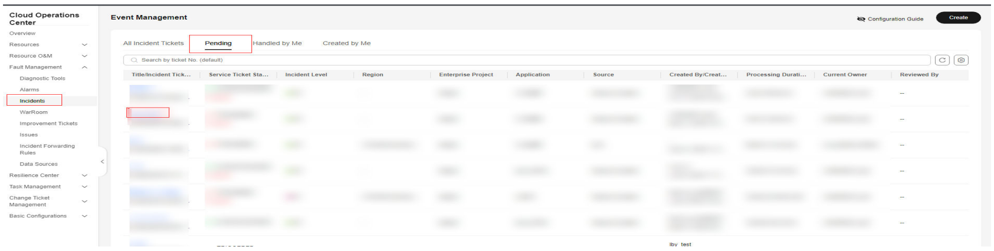
View the historical records of an incident, including the entire incident handling process.

Procedure

Step 1 Log in to **COC**.

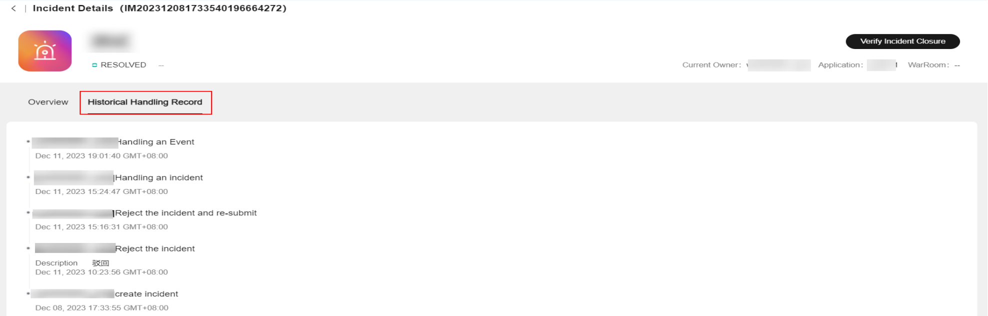
Step 2 In the navigation pane on the left, choose **Incident Management** > **Incident Center**. On the displayed page, click the **Pending** tab and click the incident title to go to the incident details page.

Figure 6-58 Incident details



Step 3 Click **Historical Handling Record**.

Figure 6-59 Viewing incident history



Incident Details (IM20231208173354019666427 2)

RESOLVED --

Current Owner: Application: WarRoom: --

- Handling an Event
  Dec 11, 2023 19:01:40 GMT+08:00
- |Handling an incident
  Dec 11, 2023 15:24:47 GMT+08:00
- |Reject the incident and re-submit
  Dec 11, 2023 15:16:31 GMT+08:00
- Reject the incident
  Description 驳回
  Dec 11, 2023 10:23:56 GMT+08:00
- create incident
  Dec 08, 2023 17:33:55 GMT+08:00

----End

6.4 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.

6.4.1 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

6.4.2 Fault Information

Scenarios

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

Procedure

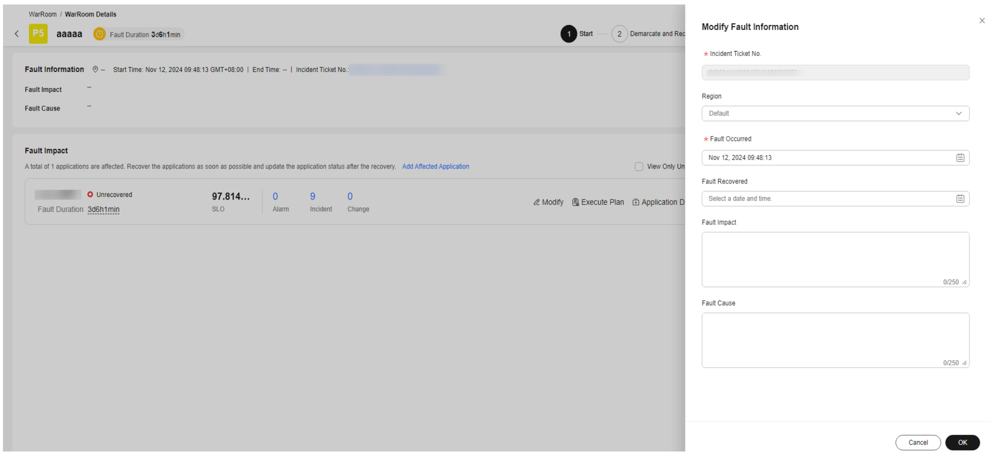
Step 1 Log in to **COC**.

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 6-60 Modifying fault information



WarRoom / WarRoom Details

P5 aaaaa Fault Duration 3d6h1min

Fault Information -- Start Time: Nov 12, 2024 09:48:13 GMT+08:00 | End Time: -- | Incident Ticket No.: [redacted]

Fault Impact --

Fault Cause --

Fault Impact

A total of 1 applications are affected. Recover the applications as soon as possible and update the application status after the recovery. Add Affected Application

[redacted] Unrecovered

Fault Duration 3d6h1min

97.814... SLO | 0 Alarm | 9 Incident | 0 Change

Modify Fault Information

* Incident Ticket No.: [redacted]

Region: Default

* Fault Occurred: Nov 12, 2024 09:48:13

Fault Recovered: Select a date and time.

Fault Impact: 0/250

Fault Cause: 0/250

----End

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

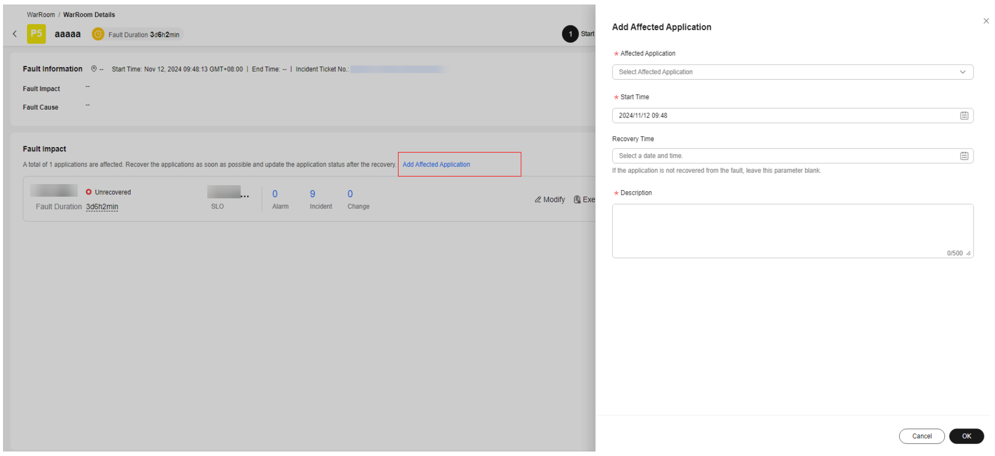
Step 3 Click a war room name in the war room list. The war room detail page is displayed.

Step 4 On the displayed page, click **Add Affected Application**.

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

Step 6 Click **OK**.

Figure 6-61 New affected applications



WarRoom / WarRoom Details

P5 aaaaa Fault Duration 3d6h2min

Fault Information -- Start Time: Nov 12, 2024 09:48:13 GMT+08:00 | End Time: -- | Incident Ticket No.: [redacted]

Fault Impact --

Fault Cause --

Fault Impact

A total of 1 applications are affected. Recover the applications as soon as possible and update the application status after the recovery. Add Affected Application

[redacted] Unrecovered

Fault Duration 3d6h2min

[redacted] SLO | 0 Alarm | 9 Incident | 0 Change

Add Affected Application

* Affected Application: Select Affected Application

* Start Time: 2024/11/12 09:48

Recovery Time: Select a date and time.

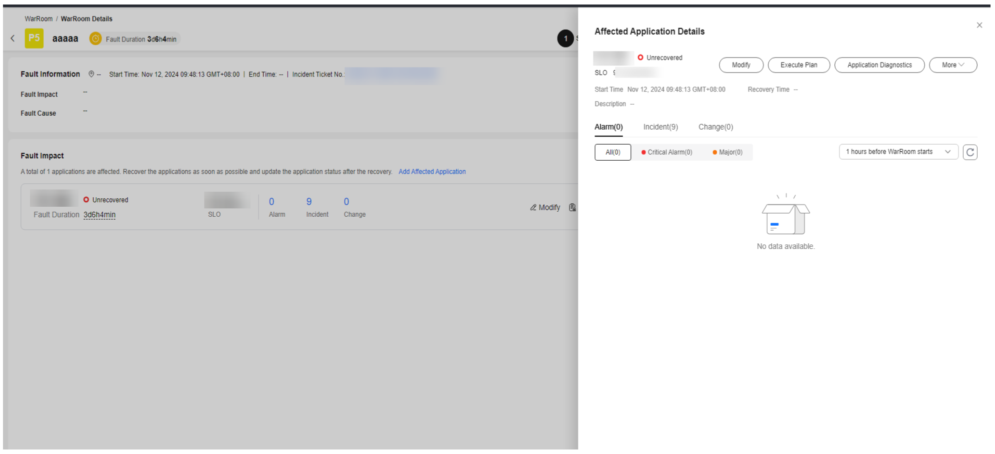
If the application is not recovered from the fault, leave this parameter blank.

* Description: 0/500

Step 7 View the added applications on the main 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 6-62 Affected application page



WarRoom / WarRoom Details

P5 aaaaa Fault Duration 3d6h4min

Fault Information -- Start Time: Nov 12, 2024 09:48:13 GMT+08:00 | End Time: -- | Incident Ticket No.: [redacted]

Fault Impact --

Fault Cause --

Fault Impact

A total of 1 applications are affected. Recover the applications as soon as possible and update the application status after the recovery. Add Affected Application

[redacted] Unrecovered

Fault Duration 3d6h4min

[redacted] SLO | 0 Alarm | 9 Incident | 0 Change

Affected Application Details

[redacted] Unrecovered

SLO [redacted]

Start Time Nov 12, 2024 09:48:13 GMT+08:00 Recovery Time --

Description --

Alarm(0) Incident(9) Change(0)

All(0) Critical Alarm(0) Major(0)

1 hours before WarRoom starts

No data available.

----End

6.4.4 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

6.4.5 Progress Notification

Scenarios

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

Procedure

Step 1 Log in to **COC**.

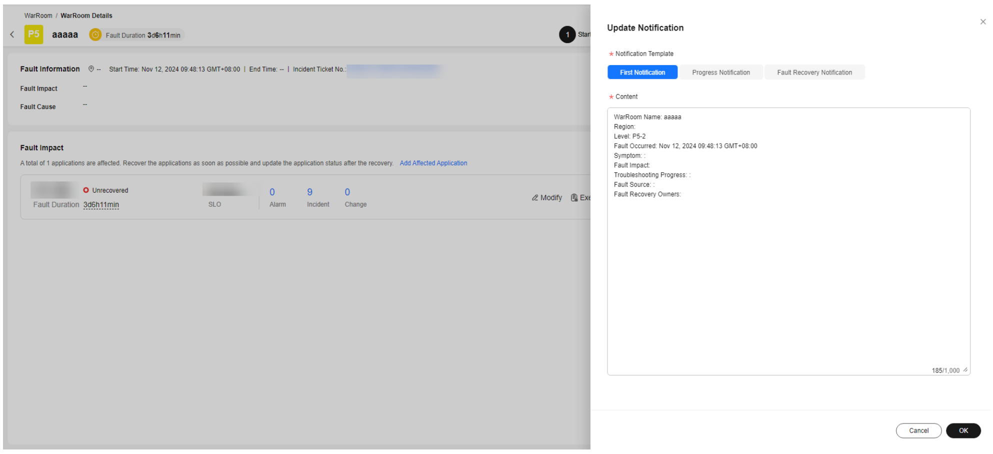
Step 2 In the navigation pane on the left, choose **Fault Management** > **WarRoom** to view the war room list.

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 6-63 Updating notification



Fault Information -- Start Time: Nov 12, 2024 09:48:13 GMT+08:00 | End Time: -- | Incident Ticket No.:

Fault Impact --

Fault Cause --

Fault Impact

A total of 1 applications are affected. Recover the applications as soon as possible and update the application status after the recovery.

Unrecovered
Fault Duration 3d6h11min

SLO

0	9	0
Alarm	Incident	Change

* Notification Template: First Notification

* Content

WarRoom Name: aaaaa
Region:
Level: P5-2
Fault Occurred: Nov 12, 2024 09:48:13 GMT+08:00
Symptom: :
Fault Impact:
Troubleshooting Progress: :
Fault Source: :
Fault Recovery Owners:

185/1,000

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

6.4.6 Adding a War Room Initiation Rule

Scenarios

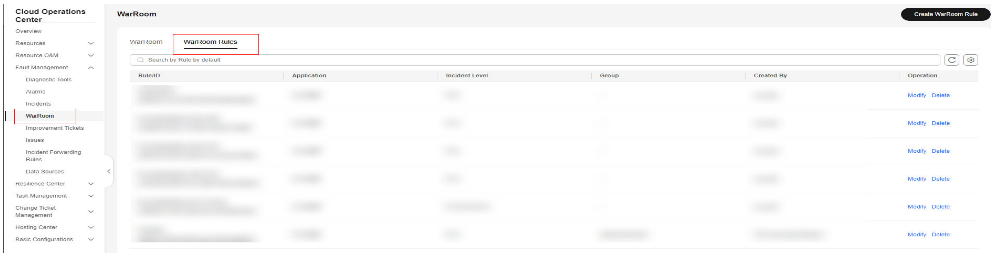
Create a war room initiation rule.

Procedure

Step 1 Log in to **COC**.

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

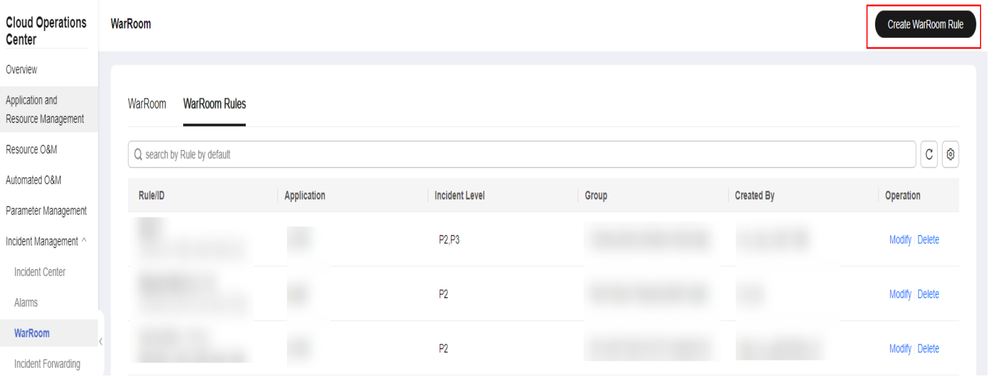
Figure 6-64 War room rules



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 App Management**.

Figure 6-65 Adding a war room rule



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

----End

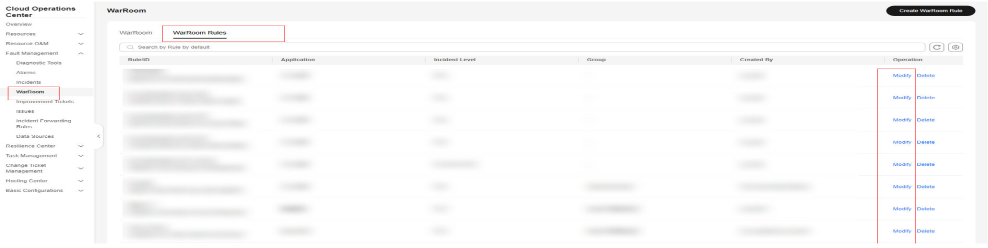
6.4.7 Modifying a War Room Rule

Procedure

Step 1 Log in to COC.

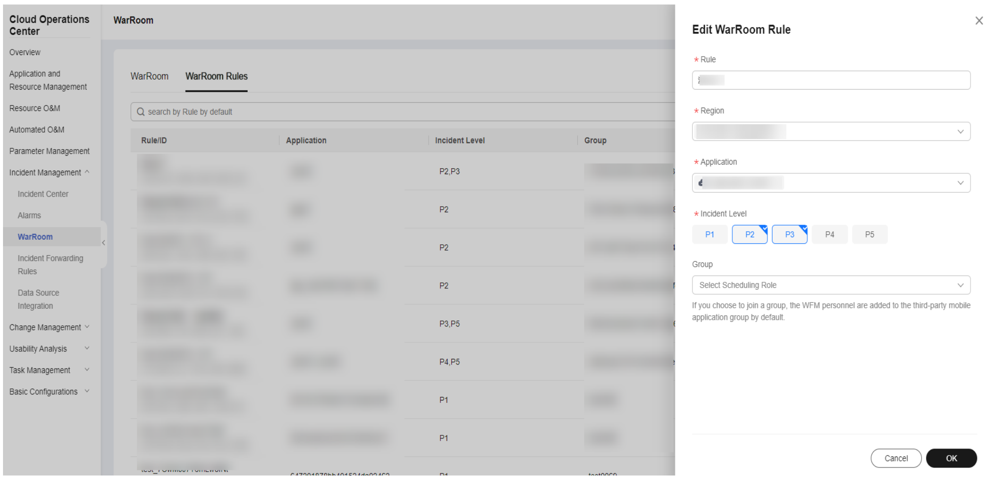
Step 2 In the navigation pane on the left, choose **Incident Management** > **WarRoom**. Click **WarRoom Rules**.

Figure 6-66 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 6-67 Modifying a war room rule



Rule/ID	Application	Incident Level	Group
[redacted]	[redacted]	P2,P3	[redacted]
[redacted]	[redacted]	P2	[redacted]
[redacted]	[redacted]	P2	[redacted]
[redacted]	[redacted]	P2	[redacted]
[redacted]	[redacted]	P3,P5	[redacted]
[redacted]	[redacted]	P4,P5	[redacted]
[redacted]	[redacted]	P1	[redacted]
[redacted]	[redacted]	P1	[redacted]

Edit WarRoom Rule

* Rule: [redacted]

* Region: [redacted]

* Application: [redacted]

* Incident Level: P1 [✓ P2] [✓ P3] P4 P5

Group: Select Scheduling Role

If you choose to join a group, the WFM personnel are added to the third-party mobile application group by default.

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

----End

6.5 Improvement Management

Improvement management refers to tracking and closing the improvement items identified during troubleshooting through improvement tickets. Improvement sources include incidents, war rooms, drills, and PRRs.

6.5.1 Improvement Management

Prerequisites

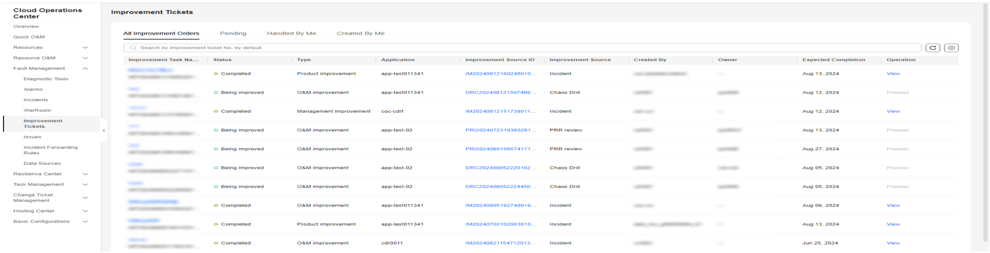
Create improvement tickets using incidents, war rooms, drills, and PRRs.

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.

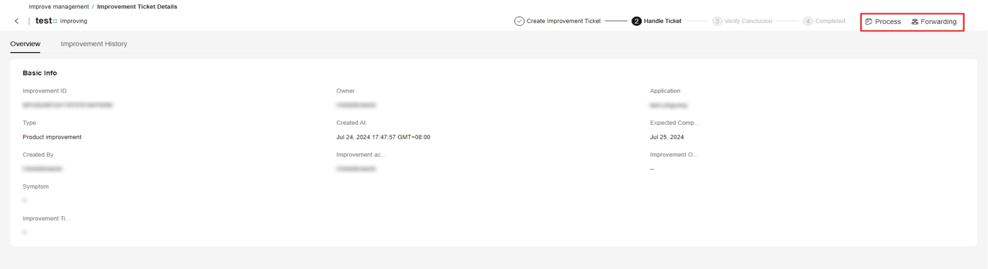
Figure 6-68 Improvement ticket list



Improvement Task Na...	Status	Type	Application	Improvement Source ID	Improvement Source	Created By	Owner	Expected Completion	Operation
[redacted]	Completed	Product improvement	app-test011341	IM20240812160248010...	Incident	[redacted]	--	Aug 13, 2024	View
[redacted]	Being improved	O&M improvement	app-test011341	DRC202408121507499...	Chaos Drill	[redacted]	[redacted]	Aug 12, 2024	Process
[redacted]	Completed	Management improvement	coc-cdrf	IM20240812151738011...	Incident	[redacted]	--	Aug 12, 2024	View
[redacted]	Being improved	O&M improvement	app-test-02	PRI2024072319360291...	PRR review	[redacted]	[redacted]	Aug 13, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	PRI2024080109574171...	PRR review	[redacted]	[redacted]	Aug 27, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	DRC202408052220102...	Chaos Drill	[redacted]	[redacted]	Aug 05, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	DRC202408052224450...	Chaos Drill	[redacted]	[redacted]	Aug 05, 2024	Process
[redacted]	Completed	O&M improvement	app-test011341	IM20240805192748016...	Incident	[redacted]	--	Aug 06, 2024	View
[redacted]	Completed	Product improvement	app-test011341	IM20240702102003010...	Incident	[redacted]	--	Aug 13, 2024	View
[redacted]	Completed	O&M improvement	cdr0011	IM20240621154712013...	Incident	[redacted]	--	Jun 25, 2024	View

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

Figure 6-69 Improvement ticket details



Improve management / Improvement Ticket Details

test Improving

Create Improvement Ticket — 2 Handle Ticket — 3 Verify Conclusion — 4 Completed

Process | Forwarding

Overview | Improvement History

Basic Info

Improvement ID: [redacted]

Owner: [redacted]

Application: [redacted]

Type: Product improvement

Created At: Jul 24, 2024 17:47:57 GMT+08:00

Expected Comp...: Jul 25, 2024

Created By: [redacted]

Improvement ac...: [redacted]

Improvement O...: --

Symptom: [redacted]

Improvement Ti...: [redacted]

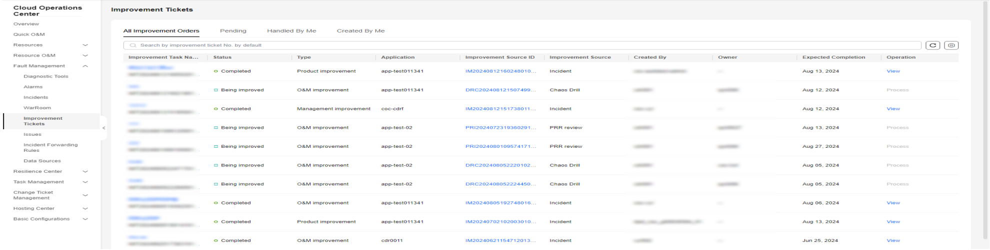
----End

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 6-70 Improvement ticket list



Improvement Tickets

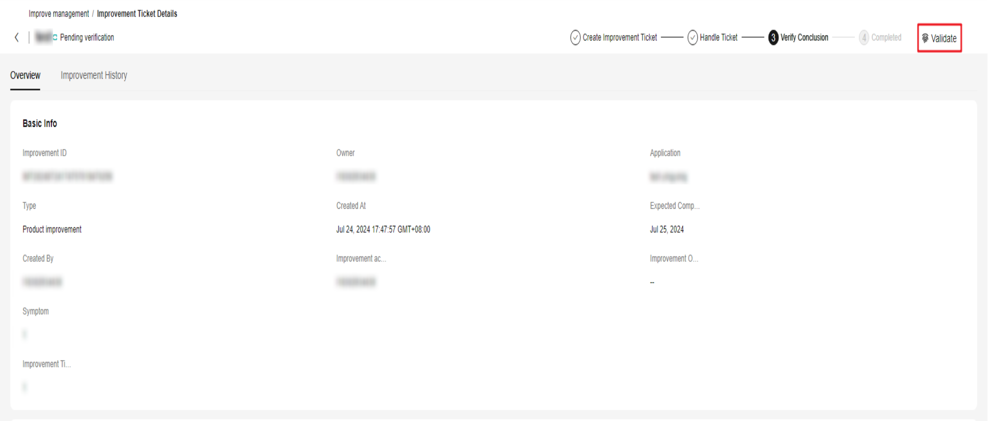
All Improvement Orders | Pending | Handled By Me | Created By Me

Search by improvement ticket No. by default

Improvement Task Na...	Status	Type	Application	Improvement Source ID	Improvement Source	Created By	Owner	Expected Completion	Operation
[redacted]	Completed	Product improvement	app-test011341	IM20240812160248010...	Incident	[redacted]	--	Aug 13, 2024	View
[redacted]	Being improved	O&M improvement	app-test011341	DRC202408121507499...	Chaos Drill	[redacted]	[redacted]	Aug 12, 2024	Process
[redacted]	Completed	Management improvement	coc-cdrf	IM20240812151738011...	Incident	[redacted]	--	Aug 12, 2024	View
[redacted]	Being improved	O&M improvement	app-test-02	PRI2024072319360291...	PRR review	[redacted]	[redacted]	Aug 13, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	PRI2024080109574171...	PRR review	[redacted]	[redacted]	Aug 27, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	DRC202408052220102...	Chaos Drill	[redacted]	[redacted]	Aug 05, 2024	Process
[redacted]	Being improved	O&M improvement	app-test-02	DRC202408052224450...	Chaos Drill	[redacted]	[redacted]	Aug 05, 2024	Process
[redacted]	Completed	O&M improvement	app-test011341	IM20240805192748016...	Incident	[redacted]	--	Aug 06, 2024	View
[redacted]	Completed	Product improvement	app-test011341	IM20240702102003010...	Incident	[redacted]	--	Aug 13, 2024	View
[redacted]	Completed	O&M improvement	cdr0011	IM20240621154712013...	Incident	[redacted]	--	Jun 25, 2024	View

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

Figure 6-71 Improvement ticket validation



Improve management / Improvement Ticket Details

[redacted] Pending verification

Create Improvement Ticket — Handle Ticket — 3 Verify Conclusion — 4 Completed

Validate

Overview | Improvement History

Basic Info

Improvement ID: [redacted]

Owner: [redacted]

Application: [redacted]

Type: Product improvement

Created At: Jul 24, 2024 17:47:57 GMT+08:00

Expected Comp...: Jul 25, 2024

Created By: [redacted]

Improvement ac...: [redacted]

Improvement O...: --

Symptom: [redacted]

Improvement Ti...: [redacted]

----End

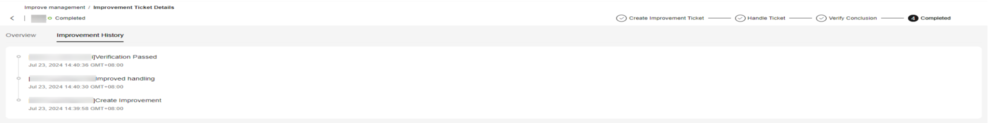
Improvement Ticket History

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 6-72 Improvement ticket history



[redacted]i]Verification Passed
Jul 23, 2024 14:40:36 GMT+08:00

[[redacted]Improved handling
Jul 23, 2024 14:40:30 GMT+08:00

[redacted]]Create Improvement
Jul 23, 2024 14:39:58 GMT+08:00

----End

6.6 Issue Management

Issue management allows you to manage all issue tickets of applications. By identifying the actual and potential causes of faults, and managing workarounds and known errors, you can avoid fault recurrence and reduce fault impact. In this module, the whole lifecycle of issues tickets is managed, including ticket creation, acceptance, rejection, transferring, handling, and closure. Issue tickets can be created manually or through northbound APIs.

You can also configure SLA rules. For details about how to configure SLA rules, see **SLA Management**.

6.6.1 Issue Process

After an issue ticket is created, its status is **Not accepted**. You can accept or reject the ticket, or transfer it to the owner.

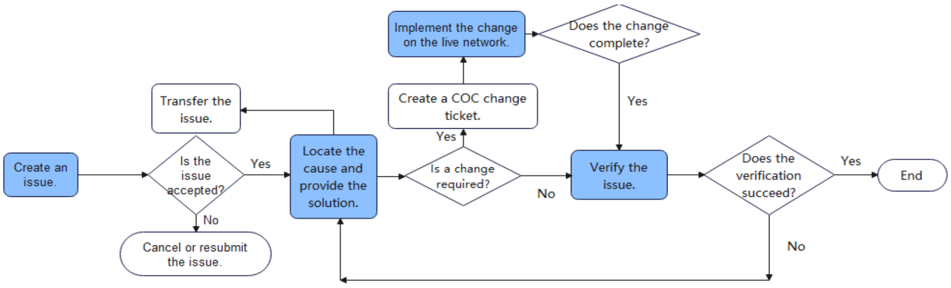
After the issue ticket is accepted, its status becomes **Locate the solution**. You can enter the issue locating result, transfer the ticket to the owner, upgrade or downgrade the ticket, or suspend it.

After an issue ticket is suspended, it needs to be approved by the creator. After the ticket is approved, the status of the issue ticket changes to **Suspend**. You can manually cancel the suspension or the suspension is automatically canceled when the specified time arrives.

When you enter the locating result, if you select change-required, the ticket status is **To be implemented on the live network**. You need to associate with a change ticket and the change ticket has the backfilling result. In this way, the issue ticket can be transferred to the next step.

If an issue ticket does not require change or the issue ticket has a change result, the ticket status is **To be verified**. The creator confirms whether the issue is resolved or not. If the issue is not resolved, the creator can reject the ticket.

Figure 6-73 Issue management process


Create an issue.
Is the issue accepted?
Yes
No
Transfer the issue.
Cancel or resubmit the issue.
Locate the cause and provide the solution.
Is a change required?
Yes
No
Create a COC change ticket.
Implement the change on the live network.
Does the change complete?
Yes
Verify the issue.
Does the verification succeed?
Yes
No
End

6.6.2 Creating an Issue Ticket

Scenarios

Create an issue ticket on COC.

Prerequisites

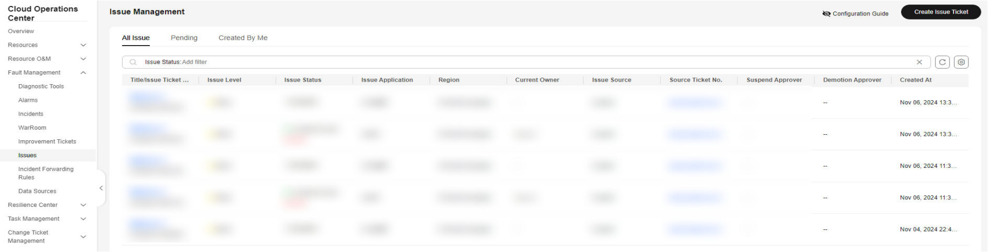
You have created an application by referring to **Application Management**.

Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Issues**. Click **Create Issue Ticket** in the upper right corner.

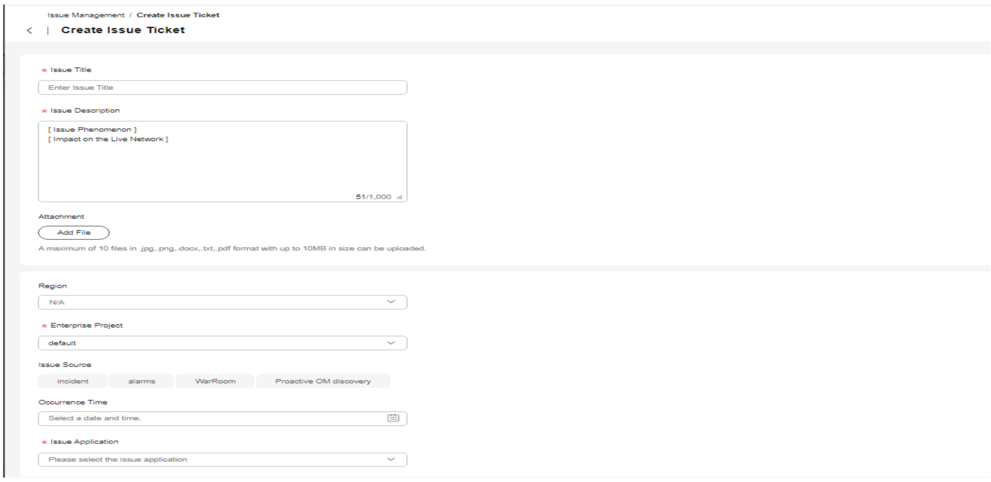
Figure 6-74 Issue list



Title/Issue Ticket ...	Issue Level	Issue Status	Issue Application	Region	Current Owner	Issue Source	Source Ticket No.	Suspend Approver	Demotion Approver	Created At
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Nov 06, 2024 13:3...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Nov 06, 2024 13:3...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Nov 06, 2024 11:3...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Nov 06, 2024 11:3...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Nov 04, 2024 22:4...

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

Figure 6-75 Page for creating an issue



Issue Management / Create Issue Ticket

< | Create Issue Ticket

* Issue Title

Enter Issue Title

* Issue Description

[Issue Phenomenon]
[Impact on the Live Network]

51/1,000

Attachment

Add File

A maximum of 10 files in .jpg,.png,.docx,.txt,.pdf format with up to 10MB in size can be uploaded.

Region

N/A

* Enterprise Project

default

Issue Source

incident | alarms | WarRoom | Proactive OM discovery

Occurrence Time

Select a date and time.

* Issue Application

Please select the issue application

Issue Title: Mandatory. Briefly describe the issue.

Issue Description: Mandatory. Describe the issue and its impact on the live network. Attachments can be uploaded.

Issue Source: Optional. Enter the issue source, which can be incidents, alarms, war rooms, or detection results in proactive O&M. If the issue is found during incident handling, select **Incident**.

Issue.table.occurTime: Optional. Enter the time when the issue occurs.

Issue Application: Mandatory. Select the application to which the issue belongs.

Issue Level: Mandatory. Select the issue level, including **Critical**, **Major**, **Minor**, and **Prompts**.

Type of Issue: Mandatory. Select the issue type.

Owner: Mandatory. After an owner is selected, the issue ticket will be transferred to the owner. Currently, **Shift** and **Individual** are supported. For details about how to set shift, see **Shift Schedule Management**.

NOTICE

To receive notifications for issues, you need to configure notification rules on the **Notification Management** page. For details, see Notification Management.

----End

6.6.3 Handling an Issue Ticket

Scenarios

After an issue ticket is created, the issue owner needs to accept the ticket, locate the root cause, and submit a solution to the issue.

6.6.3.1 Accepting an Issue Ticket

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click an issue ticket name to go to the issue details page. Click Accept in the upper right corner. After the issue ticket is accepted, you can locate and analyze the issue cause.

----End

6.6.3.2 Rejecting an Issues Ticket

Scenarios

If the issue ticket submitted by the creator is not an issue, the issue ticket can be rejected. The creator can edit the issue ticket and submit it again or directly close the issue ticket.

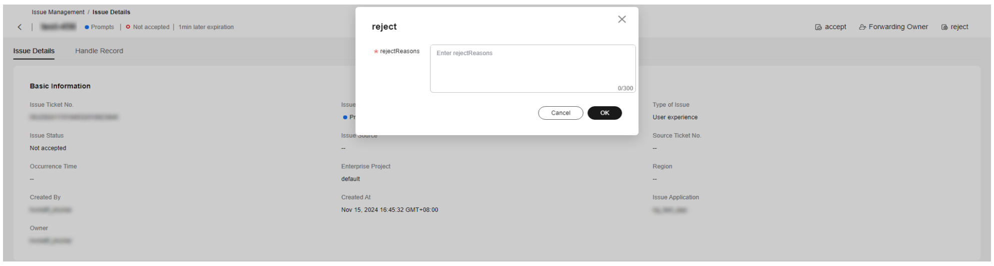
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click an issue ticket name to go to the issue details page. Click Reject in the upper right corner. The creator can modify the issue ticket and submit it again, or withdraw and close it.

Figure 6-76 Rejecting an issue ticket



Issue Ticket No.
[redacted]

Issue Status
Not accepted

Occurrence Time
--

Created By
[redacted]

Owner
[redacted]

Issue Source
--

Enterprise Project
default

Created At
Nov 15, 2024 16:45:32 GMT+08:00

Type of Issue
User experience

Source Ticket No.
--

Region
--

Issue Application
[redacted]

----End

6.6.3.3 Locating the Cause and Providing a Solution

Scenario

After an issue ticket is accepted, you need to locate and analyze the cause and provide the locating result and handling solution.

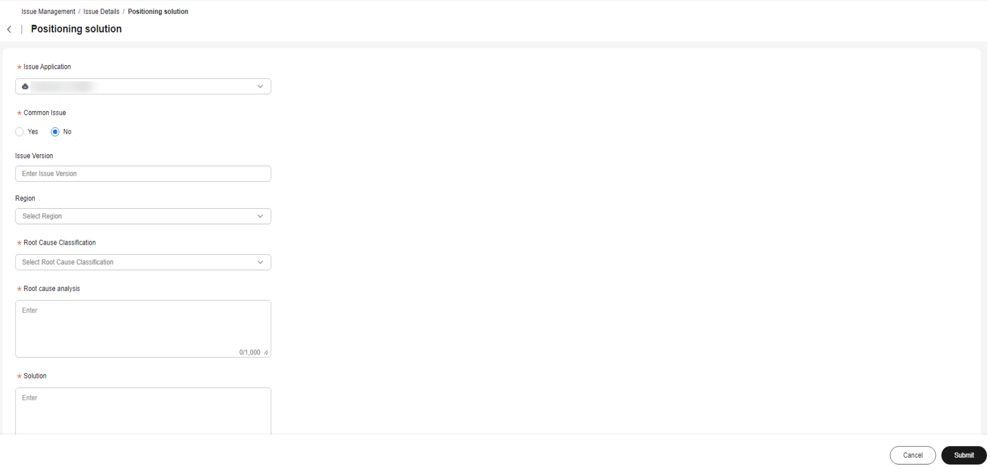
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click the issue ticket name to go to the issue details page. Click **Positioning solution** in the upper right corner to go to the page for entering the issue cause and solution. Enter the information and click submit.

Figure 6-77 Complete the solution



Issue Management / Issue Details / Positioning solution

Positioning solution

* Common Issue: ○ Yes ● No

Step 4 On the solution page, if you select change-required, the region must be specified. When the issue ticket come to the **To be implemented on the live network** status, the selected region needs to be associated with a change ticket. For details, see **Issues to Be Implemented on the Live Network**.

----End

6.6.3.4 Issues to Be Implemented on the Live Network

Scenarios

To solve this issue, change implementation is required.

Prerequisites

On the **Positioning solution** page, if you select **Need** for **Whether the live network needs to be changed**. The issue ticket enters the **To be implemented on the live network** status.

Procedure

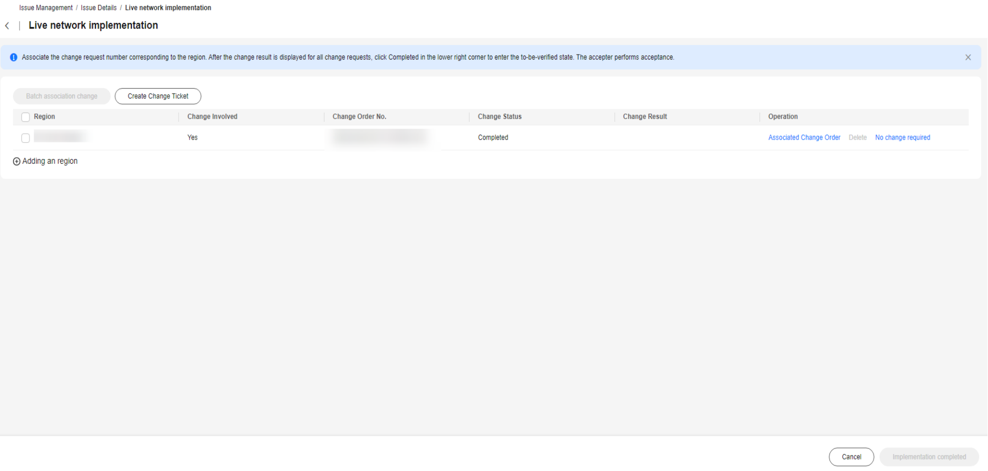
Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click the issue ticket name to go to the issue details page. Click **Live network implementation** in the upper right corner. The involved regions are displayed. Click **Associate Change Order** to associate the change tickets and obtain the change result. If some regions do not involve changes, click **No change required** in the **Operation** column.

Step 4 When you complete the change information, click **Implementation completed**. The issue enters the **To be verified** status.

Figure 6-78 Associating an issue with a change ticket



Associate the change request number corresponding to the region. After the change result is displayed for all change requests, click Completed in the lower right corner to enter the to-be-verified state. The accepter performs acceptance.

□ Region	Change Involved	Change Order No.	Change Status	Change Result	Operation
□ [redacted]	Yes	[redacted]	Completed		Associated Change Order Delete No change required

----End

6.6.3.5 Upgrading/Downgrading an Issue Ticket

Scenarios

After an issue ticket is submitted, if the issue handler thinks that the current issue level is improper, the problem handler can upgrade or degrade the issue.

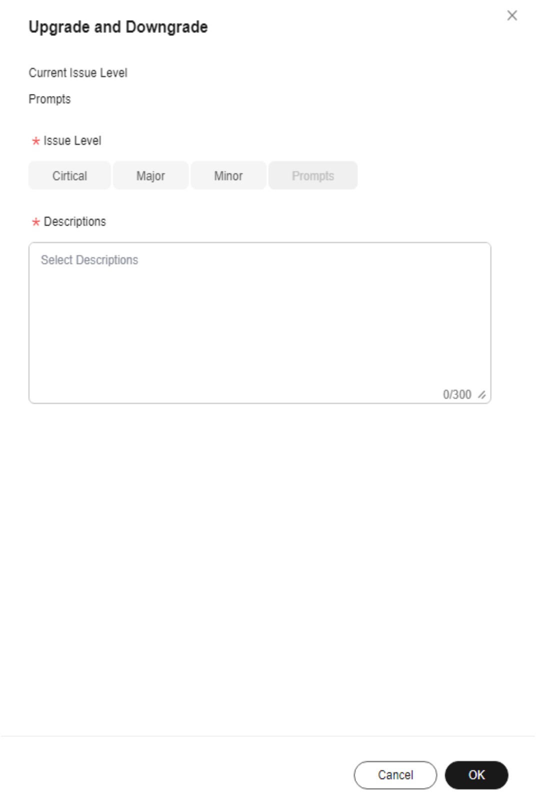
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click the issue name to go to the issue details page. Click **Upgrade and Downgrade** in the upper right corner.

Figure 6-79 Upgrading and downgrading an issue



Upgrade and Downgrade

Current Issue Level

Prompts

* Issue Level

* Descriptions

Step 4 Currently, the upgrade and downgrade do not need to be approved. After you complete the upgrade or degrade, the ticket level will be changed.

----End

6.6.3.6 Suspending an Issue Ticket

Scenarios

After an issue ticket is accepted, the ticket creator needs to provide data or other information in the fault locating phase, and approve the requests during issue implementation phase. After the issue handler suspends the ticket, the creator needs to approve the suspension.

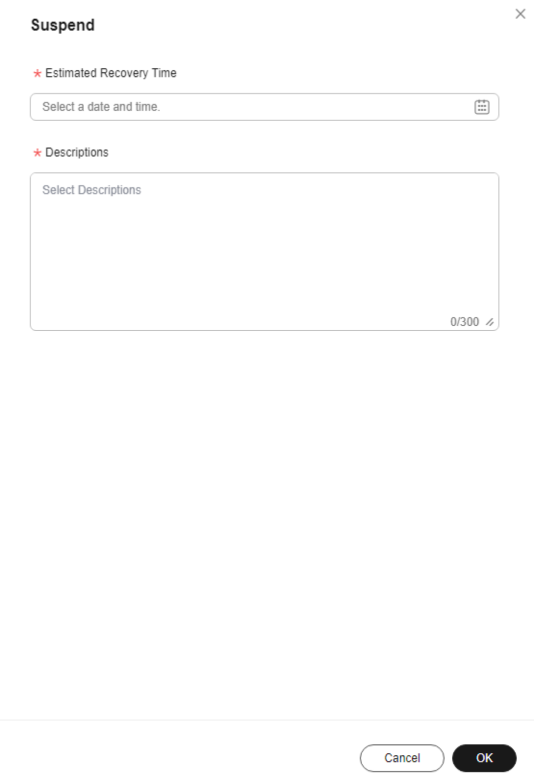
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click the issue name to go to the issue details page. Click **Suspend** in the upper right corner.

Figure 6-80 Issue ticket suspension



Suspend

* Estimated Recovery Time

Select a date and time.

* Descriptions

Select Descriptions

0/300

Step 4 After the ticket is submitted for suspension, the creator clicks the ticket name to go to the issue details page, clicks Suspend Review in the upper right corner of the page, enters review information, and submits the review result. Then the issue handling duration stops counting to prevent suspension recovery.

----End

6.6.3.7 Verifying the Issue Handling Result

Scenarios

After the issue ticket is processed, the creator checks whether the issue is solved.

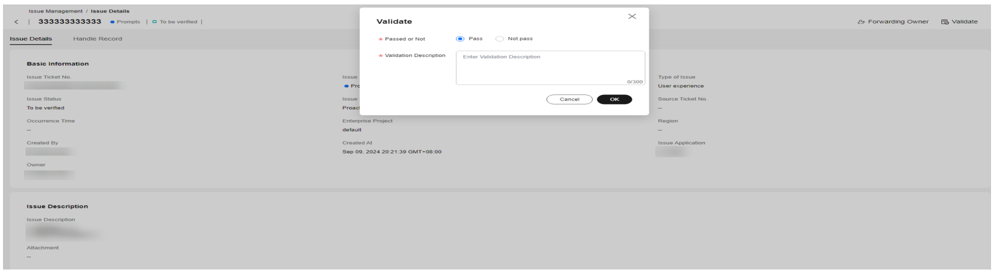
Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Fault Management** > **Issues**. On the displayed page, click **Pending**.

Step 3 Click the issue ticket name to go to the issue details page. Click **Validate** in the upper right corner to go to the verification details page. Enter information and click **OK**.

Figure 6-81 Issue ticket verification page



Issue Management / Issue Details

333333333333 Prompts | To be verified |

Forwarding Owner Validate

Issue Details Handle Record

Basic Information

Issue Ticket No.

Issue Status: To be verified

Occurrence Time: --

Created By

Owner

Enterprise Project: default

Created At: Sep 09, 2024 20:21:39 GMT+08:00

Type of Issue: User experience

Source Ticket No.: --

Region: --

Issue Application

Issue Description

Issue Description

Attachment: --

Validate

* Passed or Not: ● Pass ○ Not pass

* Validation Description: Enter Validation Description 0/300

Cancel OK

Step 4 After the verification is passed, the issue ticket is closed. If the verification fails, the issue ticket status becomes **Locate the solution**.

----End

6.6.4 Viewing Issue History

Scenarios

If you have any questions about issue handling or issue ticket information during issue backtracking, you can view the handle record.

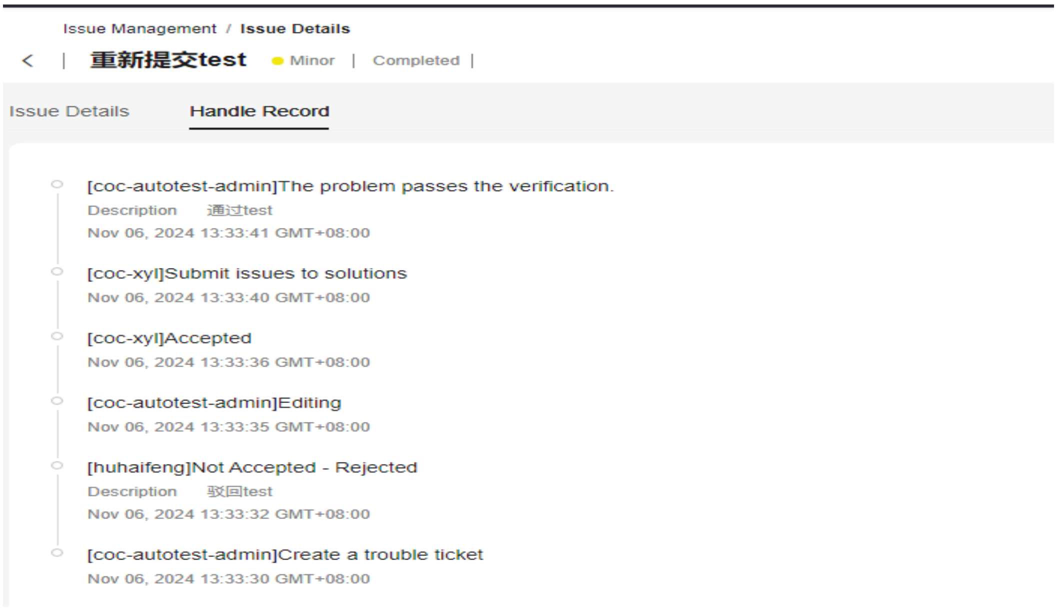
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Fault Management** > **Issues**.

Step 3 Click the issue ticket name to go to the issue details page. Click the **Handle Record** tab to view the issue handling history.

Figure 6-82 Issue handling record



Issue Management / Issue Details

< | 重新提交test ● Minor | Completed |

Issue Details Handle Record

[coc-autotest-admin]The problem passes the verification.
Description 通过test
Nov 06, 2024 13:33:41 GMT+08:00

[coc-xyl]Submit issues to solutions
Nov 06, 2024 13:33:40 GMT+08:00

[coc-xyl]Accepted
Nov 06, 2024 13:33:36 GMT+08:00

[coc-autotest-admin]Editing
Nov 06, 2024 13:33:35 GMT+08:00

[huhaifeng]Not Accepted - Rejected
Description 驳回test
Nov 06, 2024 13:33:32 GMT+08:00

[coc-autotest-admin]Create a trouble ticket
Nov 06, 2024 13:33:30 GMT+08:00

----End

6.7 Forwarding Rules

6.7.1 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.

6.7.2 Forwarding rules

This topic describes how to configure a forwarding rule.

Prerequisites

Before configuring a forwarding rule, ensure that the monitoring system for which the forwarding rule you want to configure has been connected to **Data Sources**.

Scenarios

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

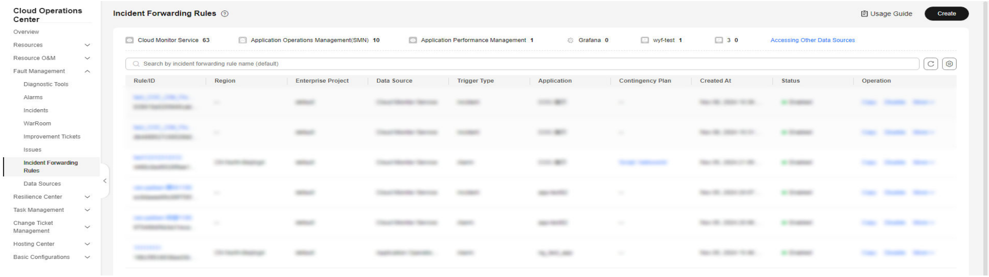
Procedure for Adding a Forwarding Rule

Step 1 Log in to **COC**.

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

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

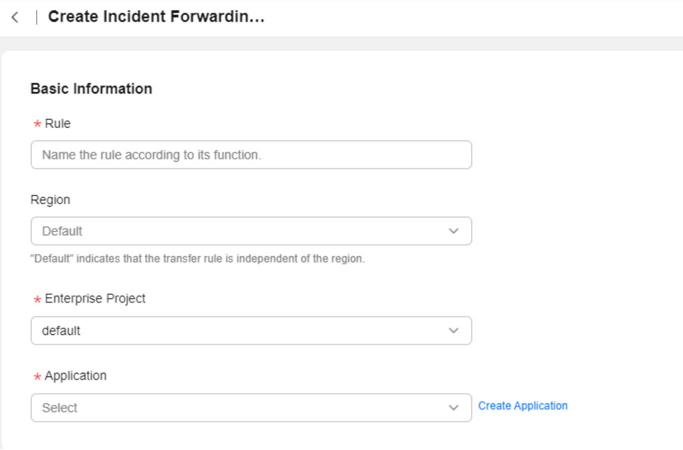
Figure 6-83 Creating an incident forwarding rule



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 6-84 Entering basic information



< | Create Incident Forwardin...

Basic Information

* Rule

Name the rule according to its function.

Region

Default

"Default" indicates that the transfer rule is independent of the region.

* Enterprise Project

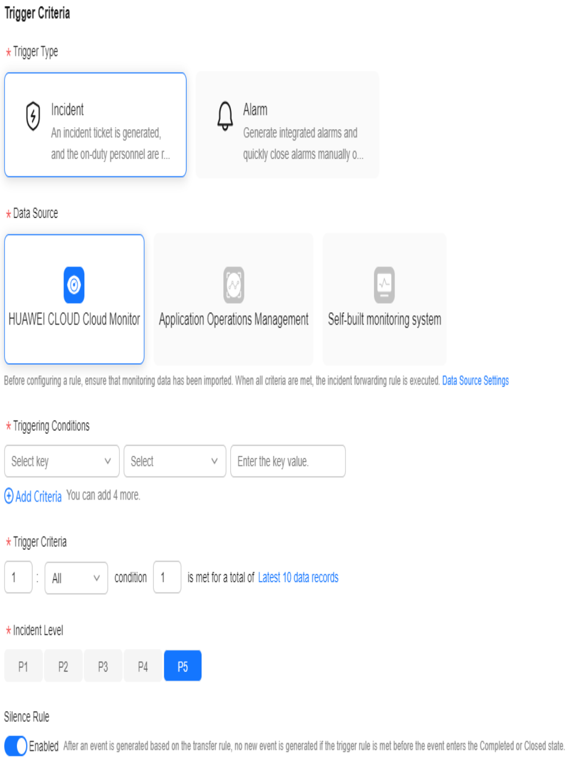
default

* Application

Select

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 6-85 Entering a trigger criteria



Trigger Criteria

* Trigger Type

Incident
An incident ticket is generated, and the on-duty personnel are r...

Alarm
Generate integrated alarms and quickly close alarms manually o...

* Data Source

HUAWEI CLOUD Cloud Monitor

Application Operations Management

Self-built monitoring system

Before configuring a rule, ensure that monitoring data has been imported. When all criteria are met, the incident forwarding rule is executed. Data Source Settings

* Triggering Conditions

Select key | Select | Enter the key value.

Add Criteria You can add 4 more.

* Trigger Criteria

1 : All condition 1 is met for a total of Latest 10 data records

* Incident Level

Silence Rule

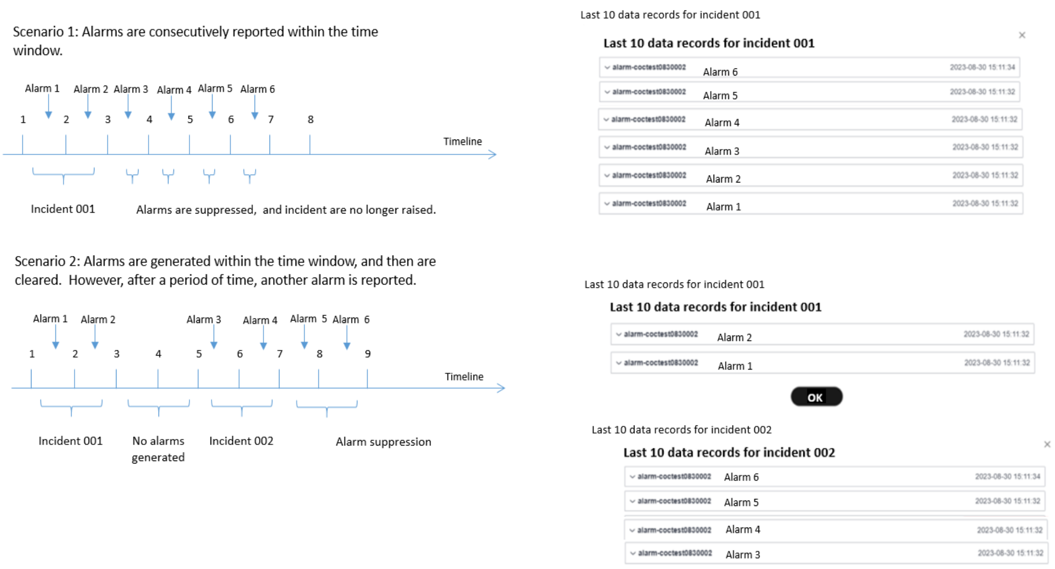
Enabled After an event is generated based on the transfer rule, no new event is generated if the trigger rule is met before the event enters the Completed or Closed state.

NOTICE

1. After an incident is generated based on such a rule, if the incident meets another rule before it is completed or closed, the incident will no longer be generated. This rule is enabled by default and can be disabled.

2. If you receive no raw alarms within the window period, the system considers the alarms generated in the previous window period as historical alarms (that is, the current alarm status is set to **Handled** by default).

Figure 6-86 Converting alarms to incident tickets



Scenario 1: Alarms are consecutively reported within the time window.

Scenario 2: Alarms are generated within the time window, and then are cleared. However, after a period of time, another alarm is reported.

Last 10 data records for incident 001

Last 10 data records for incident 001

alarm-coctest0830002 Alarm 6 2023-08-30 15:11:34
alarm-coctest0830002 Alarm 5 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 4 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 3 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 2 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 1 2023-08-30 15:11:32

Last 10 data records for incident 001

Last 10 data records for incident 001

alarm-coctest0830002 Alarm 2 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 1 2023-08-30 15:11:32

Last 10 data records for incident 002

Last 10 data records for incident 002

alarm-coctest0830002 Alarm 6 2023-08-30 15:11:34
alarm-coctest0830002 Alarm 5 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 4 2023-08-30 15:11:32
alarm-coctest0830002 Alarm 3 2023-08-30 15:11:32

The key in the trigger conditions is described as follows:

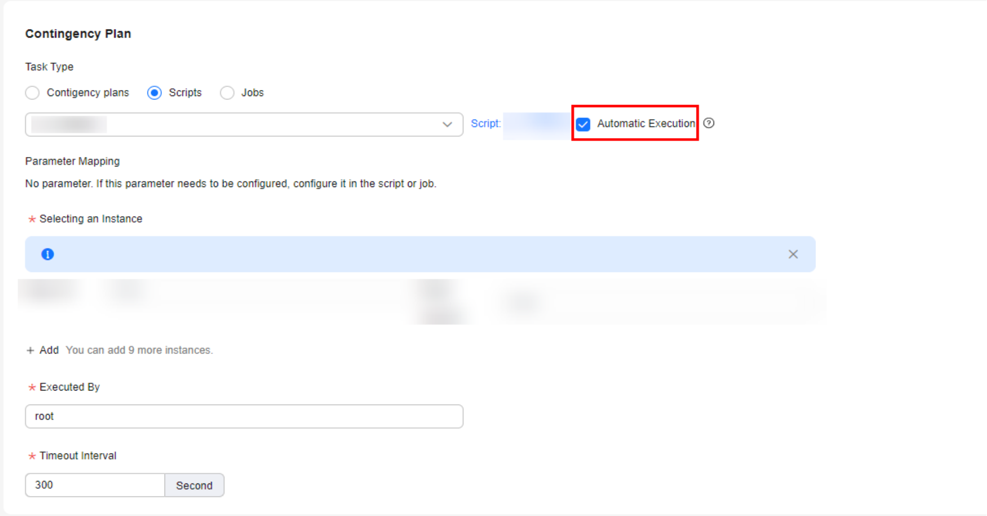
Parameter	Description	CES Alarm Field	AOM Alarm Field
alarmId	Alarm ID	alarm_id	id
alarmName	Alarm name	alarm_name	event_name in metadata
alarmLevel	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Suggestion**.	AlarmLevel	event_severity
time	Time when an alarm is generated	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 6-87 Specifying a contingency plan



Contingency Plan

Task Type

○ Contigency plans ● Scripts ○ Jobs

Script: ☑ Automatic Execution

Parameter Mapping

No parameter. If this parameter needs to be configured, configure it in the script or job.

* Selecting an Instance

+ Add You can add 9 more instances.

* Executed By

root

* Timeout Interval

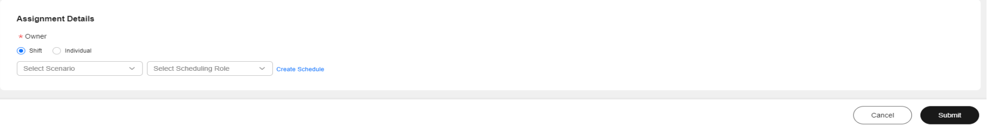
300 Second

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 6-88 Filling the assignment rule



Assignment Details

* Owner

● Shift ○ Individual

Select Scenario

Select Scheduling Role

----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 **Fault 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

6.8 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.

6.8.1 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

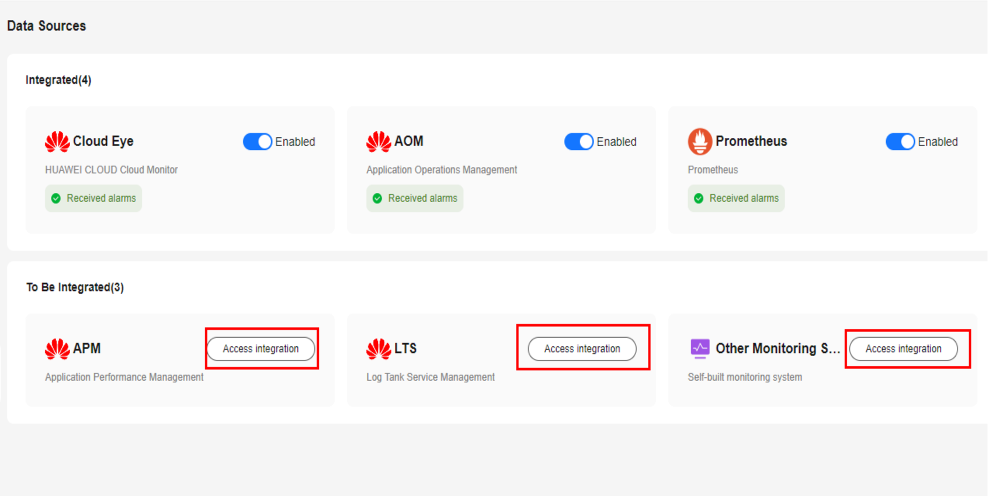
- **This part describes how to integrate Huawei Cloud and open-source monitoring systems to COC.**

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 6-89 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

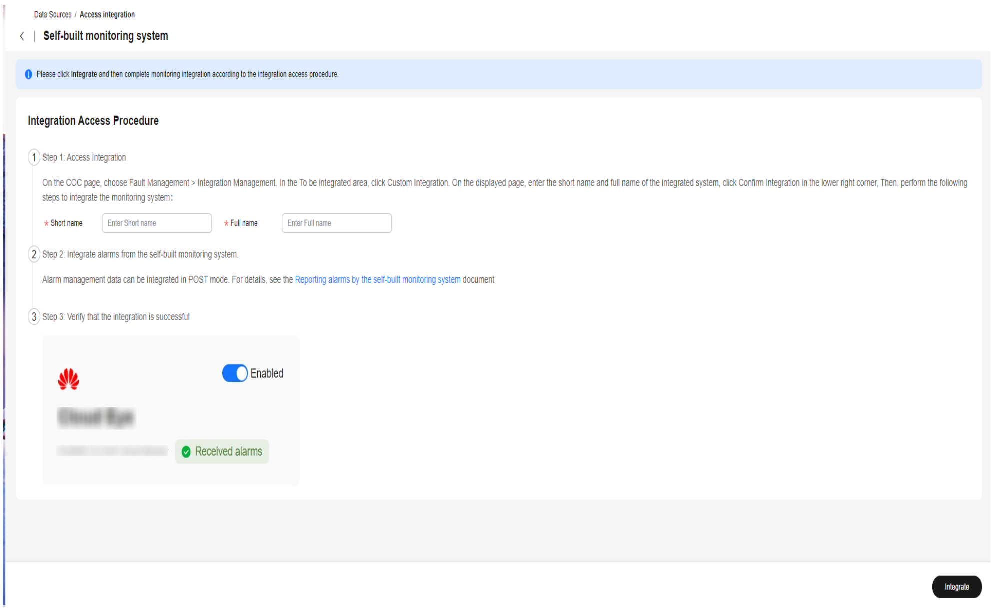
- **This part describes how to integrate monitoring systems except those mentioned in the above part into COC.**

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 6-90 Procedure for integrating a monitoring system



Data Sources / Access integration

Self-built monitoring system

Please click **Integrate** and then complete monitoring integration according to the integration access procedure.

Integration Access Procedure

1 Step 1: Access Integration

On the COC page, choose Fault Management > Integration Management. In the To be integrated area, click Custom Integration. On the displayed page, enter the short name and full name of the integrated system, click Confirm Integration in the lower right corner, Then, perform the following steps to integrate the monitoring system:

* Short name: Enter Short name
* Full name: Enter Full name

2 Step 2: Integrate alarms from the self-built monitoring system.

Alarm management data can be integrated in POST mode. For details, see the Reporting alarms by the self-built monitoring system document

3 Step 3: Verify that the integration is successful

NOTICE

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

----End

Enabling and Disabling a Monitoring System

Step 1 Log in to COC.

Step 2 In the navigation 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

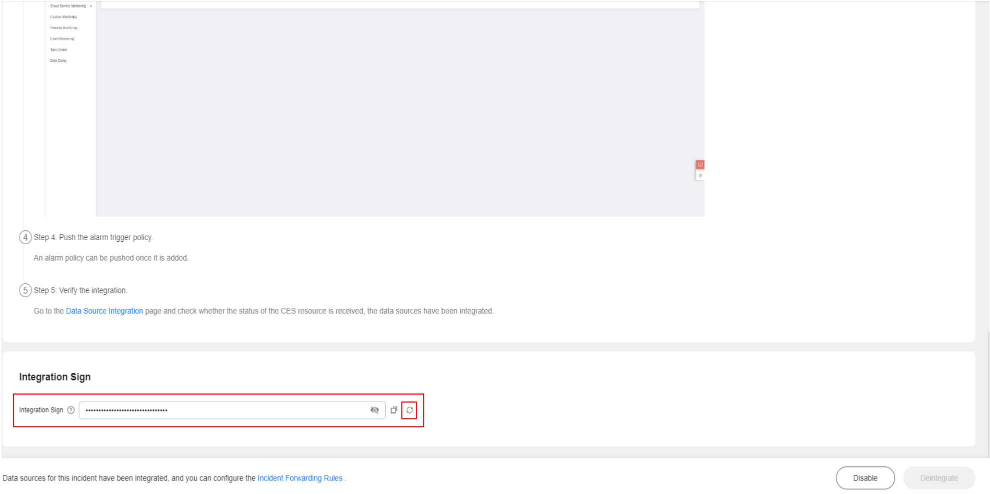
Updating an Integration Sign

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 6-91 Updating an integration sign



4 Step 4: Push the alarm trigger policy.

An alarm policy can be pushed once it is added.

5 Step 5: Verify the integration.

Go to the Data Source Integration page and check whether the status of the CES resource is received, the data sources have been integrated.

Integration Sign

Integration Sign ⓘ ••••••••••••••••••••••••••••••••

Data sources for this incident have been integrated, and you can configure the Incident Forwarding Rules .

----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 a reviewer shift by referring to **Overview**.

Precautions

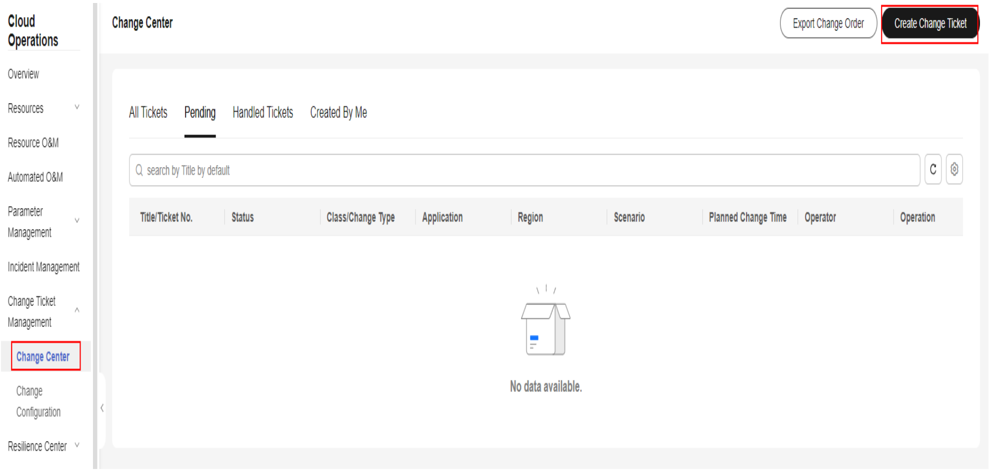
Confirm the content of change ticket and apply for the change based on the actual change requirement.

Procedure

Step 1 Log in to **COC**.

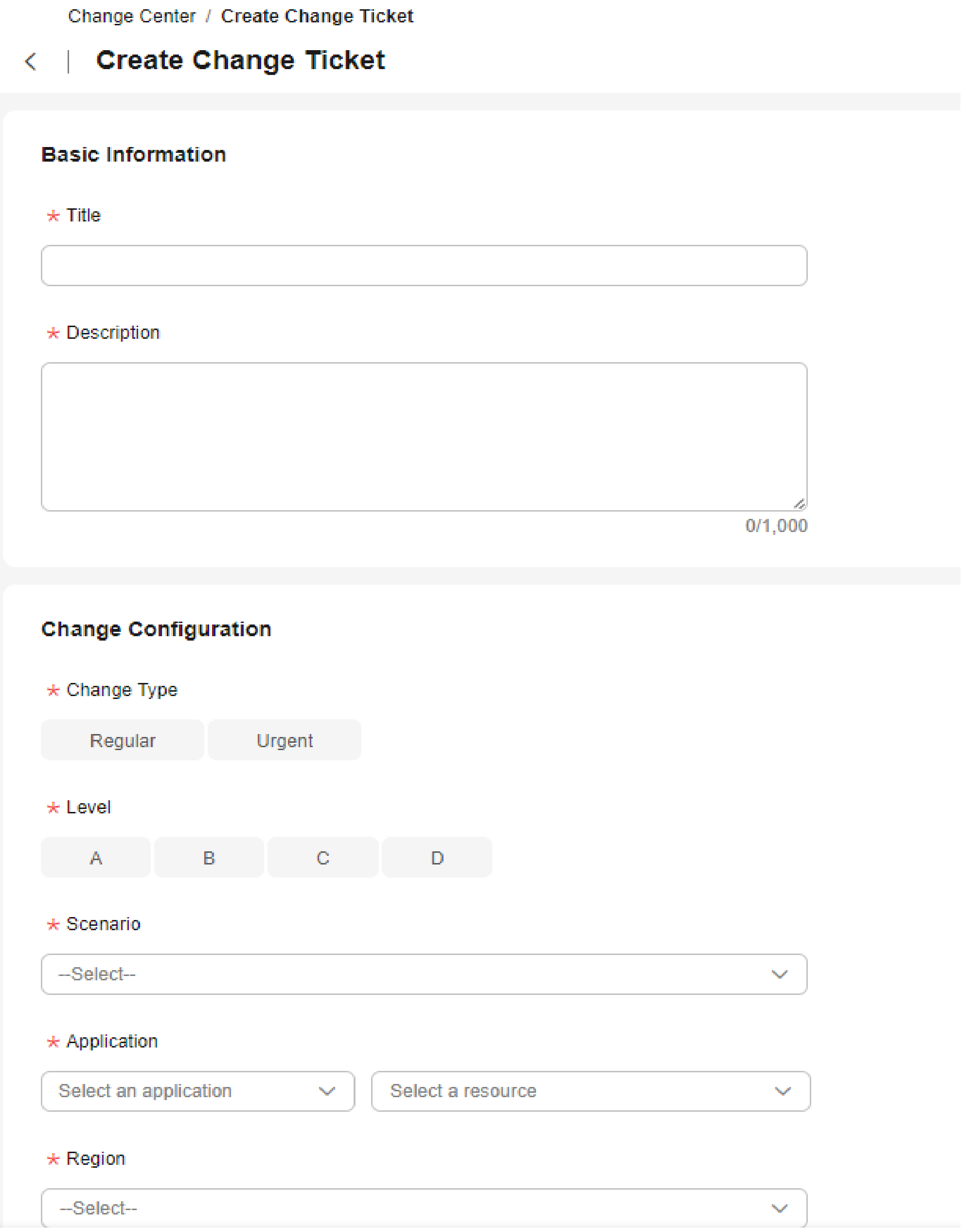
Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**. Click the **Pending** tab, and click **Create Change Ticket**.

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



Change Center / Create Change Ticket

Create Change Ticket

Basic Information

* Title

* Description

0/1,000

Change Configuration

* Change Type

* Level

* Scenario

--Select--

* Application

Select an application

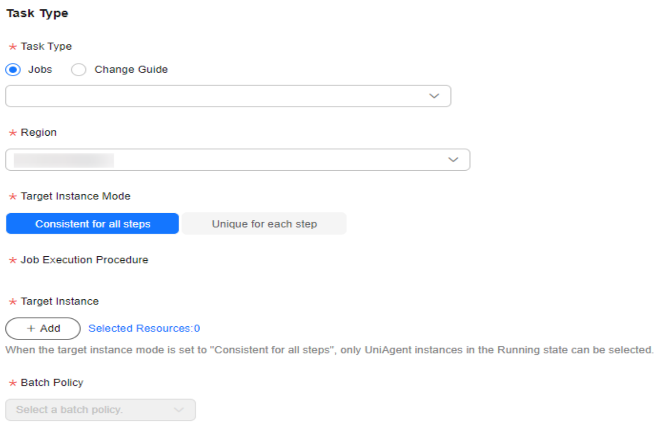
Select a resource

* Region

--Select--

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



Task Type

* Task Type

● Jobs ○ Change Guide

* Region

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

* Target Instance

Selected Resources:0

When the target instance mode is set to "Consistent for all steps", only UniAgent instances in the Running state can be selected.

* Batch Policy

Select a batch policy.

----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**.

7.1.2 Reviewing a Change Ticket

Scenarios

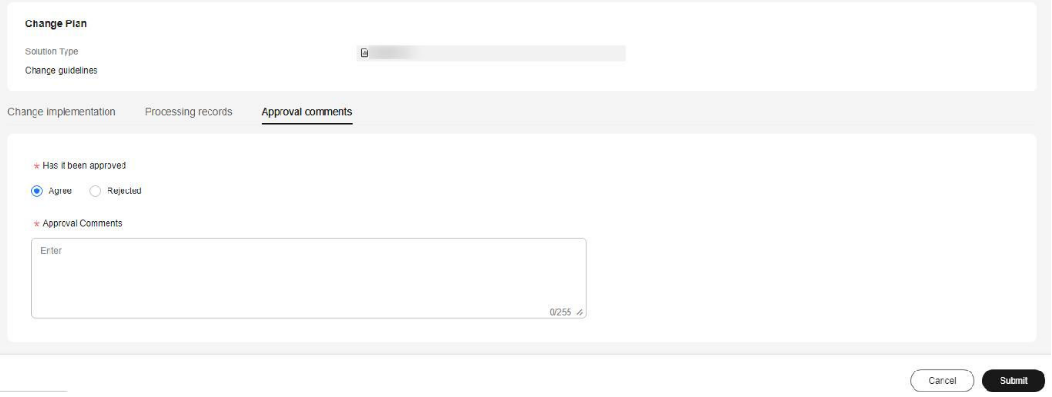
Any created change ticket needs to be reviewed.

Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**. On the displayed page, locate a pending ticket and click the ticket title or click **Deal** in the **Operation** column of a change record to view the change details and review the change.

Figure 7-4 Reviewing a change ticket



Change Plan

Solution Type [redacted]

Change guidelines

Change implementation | Processing records | Approval comments

* Has it been approved

● Agree ○ Rejected

* Approval Comments

Enter

0/255

----End

7.1.3 Implementing and Closing a Change Ticket

Scenarios

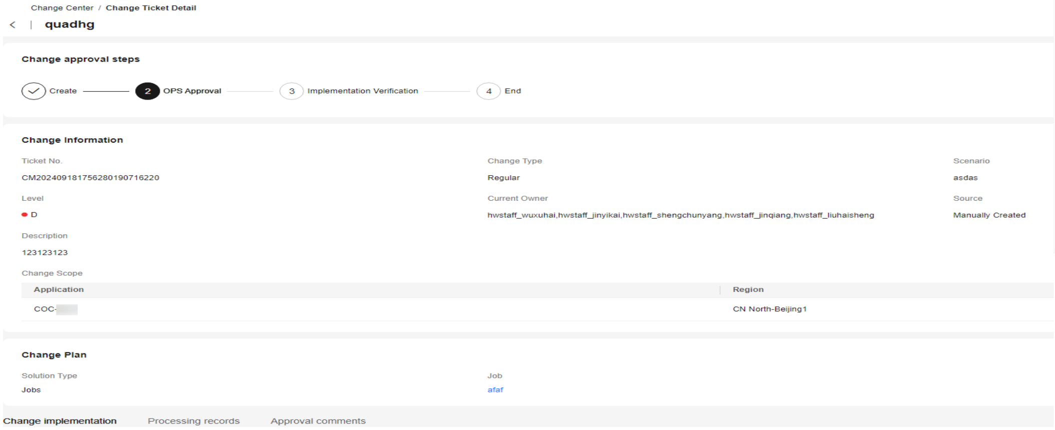
After a change ticket is approved, implement the change within the specified time window according to the change solution.

Procedure

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Center**. On the displayed page, locate a pending ticket and click the ticket title or click **Change Start** in the **Operation** column of a change record to view the change details and review the change. If the change solution is associated with a job, < execute the job first. If the change solution is associated with a change guide, implement the change according to the change guide.

Figure 7-5 Change execution



Change Center / Change Ticket Detail

< | quadhg

Change approval steps

✓ Create — 2 OPS Approval — 3 Implementation Verification — 4 End

Change Information

Ticket No.: CM20240918175628019071622O

Change Type: Regular

Scenario: asdas

Level: ● D

Current Owner: hwstaff_wuxuhai,hwstaff_jinyikai,hwstaff_shengchunyang,hwstaff_jinqiang,hwstaff_liuhaisheng

Source: Manually Created

Description: 123123123

Change Scope

Application	Region
COC-[redacted]	CN North-Beijing1

Change Plan

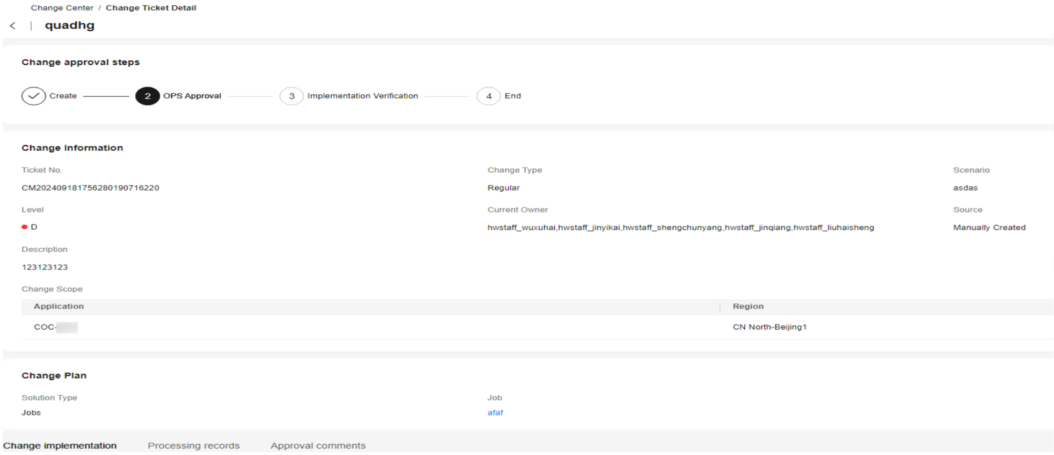
Solution Type: Jobs

Job: afaf

Change implementation | Processing records | Approval comments

Step 3 After the change is complete, click the step for finishing the change and enter the change result.

Figure 7-6 Specifying the change result



Change Center / Change Ticket Detail

quadhg

Change approval steps

Change Information

Ticket No.: CM20240918175628019071622O

Change Type: Regular

Scenario: asdas

Level: ● D

Current Owner: hwstaff_wuxuhai,hwstaff_jinyikai,hwstaff_shengchunyang,hwstaff_jinqiang,hwstaff_liuhaisheng

Source: Manually Created

Description: 123123123

Change Scope

Application	Region
COC-[redacted]	CN North-Beijing1

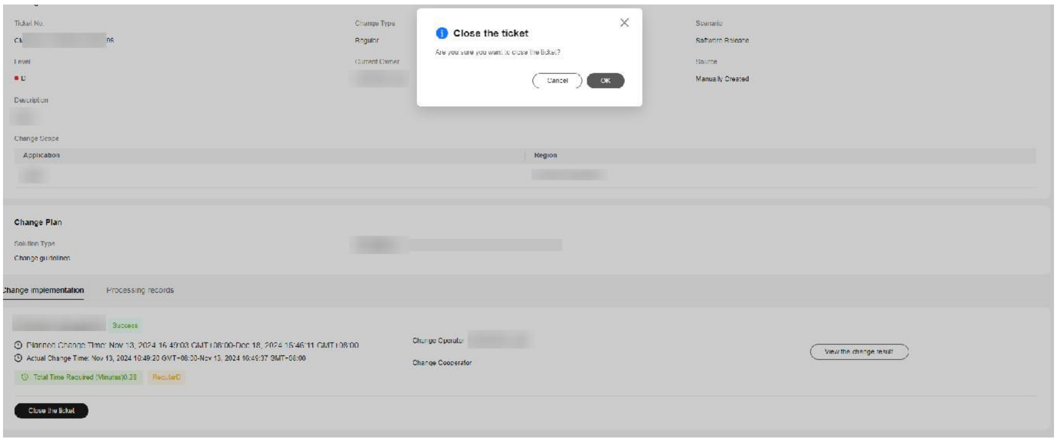
Change Plan

Solution Type: Jobs

Job: afaf

Step 4 After the change result is specified, click **Close** to close the change ticket.

Figure 7-7 Closing a change ticket



Ticket No.: CM[redacted]06

Change Type: Regular

Scenario: Software Release

Level: ● D

Current Owner: [redacted]

Source: Manually Created

Description: [redacted]

Change Scope

Application	Region
[redacted]	[redacted]

Close the ticket

Are you sure you want to close the ticket?

Change Plan

Solution Type: Change guidelines

[redacted] Success

Planned Change Time: Nov 13, 2024 16:49:03 GMT+08:00-Dec 18, 2024 15:46:11 GMT+08:00

Actual Change Time: Nov 13, 2024 16:49:20 GMT+08:00-Nov 13, 2024 16:49:37 GMT+08:00

Total Time Required (Minutes)0.28 RegularD

Change Operator: [redacted]

Change Cooperator

----End

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

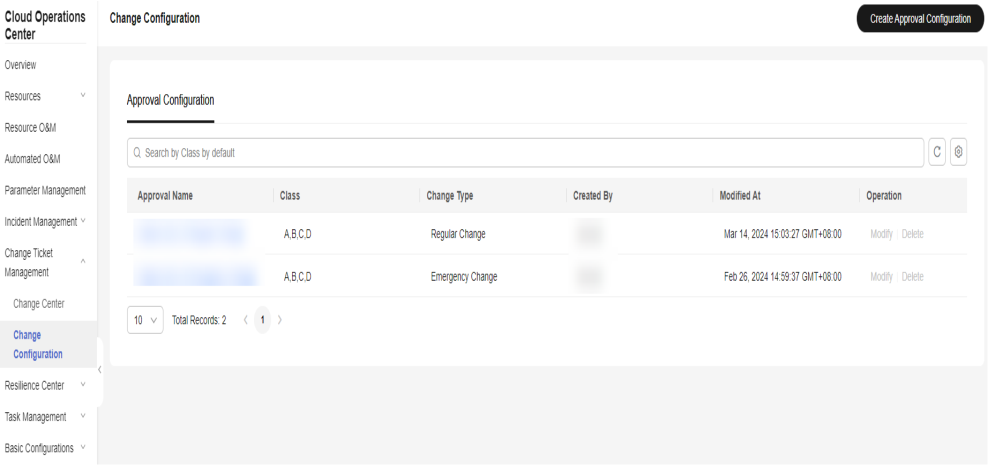
Users can configure the change type, change level, review process, and reviewer.

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 7-8 Creating a review configuration



Cloud Operations Center

- Overview
- Resources
- Resource O&M
- Automated O&M
- Parameter Management
- Incident Management
- Change Ticket Management
  - Change Center
  - Change Configuration
- Resilience Center
- Task Management
- Basic Configurations

Change Configuration

Create Approval Configuration

Approval Configuration

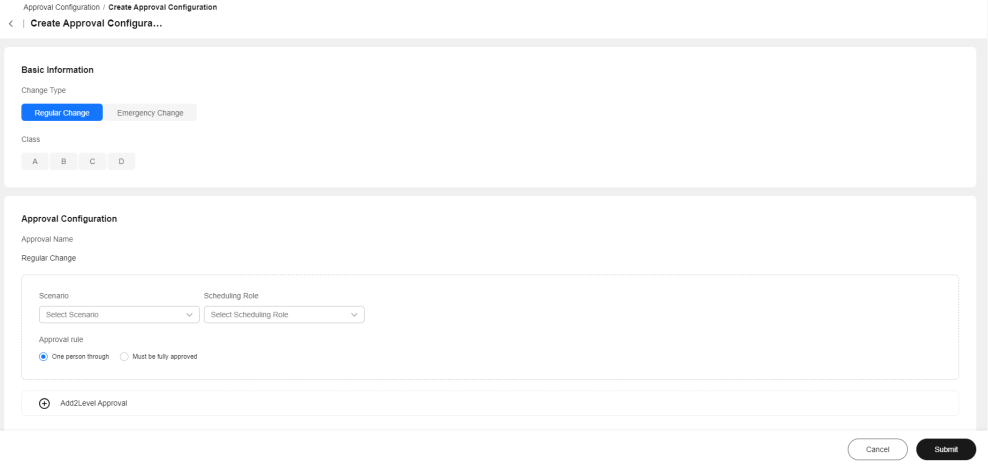
Search by Class by default

Approval Name	Class	Change Type	Created By	Modified At	Operation
[redacted]	A,B,C,D	Regular Change	[redacted]	Mar 14, 2024 15:03:27 GMT+08:00	Modify | Delete
[redacted]	A,B,C,D	Emergency Change	[redacted]	Feb 26, 2024 14:59:37 GMT+08:00	Modify | Delete

10 Total Records: 2 < 1 >

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

Figure 7-9 Setting the review configurations



Approval Configuration / Create Approval Configuration

Create Approval Configura...

Basic Information

Change Type: [✓ Regular Change] Emergency Change

Class: A B C D

Approval Configuration

Approval Name

Regular Change

Scenario: Select Scenario

Scheduling Role: Select Scheduling Role

Approval rule: ● One person through ○ Must be fully approved

Add2Level Approval

Cancel Submit

----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

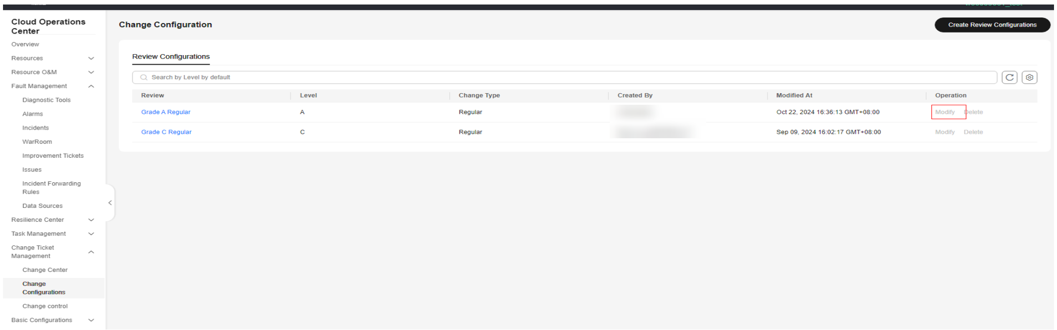
Note: A scheduling role takes effect only after the reviewer is configured. If the reviewer is not specified, the change request cannot be submitted.

Modifying the review configuration

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Management** > **Change Configurations**. On the displayed page, locate the target record, click **Modify** in the **Operation** column to modify the review configuration information.

Figure 7-10 Modifying review configuration



Review	Level	Change Type	Created By	Modified At	Operation
Grade A Regular	A	Regular	[redacted]	Oct 22, 2024 16:36:13 GMT+08:00	Modify Delete
Grade C Regular	C	Regular	[redacted]	Sep 09, 2024 16:02:17 GMT+08:00	Modify Delete

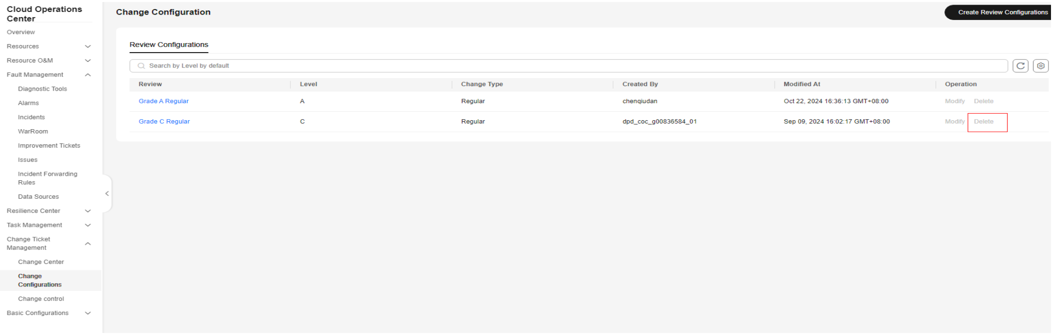
----End

Deleting review configuration

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Change Management** > **Change Configurations**. On the displayed page, locate the target record, click **Delete** in the **Operation** column to delete the review configuration information.

Figure 7-11 Deleting review configuration



Review	Level	Change Type	Created By	Modified At	Operation
Grade A Regular	A	Regular	chenqiudan	Oct 22, 2024 16:36:13 GMT+08:00	Modify Delete
Grade C Regular	C	Regular	dpd_coc_g00836584_01	Sep 09, 2024 16:02:17 GMT+08:00	Modify Delete

----End

7.3 Controlling Changes

When changing resources, you can only use the service ticket-based privilege escalation method to execute scripts, jobs, or query accounts and passwords. This ensures that the operator and operation object of a change ticket match the actual resources you want to change, preventing excessive permissions of the operator and reducing security risks.

Scenarios

You can configure whether to enable privilege escalation using a service ticket based on application scenarios. Currently, privilege escalation using incidents, war rooms, and change tickets are supported.

Precautions

1. By default, the change control policy generated by COC can only be bound to user groups for further permissions granting. Do not use the policy for other purposes.

2. You can click the editing button of actions on the COC page to control whether to determine whether to control functions corresponding to the actions. Note that all operations must be performed on COC. Do not directly edit the policy.

3. If you enabled the feature of privilege escalation using service tickets, you also need to bind the policy to your account. To disable this policy, you need to unbind the policy from your user group first.

4. During service ticket privilege escalation, the system needs to verify the region, application, and service ticket status of the resources required. If a resource does not belong to any region or application, the system does not verify the resource but will display all service tickets of the user. Verification requirements on service tickets:

Incident ticket status verification:

(1) P1, P2, P3, and P4 incident tickets in the accepted state

(2) The privilege escalation application must be the same as the one in the incident ticket analysis and handling phase.

(3) The privilege escalation operator must be the same as the current owner in the incident analysis and handling phase.

(4) The privilege escalation region must be the same as the region specified in the incident ticket.

War room status verification:

(1) The war room must be in the started or fault demarcation status.

(2) The privilege escalation application must be in the list of applications affected by the war room.

(3) The privilege escalation operator must be the fault recovery owner, a fault recovery member, or the administrator of the war room.

Change ticket status verification:

(1) The region of the privilege escalation application must be the same as that specified in the change ticket.

(2) The privilege escalation operator must be the implementer of the change ticket.

(3) The current operation time must be within the planned implementation time window of the change ticket. (The current operation time must be later than the planned start time and earlier than the planned end time.)

(4) You must click **Change Start** for a change ticket.

NOTICE

After service ticket privilege escalation is enabled, the northbound interface becomes unavailable. For example, if a script is executed to enable service ticket privilege escalation, the northbound script interface cannot be used.

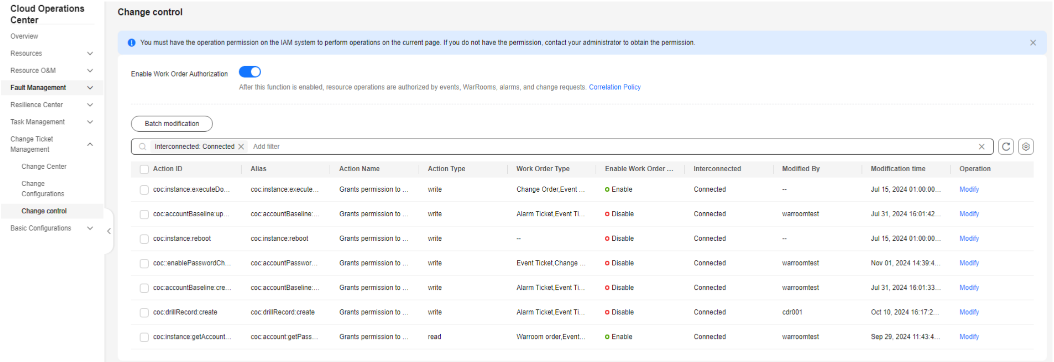
Procedure

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Change Ticket Management** > **Change Control**. By default, the service ticket-based authorization feature is disabled. To enable it, toggle the feature on.

Step 3 After this feature is enabled, all actions of COC are displayed in the list. You can enable or disable the interconnected actions. If this feature is disabled, service ticket-based privilege escalation is not required for all account operations in this scenario. If this function is enabled, service ticket privilege escalation is required.

Figure 7-12 Change control list



Change control

You must have the operation permission on the IAM system to perform operations on the current page. If you do not have the permission, contact your administrator to obtain the permission.

Enable Work Order Authorization

After this function is enabled, resource operations are authorized by events, WarRooms, alarms, and change requests. Correlation Policy

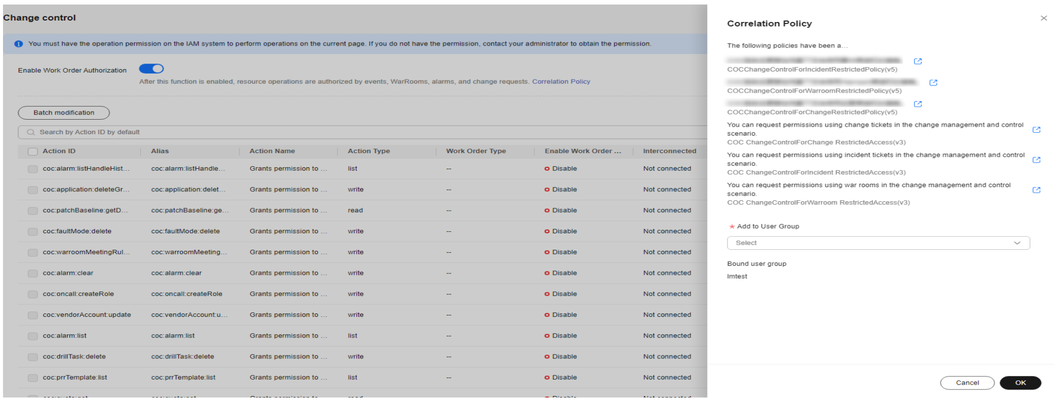
Batch modification

Interconnected: Connected Add filter

Action ID	Alias	Action Name	Action Type	Work Order Type	Enable Work Order ...	Interconnected	Modified By	Modification time	Operation
coc:instance:executeDo...	coc:instance:execute...	Grants permission to ...	write	Change Order,Event ...	Enable	Connected	--	Jul 15, 2024 01:00:00...	Modify
coc:accountBaseline:up...	coc:accountBaseline:...	Grants permission to ...	write	Alarm Ticket,Event Ti...	Disable	Connected	warroomtest	Jul 31, 2024 16:01:42...	Modify
coc:instance:reboot	coc:instance:reboot	Grants permission to ...	write	--	Disable	Connected	--	Jul 15, 2024 01:00:00...	Modify
coc::enablePasswordCh...	coc:accountPasswor...	Grants permission to ...	write	Event Ticket,Change ...	Disable	Connected	warroomtest	Nov 01, 2024 14:39:4...	Modify
coc:accountBaseline:cre...	coc:accountBaseline:...	Grants permission to ...	write	Alarm Ticket,Event Ti...	Disable	Connected	warroomtest	Jul 31, 2024 16:01:33...	Modify
coc:drillRecord:create	coc:drillRecord:create	Grants permission to ...	write	Alarm Ticket,Event Ti...	Disable	Connected	cdr001	Oct 10, 2024 16:17:2...	Modify
coc:instance:getAccount...	coc:account:getPass...	Grants permission to ...	read	Warroom order,Event...	Enable	Connected	warroomtest	Sep 29, 2024 11:43:4...	Modify

Step 4 After an action is enabled, you need to associate it with a policy: Add the autocratically generated COC policies to your user group. Then, you can use the service ticket to escalate privileges.

Figure 7-13 Associating a policy with an action



Change control

You must have the operation permission on the IAM system to perform operations on the current page. If you do not have the permission, contact your administrator to obtain the permission.

Enable Work Order Authorization

After this function is enabled, resource operations are authorized by events, WarRooms, alarms, and change requests. Correlation Policy

Batch modification

Search by Action ID by default

Action ID	Alias	Action Name	Action Type	Work Order Type	Enable Work Order ...	Interconnected
coc:alarm:listHandleHist...	coc:alarm:listHandle...	Grants permission to ...	list	--	Disable	Not connected
coc:application:deleteGr...	coc:application:delet...	Grants permission to ...	write	--	Disable	Not connected
coc:patchBaseline:getD...	coc:patchBaseline:ge...	Grants permission to ...	read	--	Disable	Not connected
coc:faultMode:delete	coc:faultMode:delete	Grants permission to ...	write	--	Disable	Not connected
coc:warroomMeetingRul...	coc:warroomMeeting...	Grants permission to ...	write	--	Disable	Not connected
coc:alarm:clear	coc:alarm:clear	Grants permission to ...	write	--	Disable	Not connected
coc:oncall:createRole	coc:oncall:createRole	Grants permission to ...	write	--	Disable	Not connected
coc:vendorAccount:update	coc:vendorAccount:u...	Grants permission to ...	write	--	Disable	Not connected
coc:alarm:list	coc:alarm:list	Grants permission to ...	list	--	Disable	Not connected
coc:drillTask:delete	coc:drillTask:delete	Grants permission to ...	write	--	Disable	Not connected
coc:prrTemplate:list	coc:prrTemplate:list	Grants permission to ...	list	--	Disable	Not connected

Correlation Policy

The following policies have been a...

[redacted]
COCChangeControlForIncidentRestrictedPolicy(v5)

[redacted]
COCChangeControlForWarroomRestrictedPolicy(v5)

[redacted]
COCChangeControlForChangeRestrictedPolicy(v5)

You can request permissions using change tickets in the change management and control scenario.
COC ChangeControlForChange RestrictedAccess(v3)

You can request permissions using incident tickets in the change management and control scenario.
COC ChangeControlForIncident RestrictedAccess(v3)

You can request permissions using war rooms in the change management and control scenario.
COC ChangeControlForWarroom RestrictedAccess(v3)

* Add to User Group

Select

Bound user group

lmtest

----End

8 Resilience Center

8.1 Chaos Drills

8.1.1 Overview

With the transformation from traditional IT infrastructure O&M to cloud service O&M, traditional O&M methods face challenges such as complex inter-service invoking, fast application iteration, massive O&M objects, and complex non-linearity systems. Service downtime will bring huge economic losses and reputational damage to the company.

Chaos engineering is introduced to the O&M process. Through periodic simulation, system weaknesses (such as software bugs, solution design defects, and fault recovery process points) can be identified before problems occur on the live network, and system availability problems can be detected and resolved in a timely manner, continuously improve application resilience and build O&M confidence. For unavoidable scenarios (such as hardware faults, abnormal server power-off, and network device board faults), formulate a quick recovery emergency plan in advance.

COC allows users to perform automatic chaos drills covering from risk identification, emergency plan management, fault injection, and review and improvement, Based on years of best practices of Huawei Cloud SRE in chaos drills, customers can proactively identify, mitigate, and verify risks of cloud applications, continuously improving the resilience of cloud applications.

Image and Weapon Version Support Statement

Two types of attack targets, including bare metal servers (BMSs) and Flexus L instances, are added to COC chaos drills, and corresponding resource and network weapons are provided for users to drill. By integrating weapon modules and functions, you can accurately simulate faults in the real world environment and detect system availability issues as early as possible, continuously improving application resilience.

The following table lists the BMS and Flexus L image versions and supported probe tools.

⚠ CAUTION

CentOS 6.10 images and earlier versions do not support probe tools because the system does not have the shared libraries (GLIBC_2.14 and GLIBCXX_3.4.15) required for running probe packages.

Table 1 lists the probes supported by each BMS image version.

Table 8-1 Bare metal server image and tool compatibility list

Weapons		Supported Image Versions
Resource weapon	Increased CPU Usage	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Memory stress	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Disk stress	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Disk I/O stress	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Process ID exhaustion	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Killing a process/ Continuously killing a process	CentOS 7.4, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
Network weapon	Network latency	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Network packet loss	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Error packets	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Duplicate packets	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Packet disorder	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	Network disconnection	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3
	NIC down	CentOS 7.3, CentOS 7.9, Ubuntu16, Ubuntu 1804, EulerOS 2.3

Table 8-2 lists the probes supported by each Flexus L image version.

Table 8-2 Flexus L instance images and probe tool compatibility list

Weapons		Supported Image Versions
Resource weapon	Increased CPU Usage	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Memory stress	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Disk stress	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Disk I/O stress	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Process ID exhaustion	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Killing a process/ Continuously killing a process	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
Network weapon	Network latency	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Network packet loss	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Error packets	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Duplicate packets	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Packet disorder	CentOS 7.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	Network disconnection	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0
	NIC down	CentOS 7.2, CentOS 8.2, Ubuntu 16.04, Ubuntu 22.04, EulerOS 2.0, Debian 8.2, Debian 11.1.0

8.1.2 Failure Modes

A failure mode refers to a specific type of problem or failure status that may occur during application running. Build a rich failure mode library and formulate corresponding prevention and recovery measures to help design a more highly available application system. By identifying potential faults, you can perform routine drills to verify whether the fault recovery measures and fault impacts meet the expectations and prepare for better response to various challenges.

Scenarios

You can analyze the possible fault points of an application, create a failure mode by describing the fault occurrence conditions, fault symptoms, and customer impacts, and apply the failure mode to routine chaos drills.

Precautions

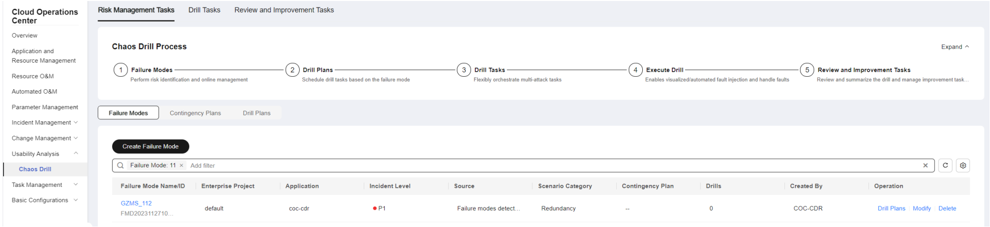
Check whether the enterprise project, application, event level, and scenario category of the failure mode are correct.

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 **Failure Modes**. On the displayed page, click **Create Failure Mode**.

Figure 8-1 Failure Modes



Chaos Drill Process

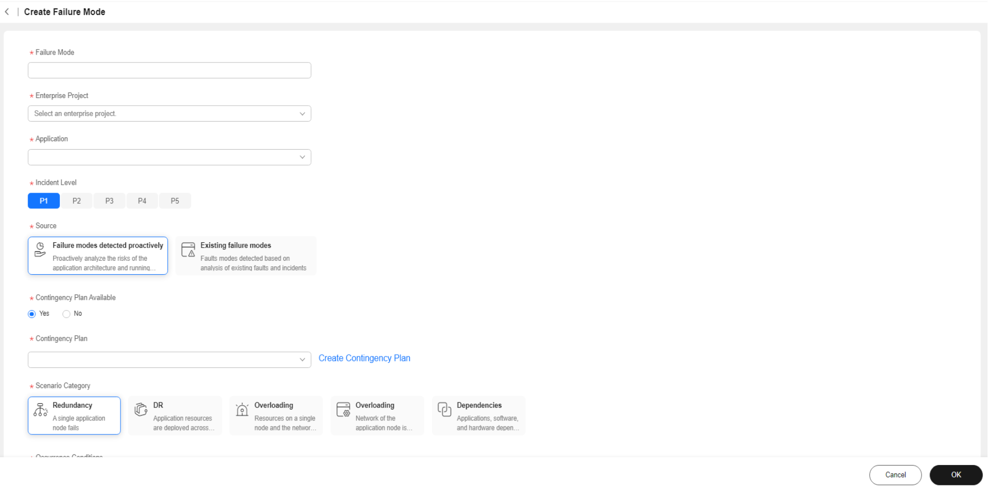
1 Failure Modes: Perform risk identification and online management
2 Drill Plans: Schedule drill tasks based on the failure mode
3 Drill Tasks: Flexibly orchestrate multi-attack tasks
4 Execute Drill: Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks: Review and summarize the drill and manage improvement task...

Failure Mode: 11

Failure Mode Name/ID	Enterprise Project	Application	Incident Level	Source	Scenario Category	Contingency Plan	Drills	Created By	Operation
GZMS_112 FMD2023112710...	default	coc-cdr	● P1	Failure modes detect...	Redundancy	--	0	COC-CDR	Drill Plans Modify Delete

Step 3 Enter the failure mode information by referring to **Table 8-3**.

Figure 8-2 Creating a failure mode



* Failure Mode

* Enterprise Project: Select an enterprise project.

* Application

* Incident Level: [✓ P1] P2 P3 P4 P5

* Source: [✓ Failure modes detected proactively — Proactively analyze the risks of the application architecture and running...] Existing failure modes — Faults modes detected based on analysis of existing faults and incidents

* Contingency Plan Available: ● Yes ○ No

* Contingency Plan

* Scenario Category: [✓ Redundancy — A single application node fails] DR — Application resources are deployed across... Overloading — Resources on a single node and the networ... Overloading — Network of the application node is... Dependencies — Applications, software, and hardware depen...

* Occurrence Conditions

Table 8-3 Failure mode parameters

Parameter	Description
Failure Mode	Custom failure mode name
Enterprise Project	Enterprise project to which the failure mode resource belongs. **default** is the preset value.
Application	Application to which the drill target belongs
Incident Level	For details about the incident level, see **Creating an Incident**.
Source	Including **Failure modes detected proactively** and **Existing failure modes**.
Contingency Plan Available	**Yes** or **No**. The default value is **Yes**.
Contingency Plan Available	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
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 drop-down list. 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 and the planned drill time. The executor creates a drill task by receiving a ticket. A drill task is associated with the fault mode and region.

Precautions

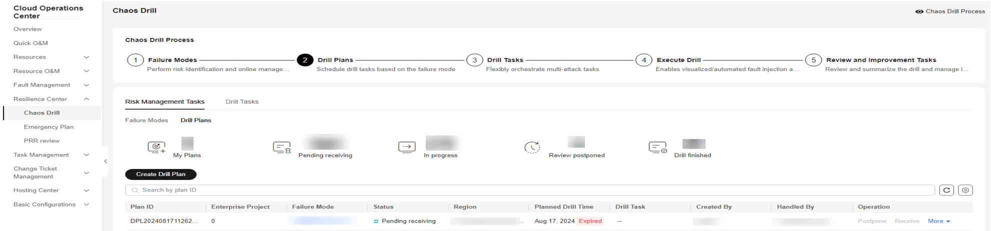
You do not need to specify the enterprise project to which the drill plan belongs. The enterprise project must be the same as that associated with the fault mode.

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**.

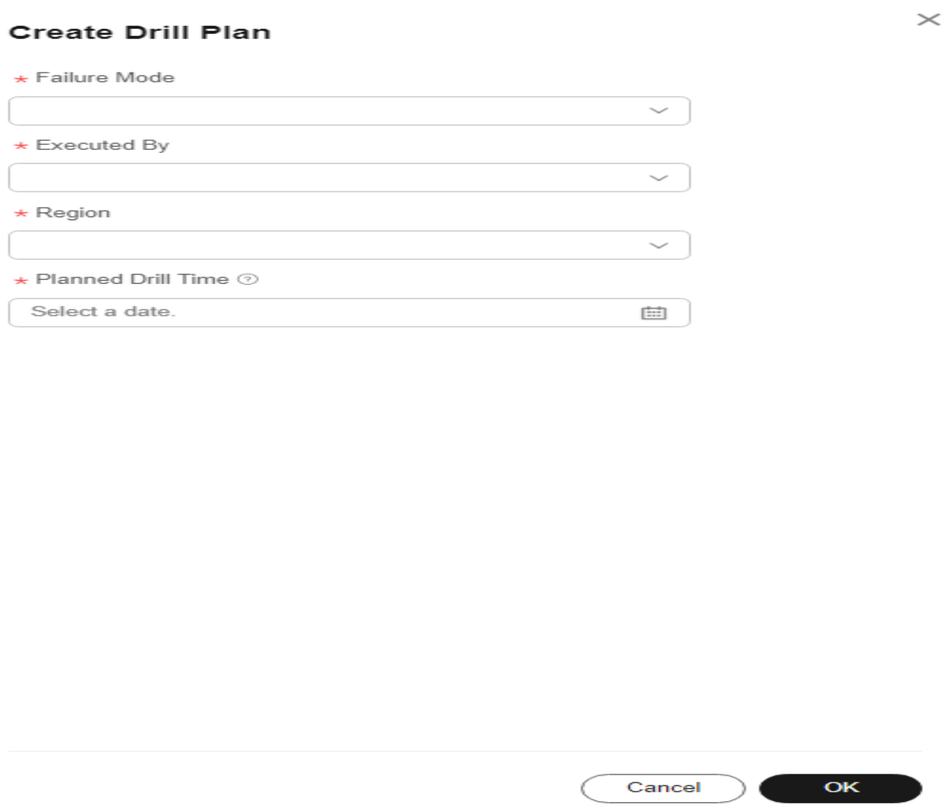
Figure 8-3 Drill Plans



Plan ID	Enterprise Project	Failure Mode	Status	Region	Planned Drill Time	Drill Task	Created By	Handled By	Operation
DPL2024081711262...	0	[redacted]	Pending receiving	[redacted]	Aug 17, 2024 Expired	--	[redacted]	[redacted]	Postpone Receive More

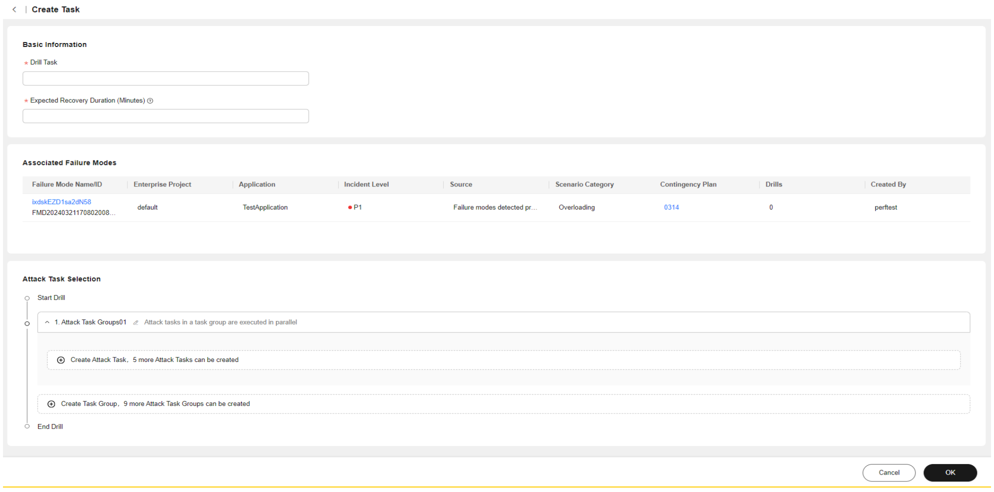
Step 3 Click **Create Drill Plan**. In the displayed dialog box, set **Failure Mode**, **Executed By**, **Region**, and **Planned Drill Time**, and click **OK**.

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



Create Task

Basic Information

* Drill Task

* Expected Recovery Duration (Minutes)

Associated Failure Modes

Failure Mode Name/ID	Enterprise Project	Application	Incident Level	Source	Scenario Category	Contingency Plan	Drills	Created By
ixdskEZD1sa2dN58 FMD20240321170802008...	default	TestApplication	● P1	Failure modes detected pr...	Overloading	0314	0	perftest

Attack Task Selection

Start Drill

1. Attack Task Groups01 Attack tasks in a task group are executed in parallel

Create Attack Task, 5 more Attack Tasks can be created

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

End Drill

----End

8.1.4 Drill Tasks

Scenarios

Manage chaos drill tasks and view drill records.

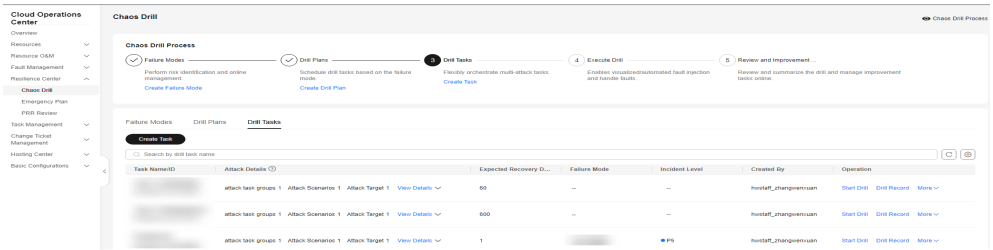
Creating a Drill Task

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 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



Chaos Drill

Chaos Drill Process

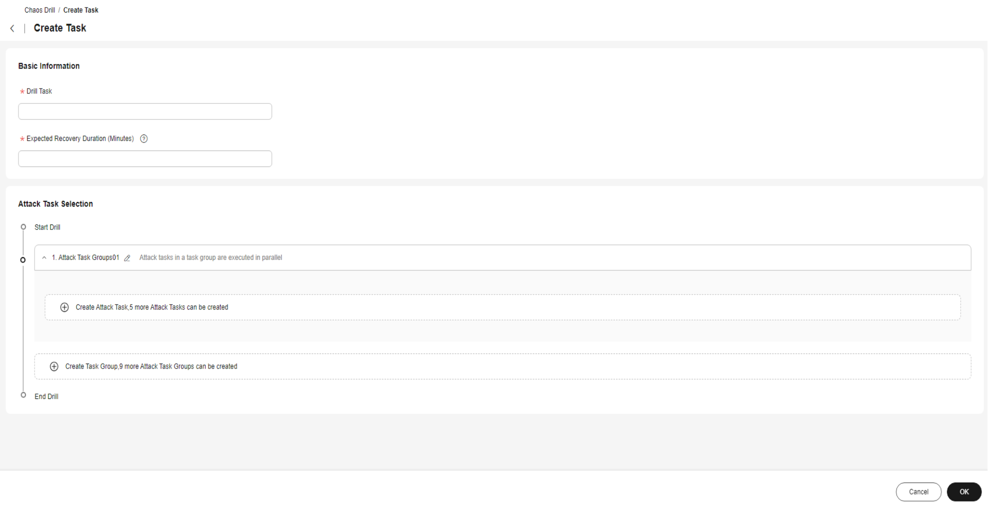
1. Failure Modes — Perform risk identification and online management. Create Failure Mode
2. Drill Plans — Schedule drill tasks based on the failure mode. Create Drill Plan
3. Drill Tasks — Flexibly orchestrate multi-attack tasks. Create Task
4. Execute Drill — Enables visualized/automated fault injection and handle faults.
5. Review and Improvement ... — Review and summarize the drill and manage improvement tasks online.

Task Name/ID	Attack Details	Expected Recovery D...	Failure Mode	Incident Level	Created By	Operation
[redacted]	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Details	60	--	--	hwstaff_zhangwenxuan	Start Drill Drill Record More
[redacted]	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Details	600	--	--	hwstaff_zhangwenxuan	Start Drill Drill Record More
[redacted]	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Details	1	[redacted]	● P5	hwstaff_zhangwenxuan	Start Drill Drill Record More

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

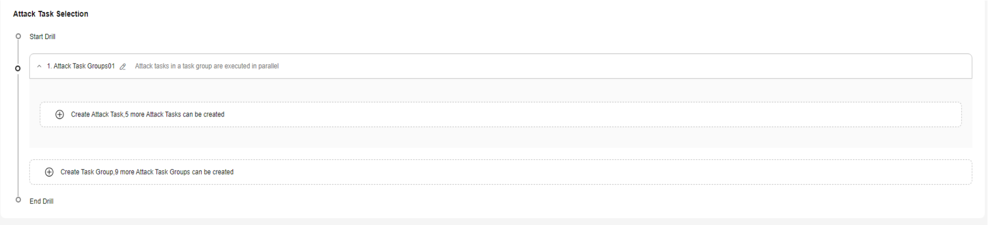
Expected Recovery Duration (Minutes): indicates the expected time for the application to automatically recover or recover to the normal state during emergency plan execution after a fault is injected. This time does not affect the drill task.

Figure 8-7 Basic information of a drill task


Chaos Drill / Create Task
Create Task
Basic Information
* Drill Task
* Expected Recovery Duration (Minutes)
Attack Task Selection
Start Drill
1. Attack Task Groups01
Attack tasks in a task group are executed in parallel
Create Attack Task,5 more Attack Tasks can be created
Create Task Group,9 more Attack Task Groups can be created
End Drill
Cancel
OK

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


Attack Task Selection
Start Drill
1. Attack Task Groups01
Attack tasks in a task group are executed in parallel
Create Attack Task,5 more Attack Tasks can be created
Create Task Group,9 more Attack Task Groups can be created
End Drill

NOTE

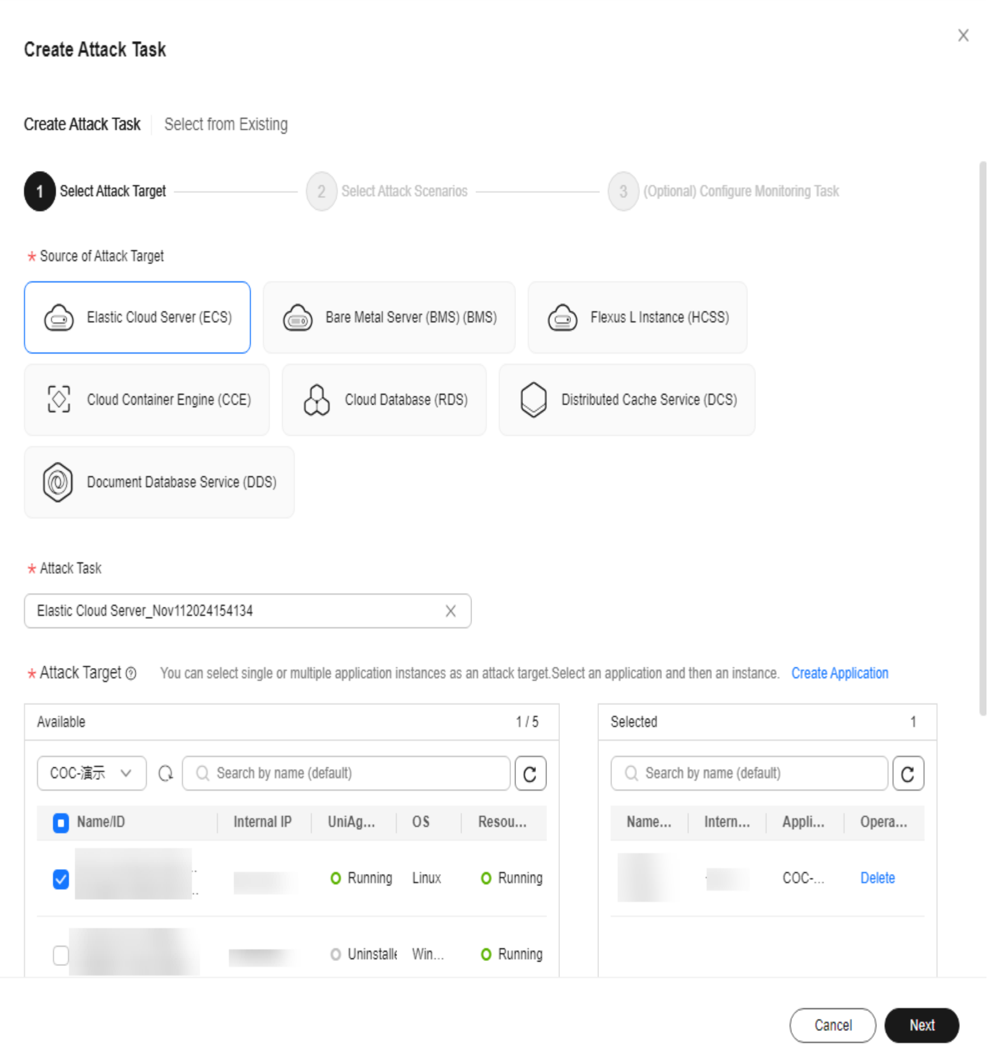
1. Tasks between different task groups are executed in serial mode, and tasks in a task group are executed in parallel mode.

2. Currently, multiple fault injections for the same resource in a task group are not supported.

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 To create an attack task, you need to select an attack target, an attack scenario, and configure a monitoring task (optional). Different attack targets correspond to different attack scenarios. Enter the attack task name. The attack target can be Elastic Cloud Server (ECS), Cloud Container Engine (CCE), Relational Database Service (RDS), Distributed Cache Service (DCS), or Document Database Service (DDS). Click **Next**. (The following uses an ECS as an example. Select an ECS instance of the application to be attacked.)

Figure 8-9 Selecting ECS as the attack target source



Create Attack Task

Create Attack Task | Select from Existing

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

* Source of Attack Target

Elastic Cloud Server (ECS) | Bare Metal Server (BMS) (BMS) | Flexus L Instance (HCSS) | Cloud Container Engine (CCE) | Cloud Database (RDS) | Distributed Cache Service (DCS) | Document Database Service (DDS)

* Attack Task

Elastic Cloud Server_Nov112024154134

* Attack Target You can select single or multiple application instances as an attack target.Select an application and then an instance. Create Application

Available 1 / 5

COC-演示

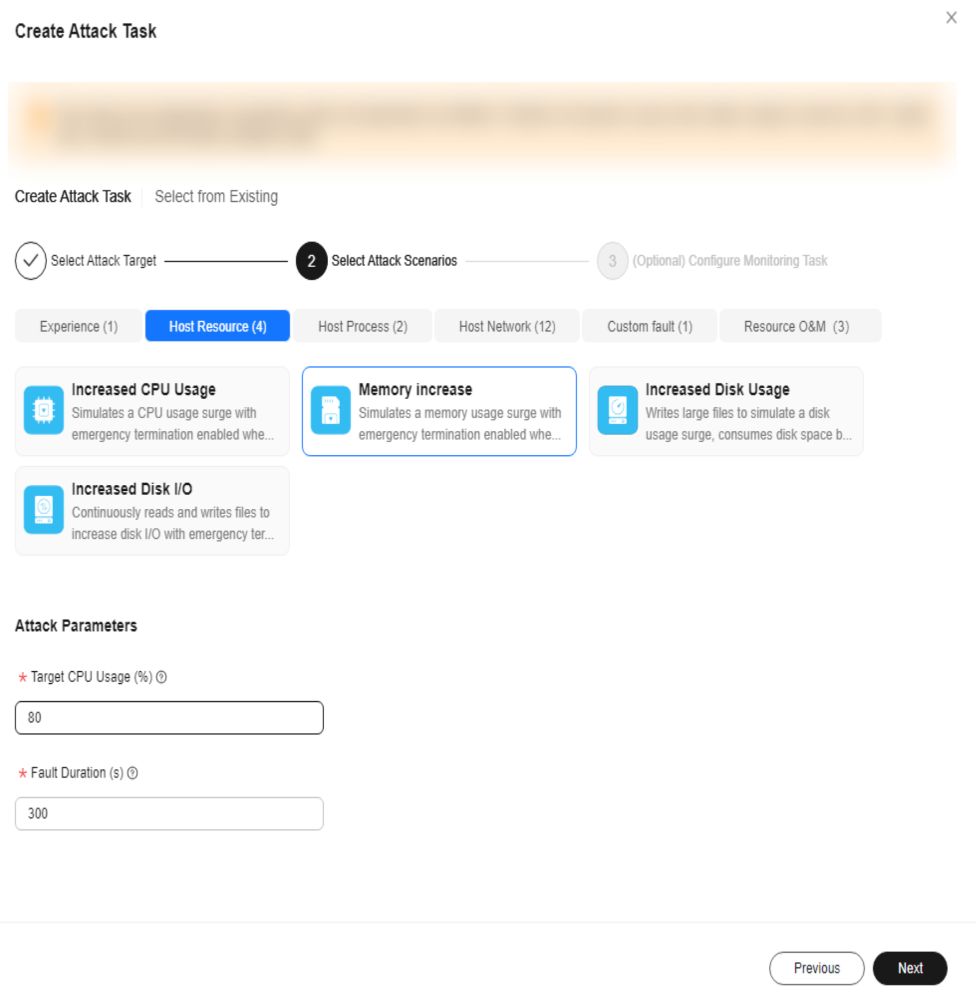
	Name/ID	Internal IP	UniAg...	OS	Resou...
☑			Running	Linux	Running
□			Uninstalle	Win...	Running

Selected 1

Name...	Intern...	Appli...	Opera...
		COC-...	Delete

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



Increased CPU Usage
Simulates a CPU usage surge with emergency termination enabled whe...

Memory increase
Simulates a memory usage surge with emergency termination enabled whe...

Increased Disk Usage
Writes large files to simulate a disk usage surge, consumes disk space b...

Increased Disk I/O
Continuously reads and writes files to increase disk I/O with emergency ter...

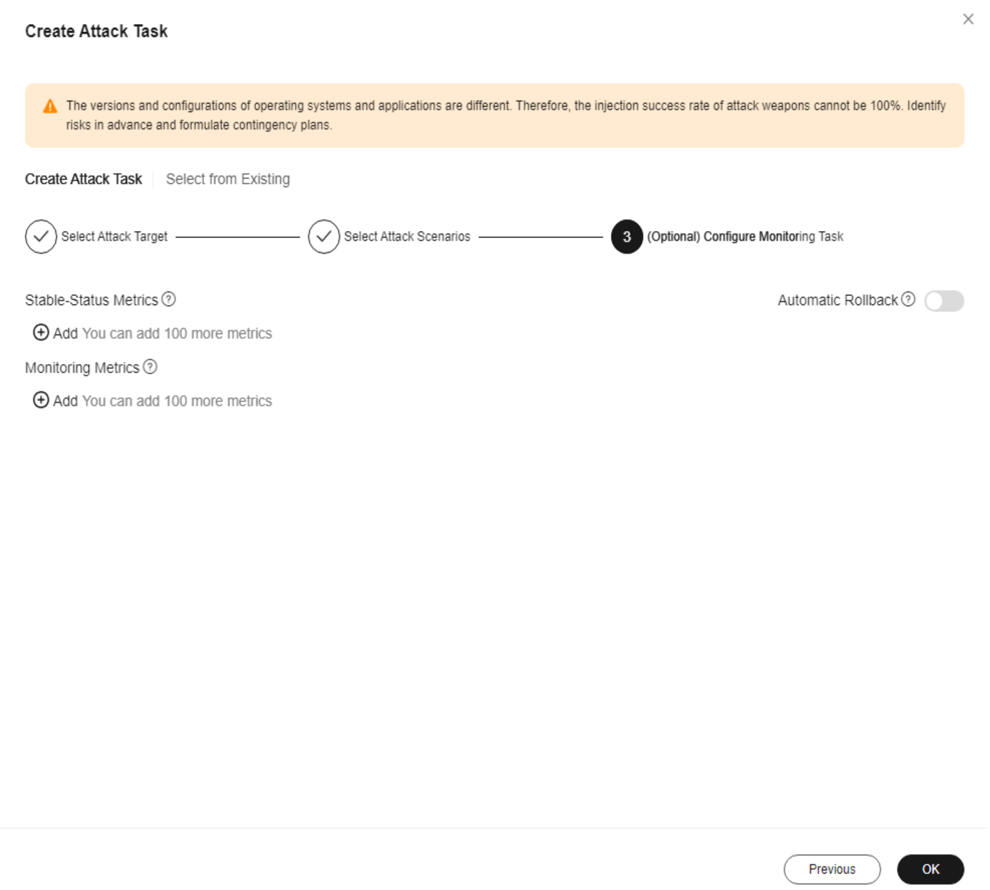
Attack Parameters

* Target CPU Usage (%) ⓘ
80

* Fault Duration (s) ⓘ
300

Step 9 You can configure drill monitoring task metric, including stable-status metrics and monitoring metrics. Stable-status metrics are key metrics used to measure whether applications are running properly during the drill. If the stable-status metrics are not within the upper and lower limits before or during the drill, the drill automatically stops. Monitoring metrics are used to monitor some service metrics during the drill. You can determine drill risks and whether applications are running properly based on the monitoring data. You can configure a monitoring task by specifying the host in the attack target, the name of the monitored metric, and the upper and lower limits of the metric.

Figure 8-11 ECS attack scenario drill monitoring configuration

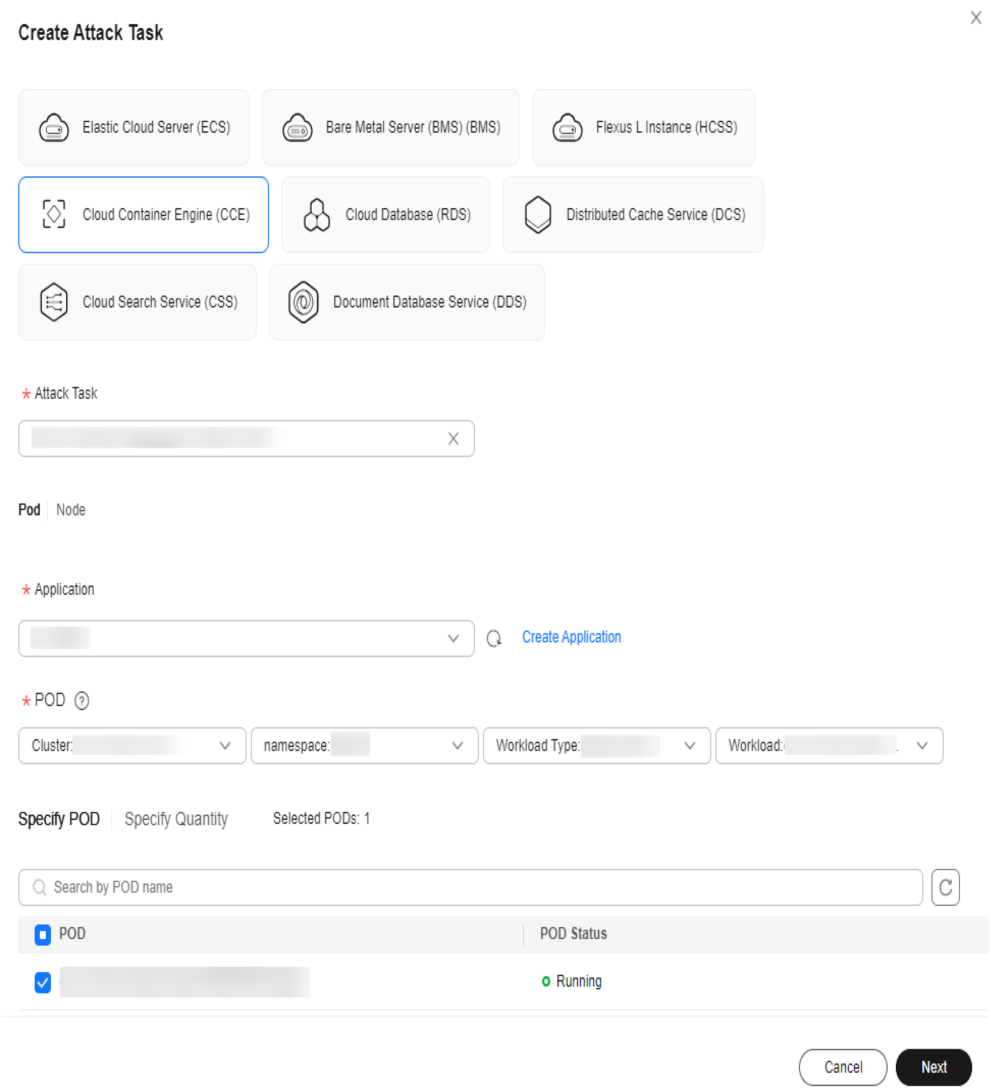


Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Step 10 If you select **Cloud Container Engine (CCE)** as the attack target source, you 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. If the number of PODs are specified, the random policy is used. For example, if you set the quantity to 10, 10 PODs will be randomly selected for fault injection.) Then, click **Next**.

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



Create Attack Task

Elastic Cloud Server (ECS)
Bare Metal Server (BMS) (BMS)
Flexus L Instance (HCSS)
Cloud Container Engine (CCE)
Cloud Database (RDS)
Distributed Cache Service (DCS)
Cloud Search Service (CSS)
Document Database Service (DDS)

* Attack Task

* Application

* POD

Cluster:

namespace:

Workload Type:

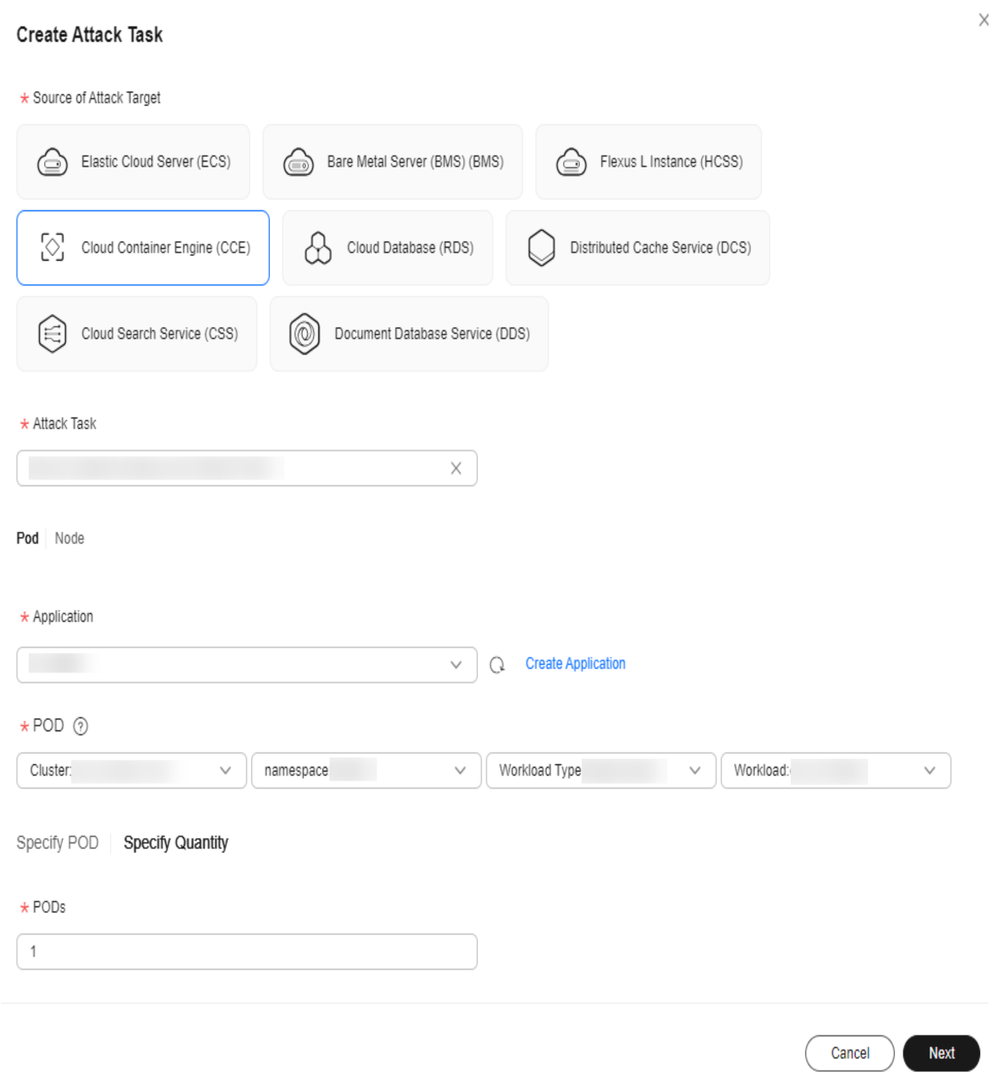
Workload:

Specify POD
Specify Quantity

Selected PODs: 1

☑ POD	POD Status
☑	Running

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



Create Attack Task

* Source of Attack Target

Elastic Cloud Server (ECS) | Bare Metal Server (BMS) (BMS) | Flexus L Instance (HCSS)

Cloud Container Engine (CCE) | Cloud Database (RDS) | Distributed Cache Service (DCS)

Cloud Search Service (CSS) | Document Database Service (DDS)

* Attack Task

[redacted]

Pod | Node

* Application

[redacted]

Create Application

* POD

Cluster: [redacted] | namespace [redacted] | Workload Type [redacted] | Workload: [redacted]

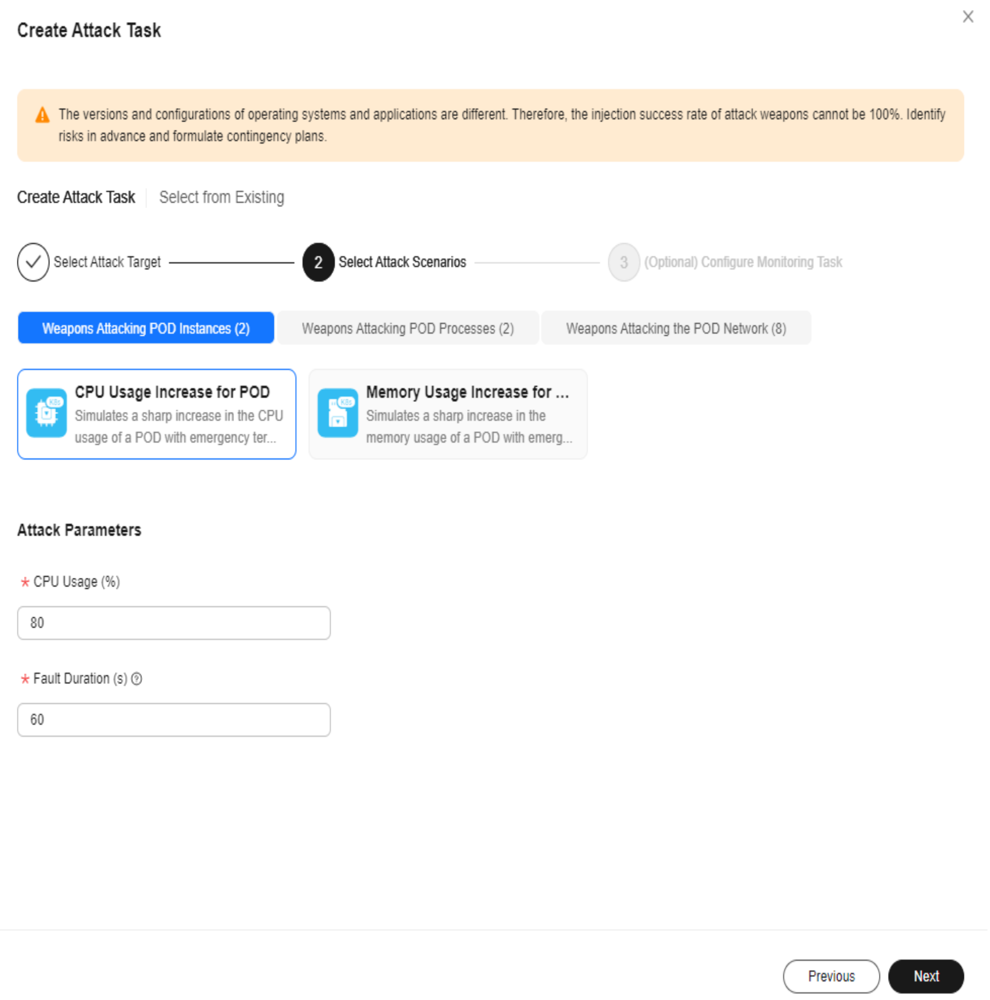
Specify POD | Specify Quantity

* PODs

1

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



Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task
Select from Existing
Select Attack Target
2 Select Attack Scenarios
3 (Optional) Configure Monitoring Task
Weapons Attacking POD Instances (2)
Weapons Attacking POD Processes (2)
Weapons Attacking the POD Network (8)

CPU Usage Increase for POD
Simulates a sharp increase in the CPU usage of a POD with emergency ter...

Memory Usage Increase for ...
Simulates a sharp increase in the memory usage of a POD with emerg...

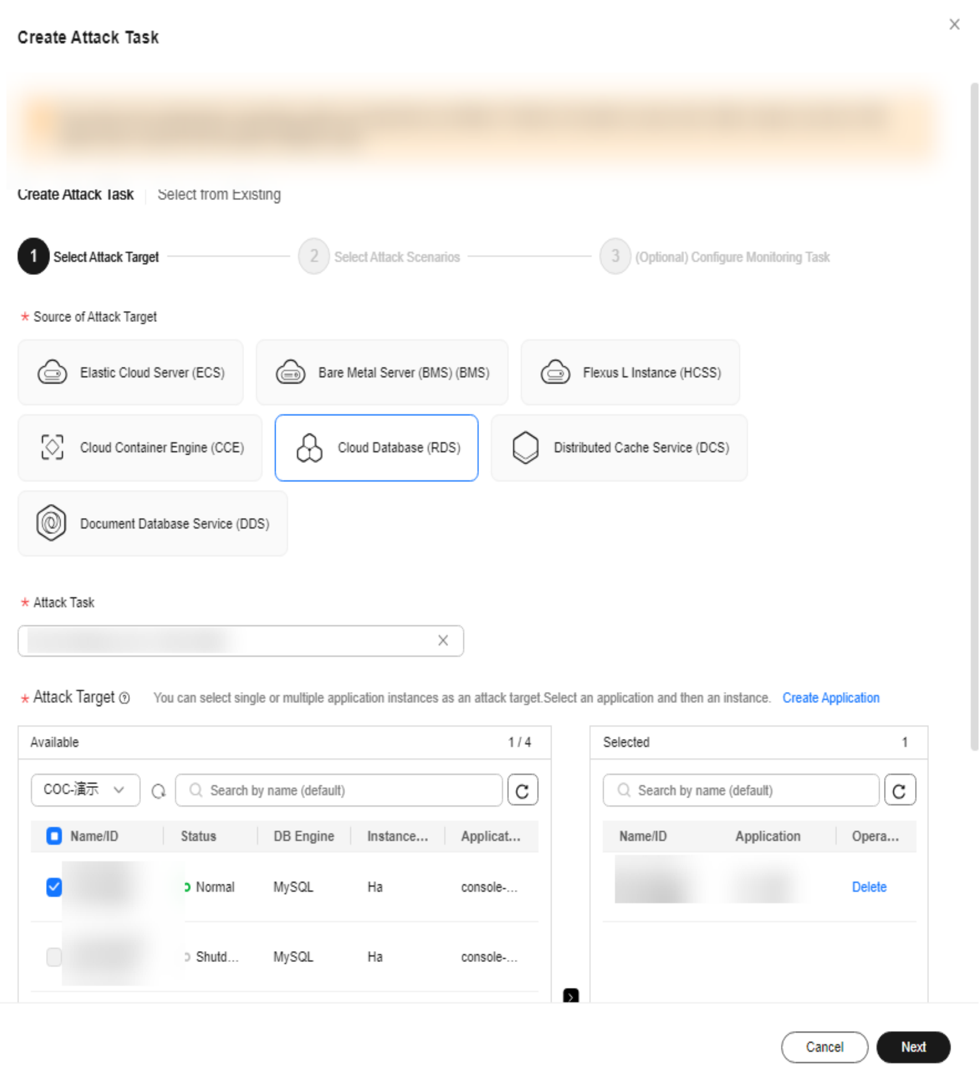
Attack Parameters

* CPU Usage (%)
80

* Fault Duration (s)
60

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



Create Attack Task

Create Attack Task | Select from Existing

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

* Source of Attack Target

Elastic Cloud Server (ECS) | Bare Metal Server (BMS) (BMS) | Flexus L Instance (HCSS)

Cloud Container Engine (CCE) | Cloud Database (RDS) | Distributed Cache Service (DCS)

Document Database Service (DDS)

* Attack Task

* Attack Target You can select single or multiple application instances as an attack target.Select an application and then an instance. Create Application

Available 1 / 4

COC-演示 | Search by name (default)

☐	Name/ID	Status	DB Engine	Instance...	Applicat...
☑		Normal	MySQL	Ha	console-...
☐		Shutd...	MySQL	Ha	console-...

Selected 1

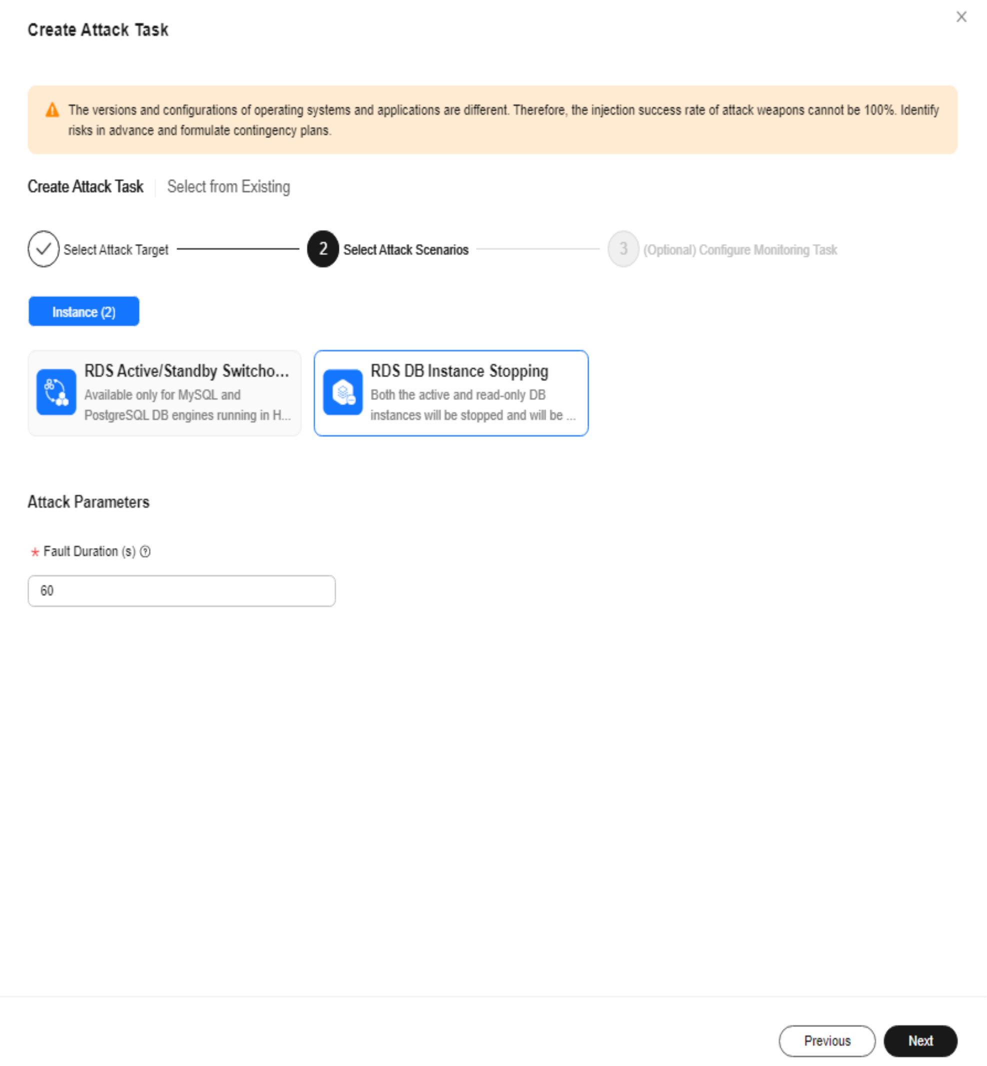
Search by name (default)

Name/ID	Application	Opera...
		Delete

Cancel | Next

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

Figure 8-16 Cloud Database (RDS) attack scenarios



Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

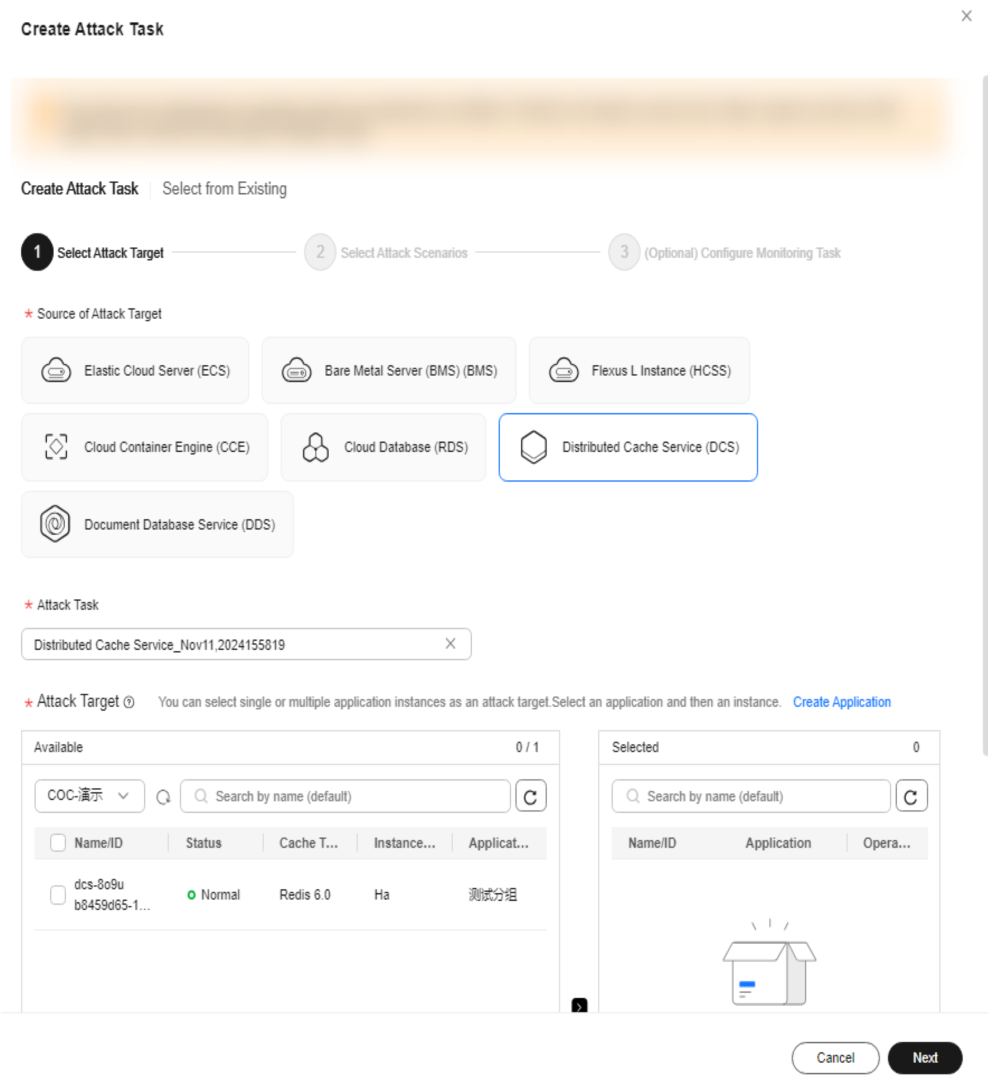
Create Attack Task
Select from Existing
Select Attack Target
2 Select Attack Scenarios
3 (Optional) Configure Monitoring Task
Instance (2)
RDS Active/Standby Switcho...
Available only for MySQL and PostgreSQL DB engines running in H...
RDS DB Instance Stopping
Both the active and read-only DB instances will be stopped and will be ...
Previous
Next

Attack Parameters

* Fault Duration (s): 60

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

Figure 8-17 Selecting Distributed Cache Service (DCS) as the attack target



Create Attack Task

Create Attack Task | Select from Existing

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

* Source of Attack Target

Elastic Cloud Server (ECS) | Bare Metal Server (BMS) (BMS) | Flexus L Instance (HCSS) | Cloud Container Engine (CCE) | Cloud Database (RDS) | Distributed Cache Service (DCS) | Document Database Service (DDS)

* Attack Task

Distributed Cache Service_Nov11,2024155819

* Attack Target ⓘ You can select single or multiple application instances as an attack target.Select an application and then an instance. Create Application

Available 0 / 1

COC-演示 | Search by name (default)

□ Name/ID	Status	Cache T...	Instance...	Applicat...
□ dcs-8o9u b8459d65-1...	○ Normal	Redis 6.0	Ha	测试分组

Selected 0

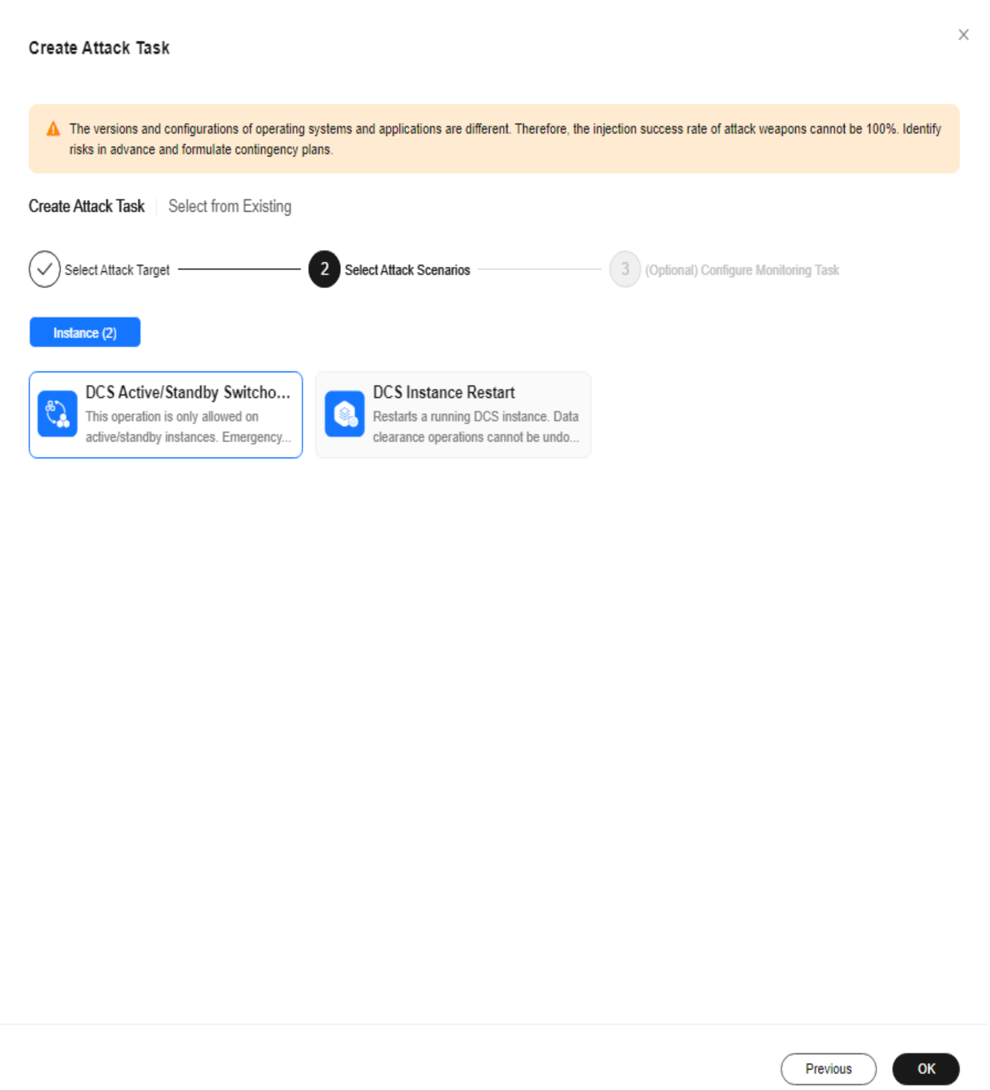
Search by name (default)

Name/ID	Application	Opera...

Cancel | Next

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

Figure 8-18 DCS attack scenarios



Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task | Select from Existing

✓ Select Attack Target — 2 Select Attack Scenarios — 3 (Optional) Configure Monitoring Task

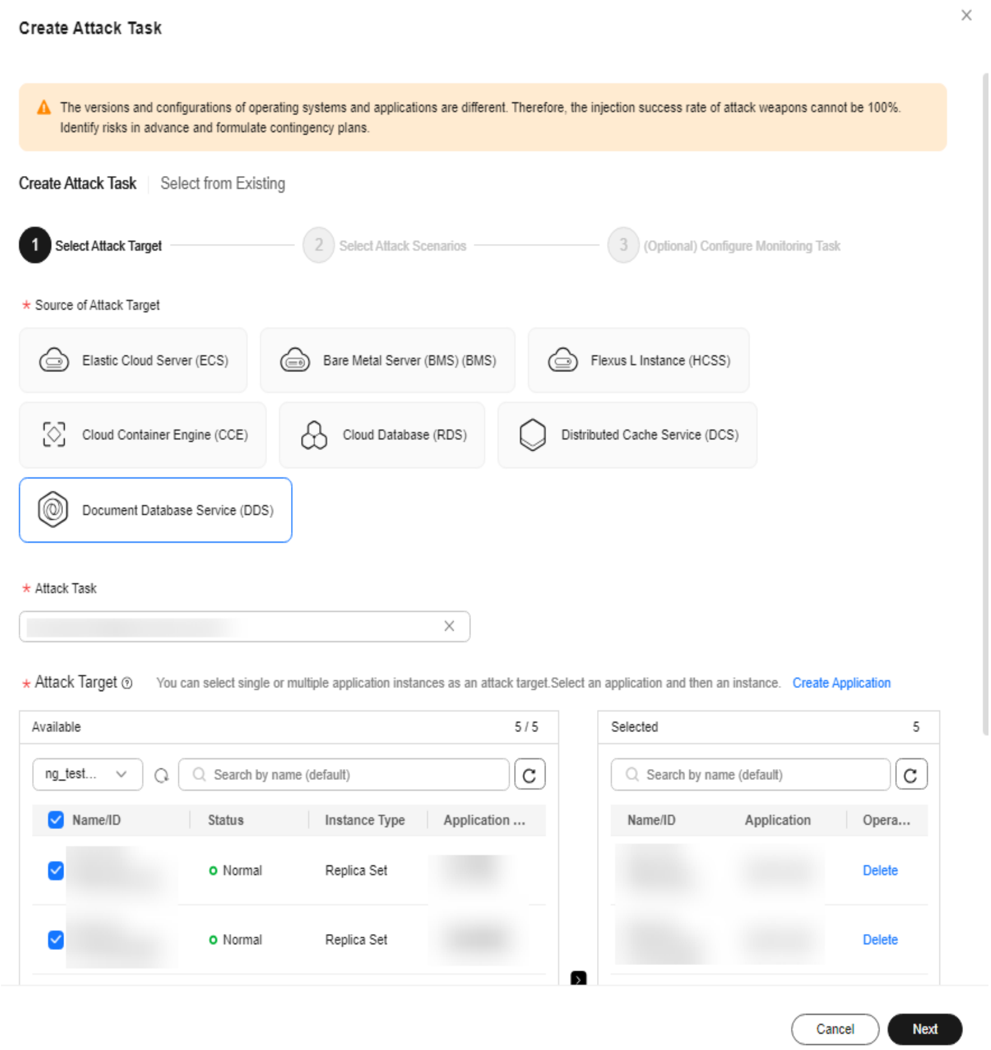
Instance (2)

DCS Active/Standby Switcho...
This operation is only allowed on active/standby instances. Emergency...

DCS Instance Restart
Restarts a running DCS instance. Data clearance operations cannot be undo...

Step 16 If you select DDS as the attack target, select a DDS instance and click **Next**.

Figure 8-19 Selecting Document Database Service (DDS) as the attack target



Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task | Select from Existing

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

* Source of Attack Target

- Elastic Cloud Server (ECS)
- Bare Metal Server (BMS) (BMS)
- Flexus L Instance (HCSS)
- Cloud Container Engine (CCE)
- Cloud Database (RDS)
- Distributed Cache Service (DCS)
- Document Database Service (DDS)

* Attack Task

[redacted]

* Attack Target ⓘ You can select single or multiple application instances as an attack target.Select an application and then an instance. Create Application

Available 5 / 5

ng_test... Search by name (default)

☑ Name/ID	Status	Instance Type	Application ...
☑ [redacted]	○ Normal	Replica Set	[redacted]
☑ [redacted]	○ Normal	Replica Set	[redacted]

Selected 5

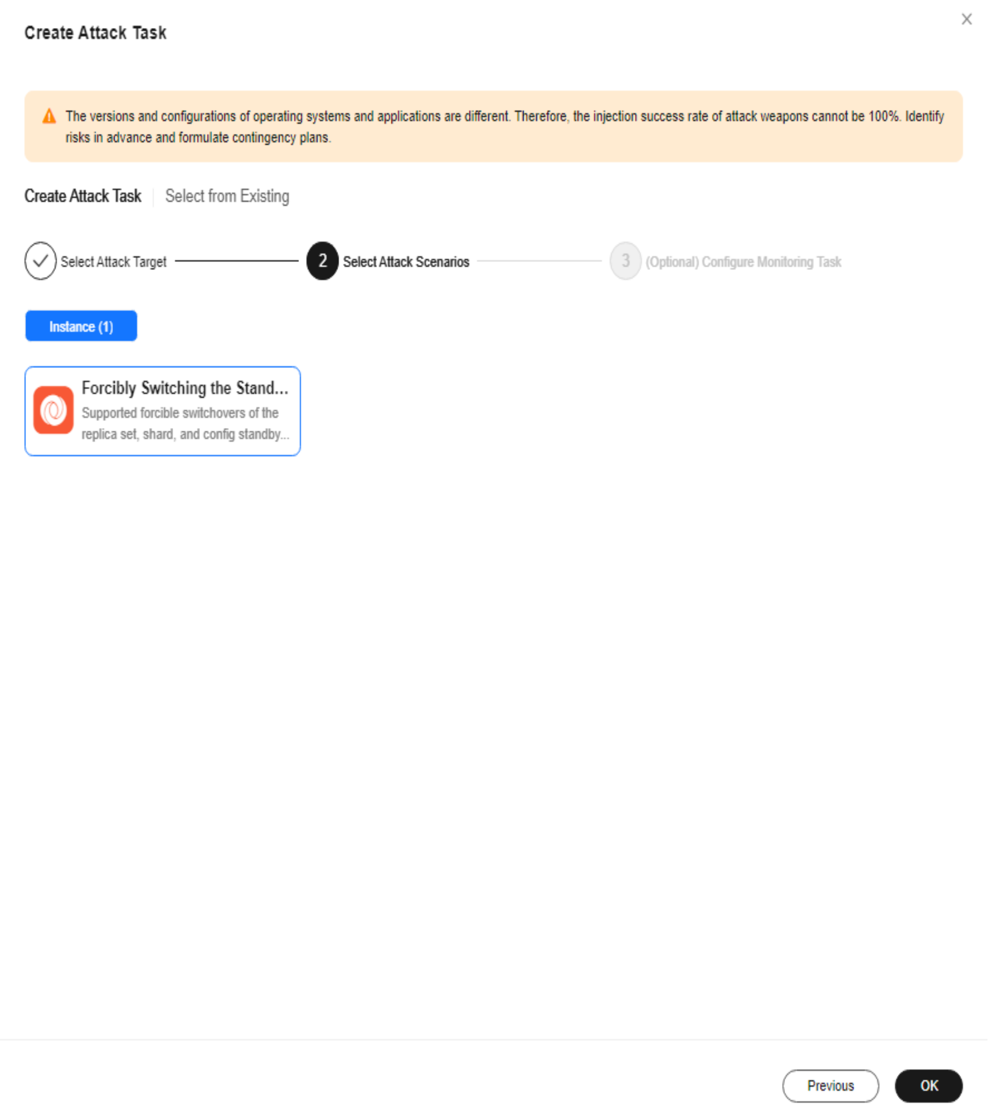
Search by name (default)

Name/ID	Application	Opera...
[redacted]	[redacted]	Delete
[redacted]	[redacted]	Delete

Cancel Next

Step 17 Select the DDS attack scenario and click **OK**.

Figure 8-20 Document Database Service (DDS) attack scenario



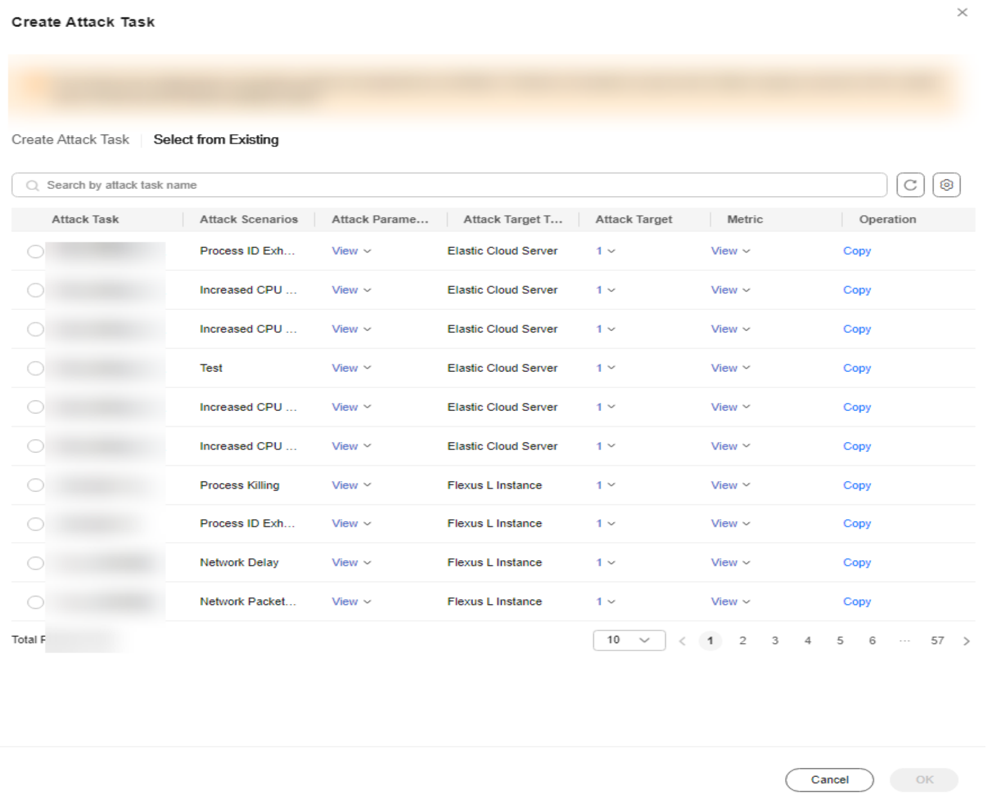
Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task
Select from Existing
✓ Select Attack Target
2 Select Attack Scenarios
3 (Optional) Configure Monitoring Task
Instance (1)
Forcibly Switching the Stand...
Supported forcible switchovers of the replica set, shard, and config standby...
Previous
OK

Step 18 If you select **Select from Existing**, select the created attack task from the task list below and click **OK**.

Figure 8-21 Selecting an existing attack task



Create Attack Task

[redacted]

Create Attack Task | **Select from Existing**

Search by attack task name

	Attack Task	Attack Scenarios	Attack Parame...	Attack Target T...	Attack Target	Metric	Operation
○	[redacted]	Process ID Exh...	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Increased CPU ...	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Increased CPU ...	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Test	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Increased CPU ...	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Increased CPU ...	View	Elastic Cloud Server	1	View	Copy
○	[redacted]	Process Killing	View	Flexus L Instance	1	View	Copy
○	[redacted]	Process ID Exh...	View	Flexus L Instance	1	View	Copy
○	[redacted]	Network Delay	View	Flexus L Instance	1	View	Copy
○	[redacted]	Network Packet...	View	Flexus L Instance	1	View	Copy

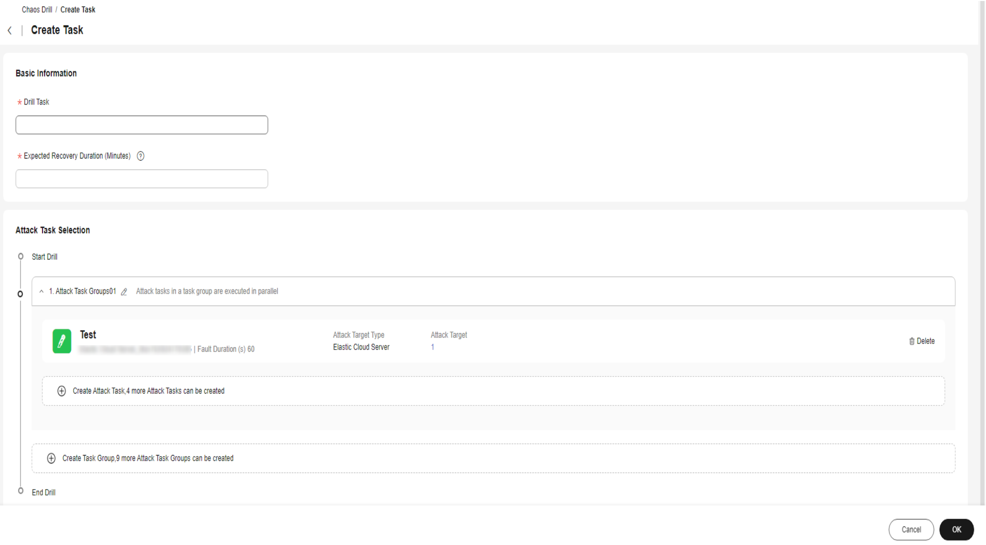
Total F[redacted]

10 < 1 2 3 4 5 6 ··· 57 >

Cancel OK

Step 19 Click **OK**. The drill task is created.

Figure 8-22 Clicking OK



Chaos Drill / Create Task

< | Create Task

Basic Information

* Drill Task

* Expected Recovery Duration (Minutes)

Attack Task Selection

Start Drill

1. Attack Task Groups01 Attack tasks in a task group are executed in parallel

Test

[redacted] | Fault Duration (s) 60

Attack Target Type: Elastic Cloud Server

Attack Target: 1

Delete

Create Attack Task,4 more Attack Tasks can be created

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

End Drill

Cancel OK

----End

Editing a Drill Task

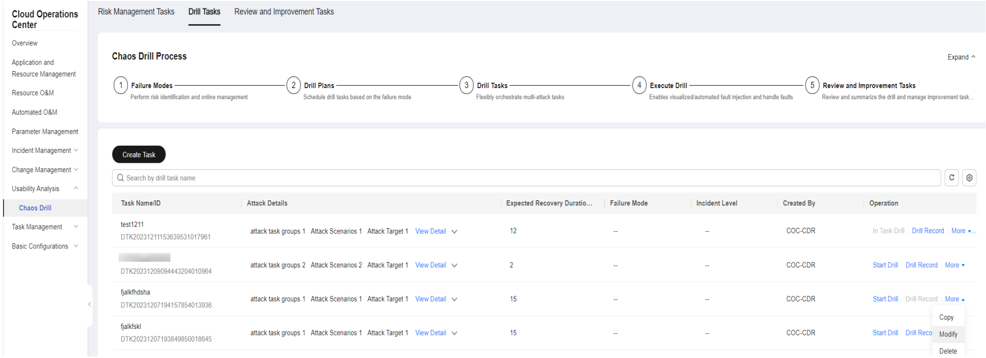
You can edit a drill task. However, if a drill record has been generated for the drill task, the task cannot be edited.

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 8-23 Clicking Modify



Chaos Drill Process

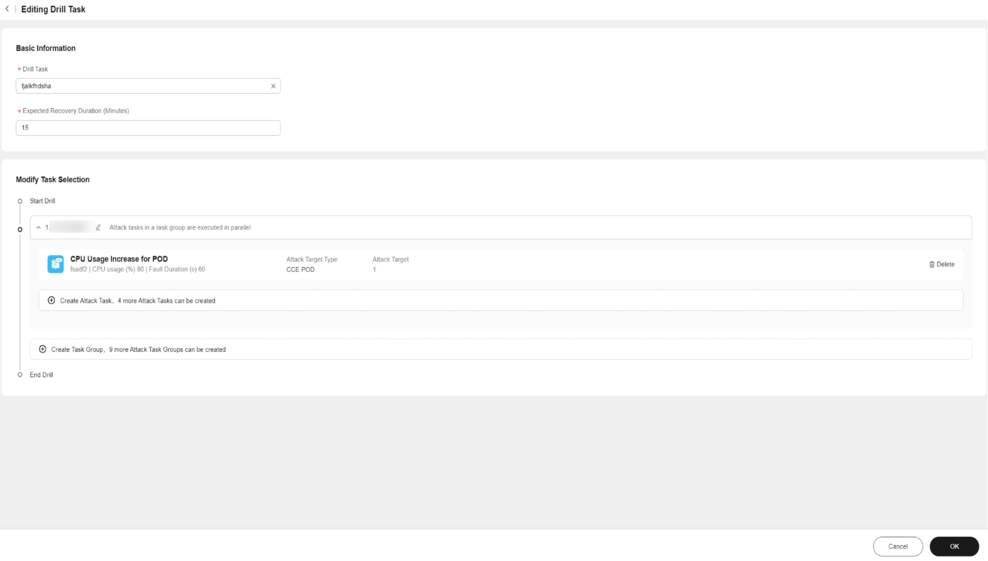
1 Failure Modes: Perform risk identification and online management
2 Drill Plans: Schedule drill tasks based on the failure mode
3 Drill Tasks: Flexibly orchestrate multi-attack tasks
4 Execute Drill: Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks: Review and summarize the drill and manage improvement task...

Task Name/ID	Attack Details	Expected Recovery Duratio...	Failure Mode	Incident Level	Created By	Operation
test1211 DTK20231211153639531017961	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	12	--	--	COC-CDR	In Task Drill Drill Record More
[redacted] DTK20231209094443204010964	attack task groups 2 Attack Scenarios 2 Attack Target 1 View Detail	2	--	--	COC-CDR	Start Drill Drill Record More
fjalkfhdsha DTK20231207194157854013936	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	15	--	--	COC-CDR	Start Drill Drill Record More
fjalkfskl DTK20231207193849850018645	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	15	--	--	COC-CDR	Start Drill Drill Reco

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 8-24 Modifying a drill task



Basic Information

* Drill Task: fjalkfhdsha

* Expected Recovery Duration (Minutes): 15

Modify Task Selection

1. [redacted] Attack tasks in a task group are executed in parallel

CPU Usage Increase for POD
fsadf2 | CPU usage (%) 80 | Fault Duration (s) 60
Attack Target Type: CCE POD
Attack Target: 1

Create Attack Task, 4 more Attack Tasks can be created

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

----End

Deleting a Drill Task

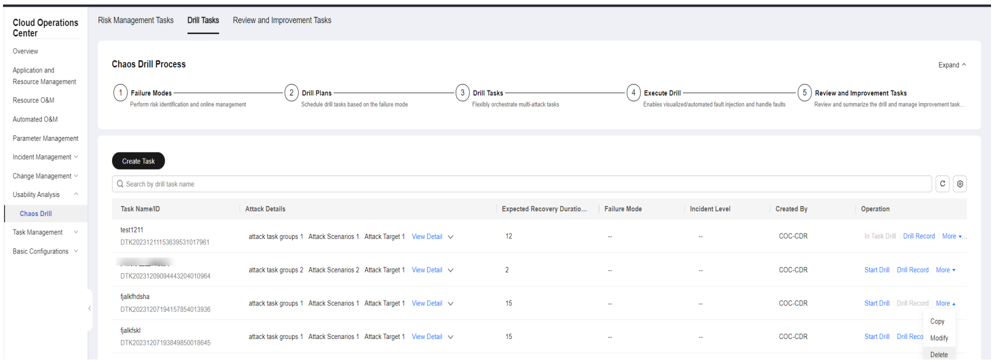
Delete a created drill task. A task that has generated drill records or has associated with drill plans cannot be deleted.

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.

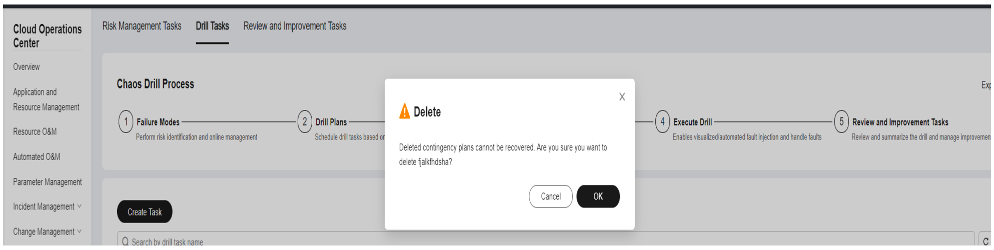
Figure 8-25 Drill task list


Cloud Operations Center
Overview
Application and Resource Management
Resource O&M
Automated O&M
Parameter Management
Incident Management
Change Management
Usability Analysis
Chaos Drill
Task Management
Basic Configurations
Risk Management Tasks
Drill Tasks
Review and Improvement Tasks
Chaos Drill Process
Expand
1 Failure Modes
Perform risk identification and online management
2 Drill Plans
Schedule drill tasks based on the failure mode
3 Drill Tasks
Flexibly orchestrate multi-attack tasks
4 Execute Drill
Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks
Review and summarize the drill and manage improvement task...
Create Task
Search by drill task name
Copy
Modify
Delete

Task Name/ID	Attack Details	Expected Recovery Duratio...	Failure Mode	Incident Level	Created By	Operation
test1211 DTK20231211153639531017961	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	12	--	--	COC-CDR	In Task Drill Drill Record More
[redacted] DTK20231209094443204010964	attack task groups 2 Attack Scenarios 2 Attack Target 1 View Detail	2	--	--	COC-CDR	Start Drill Drill Record More
fjalkfhdsha DTK20231207194157854013936	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	15	--	--	COC-CDR	Start Drill Drill Record More
fjalkfskl DTK20231207193849850018645	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	15	--	--	COC-CDR	Start Drill Drill Reco

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

Figure 8-26 Deleting a drill task


Cloud Operations Center
Overview
Application and Resource Management
Resource O&M
Automated O&M
Parameter Management
Incident Management
Change Management
Risk Management Tasks
Drill Tasks
Review and Improvement Tasks
Chaos Drill Process
1 Failure Modes
Perform risk identification and online management
2 Drill Plans
Schedule drill tasks based or
4 Execute Drill
Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks
Review and summarize the drill and manage improvemen
Create Task
Search by drill task name
Delete
Cancel
OK

Deleted contingency plans cannot be recovered. Are you sure you want to delete fjalkfhdsha?

----End

Starting a Drill Task

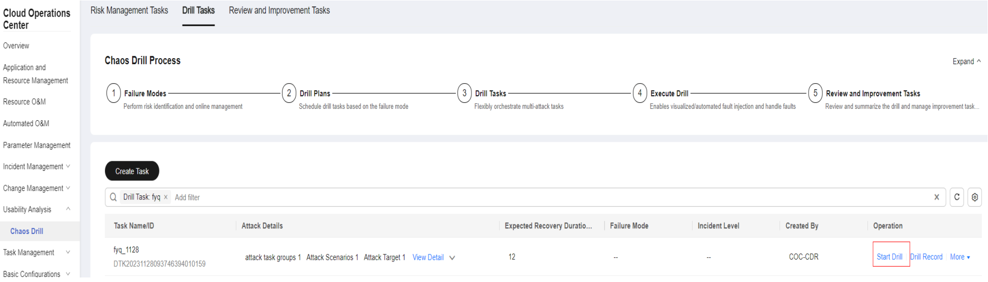
Start a drill task.

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 8-27 Starting a drill task


Cloud Operations Center
Overview
Application and Resource Management
Resource O&M
Automated O&M
Parameter Management
Incident Management
Change Management
Usability Analysis
Chaos Drill
Task Management
Basic Configurations
Risk Management Tasks
Drill Tasks
Review and Improvement Tasks
Chaos Drill Process
Expand
1 Failure Modes
Perform risk identification and online management
2 Drill Plans
Schedule drill tasks based on the failure mode
3 Drill Tasks
Flexibly orchestrate multi-attack tasks
4 Execute Drill
Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks
Review and summarize the drill and manage improvement task...
Create Task
Drill Task: fyq
Add filter

Task Name/ID	Attack Details	Expected Recovery Duratio...	Failure Mode	Incident Level	Created By	Operation
fyq_1128 DTK20231128093746394010159	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	12	--	--	COC-CDR	Start Drill Drill Record More

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 8-28 Attack progress

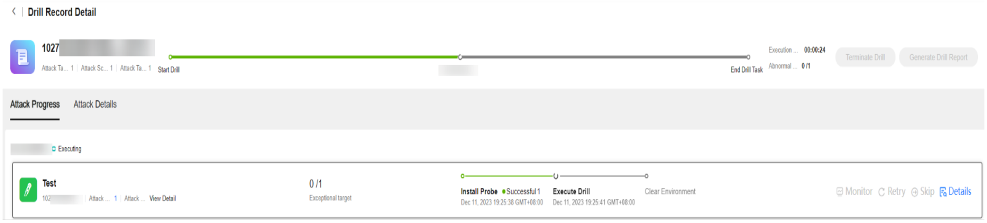
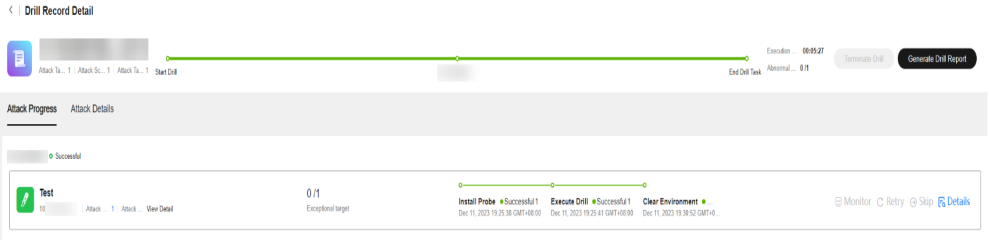
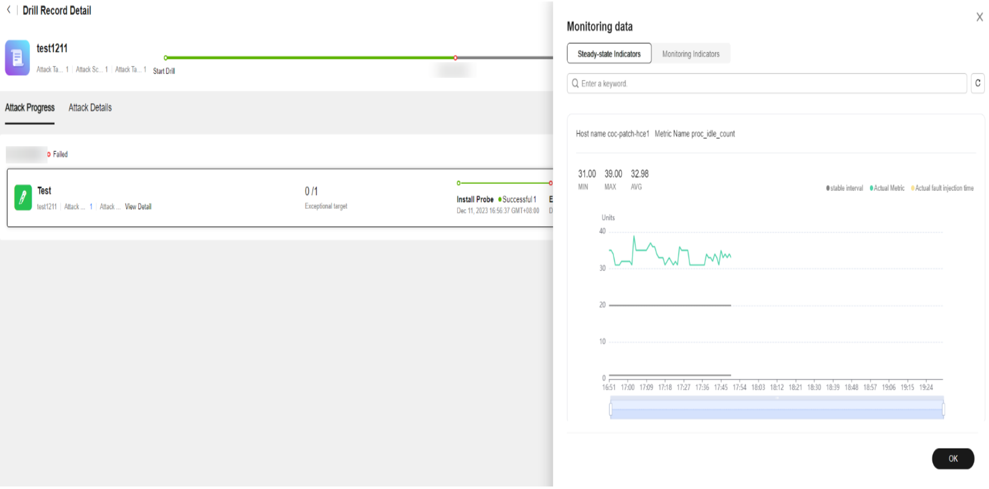


Figure 8-29 Attack completed


Drill Record Detail
Attack Ta... 1 | Attack Sc... 1 | Attack Ta... 1
Start Drill
End Drill Task
Execution ... 00:05:27
Abnormal ... 0 /1
Terminate Drill
Generate Drill Report
Attack Progress
Attack Details
Successful
Test
10
Attack ... 1 | Attack ... View Detail
0 /1
Exceptional target
Install Probe ●Successful 1
Dec 11, 2023 19:25:38 GMT+08:00
Execute Drill ●Successful 1
Dec 11, 2023 19:25:41 GMT+08:00
Clear Environment ●
Dec 11, 2023 19:30:52 GMT+0...
Monitor
Retry
Skip
Details

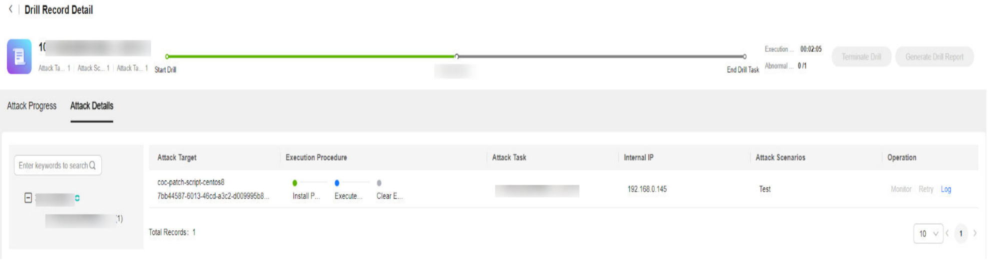
Step 5 During the drill task execution, you can click **Terminate Drill** to end the drill task, click **Retry** to retry the current step, or click **Skip** to skip the current step and go to the next step. If you have configured a drill monitoring task when creating the attack task, you can click **Monitor**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

Figure 8-30 Drill monitoring data



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

Figure 8-31 Attack details



Attack Target	Execution Procedure	Attack Task	Internal IP	Attack Scenarios	Operation
coc-patch-script-centos8 7bb44587-6013-46cd-a3c2-d009995b8...	Install P... Execute... Clear E...	[redacted]	192.168.0.145	Test	Monitor Retry Log

----End

Viewing Drill Records

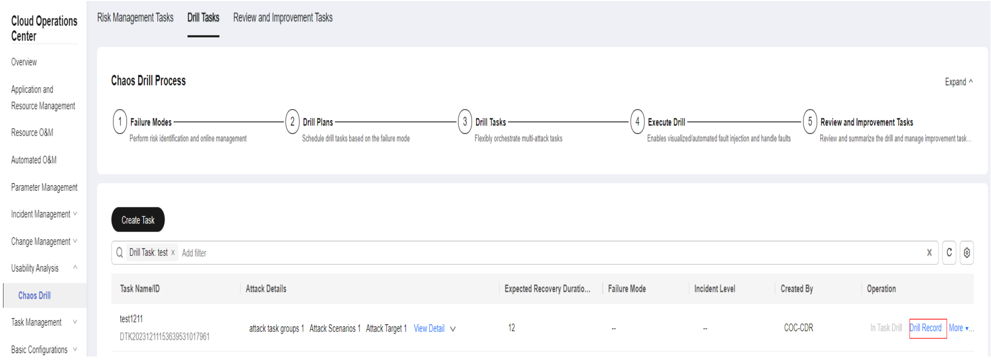
View the drill records of a drill task. A drill task that has not been drilled does not contain drill record.

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 and click **Drill Record** in the **Operation** column.

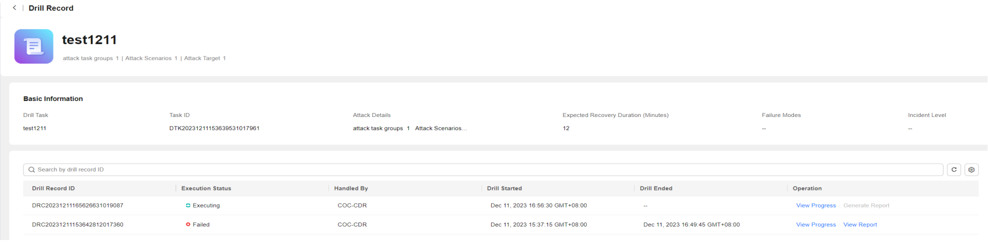
Figure 8-32 Drill task list


Cloud Operations Center
Overview
Application and Resource Management
Resource O&M
Automated O&M
Parameter Management
Incident Management
Change Management
Usability Analysis
Chaos Drill
Task Management
Basic Configurations
Risk Management Tasks
Drill Tasks
Review and Improvement Tasks
Chaos Drill Process
Expand
1 Failure Modes
Perform risk identification and online management
2 Drill Plans
Schedule drill tasks based on the failure mode
3 Drill Tasks
Flexibly orchestrate multi-attack tasks
4 Execute Drill
Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks
Review and summarize the drill and manage improvement task...
Create Task
Drill Task: test
Add filter

Task Name/ID	Attack Details	Expected Recovery Duratio...	Failure Mode	Incident Level	Created By	Operation
test1211 DTK20231211153639531017961	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	12	--	--	COC-CDR	In Task Drill Drill Record More ▾...

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 8-33 Drill Records


Drill Record
test1211
attack task groups 1 | Attack Scenarios 1 | Attack Target 1
Search by drill record ID

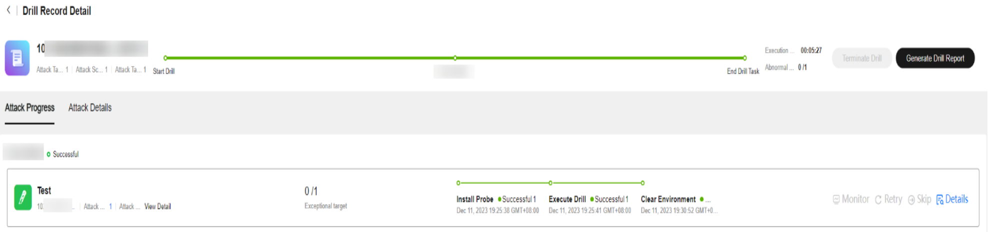
Basic Information

Drill Task	Task ID	Attack Details	Expected Recovery Duration (Minutes)	Failure Modes	Incident Level
test1211	DTK20231211153639531017961	attack task groups 1 Attack Scenarios...	12	--	--

Drill Record ID	Execution Status	Handled By	Drill Started	Drill Ended	Operation
DRC20231211165626631019087	Executing	COC-CDR	Dec 11, 2023 16:56:30 GMT+08:00	--	View Progress Generate Report
DRC20231211153642812017360	Failed	COC-CDR	Dec 11, 2023 15:37:15 GMT+08:00	Dec 11, 2023 16:49:45 GMT+08:00	View Progress View Report

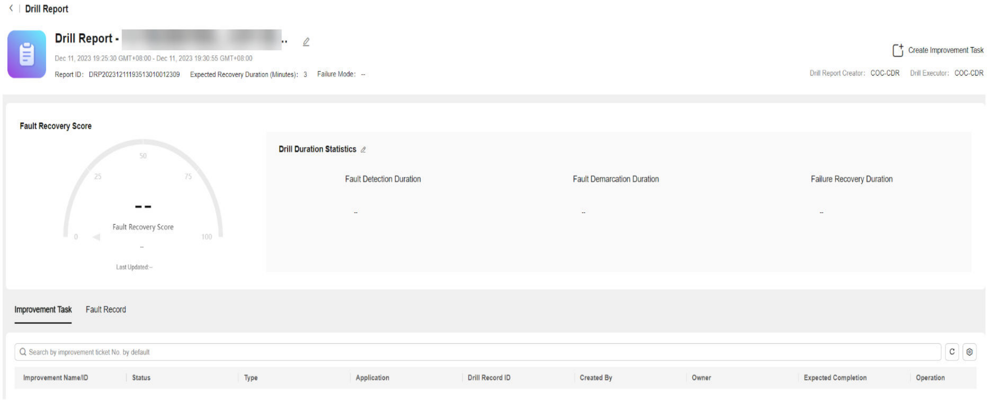
Step 5 Click **View Progress** to view the attack progress and attack details of the current drill task.

Figure 8-34 Attack progress


Drill Record Detail
10[redacted]
Attack Ta... 1 | Attack Sc... 1 | Attack Ta... 1
Start Drill
End Drill Task
Execution ... 00:05:27
Abnormal ... 0 /1
Terminate Drill
Generate Drill Report
Attack Progress
Attack Details
Successful
Test
10[redacted] | Attack ... 1 | Attack ... View Detail
0 /1
Exceptional target
Install Probe ● Successful 1
Dec 11, 2023 19:25:38 GMT+08:00
Execute Drill ● Successful 1
Dec 11, 2023 19:25:41 GMT+08:00
Clear Environment ● ...
Dec 11, 2023 19:30:52 GMT+0...
Monitor
Retry
Skip
Details

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

Figure 8-35 Viewing a drill report


Drill Report
Drill Report - [redacted]..
Dec 11, 2023 19:25:30 GMT+08:00 - Dec 11, 2023 19:30:55 GMT+08:00
Report ID: DRP20231211193513010012309
Expected Recovery Duration (Minutes): 3
Failure Mode: --
Create Improvement Task
Drill Report Creator: COC-CDR
Drill Executor: COC-CDR
Fault Recovery Score
50
25
75
0
100
--
Fault Recovery Score
Last Updated:--
Drill Duration Statistics
Fault Detection Duration
--
Fault Demarcation Duration
--
Failure Recovery Duration
--
Improvement Task
Fault Record
Search by improvement ticket No. by default
Improvement Name/ID
Status
Type
Application
Drill Record ID
Created By
Owner
Expected Completion
Operation

----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

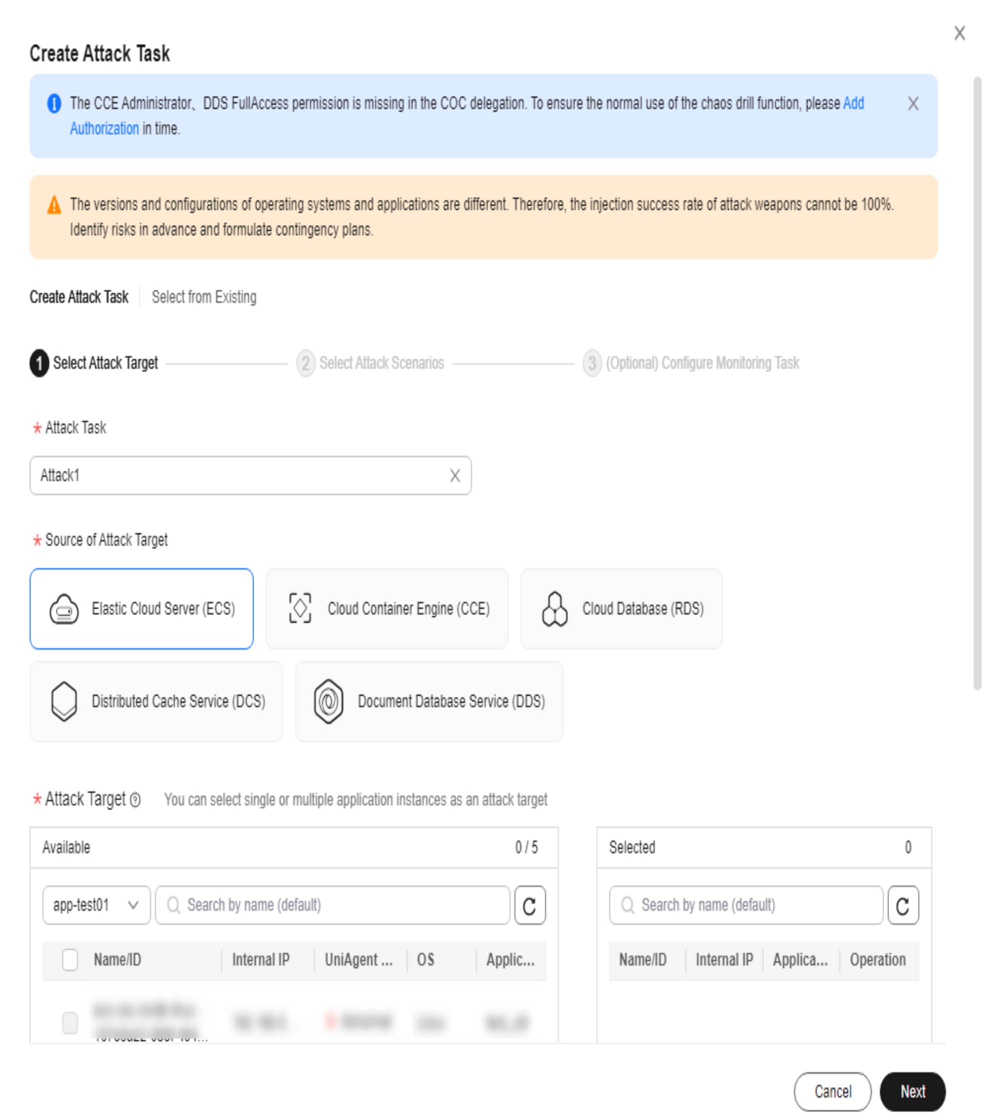
Create a drill task for a custom fault attack scenario on COC.

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 8-36 Selecting ECS as the attack target source



Create Attack Task

The CCE Administrator、DDS FullAccess permission is missing in the COC delegation. To ensure the normal use of the chaos drill function, please Add Authorization in time.

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task | Select from Existing

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

* Attack Task: Attack1

* Source of Attack Target: Elastic Cloud Server (ECS) | Cloud Container Engine (CCE) | Cloud Database (RDS) | Distributed Cache Service (DCS) | Document Database Service (DDS)

* Attack Target You can select single or multiple application instances as an attack target

Available 0 / 5

app-test01 | Search by name (default)

□	Name/ID	Internal IP	UniAgent ...	OS	Applic...
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Selected 0

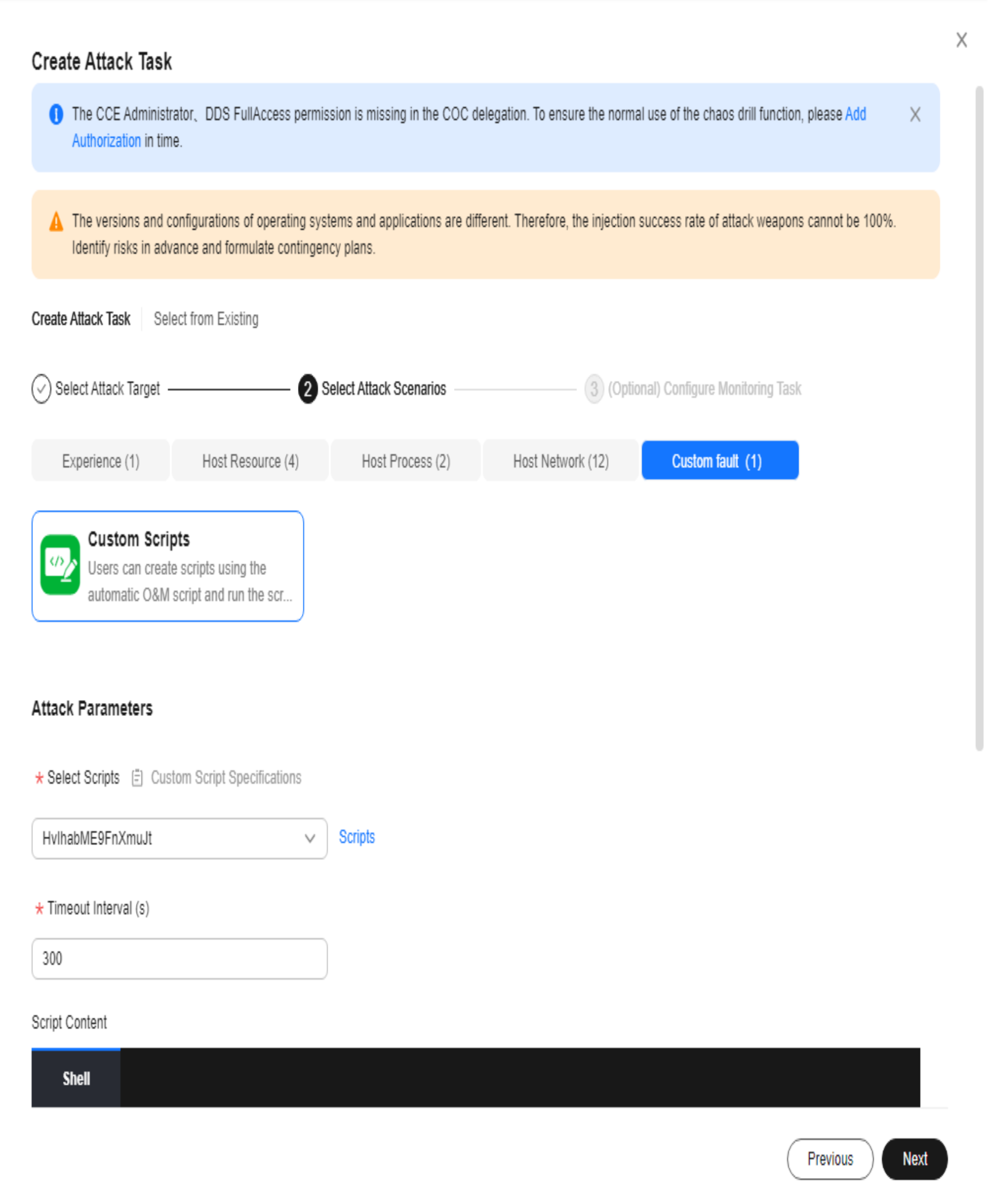
Search by name (default)

Name/ID	Internal IP	Applica...	Operation

Cancel | Next

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 8-37 Selecting the custom fault



Create Attack Task

The CCE Administrator、DDS FullAccess permission is missing in the COC delegation. To ensure the normal use of the chaos drill function, please Add Authorization in time.

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task | Select from Existing

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

Experience (1) | Host Resource (4) | Host Process (2) | Host Network (12) | Custom fault (1)

Custom Scripts
Users can create scripts using the automatic O&M script and run the scr...

Attack Parameters

* Select Scripts: HvlhabME9FnXmuJt (Custom Script Specifications, Scripts)

* Timeout Interval (s): 300

Script Content

NOTE

1. **Timeout Interval (s)**: used to limit the maximum time allowed for script execution. The timeout interval must be longer than the script execution time. You are advised to set the timeout interval to at least 30 seconds.

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 8-4 Mandatory parameters for customizing a fault script

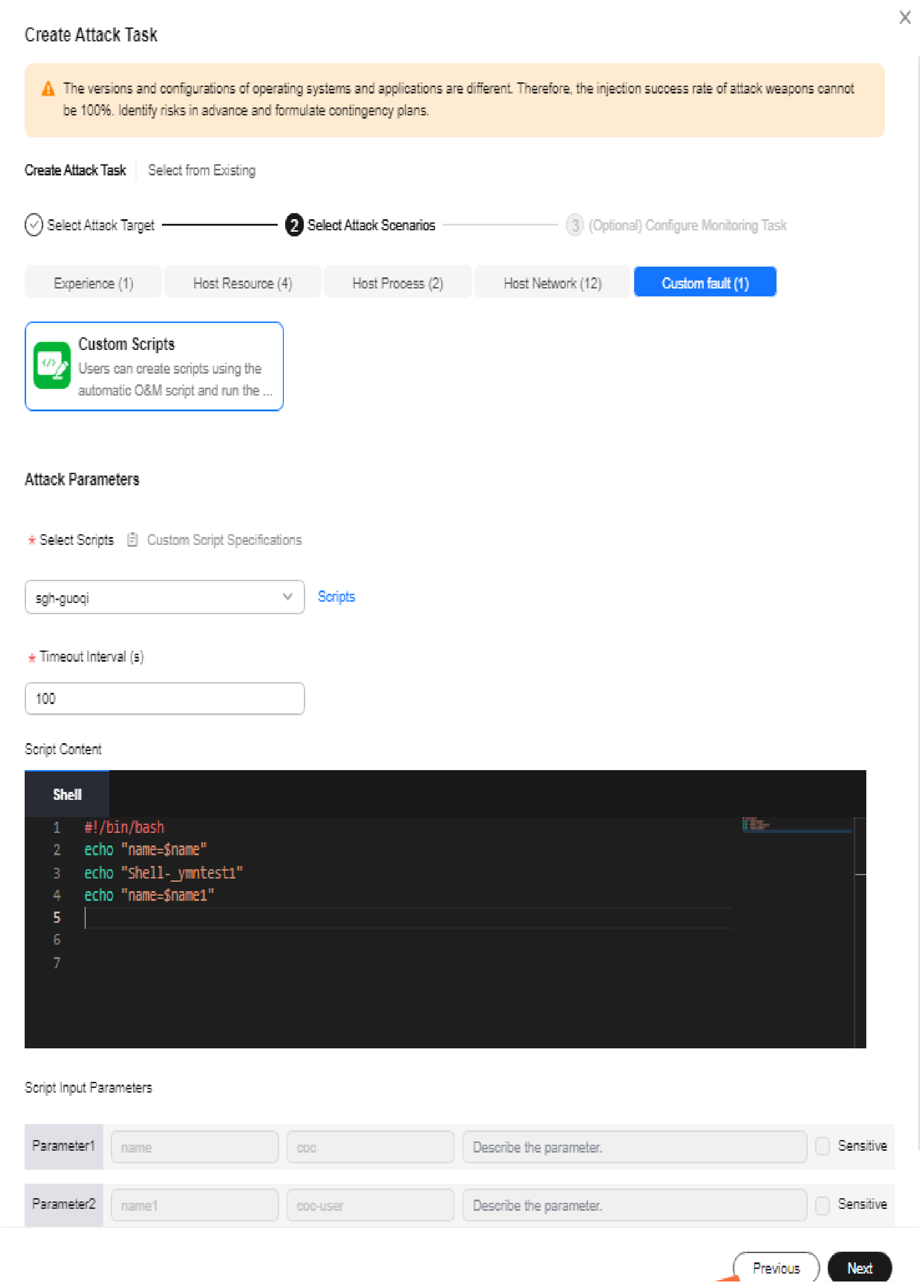
Parameter	Value	Description
ACTION	inject_fault	Drill operation action. The value is automatically changed by the system background in different drill phases. The value can be: ● **inject_fault**: The drill is in the fault injection phase. ● **check_fault_status**: The drill is in the fault query phase. ● **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.

NOTE

1. In the **inject_fault** function, add a flag indicating that the fault injection is successful, and check whether the flag exists in the **check_fault_status** function. If yes, the **check_fault_status** function can return normally (for example, **exit 0**). If no, the **check_fault_status** function can return abnormally (for example, **exit 1**).

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 8-38 Selecting a custom script



Create Attack Task

The versions and configurations of operating systems and applications are different. Therefore, the injection success rate of attack weapons cannot be 100%. Identify risks in advance and formulate contingency plans.

Create Attack Task | Select from Existing

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

Experience (1) | Host Resource (4) | Host Process (2) | Host Network (12) | Custom fault (1)

Custom Scripts
Users can create scripts using the automatic O&M script and run the ...

Attack Parameters

* Select Scripts Custom Script Specifications

sgh-guoqi Scripts

* Timeout Interval (s)

100

Script Content

Shell

```
#!/bin/bash
echo "name=$name"
echo "Shell-_ymntest1"
echo "name=$name1"
```

Script Input Parameters

Parameter1	name	coc	Describe the parameter.	□ Sensitive
Parameter2	name1	coc-user	Describe the parameter.	□ Sensitive

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">${FILE}
    fi
    echo "successfully inject">${FILE}
    echo "============end inject fault============"
}

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

    if [ -f ${FILE} ]; then
        if [[ "$(sed -n '1p' ${FILE})" = "${SUCCESS_FLAG}" ]]; then
            echo "fault inject successfully"
        else
            echo "fault inject failed"
            exit 1
        fi
    else
        echo "inject finished"
        exit 0
    fi
    sleep ${DURATION}
    echo "============end check fault status============"
}

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

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

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

The input parameters of the script are as follows:

Table 8-5 Script input parameters of the customized script example

Parameter	Value	Description
ACTION	inject_fault	Drill operation action
CAN_ROLLBACK	false	Rollback is not supported.
SCRIPT_PATH	/tmp	Root directory of the custom fault log
DIR_NAME	test_script	Parent directory of the custom fault log
FILE	test.log	Custom fault log name
DURATION	10	Duration of a simulated custom fault, in seconds. (This parameter does not take effect when it is placed in the **inject_fault** function.)

NOTE

1. In the sample **inject_fault** function, the injected fault is to **create a {FILE} file and add content to the {FILE} file**. If **successfully inject** is entered in the {FILE} file, the fault injection is successful.

2. In the example, the **check_fault_status** function checks whether the {FILE} file exists. If no, the fault may have been cleared. In this case, **exit 1** is returned. If yes, check whether the flag indicating that the fault injection is successful exists. If the flag exists, the fault injection is successful. Here, **sleep {DURATION}** is used to simulate the fault duration. If the flag does not exist, the fault injection fails.

8.1.6 Drill Report

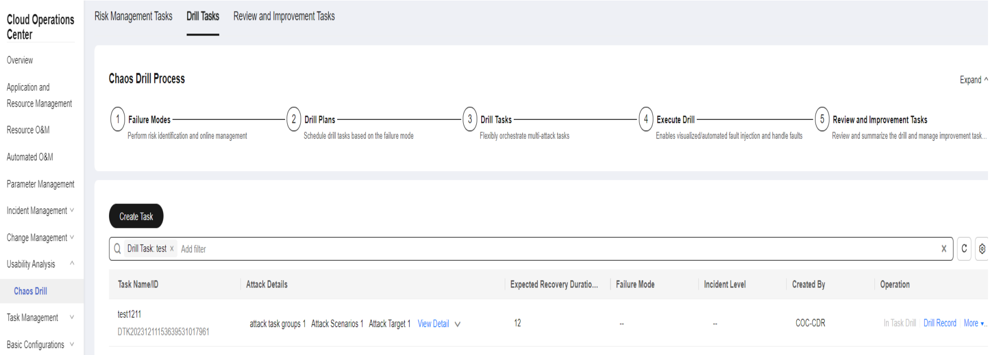
Creating a Drill Report

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

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.

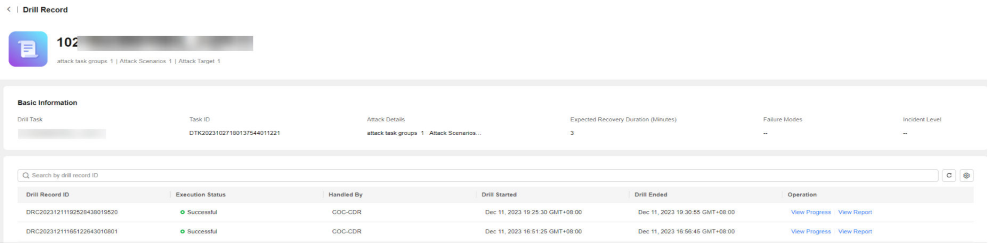
Figure 8-39 Drill tasks


Cloud Operations Center
Overview
Application and Resource Management
Resource O&M
Automated O&M
Parameter Management
Incident Management
Change Management
Usability Analysis
Chaos Drill
Task Management
Basic Configurations
Risk Management Tasks
Drill Tasks
Review and Improvement Tasks
Chaos Drill Process
Expand
1 Failure Modes
Perform risk identification and online management
2 Drill Plans
Schedule drill tasks based on the failure mode
3 Drill Tasks
Flexibly orchestrate multi-attack tasks
4 Execute Drill
Enables visualized/automated fault injection and handle faults
5 Review and Improvement Tasks
Review and summarize the drill and manage improvement task...
Create Task
Drill Task: test
Add filter

Task Name/ID	Attack Details	Expected Recovery Duratio...	Failure Mode	Incident Level	Created By	Operation
test1211 DTK20231211153639531017961	attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail	12	--	--	COC-CDR	In Task Drill Drill Record More

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

Figure 8-40 Drill record list



102[redacted]

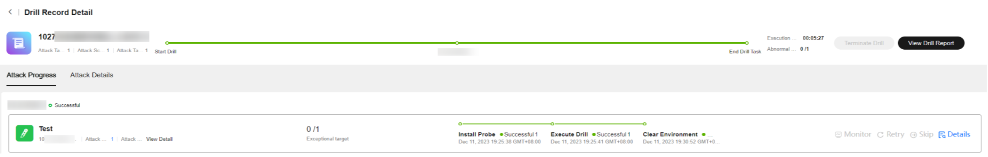
attack task groups 1 | Attack Scenarios 1 | Attack Target 1

Basic Information

Drill Task	Task ID	Attack Details	Expected Recovery Duration (Minutes)	Failure Modes	Incident Level
[redacted]	DTK20231027180137544011221	attack task groups 1 Attack Scenarios...	3	--	--

Drill Record ID	Execution Status	Handled By	Drill Started	Drill Ended	Operation
DRC20231211192528438019520	Successful	COC-CDR	Dec 11, 2023 19:25:30 GMT+08:00	Dec 11, 2023 19:30:55 GMT+08:00	View Progress View Report
DRC20231211165122643010801	Successful	COC-CDR	Dec 11, 2023 16:51:25 GMT+08:00	Dec 11, 2023 16:56:45 GMT+08:00	View Progress View Report

Figure 8-41 Drill Record Detail page



1027[redacted]

Attack Ta... 1 | Attack Sc... 1 | Attack Ta... 1

[redacted]

Execution ... 00:05:27

Abnormal ... 0 /1

[redacted] Successful

Test

10[redacted] Attack ... 1 Attack ... View Detail

0 /1
Exceptional target

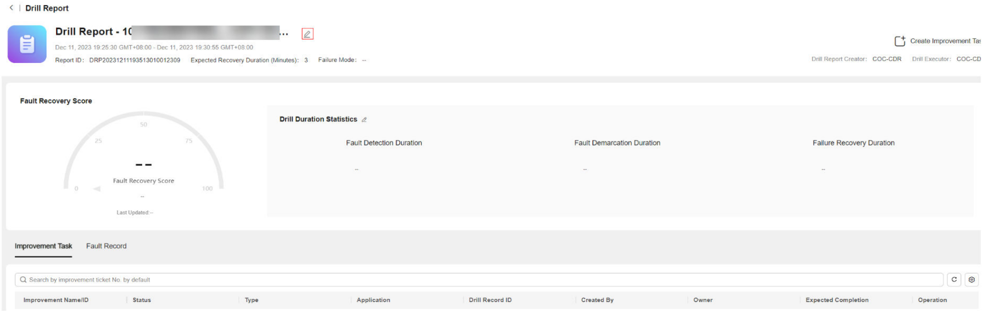
Install Probe Successful 1
Dec 11, 2023 19:25:38 GMT+08:00

Execute Drill Successful 1
Dec 11, 2023 19:25:41 GMT+08:00

Clear Environment ...
Dec 11, 2023 19:30:52 GMT+0...

Step 4 On the displayed **Drill Report** page and update the report name.

Figure 8-42 Drill report details



Drill Report

Drill Report - 10[redacted]...

Dec 11, 2023 19:25:30 GMT+08:00 - Dec 11, 2023 19:30:55 GMT+08:00

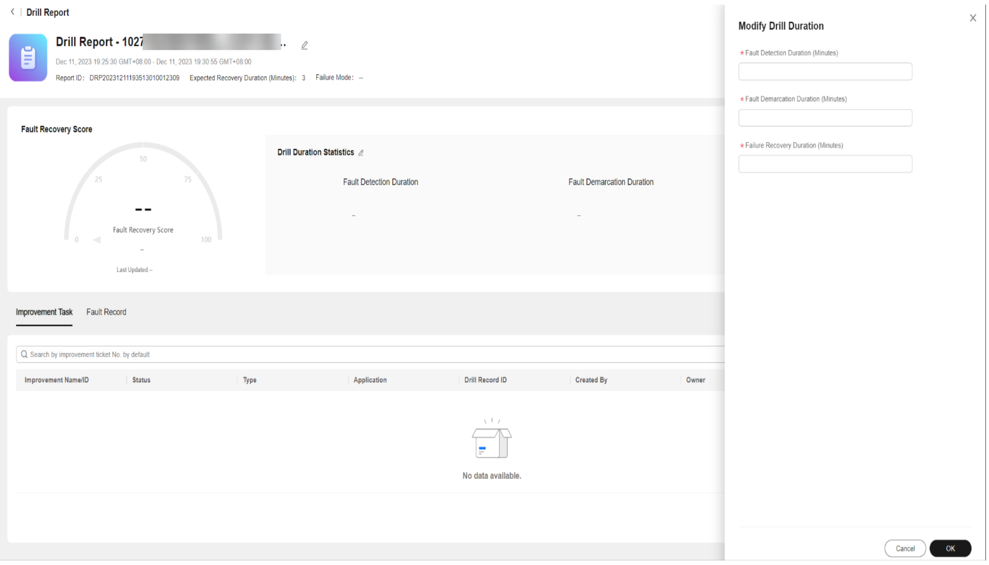
Report ID: DRP20231211193513010012309 Expected Recovery Duration (Minutes): 3 Failure Mode: --

Drill Report Creator: COC-CDR Drill Executor: COC-CD

Improvement Name/ID	Status	Type	Application	Drill Record ID	Created By	Owner	Expected Completion	Operation

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

Figure 8-43 Modifying drill duration



Drill Report

Drill Report - 1027[redacted]..

Dec 11, 2023 19:25:30 GMT+08:00 - Dec 11, 2023 19:30:55 GMT+08:00

Report ID: DRP20231211193513010012309 Expected Recovery Duration (Minutes): 3 Failure Mode: --

Modify Drill Duration

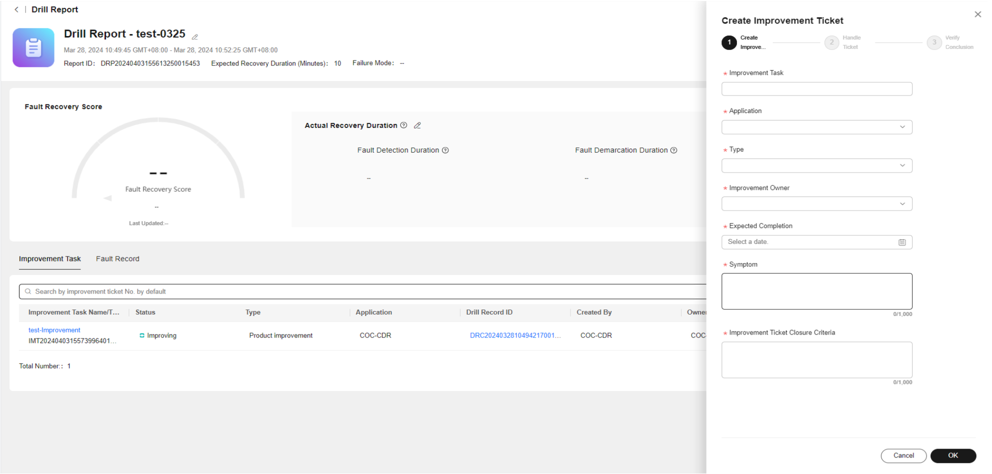
* Fault Detection Duration (Minutes)

* Fault Demarcation Duration (Minutes)

* Failure Recovery Duration (Minutes)

Step 6 On the drill report page, click **Create Improvement Task**, enter information about the improvement item, and click **OK** to save the created improvement ticket. For details about the follow-up handling of improvement ticket, see **Improvement Management**.

Figure 8-44 Creating Improvement Item



Drill Report

Drill Report - test-0325

Mar 28, 2024 10:49:45 GMT+08:00 - Mar 28, 2024 10:52:25 GMT+08:00

Report ID: DRP20240403155613250015453 Expected Recovery Duration (Minutes): 10 Failure Mode: --

Fault Recovery Score

-- Fault Recovery Score -- Last Updated:--

Actual Recovery Duration

Fault Detection Duration --

Fault Demarcation Duration --

Improvement Task | Fault Record

Search by improvement ticket No. by default

Improvement Task Name/T...	Status	Type	Application	Drill Record ID	Created By	Owne
test-Improvement IMT2024040315573996401...	Improving	Product improvement	COC-CDR	DRC2024032810494217001...	COC-CDR	COC

Total Number:: 1

Create Improvement Ticket

1 Create Improve... — 2 Handle Ticket — 3 Verify Conclusion

* Improvement Task

* Application

* Type

* Improvement Owner

* Expected Completion

Select a date.

* Symptom

0/1,000

* Improvement Ticket Closure Criteria

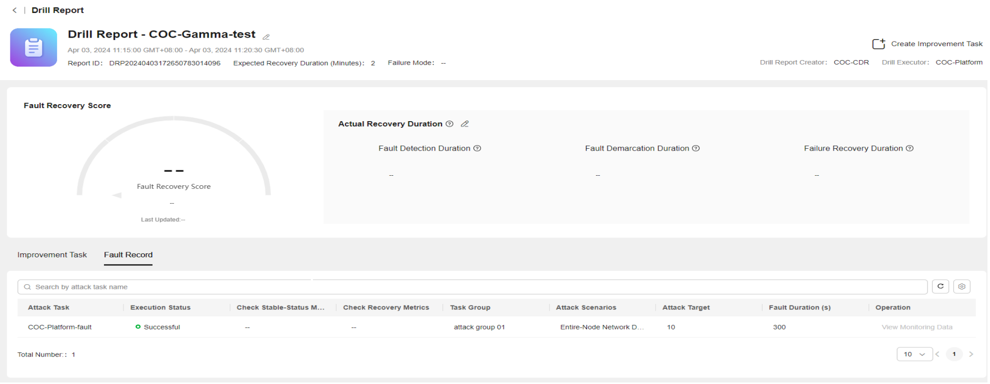
0/1,000

Table 8-6 Improvement ticket parameters

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

Step 7 On the **Drill Report** page, click the **Fault Record** tab to view fault records.

Figure 8-45 Fault record



Drill Report

Drill Report - COC-Gamma-test

Apr 03, 2024 11:15:00 GMT+08:00 - Apr 03, 2024 11:20:30 GMT+08:00

Report ID: DRP20240403172650783014096 Expected Recovery Duration (Minutes): 2 Failure Mode: --

Create Improvement Task

Drill Report Creator: COC-CDR Drill Executor: COC-Platform

Fault Recovery Score

-- Fault Recovery Score -- Last Updated:--

Actual Recovery Duration

Fault Detection Duration --

Fault Demarcation Duration --

Failure Recovery Duration --

Improvement Task | Fault Record

Search by attack task name

Attack Task	Execution Status	Check Stable-Status M...	Check Recovery Metrics	Task Group	Attack Scenarios	Attack Target	Fault Duration (s)	Operation
COC-Platform-fault	Successful	--	--	attack group 01	Entire-Node Network D...	10	300	View Monitoring Data

Total Number:: 1

----End

8.2 Emergency Plan

Scenarios

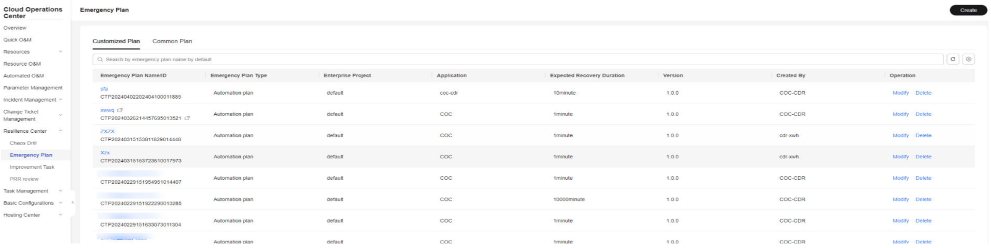
You can create an emergency plan for a system fault that may occur and rectify the fault by referring to the emergency plan.

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.

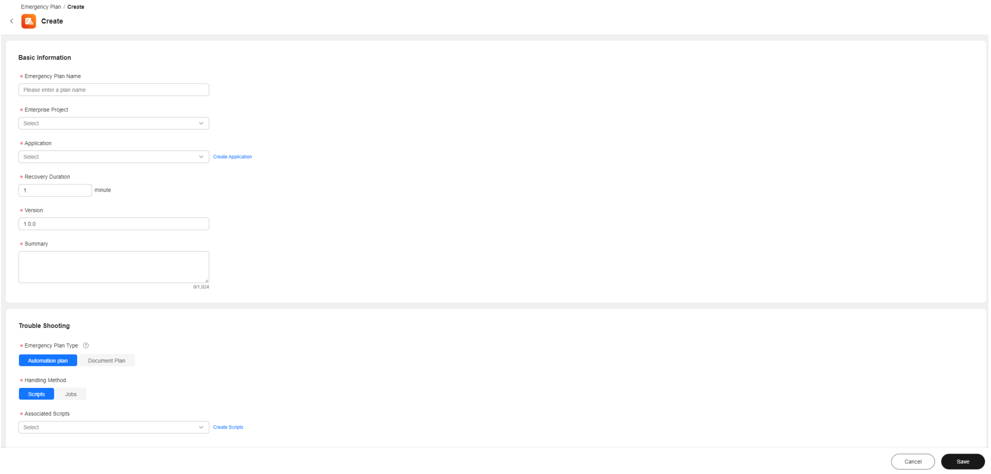
Figure 8-46 Customized Plan tab page



Emergency Plan Name/ID	Emergency Plan Type	Enterprise Project	Application	Expected Recovery Duration	Version	Created By	Operation
sfa CTP20240402202404100011885	Automation plan	default	coc-cdr	10minute	1.0.0	COC-CDR	Modify Delete
xwwq CTP20240326214457695013521	Automation plan	default	COC	1minute	1.0.0	COC-CDR	Modify Delete
ZXZX CTP20240315153811829014448	Automation plan	default	COC	1minute	1.0.0	cdr-xwh	Modify Delete
Xzx CTP20240315153723610017973	Automation plan	default	COC	1minute	1.0.0	cdr-xwh	Modify Delete
[redacted] CTP20240229151954951014407	Automation plan	default	COC	1minute	1.0.0	COC-CDR	Modify Delete
[redacted] CTP20240229151922290013285	Automation plan	default	COC	10000minute	1.0.0	COC-CDR	Modify Delete
[redacted] CTP20240229151633073011304	Automation plan	default	COC	1minute	1.0.0	COC-CDR	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	COC-CDR	Modify Delete

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

Figure 8-47 Creating an emergency plan



Basic Information

* Emergency Plan Name: Please enter a plan name

* Enterprise Project: Select

* Application: Select

* Recovery Duration: 1 minute

* Version: 1.0.0

* Summary: 0/1,024

Trouble Shooting

* Emergency Plan Type: [✓ Automation plan] Document Plan

* Handling Method: [✓ Scripts] Jobs

* Associated Scripts: Select

Table 8-7 Parameters for configuring basic information about an emergency plan

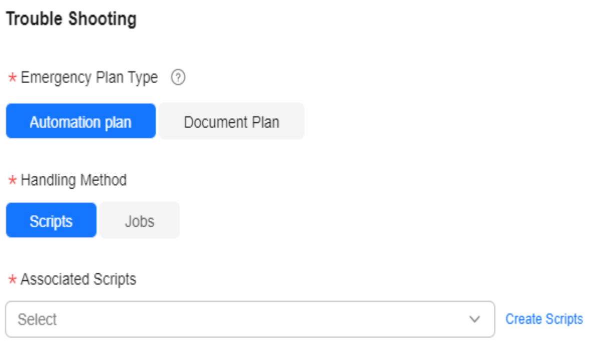
Parameter	Description
Emergency Plan Name	Customized emergency plan name

Parameter	Description
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	Expected 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 8-48 Troubleshooting


Trouble Shooting

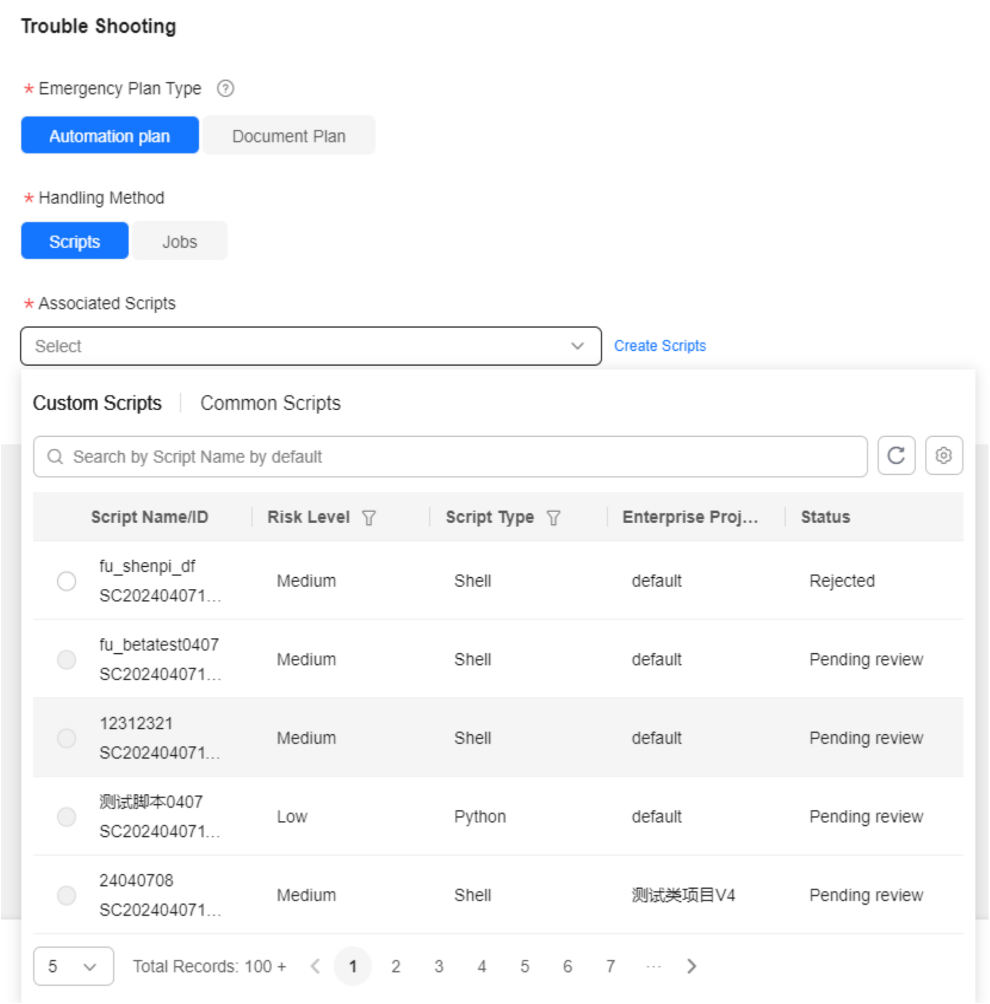
* Emergency Plan Type: Automation plan (selected) | Document Plan

* Handling Method: Scripts (selected) | Jobs

* Associated Scripts: Select

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

Figure 8-49 Associating a custom script



Trouble Shooting

* Emergency Plan Type ?

Automation plan | Document Plan

* Handling Method

Scripts | Jobs

* Associated Scripts

Select Create Scripts

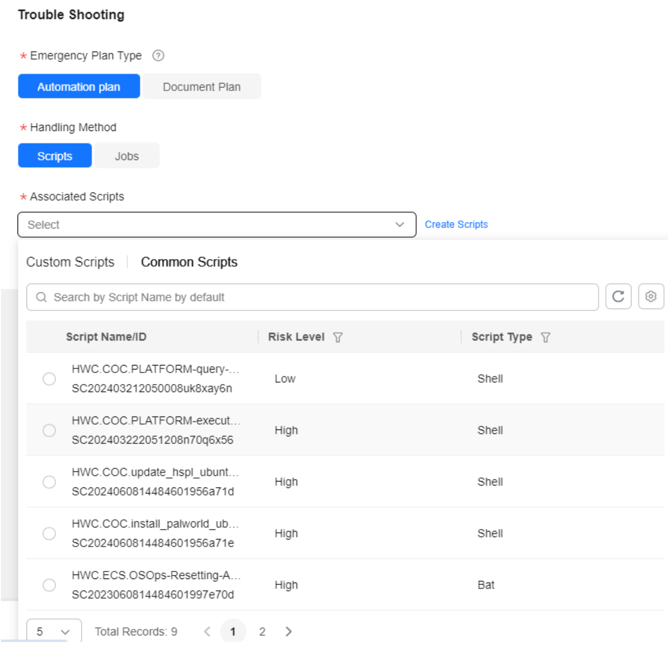
Custom Scripts | Common Scripts

Search by Script Name by default

	Script Name/ID	Risk Level	Script Type	Enterprise Proj...	Status
○	fu_shenpi_df SC202404071...	Medium	Shell	default	Rejected
○	fu_betatest0407 SC202404071...	Medium	Shell	default	Pending review
○	12312321 SC202404071...	Medium	Shell	default	Pending review
○	测试脚本0407 SC202404071...	Low	Python	default	Pending review
○	24040708 SC202404071...	Medium	Shell	测试类项目V4	Pending review

5 Total Records: 100 + < 1 2 3 4 5 6 7 ··· >

Figure 8-50 Associating a common script



Trouble Shooting

* Emergency Plan Type

Automation plan | Document Plan

* Handling Method

Scripts | Jobs

* Associated Scripts

Select

Create Scripts

Custom Scripts | Common Scripts

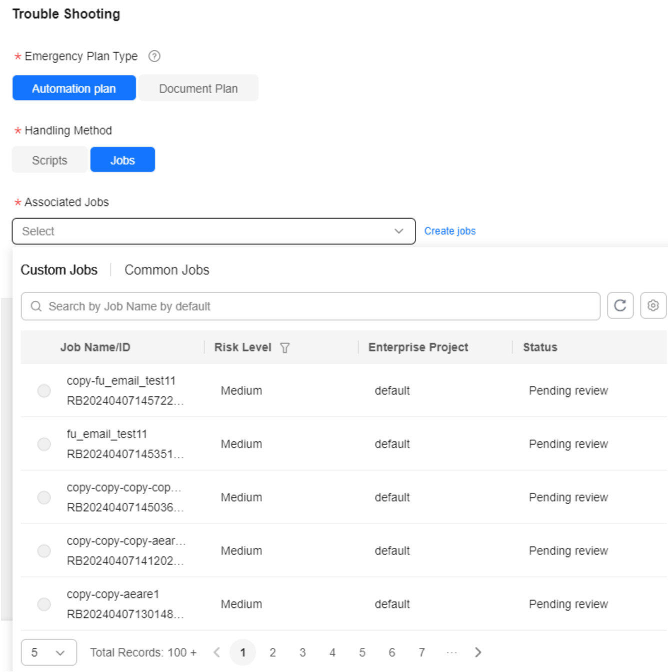
Search by Script Name by default

	Script Name/ID	Risk Level	Script Type
○	HWC.COC.PLATFORM-query-... SC202403212050008uk8xay6n	Low	Shell
○	HWC.COC.PLATFORM-execut... SC202403222051208n70q6x56	High	Shell
○	HWC.COC.update_hspl_ubunt... SC2024060814484601956a71d	High	Shell
○	HWC.COC.install_palworld_ub... SC2024060814484601956a71e	High	Shell
○	HWC.ECS.OSOps-Resetting-A... SC2023060814484601997e70d	High	Bat

5 Total Records: 9 < 1 2 >

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

Figure 8-51 Associating a custom job



Trouble Shooting

* Emergency Plan Type

Automation plan | Document Plan

* Handling Method

Scripts | Jobs

* Associated Jobs

Select

Create jobs

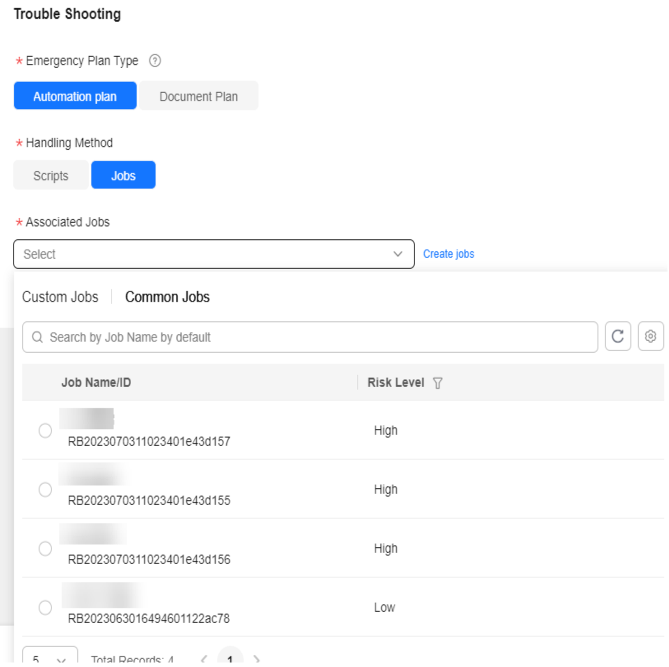
Custom Jobs | Common Jobs

Search by Job Name by default

	Job Name/ID	Risk Level	Enterprise Project	Status
○	copy-fu_email_test11 RB20240407145722...	Medium	default	Pending review
○	fu_email_test11 RB20240407145351...	Medium	default	Pending review
○	copy-copy-copy-cop... RB20240407145036...	Medium	default	Pending review
○	copy-copy-copy-aear... RB20240407141202...	Medium	default	Pending review
○	copy-copy-aeare1 RB20240407130148...	Medium	default	Pending review

5 Total Records: 100 + < 1 2 3 4 5 6 7 ··· >

Figure 8-52 Associating a common job



Trouble Shooting

* Emergency Plan Type

Automation plan | Document Plan

* Handling Method

Scripts | Jobs

* Associated Jobs

Select

Create jobs

Custom Jobs | Common Jobs

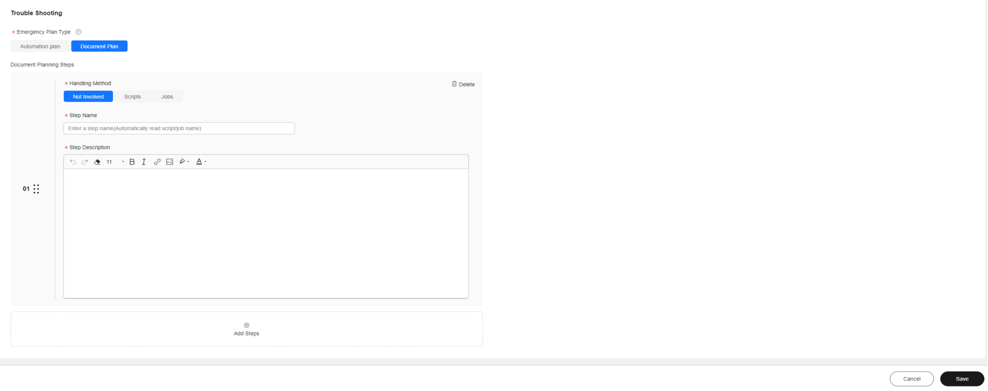
Search by Job Name by default

	Job Name/ID	Risk Level
○	[redacted] RB2023070311023401e43d157	High
○	[redacted] RB2023070311023401e43d155	High
○	[redacted] RB2023070311023401e43d156	High
○	[redacted] RB2023063016494601122ac78	Low

5 Total Records: 4 ‹ 1 ›

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 8-53 Document plan steps



Trouble Shooting

* Emergency Plan Type

Automation plan | Document Plan

Document Planning Steps

01

* Handling Method

Not Involved | Scripts | Jobs

Delete

* Step Name

Enter a step name(Automatically read script/job name)

* Step Description

Add Steps

Cancel | Save

----End

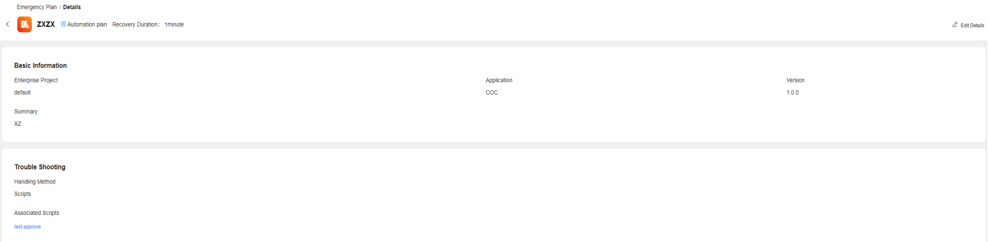
Viewing Emergency Plan Details

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 8-54 Viewing emergency plan details



Recovery Duration: 1minute

Basic Information

Enterprise Project: default

Application: COC

Version: 1.0.0

Summary: XZ

Trouble Shooting

Handling Method: Scripts

Associated Scripts: test-approve

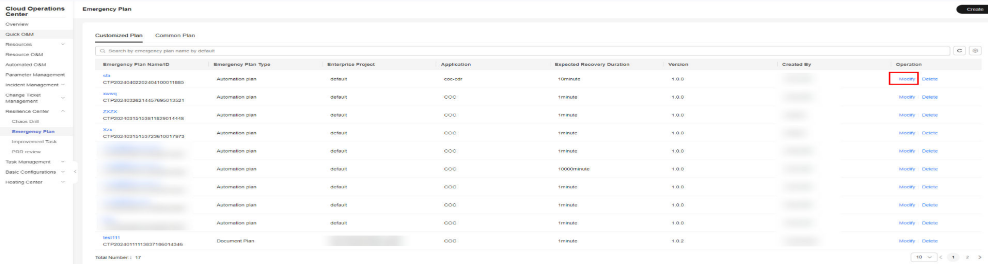
----End

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 8-55 Customized Plan

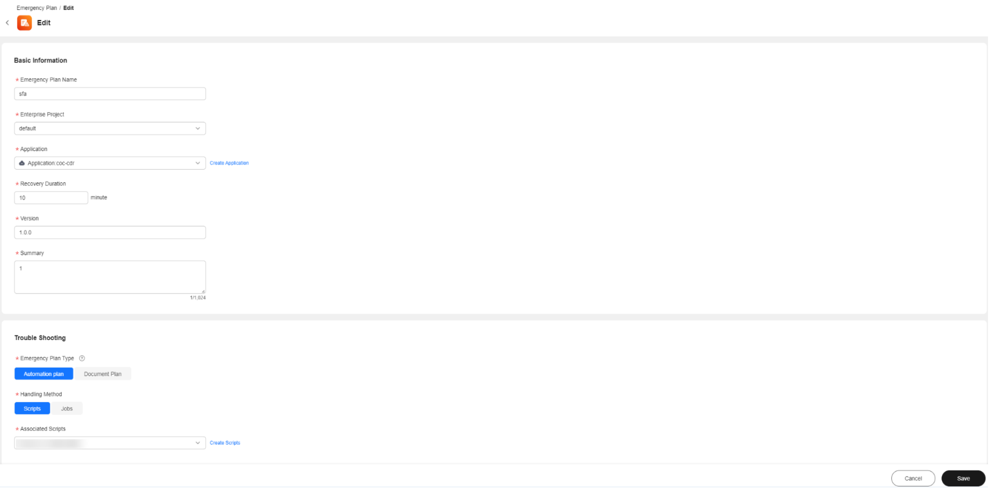


Emergency Plan Name/ID	Emergency Plan Type	Enterprise Project	Application	Expected Recovery Duration	Version	Created By	Operation
sfa CTP20240402202404100011885	Automation plan	default	coc-cdr	10minute	1.0.0	[redacted]	Modify Delete
xwwq CTP20240326214457695013521	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
ZXZX CTP20240315153811829014448	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
Xzx CTP20240315153723610017973	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	10000minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
test111 CTP20240111113837186014346	Document Plan	[redacted]	COC	1minute	1.0.2	[redacted]	Modify Delete

Total Number: : 17

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

Figure 8-56 Modifying an Emergency Plan



Basic Information

* Emergency Plan Name: sfa

* Enterprise Project: default

* Application: Application:coc-cdr

* Recovery Duration: 10 minute

* Version: 1.0.0

* Summary: 1

1/1,024

Trouble Shooting

* Emergency Plan Type: ● Automation plan ○ Document Plan

* Handling Method: ● Scripts ○ Jobs

* Associated Scripts: [redacted]

----End

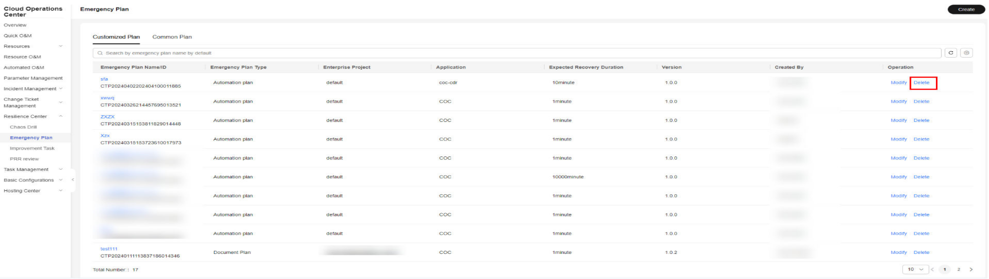
Deleting an Emergency Plan

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 8-57 Emergency plans

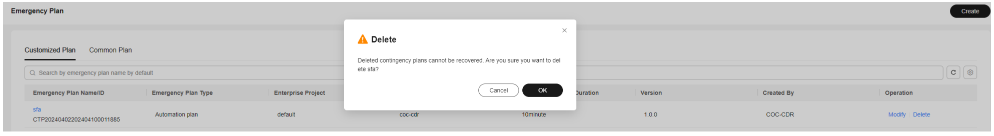


Emergency Plan Name/ID	Emergency Plan Type	Enterprise Project	Application	Expected Recovery Duration	Version	Created By	Operation
sfa CTP20240402202404100011885	Automation plan	default	coc-cdr	10minute	1.0.0	[redacted]	Modify Delete
xwwq CTP20240326214457695013521	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
ZXZX CTP20240315153811829014448	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
Xzx CTP20240315153723610017973	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	10000minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
[redacted]	Automation plan	default	COC	1minute	1.0.0	[redacted]	Modify Delete
test111 CTP20240111113837186014346	Document Plan	[redacted]	COC	1minute	1.0.2	[redacted]	Modify Delete

Total Number: : 17

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

Figure 8-58 Deleting an emergency plan



Delete

Deleted contingency plans cannot be recovered. Are you sure you want to del ete sfa?

----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.

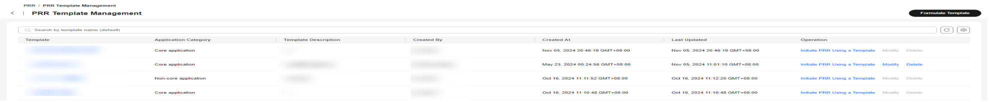
8.3.2 PRR Template Management

Creating a PRR Template

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click **PRR Template Management**.

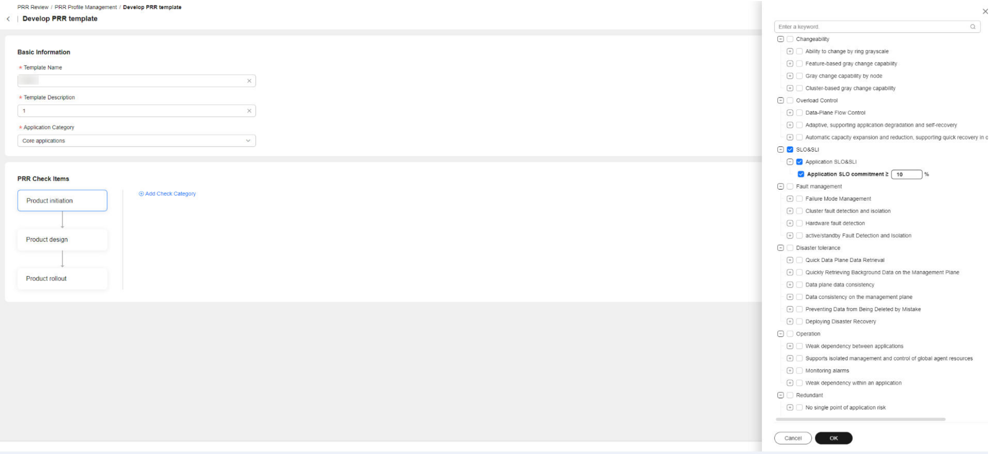
Figure 8-59 PRR template management



PRR / PRR Template Management
PRR Template Management
Formulate Template
Search by template name (default)

Template	Application Category	Template Description	Created By	Created At	Last Updated	Operation
[redacted]	Core application	[redacted]	[redacted]	Nov 05, 2024 20:46:19 GMT+08:00	Nov 05, 2024 20:46:19 GMT+08:00	Initiate PRR Using a Template Modify Delete
[redacted]	Core application	[redacted]	[redacted]	May 23, 2024 00:24:56 GMT+08:00	Nov 05, 2024 11:01:10 GMT+08:00	Initiate PRR Using a Template Modify Delete
[redacted]	Non-core application	[redacted]	[redacted]	Oct 16, 2024 11:11:52 GMT+08:00	Oct 16, 2024 11:12:20 GMT+08:00	Initiate PRR Using a Template Modify Delete
[redacted]	Core application	[redacted]	[redacted]	Oct 16, 2024 11:10:48 GMT+08:00	Oct 16, 2024 11:10:48 GMT+08:00	Initiate PRR Using a Template Modify Delete

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



Template Description: 1

Application Category: Core applications

Application SLO commitment ≥ 10 %

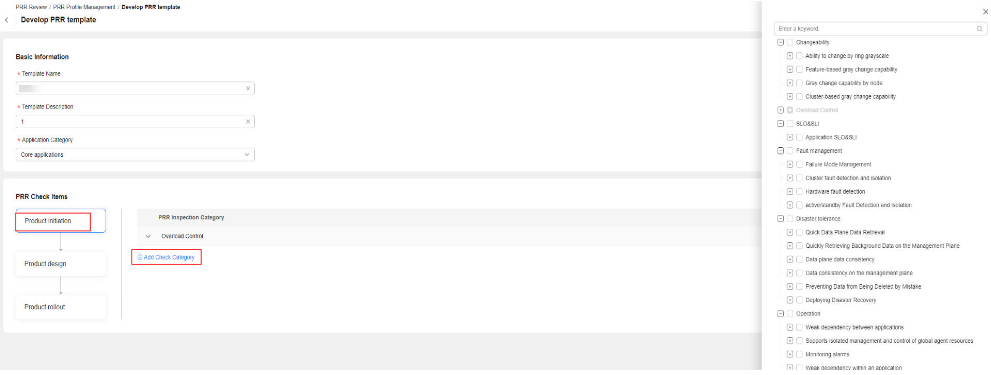
PRR Review / PRR Profile Management / Develop PRR template
Develop PRR template
Basic Information
Template Name
Template Description
Application Category
PRR Check Items
Product initiation
Product design
Product rollout
Add Check Category
Enter a keyword.
Changeability
Ability to change by ring grayscale
Feature-based gray change capability
Gray change capability by node
Cluster-based gray change capability
Overload Control
Data-Plane Flow Control
Adaptive, supporting application degradation and self-recovery
Automatic capacity expansion and reduction, supporting quick recovery in c
SLO&SLI
Application SLO&SLI
Fault management
Failure Mode Management
Cluster fault detection and isolation
Hardware fault detection
active/standby Fault Detection and Isolation
Disaster tolerance
Quick Data Plane Data Retrieval
Quickly Retrieving Background Data on the Management Plane
Data plane data consistency
Data consistency on the management plane
Preventing Data from Being Deleted by Mistake
Deploying Disaster Recovery
Operation
Weak dependency between applications
Supports isolated management and control of global agent resources
Monitoring alarms
Weak dependency within an application
Redundant
No single point of application risk
Cancel
OK

Figure 8-60 Creating a PRR template

Table 8-8 Parameters for creating a PRR template

Parameter	Description
Template	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 rollout 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 items as required.



Template Description: 1

Application Category: Core applications

PRR Review / PRR Profile Management / Develop PRR template
Develop PRR template
Basic Information
Template Name
Template Description
Application Category
PRR Check Items
Product initiation
Product design
Product rollout
PRR Inspection Category
Overload Control
Add Check Category
Enter a keyword.
Changeability
Ability to change by ring grayscale
Feature-based gray change capability
Gray change capability by node
Cluster-based gray change capability
Overload Control
SLO&SLI
Application SLO&SLI
Fault management
Failure Mode Management
Cluster fault detection and isolation
Hardware fault detection
active/standby Fault Detection and Isolation
Disaster tolerance
Quick Data Plane Data Retrieval
Quickly Retrieving Background Data on the Management Plane
Data plane data consistency
Data consistency on the management plane
Preventing Data from Being Deleted by Mistake
Deploying Disaster Recovery
Operation
Weak dependency between applications
Supports isolated management and control of global agent resources
Monitoring alarms
Weak dependency within an application

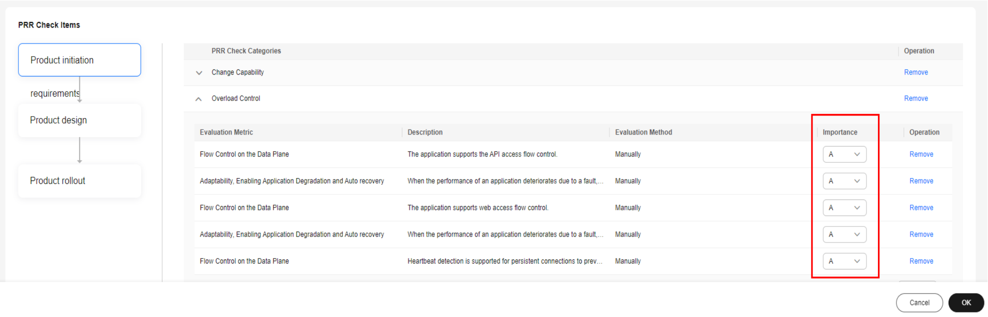
Figure 8-61 Specifying check items

Step 5 select the importance level of the selected check item.

CAUTION

If an A-level check item fails, the PRR review fails.

Figure 8-62 Selecting the importance level of a check item



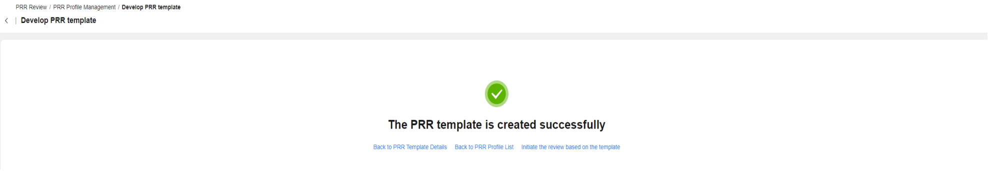
PRR Check Items

PRR Check Categories	Operation
Change Capability	Remove
Overload Control	Remove

Evaluation Metric	Description	Evaluation Method	Importance	Operation
Flow Control on the Data Plane	The application supports the API access flow control.	Manually	A	Remove
Adaptability, Enabling Application Degradation and Auto recovery	When the performance of an application deteriorates due to a fault,...	Manually	A	Remove
Flow Control on the Data Plane	The application supports web access flow control.	Manually	A	Remove
Adaptability, Enabling Application Degradation and Auto recovery	When the performance of an application deteriorates due to a fault,...	Manually	A	Remove
Flow Control on the Data Plane	Heartbeat detection is supported for persistent connections to prev...	Manually	A	Remove

Step 6 Click **OK**.

Figure 8-63 PRR template created



PRR Review / PRR Profile Management / Develop PRR template

Develop PRR template

The PRR template is created successfully

Back to PRR Template Details
Back to PRR Profile List
Initiate the review based on the template

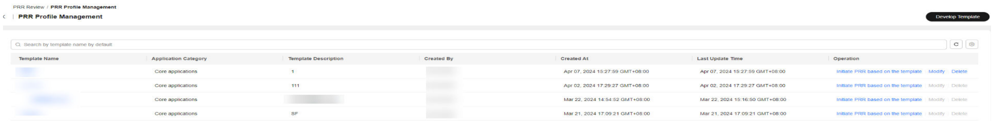
----End

Viewing PRR Template Details

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click **PRR Template Management**.

Figure 8-64 PRR template list



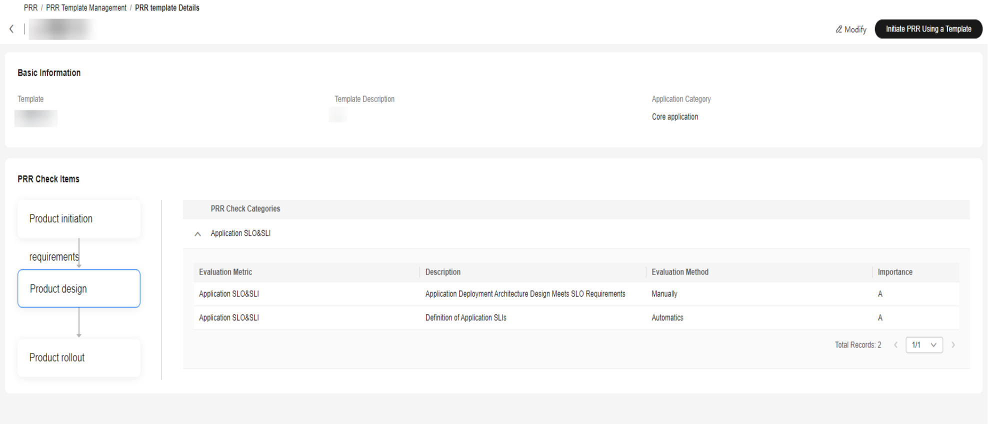
PRR Review / PRR Profile Management

PRR Profile Management

Template Name	Application Category	Template Description	Created By	Created At	Last Update Time	Operation
[redacted]	Core applications	1	[redacted]	Apr 07, 2024 15:27:59 GMT+08:00	Apr 07, 2024 15:27:59 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	111	[redacted]	Apr 02, 2024 17:29:27 GMT+08:00	Apr 02, 2024 17:29:27 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	[redacted]	[redacted]	Mar 22, 2024 14:54:52 GMT+08:00	Mar 22, 2024 15:16:50 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	SF	[redacted]	Mar 21, 2024 17:09:21 GMT+08:00	Mar 21, 2024 17:09:21 GMT+08:00	Initiate PRR based on the template Modify Delete

Step 3 In the **Template** column, click a template name. The **PRR template Details** page is displayed.

Figure 8-65 PRR template details



PRR / PRR Template Management / PRR template Details

Basic Information

Template	Template Description	Application Category
		Core application

PRR Check Items

PRR Check Categories

Application SLO&SLI

Evaluation Metric	Description	Evaluation Method	Importance
Application SLO&SLI	Application Deployment Architecture Design Meets SLO Requirements	Manually	A
Application SLO&SLI	Definition of Application SLIs	Automatics	A

Total Records: 2 1/1

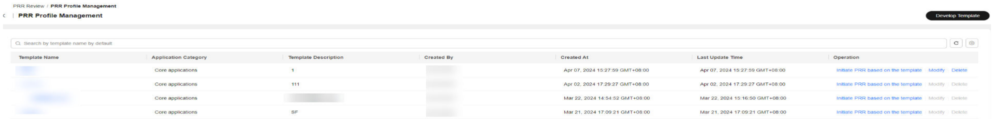
----End

Modifying a PRR Template

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click **PRR Template Management**.

Figure 8-66 PRR template list



PRR Review / PRR Profile Management

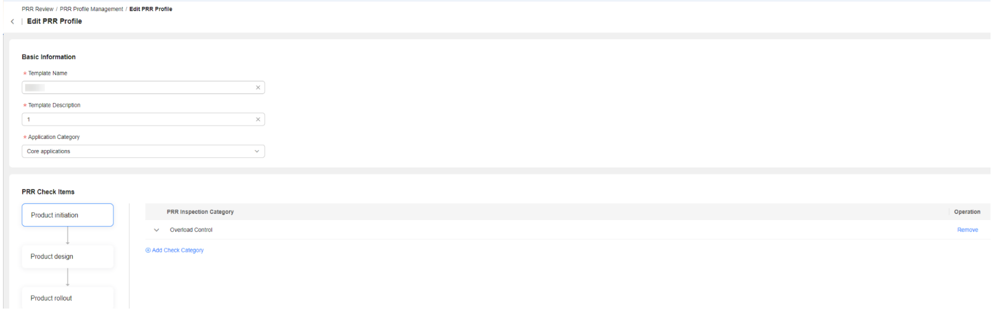
PRR Profile Management

Search by template name by default

Template Name	Application Category	Template Description	Created By	Created At	Last Update Time	Operation
	Core applications	1		Apr 07, 2024 15:27:59 GMT+08:00	Apr 07, 2024 15:27:59 GMT+08:00	Initiate PRR based on the template Modify Delete
	Core applications	111		Apr 02, 2024 17:29:27 GMT+08:00	Apr 02, 2024 17:29:27 GMT+08:00	Initiate PRR based on the template Modify Delete
	Core applications			Mar 22, 2024 14:54:52 GMT+08:00	Mar 22, 2024 15:16:50 GMT+08:00	Initiate PRR based on the template Modify Delete
	Core applications	SF		Mar 21, 2024 17:09:21 GMT+08:00	Mar 21, 2024 17:09:21 GMT+08:00	Initiate PRR based on the template Modify Delete

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

Figure 8-67 Modifying a PRR template



PRR Review / PRR Profile Management / Edit PRR Profile

Edit PRR Profile

Basic Information

* Template Name:
* Template Description: 1
* Application Category: Core applications

PRR Check Items

PRR Inspection Category	Operation
Overload Control	Remove

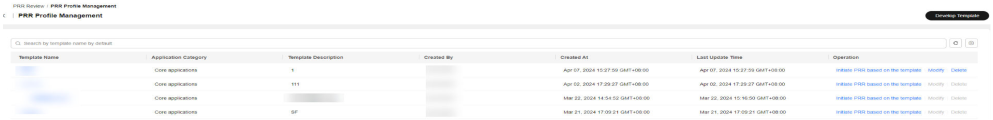
----End

Deleting a PRR Template

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Resilience Center** > **PRR review**. On the displayed page, click **PRR Template Management**.

Figure 8-68 PRR template list



PRR Review / **PRR Profile Management**

PRR Profile Management

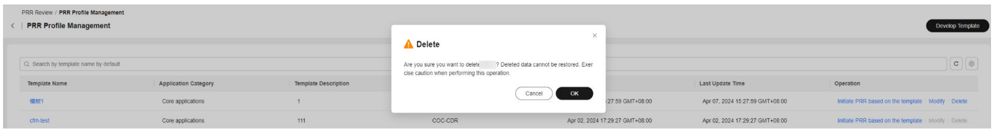
Develop Template

Search by template name by default

Template Name	Application Category	Template Description	Created By	Created At	Last Update Time	Operation
[redacted]	Core applications	1	[redacted]	Apr 07, 2024 15:27:59 GMT+08:00	Apr 07, 2024 15:27:59 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	111	[redacted]	Apr 02, 2024 17:29:27 GMT+08:00	Apr 02, 2024 17:29:27 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	[redacted]	[redacted]	Mar 22, 2024 14:54:52 GMT+08:00	Mar 22, 2024 15:16:50 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	SF	[redacted]	Mar 21, 2024 17:09:21 GMT+08:00	Mar 21, 2024 17:09:21 GMT+08:00	Initiate PRR based on the template Modify Delete

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

Figure 8-69 Deleting a PRR template



PRR Review / **PRR Profile Management**

PRR Profile Management

Develop Template

Delete

Are you sure you want to delete [redacted]? Deleted data cannot be restored. Exercise caution when performing this operation.

Cancel OK

Search by template name by default

Template Name	Application Category	Template Description			Last Update Time	Operation
模板1	Core applications	1		:27:59 GMT+08:00	Apr 07, 2024 15:27:59 GMT+08:00	Initiate PRR based on the template Modify Delete
cfm-test	Core applications	111	COC-CDR	Apr 02, 2024 17:29:27 GMT+08:00	Apr 02, 2024 17:29:27 GMT+08:00	Initiate PRR based on the template Modify Delete

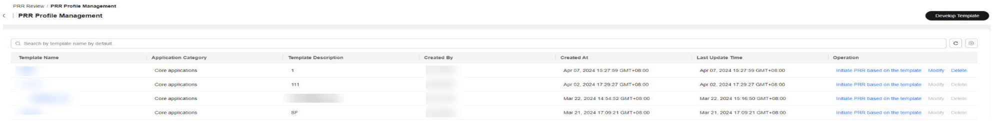
----End

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**. On the displayed page, click **PRR Template Management**.

Figure 8-70 PRR template list



PRR Review / **PRR Profile Management**

PRR Profile Management

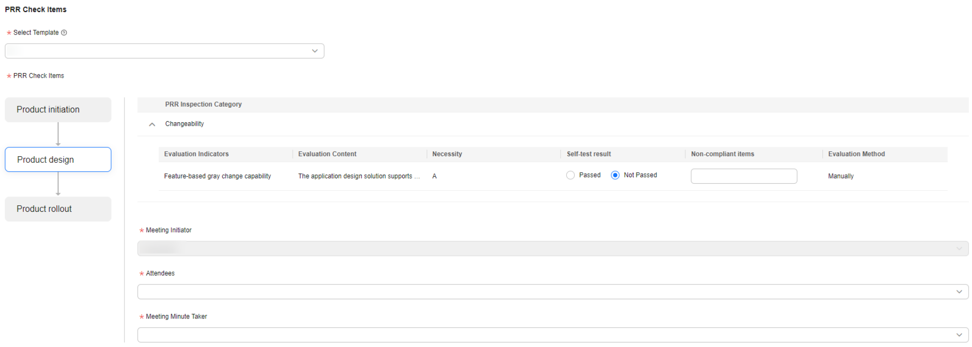
Develop Template

Search by template name by default

Template Name	Application Category	Template Description	Created By	Created At	Last Update Time	Operation
[redacted]	Core applications	1	[redacted]	Apr 07, 2024 15:27:59 GMT+08:00	Apr 07, 2024 15:27:59 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	111	[redacted]	Apr 02, 2024 17:29:27 GMT+08:00	Apr 02, 2024 17:29:27 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	[redacted]	[redacted]	Mar 22, 2024 14:54:52 GMT+08:00	Mar 22, 2024 15:16:50 GMT+08:00	Initiate PRR based on the template Modify Delete
[redacted]	Core applications	SF	[redacted]	Mar 21, 2024 17:09:21 GMT+08:00	Mar 21, 2024 17:09:21 GMT+08:00	Initiate PRR based on the template Modify Delete

Step 3 Locate the target template, and click **Initiate PRR Using a Template** in the **Operation** column. This template is selected to initiate PRR by default. For details about how to initiate PRR, see **PRR Management**.

Figure 8-71 Initiating PRR based on a template



PRR Check Items

* Select Template

* PRR Check Items

PRR Inspection Category

Changeability

Evaluation Indicators	Evaluation Content	Necessity	Self-test result	Non-compliant items	Evaluation Method
Feature-based gray change capability	The application design solution supports ...	A	○ Passed ● Not Passed		Manually

* Meeting Initiator

* Attendees

* Meeting Minute Taker

----End

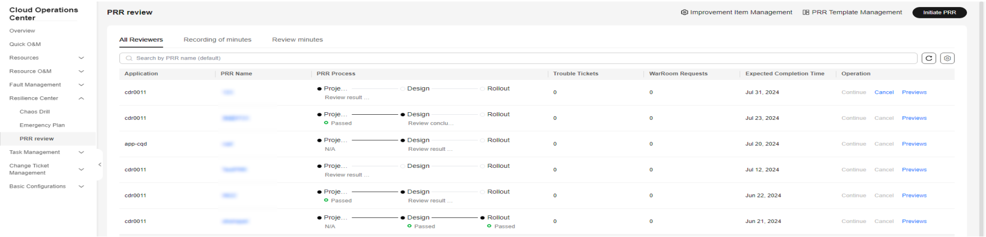
8.3.3 PRR Management

Initiating PRR

Step 1 Log in to **COC**.

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

Figure 8-72 PRR list



Cloud Operations Center

- Overview
- Quick O&M
- Resources
- Resource O&M
- Fault Management
- Resilience Center
  - Chaos Drill
  - Emergency Plan
  - PRR review
- Task Management
- Change Ticket Management
- Basic Configurations

PRR review

Improvement Item Management | PRR Template Management | Initiate PRR

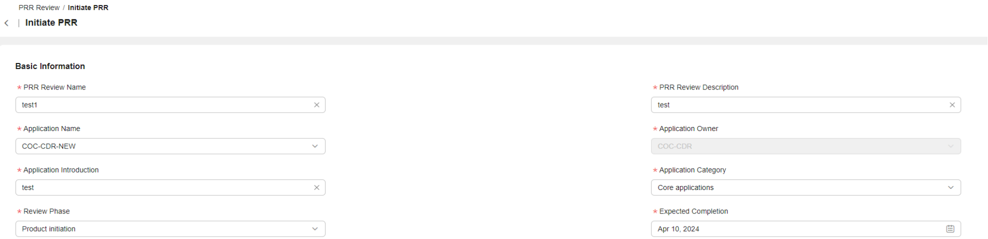
All Reviewers | Recording of minutes | Review minutes

Search by PRR name (default)

Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
cdr0011	[redacted]	Proje… Review result … — Design — Rollout	0	0	Jul 31, 2024	Continue Cancel Previews
cdr0011	[redacted]	Proje… Passed — Design Review conclu… — Rollout	0	0	Jul 23, 2024	Continue Cancel Previews
app-cqd	[redacted]	Proje… N/A — Design Review result … — Rollout	0	0	Jul 20, 2024	Continue Cancel Previews
cdr0011	[redacted]	Proje… Review result … — Design — Rollout	0	0	Jul 12, 2024	Continue Cancel Previews
cdr0011	[redacted]	Proje… Passed — Design Review result … — Rollout	0	0	Jun 22, 2024	Continue Cancel Previews
cdr0011	[redacted]	Proje… N/A — Design Passed — Rollout Passed	0	0	Jun 21, 2024	Continue Cancel Previews

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

Figure 8-73 Initiating PRR - Specifying PRR basic information



PRR Review / Initiate PRR

Initiate PRR

Basic Information

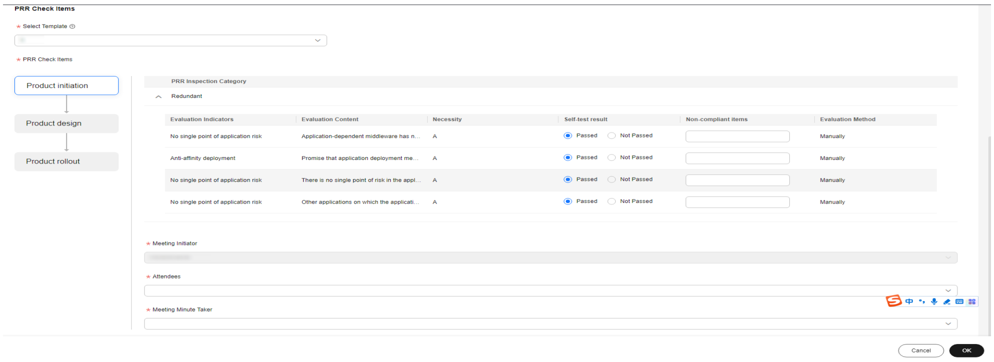
- * PRR Review Name: test1
- * PRR Review Description: test
- * Application Name: COC-CDR-NEW
- * Application Owner: COC-CDR
- * Application Introduction: test
- * Application Category: Core applications
- * Review Phase: Product initiation
- * Expected Completion: Apr 10, 2024

Table 8-9 Basic parameters for initiating PRR

Parameter	Description
PRR Name	Name of the PRR
PRR Description	Description of the PRR
Application	Name of the application to which the PRR belongs
Owner	Owner of the application to which the PRR belongs
Application Description	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
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 8-74 Initiating PRR - Specifying PRR check items



PRR Check Items

* Select Template

* PRR Check Items

PRR Inspection Category

Redundant

Evaluation Indicators	Evaluation Content	Necessity	Self-test result	Non-compliant items	Evaluation Method
No single point of application risk	Application-dependent middleware has n...	A	● Passed ○ Not Passed		Manually
Anti-affinity deployment	Promise that application deployment me...	A	● Passed ○ Not Passed		Manually
No single point of application risk	There is no single point of risk in the appl...	A	● Passed ○ Not Passed		Manually
No single point of application risk	Other applications on which the applicati...	A	● Passed ○ Not Passed		Manually

* Meeting Initiator

* Attendees

* Meeting Minute Taker

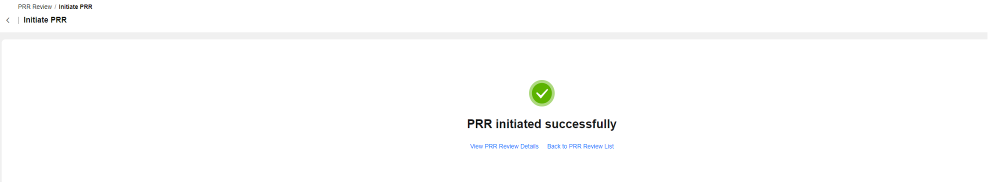
Table 8-10 Parameters of check items

Parameter	Description
Self-Check Result	Self-check results of check items. (If an A-level check item fails, the self-check cannot be initiated.) The self-check results are automatically displayed in automatic evaluation mode.
Violated Item	Item that does not pass the check. When automatic evaluation is enabled, you can view the details about the violated item.
Conference Initiator	Initiator of the PRR conference
Participant	Participant of the PRR conference
Minutes Recorded By	Minutes maker of the PRR conference

Step 5 Click **Add self-check materials** to upload self-check materials.

Step 6 Click **OK**.

Figure 8-75 PRR initiated



PRR initiated successfully

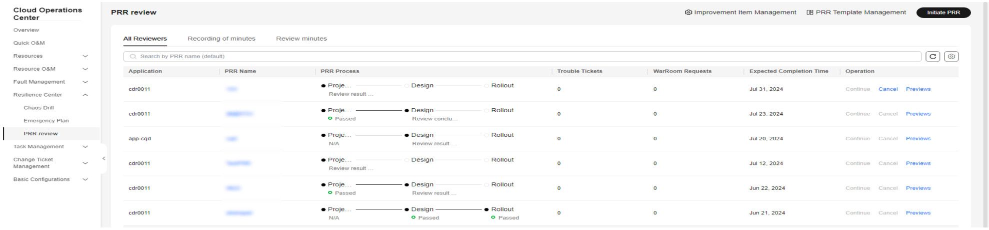
----End

Viewing PRR Details

Step 1 Log in to COC.

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

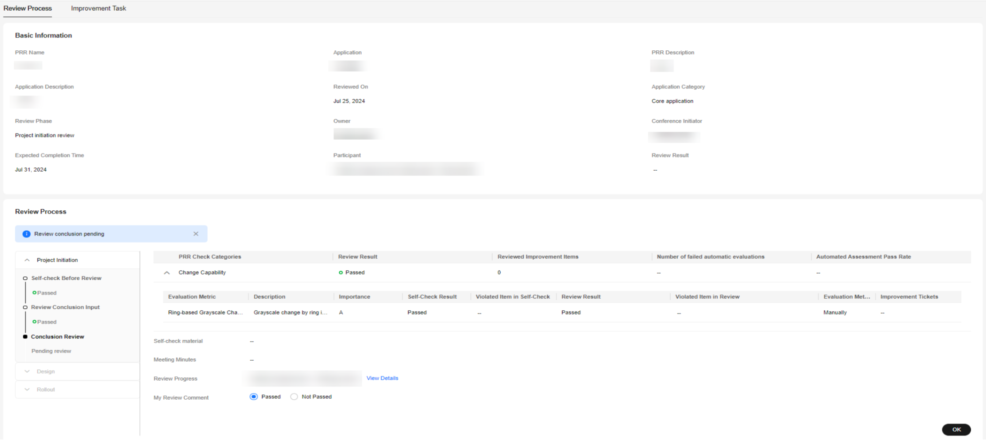
Figure 8-76 PRR list



Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
cdr0011	[redacted]	● Proje… Review result … ○ Design ○ Rollout	0	0	Jul 31, 2024	Continue Cancel Previews
cdr0011	[redacted]	● Proje… Passed ● Design Review conclu… ○ Rollout	0	0	Jul 23, 2024	Continue Cancel Previews
app-cqd	[redacted]	● Proje… N/A ● Design Review result … ○ Rollout	0	0	Jul 20, 2024	Continue Cancel Previews
cdr0011	[redacted]	● Proje… Review result … ○ Design ○ Rollout	0	0	Jul 12, 2024	Continue Cancel Previews
cdr0011	[redacted]	● Proje… Passed ● Design Review result … ○ Rollout	0	0	Jun 22, 2024	Continue Cancel Previews
cdr0011	[redacted]	● Proje… N/A ● Design Passed ● Rollout Passed	0	0	Jun 21, 2024	Continue Cancel Previews

Step 3 In the **PRR Name** column, click a PRR name.

Figure 8-77 PRR details



Basic Information

PRR Name: [redacted]
Application: [redacted]
PRR Description: [redacted]
Application Description: [redacted]
Reviewed On: Jul 25, 2024
Application Category: Core application
Review Phase: Project initiation review
Owner: [redacted]
Conference Initiator: [redacted]
Expected Completion Time: Jul 31, 2024
Participant: [redacted]
Review Result: --

Review Process

PRR Check Categories	Review Result	Reviewed Improvement Items	Number of failed automatic evaluations	Automated Assessment Pass Rate
Change Capability	Passed	0	--	--

Evaluation Metric	Description	Importance	Self-Check Result	Violated Item in Self-Check	Review Result	Violated Item in Review	Evaluation Met…	Improvement Tickets
Ring-based Grayscale Cha…	Grayscale change by ring i…	A	Passed	--	Passed	--	Manually	--

Self-check material --
Meeting Minutes: --
Review Progress: [redacted]
My Review Comment: ● Passed ○ Not Passed

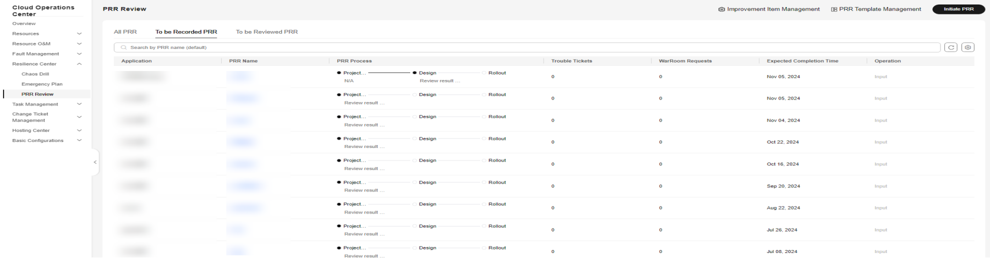
----End

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 **To be recorded PRR** tab.

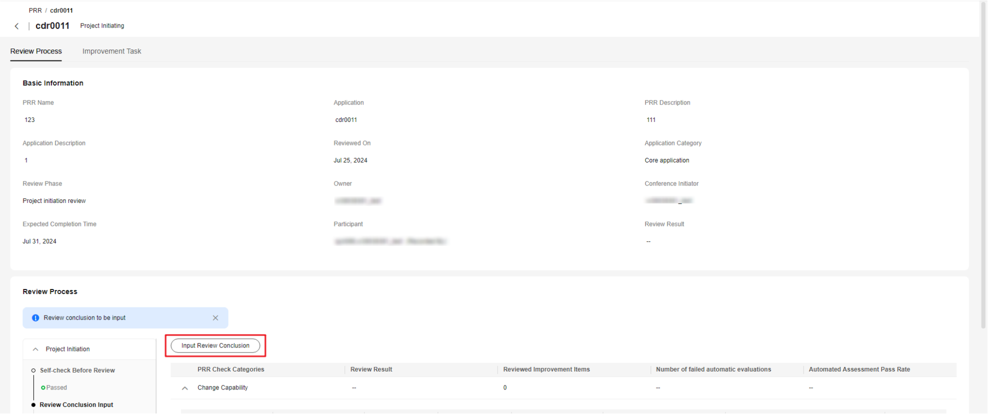
Figure 8-78 To be recorded PRR



Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
[redacted]	[redacted]	● Project… N/A ● Design Review result … ○ Rollout	0	0	Nov 05, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Nov 05, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Nov 04, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Oct 22, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Oct 16, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Sep 20, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Aug 22, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Jul 26, 2024	Input
[redacted]	[redacted]	● Project… Review result … ○ Design ○ Rollout	0	0	Jul 08, 2024	Input

Step 3 Locate the target PRR record, and click **Input** in the **Operation** column. On the displayed PRR details page, click **Input Review Conclusion** to enter the review minutes.

Figure 8-79 PRR details - inputting review conclusion



PRR / cdr0011

cdr0011 Project Initiating

Review Process | Improvement Task

Basic Information

PRR Name: 123

Application: cdr0011

PRR Description: 111

Application Description: 1

Reviewed On: Jul 25, 2024

Application Category: Core application

Review Phase: Project initiation review

Owner: [redacted]

Conference Initiator: [redacted]

Expected Completion Time: Jul 31, 2024

Participant: [redacted]

Review Result: --

Review Process

Review conclusion to be input

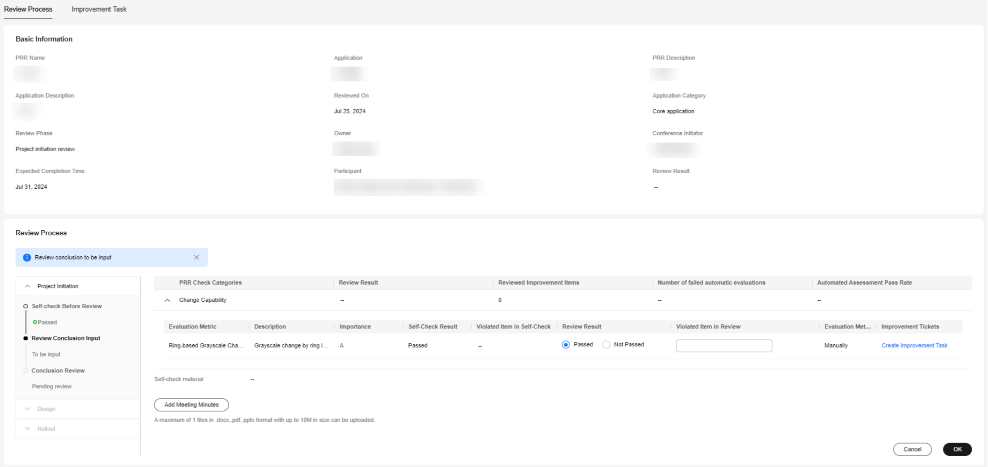
Project Initiation
- Self-check Before Review
  - Passed
- Review Conclusion Input

Input Review Conclusion

	PRR Check Categories	Review Result	Reviewed Improvement Items	Number of failed automatic evaluations	Automated Assessment Pass Rate
^	Change Capability	--	0	--	--

Step 4 Enter review conclusion.

Figure 8-80 Entering review conclusion



Review Process | Improvement Task

Basic Information

PRR Name: [redacted]

Application: [redacted]

PRR Description: [redacted]

Application Description: [redacted]

Reviewed On: Jul 25, 2024

Application Category: Core application

Review Phase: Project initiation review

Owner: [redacted]

Conference Initiator: [redacted]

Expected Completion Time: Jul 31, 2024

Participant: [redacted]

Review Result: --

Review Process

Review conclusion to be input

Project Initiation
- Self-check Before Review
  - Passed
- Review Conclusion Input
  - To be input
- Conclusion Review
  - Pending review

Design

Rollout

	PRR Check Categories	Review Result	Reviewed Improvement Items	Number of failed automatic evaluations	Automated Assessment Pass Rate
^	Change Capability	--	0	--	--

Evaluation Metric	Description	Importance	Self-Check Result	Violated Item in Self-Check	Review Result	Violated Item in Review	Evaluation Met...	Improvement Tickets
Ring-based Grayscale Cha...	Grayscale change by ring i...	A	Passed	--	● Passed ○ Not Passed		Manually	Create Improvement Task

Self-check material --

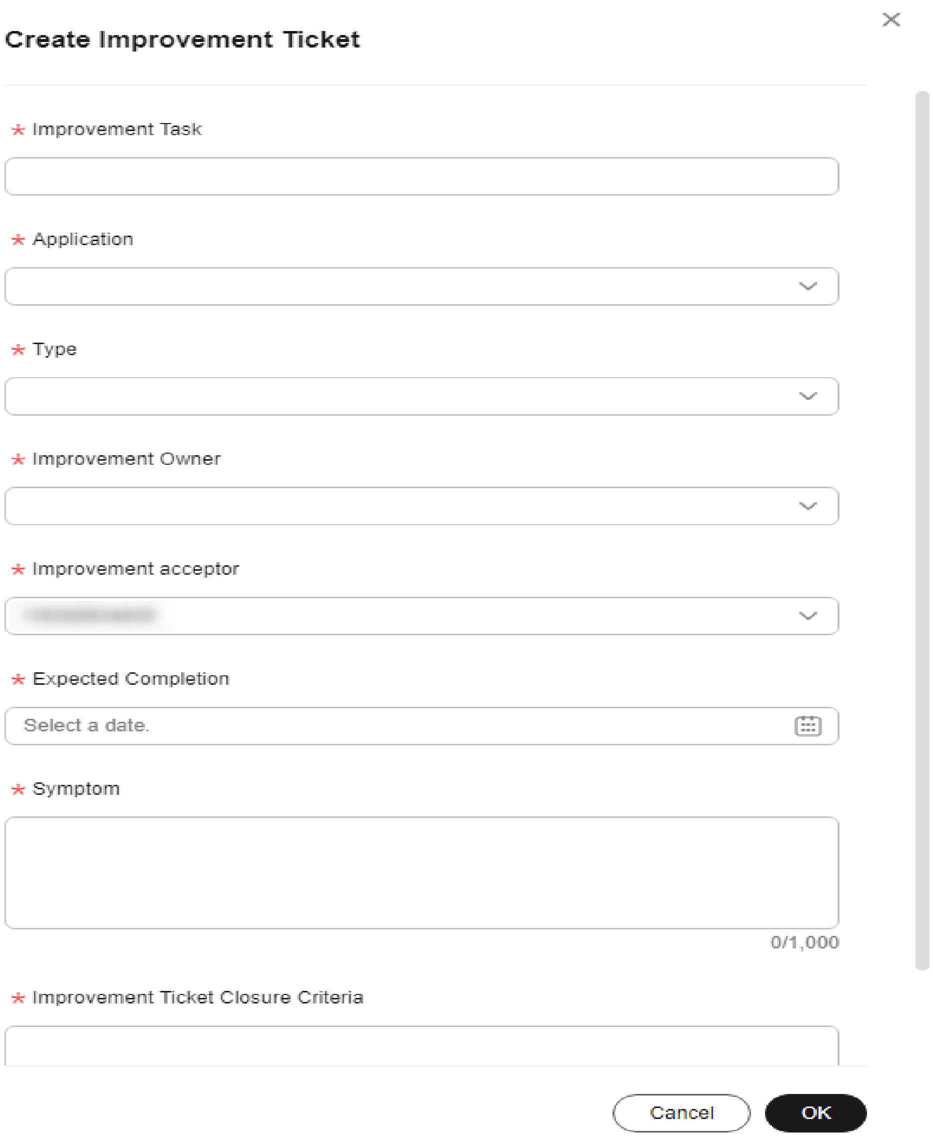
Add Meeting Minutes

A maximum of 1 files in .docx,.pdf,.pptx format with up to 10M in size can be uploaded.

Cancel | OK

Step 5 Locate the target check item, and click **Create Improvement Task** in the **Improvement Tickets** column. On the displayed page, specify the information about the improvement ticket and click **OK**.

Figure 8-81 Entering review minutes - creating an improvement ticket



Create Improvement Ticket

* Improvement Task

* Application

* Type

* Improvement Owner

* Improvement acceptor

[redacted]

* Expected Completion

Select a date.

* Symptom

0/1,000

* Improvement Ticket Closure Criteria

Table 8-11 Improvement ticket parameters

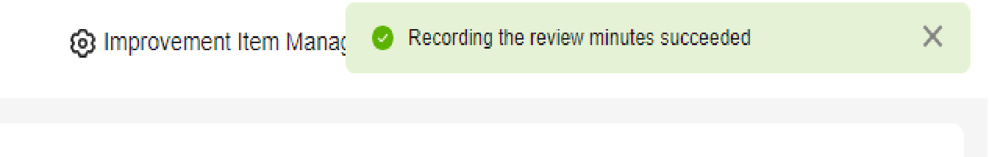
Parameter	Description
Improvement Task	Improvement ticket name
Application	Application the improvement ticket belongs to
Type	Type of the improvement ticket
Improvement Owner	Owner of the improvement ticket
Improvement acceptor	Acceptor of the improvement item

Parameter	Description
Expected Completion	Expected time when the improvement ticket ends
Symptom	Issue symptoms
Improvement Ticket Closure Criteria	Criteria for the closure of the improvement ticket

Step 6 Click **Add Meeting Minutes** to add meeting minutes for the PRR conference.

Step 7 Click **OK**.

Figure 8-82 Review minutes recorded



Recording the review minutes succeeded

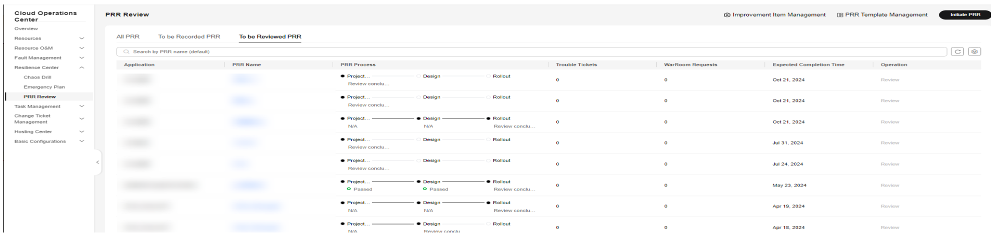
----End

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 **To be reviewed PRR** tab.

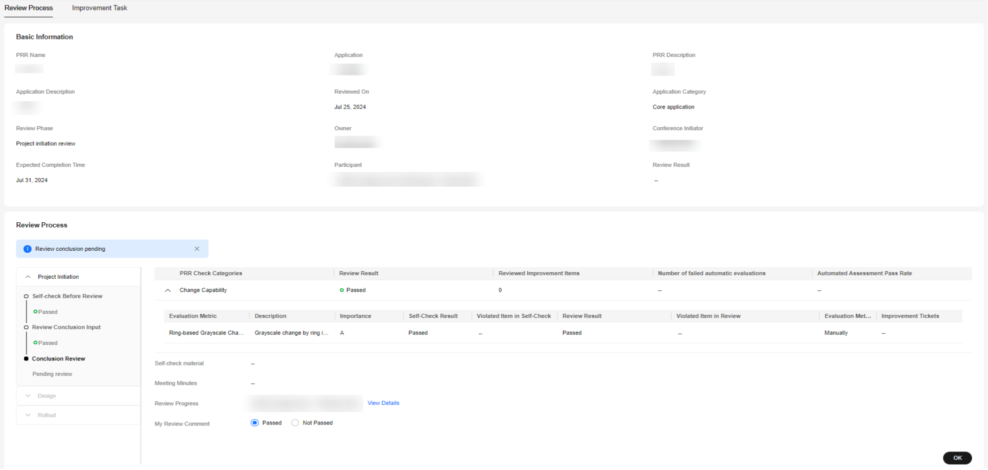
Figure 8-83 To be reviewed PRR



Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
[redacted]	[redacted]	Project... Review conclu... — Design — Rollout	0	0	Oct 21, 2024	Review
[redacted]	[redacted]	Project... Review conclu... — Design — Rollout	0	0	Oct 21, 2024	Review
[redacted]	[redacted]	Project... N/A — Design N/A — Rollout Review conclu...	0	0	Oct 21, 2024	Review
[redacted]	[redacted]	Project... Review conclu... — Design — Rollout	0	0	Jul 31, 2024	Review
[redacted]	[redacted]	Project... Review conclu... — Design — Rollout	0	0	Jul 24, 2024	Review
[redacted]	[redacted]	Project... Passed — Design Passed — Rollout Review conclu...	0	0	May 23, 2024	Review
[redacted]	[redacted]	Project... N/A — Design N/A — Rollout Review conclu...	0	0	Apr 19, 2024	Review
[redacted]	[redacted]	Project... N/A — Design Review conclu — Rollout	0	0	Apr 18, 2024	Review

Step 3 Locate the target PRR record, and click **Review** in the **Operation** column. On the displayed page, you can view the review progress of the current PRR, and enter the review conclusion.

Figure 8-84 Recording the review conclusion



Basic Information

PRR Name	Application	PRR Description
Application Description	Reviewed On	Application Category
	Jul 25, 2024	Core application
Review Phase	Owner	Conference Initiator
Project initiation review		
Expected Completion Time	Participant	Review Result
Jul 31, 2024		--

Review Process

Review conclusion pending

PRR Check Categories	Review Result	Reviewed Improvement Items	Number of failed automatic evaluations	Automated Assessment Pass Rate
Change Capability	Passed	0	--	--

Evaluation Metric	Description	Importance	Self-Check Result	Violated Item in Self-Check	Review Result	Violated Item in Review	Evaluation Met...	Improvement Tickets
Ring-based Grayscale Cha...	Grayscale change by ring i...	A	Passed	--	Passed	--	Manually	--

Self-check material --

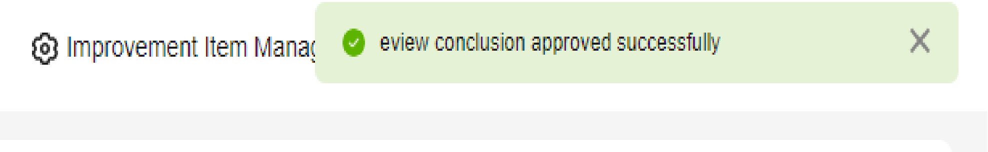
Meeting Minutes --

Review Progress View Details

My Review Comment ● Passed ○ Not Passed

Step 4 Click **OK**.

Figure 8-85 Review conclusion recorded



eview conclusion approved successfully

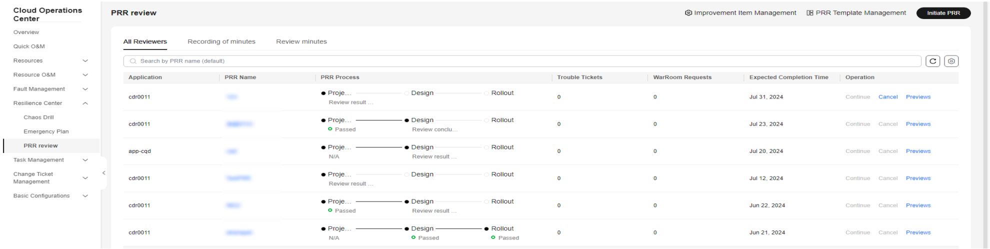
----End

Continuing to Initiate PRR

Step 1 Log in to COC.

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

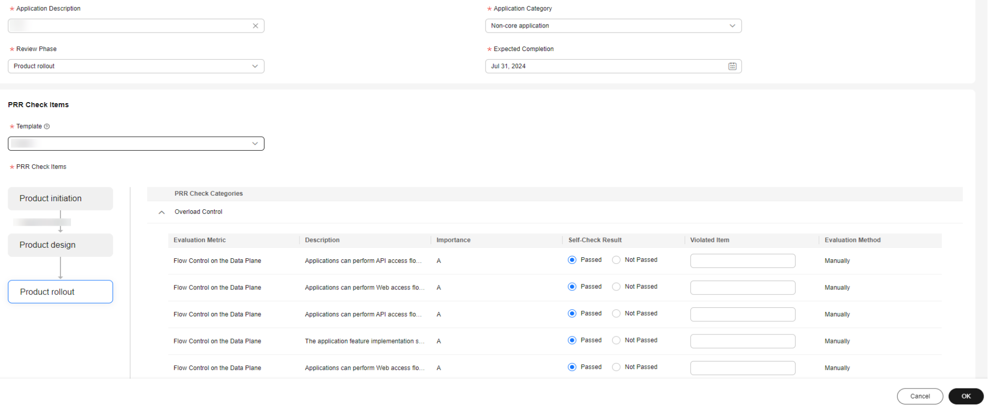
Figure 8-86 PRR list



Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
cdr0011		Proje... Review result ... Design Rollout	0	0	Jul 31, 2024	Continue Cancel Previews
cdr0011		Proje... Passed Design Review conclu... Rollout	0	0	Jul 23, 2024	Continue Cancel Previews
app-cqd		Proje... N/A Design Review result ... Rollout	0	0	Jul 20, 2024	Continue Cancel Previews
cdr0011		Proje... Review result ... Design Rollout	0	0	Jul 12, 2024	Continue Cancel Previews
cdr0011		Proje... Passed Design Review result ... Rollout	0	0	Jun 22, 2024	Continue Cancel Previews
cdr0011		Proje... N/A Design Passed Rollout Passed	0	0	Jun 21, 2024	Continue Cancel Previews

Step 3 Locate the target PRR record, click **Continue** 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 8-87 Continuing to initiate PRR



* Application Description: [illegible]

* Application Category: Non-core application

* Review Phase: Product rollout

* Expected Completion: Jul 31, 2024

PRR Check Items

* Template: [illegible]

* PRR Check Items

PRR Check Categories

Overload Control

Evaluation Metric	Description	Importance	Self-Check Result	Violated Item	Evaluation Method
Flow Control on the Data Plane	Applications can perform API access flo...	A	● Passed ○ Not Passed		Manually
Flow Control on the Data Plane	Applications can perform Web access flo...	A	● Passed ○ Not Passed		Manually
Flow Control on the Data Plane	Applications can perform API access flo...	A	● Passed ○ Not Passed		Manually
Flow Control on the Data Plane	The application feature implementation s...	A	● Passed ○ Not Passed		Manually
Flow Control on the Data Plane	Applications can perform Web access flo...	A	● Passed ○ Not Passed		Manually

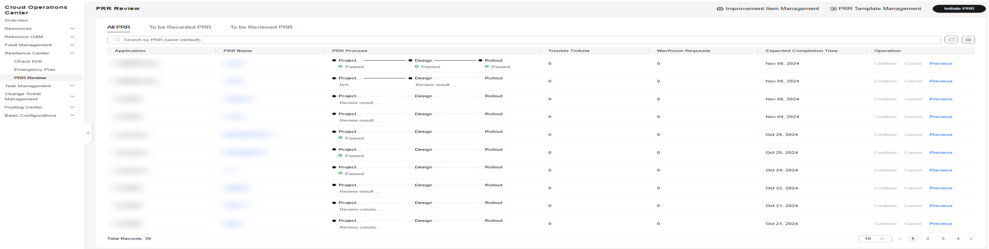
----End

Canceling the PRR

Step 1 Log in to **COC**.

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

Figure 8-88 PRR list

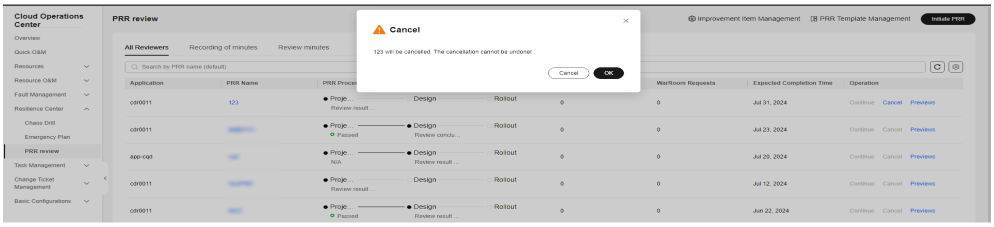


Application	PRR Name	PRR Process	Trouble Tickets	WarRoom Requests	Expected Completion Time	Operation
[illegible]	[illegible]	Project... Passed — Design Passed — Rollout Passed	0	0	Nov 05, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... N/A — Design Review result ... — Rollout	0	0	Nov 05, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Review result ... — Design — Rollout	0	0	Nov 05, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Review result ... — Design — Rollout	0	0	Nov 04, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Passed — Design — Rollout	0	0	Oct 25, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Passed — Design — Rollout	0	0	Oct 25, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Passed — Design — Rollout	0	0	Oct 24, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Review result ... — Design — Rollout	0	0	Oct 22, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Review conclu... — Design — Rollout	0	0	Oct 21, 2024	Continue Cancel Previews
[illegible]	[illegible]	Project... Review conclu... — Design — Rollout	0	0	Oct 21, 2024	Continue Cancel Previews

Total Records: 39

Step 3 Locate the target PRR record, and click **Cancel** in the **Operation** column.

Figure 8-89 Canceling the PRR



Cancel

123 will be cancelled. The cancellation cannot be undone!

Application	PRR Name	PRR Proces	WarRoom Requests	Expected Completion Time	Operation
cdr0011	123	Proje... Review result ... — Design — Rollout	0	0	Jul 31, 2024	Continue Cancel Previews
cdr0011	[illegible]	Proje... Passed — Design Review conclu... — Rollout	0	0	Jul 23, 2024	Continue Cancel Previews
app-cqd	[illegible]	Proje... N/A — Design Review result ... — Rollout	0	0	Jul 20, 2024	Continue Cancel Previews
cdr0011	[illegible]	Proje... Review result ... — Design — Rollout	0	0	Jul 12, 2024	Continue Cancel Previews
cdr0011	[illegible]	Proje... Passed — Design Review result ... — Rollout	0	0	Jun 22, 2024	Continue Cancel Previews

----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

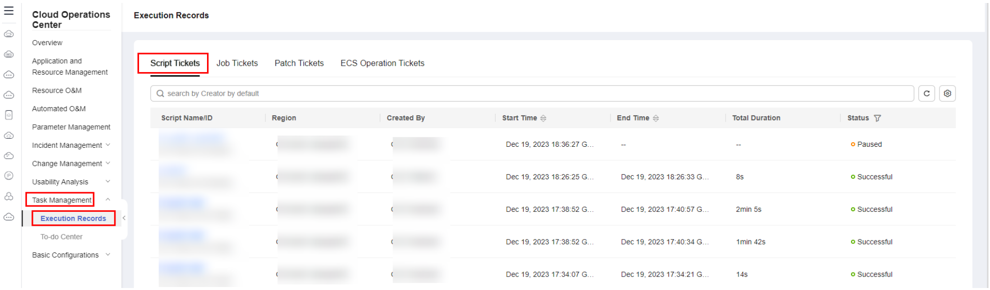
View script tickets on the **Cloud Operations Center** page.

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.

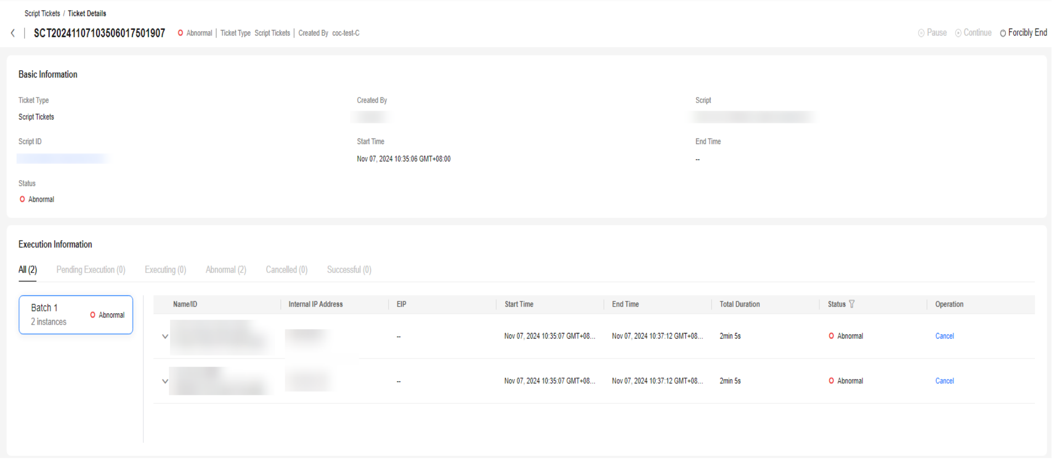
Figure 9-1 Script Tickets



Script Name/ID	Region	Created By	Start Time	End Time	Total Duration	Status
[redacted]	[redacted]	[redacted]	Dec 19, 2023 18:36:27 G...	--	--	Paused
[redacted]	[redacted]	[redacted]	Dec 19, 2023 18:26:25 G...	Dec 19, 2023 18:26:33 G...	8s	Successful
[redacted]	[redacted]	[redacted]	Dec 19, 2023 17:38:52 G...	Dec 19, 2023 17:40:57 G...	2min 5s	Successful
[redacted]	[redacted]	[redacted]	Dec 19, 2023 17:38:52 G...	Dec 19, 2023 17:40:34 G...	1min 42s	Successful
[redacted]	[redacted]	[redacted]	Dec 19, 2023 17:34:07 G...	Dec 19, 2023 17:34:21 G...	14s	Successful

Step 3 Select a script service ticket in the **Abnormal** status and click the script name. The **Ticket Details** page is displayed.

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



Script Tickets / Ticket Details

SCT20241107103506017501907 ○ Abnormal | Ticket Type Script Tickets | Created By coc-test-C

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script ID: [redacted]

Start Time: Nov 07, 2024 10:35:06 GMT+08:00

End Time: --

Status: ○ Abnormal

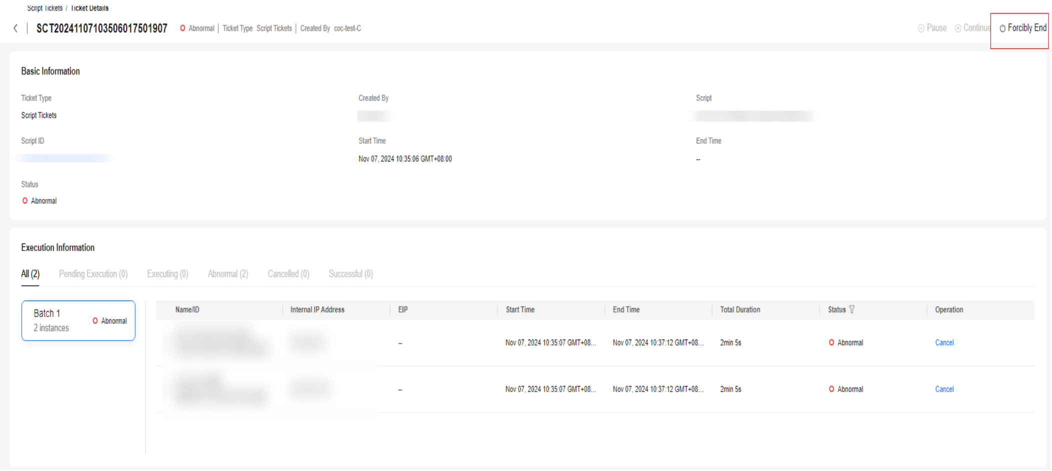
Execution Information

Batch 1 ○ Abnormal
2 instances

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Nov 07, 2024 10:35:07 GMT+08...	Nov 07, 2024 10:37:12 GMT+08...	2min 5s	○ Abnormal	Cancel
[redacted]	[redacted]	--	Nov 07, 2024 10:35:07 GMT+08...	Nov 07, 2024 10:37:12 GMT+08...	2min 5s	○ Abnormal	Cancel

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

Figure 9-3 Closing an abnormal script ticket



Script Tickets / Ticket Details

SCT20241107103506017501907 ○ Abnormal | Ticket Type Script Tickets | Created By coc-test-C

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script ID: [redacted]

Start Time: Nov 07, 2024 10:35:06 GMT+08:00

End Time: --

Status: ○ Abnormal

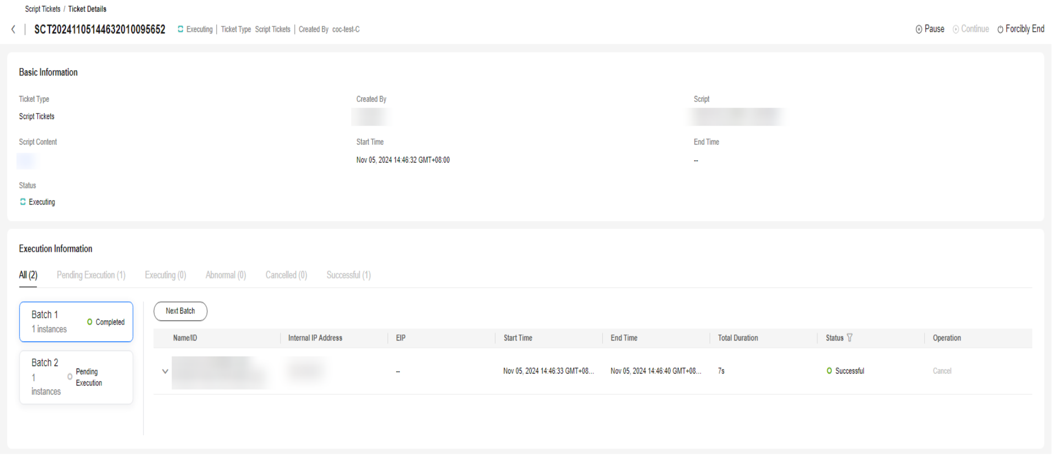
Execution Information

Batch 1 ○ Abnormal
2 instances

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Nov 07, 2024 10:35:07 GMT+08...	Nov 07, 2024 10:37:12 GMT+08...	2min 5s	○ Abnormal	Cancel
[redacted]	[redacted]	--	Nov 07, 2024 10:35:07 GMT+08...	Nov 07, 2024 10:37:12 GMT+08...	2min 5s	○ Abnormal	Cancel

Step 5 Locate a script service ticket in the **Executing** status and click the script name. The **Ticket Details** page is displayed.

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



Script Tickets / Ticket Details

SCT20241105144632010095652 Executing | Ticket Type Script Tickets | Created By coc-test-C

Pause Continue Forcibly End

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script Content: [redacted]

Start Time: Nov 05, 2024 14:46:32 GMT+08:00

End Time: --

Status: Executing

Execution Information

All (2) Pending Execution (1) Executing (0) Abnormal (0) Cancelled (0) Successful (1)

Batch 1 1 instances Completed

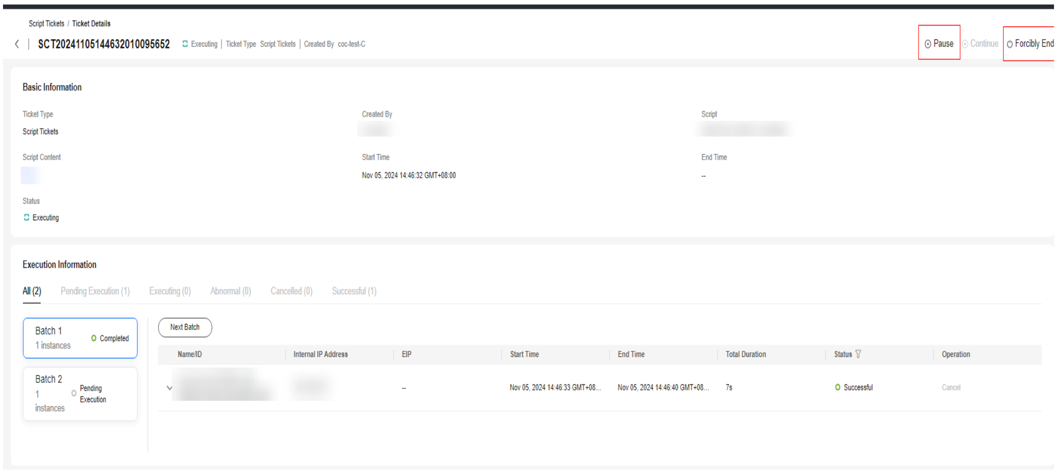
Batch 2 1 instances Pending Execution

Next Batch

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Nov 05, 2024 14:46:33 GMT+08...	Nov 05, 2024 14:46:40 GMT+08...	7s	Successful	Cancel

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

Figure 9-5 Pausing or closing a script ticket



Script Tickets / Ticket Details

SCT20241105144632010095652 Executing | Ticket Type Script Tickets | Created By coc-test-C

Pause Continue Forcibly End

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script Content: [redacted]

Start Time: Nov 05, 2024 14:46:32 GMT+08:00

End Time: --

Status: Executing

Execution Information

All (2) Pending Execution (1) Executing (0) Abnormal (0) Cancelled (0) Successful (1)

Batch 1 1 instances Completed

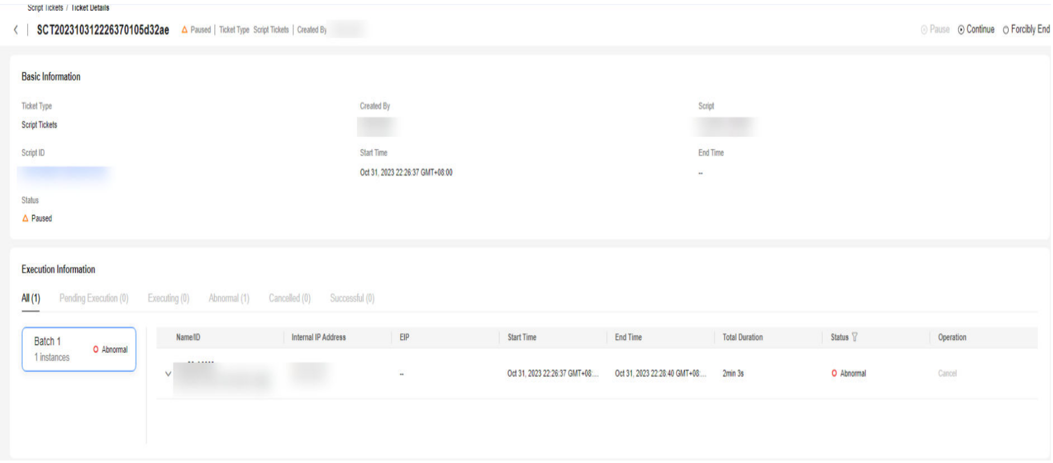
Batch 2 1 instances Pending Execution

Next Batch

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Nov 05, 2024 14:46:33 GMT+08...	Nov 05, 2024 14:46:40 GMT+08...	7s	Successful	Cancel

Step 7 Locate a script service ticket in the **Paused** status and click the script name. The **Ticket Details** page is displayed.

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



Script Tickets / Ticket Details

SCT202310312226370105d32ae △ Paused | Ticket Type Script Tickets | Created By [redacted]

Pause · Continue · Forcibly End

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script ID: [redacted]

Start Time: Oct 31, 2023 22:26:37 GMT+08:00

End Time: --

Status: △ Paused

Execution Information

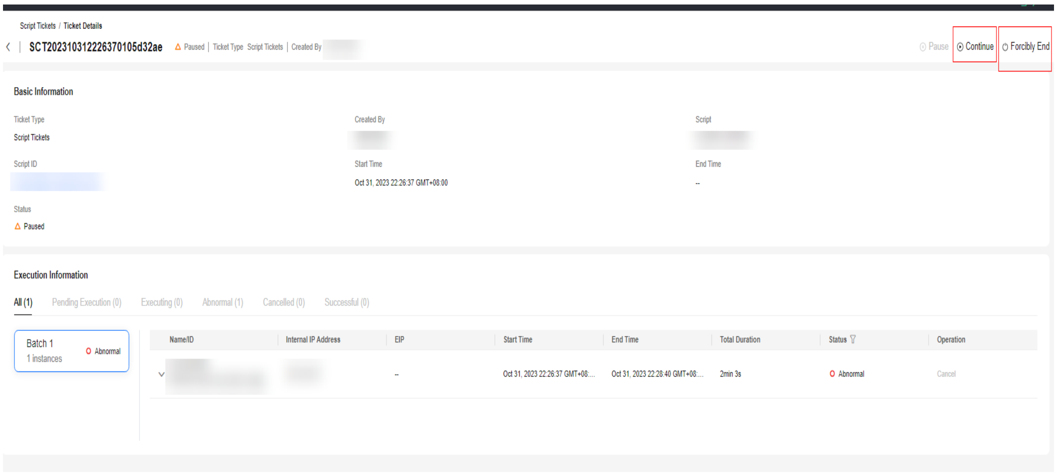
All (1) · Pending Execution (0) · Executing (0) · Abnormal (1) · Cancelled (0) · Successful (0)

Batch 1 · 1 instances · Abnormal

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Oct 31, 2023 22:26:37 GMT+08:...	Oct 31, 2023 22:28:40 GMT+08:...	2min 3s	Abnormal	Cancel

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

Figure 9-7 Continuing or closing a paused script ticket



Script Tickets / Ticket Details

SCT202310312226370105d32ae △ Paused | Ticket Type Script Tickets | Created By [redacted]

Pause · Continue · Forcibly End

Basic Information

Ticket Type: Script Tickets

Created By: [redacted]

Script: [redacted]

Script ID: [redacted]

Start Time: Oct 31, 2023 22:26:37 GMT+08:00

End Time: --

Status: △ Paused

Execution Information

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

Batch 1 · 1 instances · Abnormal

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]	[redacted]	--	Oct 31, 2023 22:26:37 GMT+08:...	Oct 31, 2023 22:28:40 GMT+08:...	2min 3s	Abnormal	Cancel

----End

9.1.2 Job Tickets

You can view and manage job tickets.

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

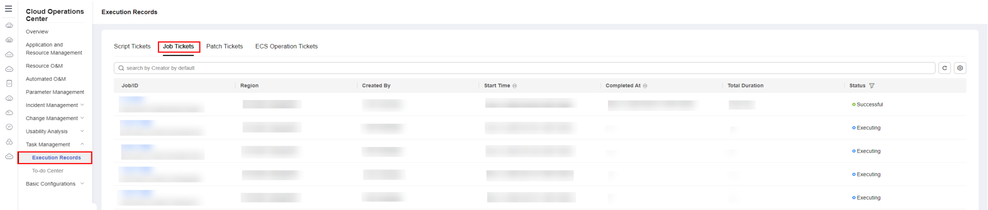
Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Task Management** > **Execution Records** and click the **Job Tickets** tab. You can clone a service ticket and

modify its tag.

- Cloning a ticket: Locate a service ticket, click **Clone** in the **Operation** column 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 the tag of a job ticket by following the instructions provided in **Managing Tags**.

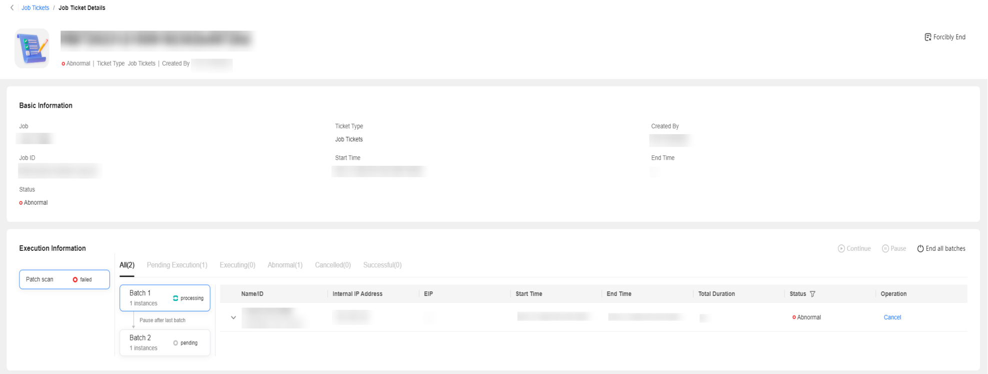
Figure 9-8 Job tickets



Job/ID	Region	Created By	Start Time	Completed At	Total Duration	Status
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Successful
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Executing
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Executing
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Executing
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Executing

Step 3 Locate a job ticket in the **Executing**, **Abnormal**, or **Paused** status and click the job ticket name. The **Ticket Details** page is displayed.

Figure 9-9 Job ticket details



Basic Information

Job

Ticket Type: Job Tickets

Created By

Job ID

Start Time

End Time

Status: Abnormal

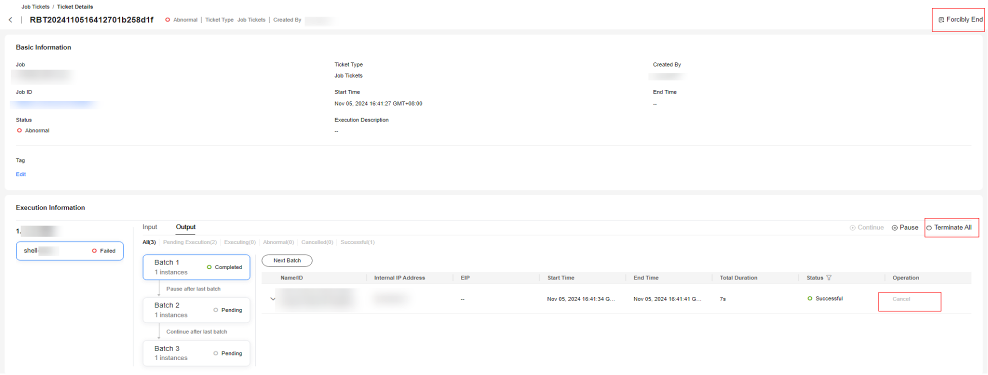
Execution Information

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Abnormal	Cancel

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

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

Figure 9-10 Managing a job ticket



Job Tickets / Ticket Details

RBT2024110516412701b258d1f ○ Abnormal | Ticket Type Job Tickets | Created By

Forcibly End

Basic Information

Job

Ticket Type
Job Tickets

Created By

Job ID

Start Time
Nov 05, 2024 16:41:27 GMT+08:00

End Time
--

Status
○ Abnormal

Execution Description
--

Tag
Edit

Execution Information

1.

shell- ○ Failed

Input Output

Continue Pause Terminate All

All(3) Pending Execution(2) Executing(0) Abnormal(0) Cancelled(0) Successful(1)

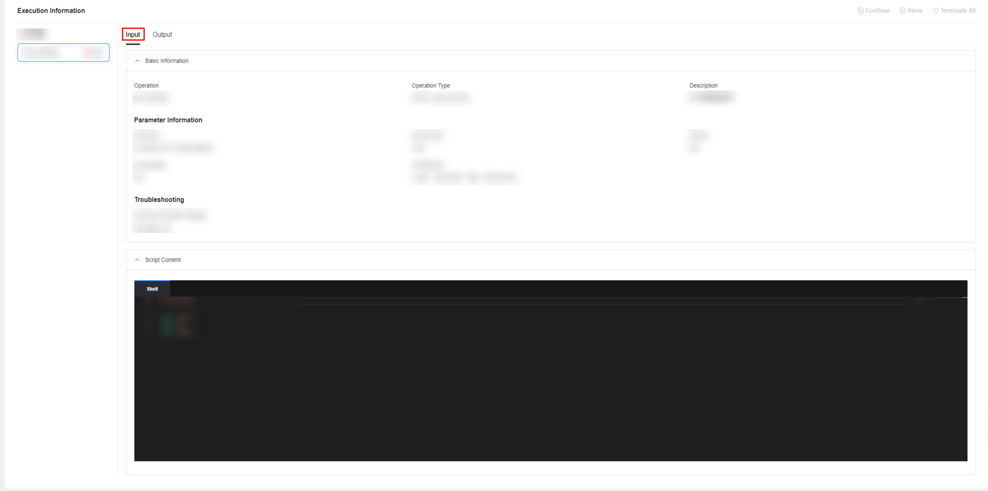
Batch 1 1 instances ○ Completed
Pause after last batch
Batch 2 1 instances ○ Pending
Continue after last batch
Batch 3 1 instances ○ Pending

Next Batch

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
		--	Nov 05, 2024 16:41:34 G...	Nov 05, 2024 16:41:41 G...	7s	○ Successful	Cancel

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

Figure 9-11 Viewing the job details



Execution Information

Continue Pause Terminate All

Input Output

Basic Information

Operation

Operation Type

Description

Parameter Information

Troubleshooting

Script Content

Shell

----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.

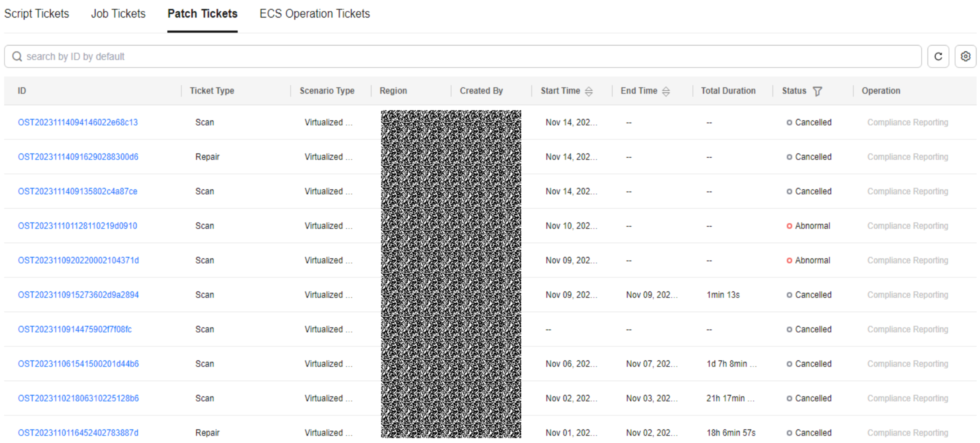
Procedure

Step 1 Log in to COC.

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

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

Figure 9-12 Patch ticket list



Script Tickets | Job Tickets | **Patch Tickets** | ECS Operation Tickets

search by ID by default

ID	Ticket Type	Scenario Type	Region	Created By	Start Time	End Time	Total Duration	Status	Operation
OST20231114094146022e68c13	Scan	Virtualized ...	[redacted]	[redacted]	Nov 14, 202...	--	--	○ Cancelled	Compliance Reporting
OST20231114091629028830d6	Repair	Virtualized ...	[redacted]	[redacted]	Nov 14, 202...	--	--	○ Cancelled	Compliance Reporting
OST2023111409135802c4a87ce	Scan	Virtualized ...	[redacted]	[redacted]	Nov 14, 202...	--	--	○ Cancelled	Compliance Reporting
OST20231110112811021 9d0910	Scan	Virtualized ...	[redacted]	[redacted]	Nov 10, 202...	--	--	○ Abnormal	Compliance Reporting
OST2023110920220002104371d	Scan	Virtualized ...	[redacted]	[redacted]	Nov 09, 202...	--	--	○ Abnormal	Compliance Reporting
OST2023110915273602d9a2894	Scan	Virtualized ...	[redacted]	[redacted]	Nov 09, 202...	Nov 09, 202...	1min 13s	○ Cancelled	Compliance Reporting
OST202311091447590 2f7f08fc	Scan	Virtualized ...	[redacted]	[redacted]	--	--	--	○ Cancelled	Compliance Reporting
OST2023110615415002 01d44b6	Scan	Virtualized ...	[redacted]	[redacted]	Nov 06, 202...	Nov 07, 202...	1d 7h 8min ...	○ Cancelled	Compliance Reporting
OST2023110218063102 25128b6	Scan	Virtualized ...	[redacted]	[redacted]	Nov 02, 202...	Nov 03, 202...	21h 17min ...	○ Cancelled	Compliance Reporting
OST2023110116452402783887d	Repair	Virtualized ...	[redacted]	[redacted]	Nov 01, 202...	Nov 02, 202...	18h 6min 57s	○ Cancelled	Compliance Reporting

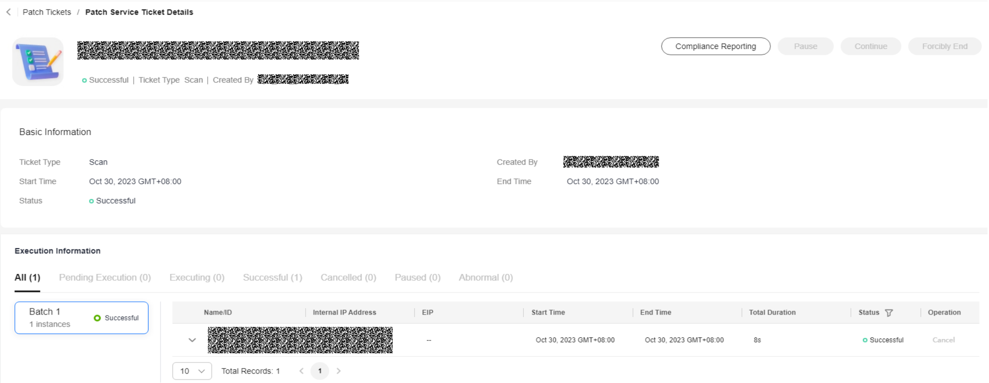
NOTE

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

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

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

Figure 9-13 Service ticket details



[redacted]

○ Successful | Ticket Type Scan | Created By [redacted]

Basic Information

Ticket Type	Scan	Created By	[redacted]
Start Time	Oct 30, 2023 GMT+08:00	End Time	Oct 30, 2023 GMT+08:00
Status	○ Successful		

Execution Information

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

Batch 1 ○ Successful
1 instances

Name/ID	Internal IP Address	EIP	Start Time	End Time	Total Duration	Status	Operation
[redacted]		--	Oct 30, 2023 GMT+08:00	Oct 30, 2023 GMT+08:00	8s	○ Successful	Cancel

10 Total Records: 1 < 1 >

----End

9.1.4 Resource Operation Tickets

You can view resource operation tickets.

Prerequisites

When you perform operations on ECS instances, RDS DB instances, BMS instances, and Flexus L instances, the system generates a service ticket.

Scenarios

View the ECS, RDS, BMS, and FlexusL service tickets on Cloud Operations Center.

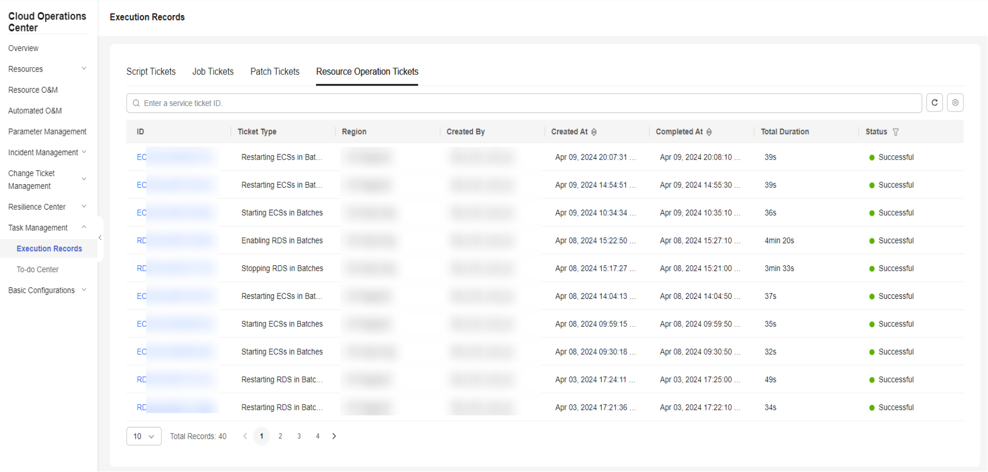
Procedure

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



Execution Records

Script Tickets | Job Tickets | Patch Tickets | Resource Operation Tickets

Enter a service ticket ID.

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

10 Total Records: 40 < 1 2 3 4 >

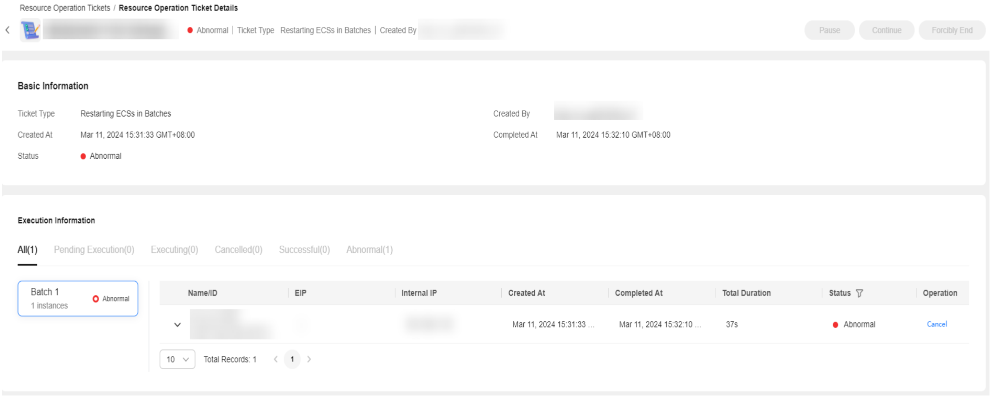
NOTE

Status: **Paused**, **Executing**, **Cancelled**, **Successful**, **Abnormal**.

Step 4 Click a resource operation ticket ID in the **ID** column to query 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



Resource Operation Tickets / Resource Operation Ticket Details

[redacted] ● Abnormal | Ticket Type Restarting ECSs in Batches | Created By [redacted]

Basic Information

Ticket Type Restarting ECSs in Batches

Created At Mar 11, 2024 15:31:33 GMT+08:00

Status ● Abnormal

Created By [redacted]

Completed At Mar 11, 2024 15:32:10 GMT+08:00

Execution Information

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

Batch 1 ○ Abnormal
1 instances

Name/ID	EIP	Internal IP	Created At	Completed At	Total Duration	Status	Operation
[redacted]	[redacted]	[redacted]	Mar 11, 2024 15:31:33 ...	Mar 11, 2024 15:32:10 ...	37s	● Abnormal	Cancel

10 Total Records: 1 < 1 >

----End

9.2 To-do Center

Overview

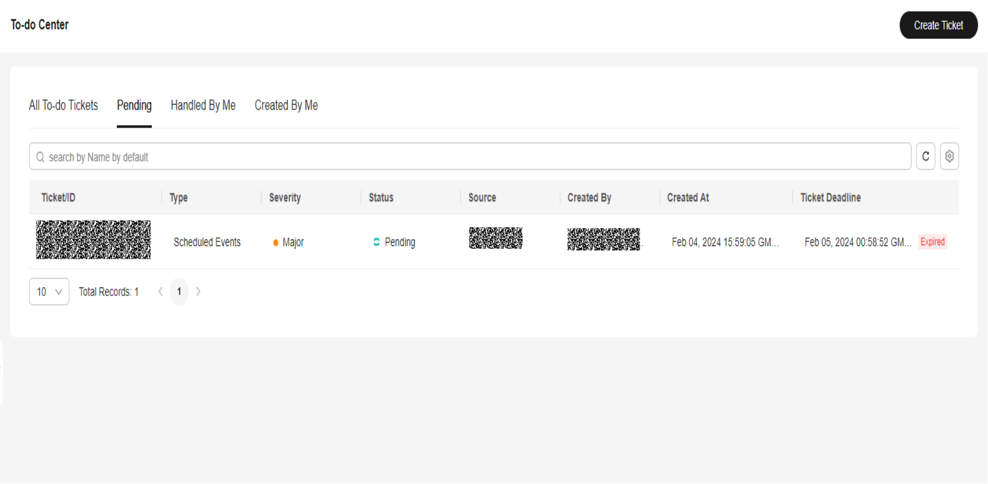
Main function of To-do Center: You can use a HUAWEI ID (primary SRE of the tenant) to create tasks for IAM users (sub-SREs of the tenant). For example, a company can create IAM accounts for different departments.

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 list



To-do Center

Create Ticket

All To-do Tickets | Pending | Handled By Me | Created By Me

search by Name by default

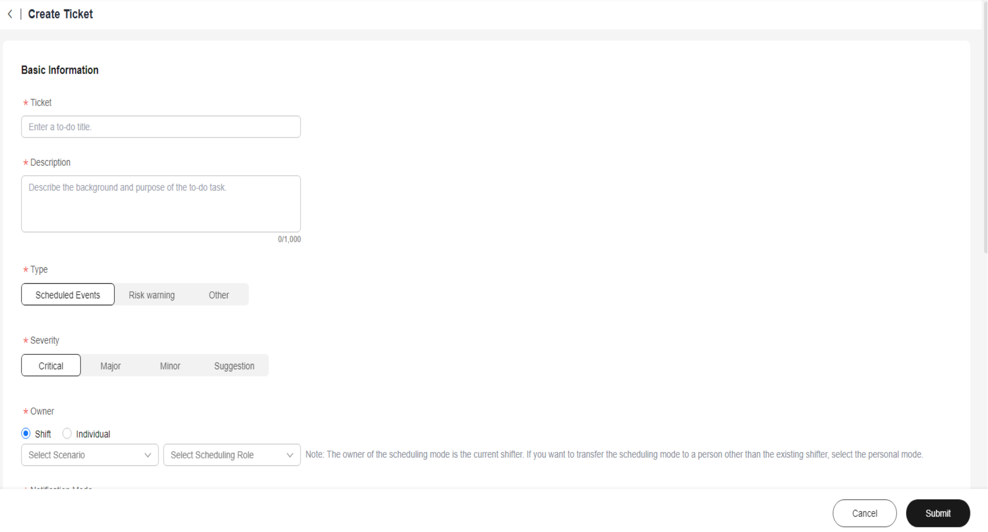
Ticket/ID	Type	Severity	Status	Source	Created By	Created At	Ticket Deadline
[redacted]	Scheduled Events	● Major	Pending	[redacted]	[redacted]	Feb 04, 2024 15:59:05 GM...	Feb 05, 2024 00:58:52 GM... Expired

10 Total Records: 1 ‹ 1 ›

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.

Figure 9-17 Creating a to-do ticket



< | Create Ticket

Basic Information

* Ticket

Enter a to-do title.

* Description

Describe the background and purpose of the to-do task.

0/1,000

* Type

Scheduled Events | Risk warning | Other

* Severity

Critical | Major | Minor | Suggestion

* Owner

● Shift ○ Individual

Select Scenario | Select Scheduling Role

Note: The owner of the scheduling mode is the current shifter. If you want to transfer the scheduling mode to a person other than the existing shifter, select the personal mode.

Cancel | Submit

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 Events ● Risk warning ● Other

Parameter	Description
Severity	Mandatory. The 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 ● Lark ● 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 a message indicating the creation succeeded 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.

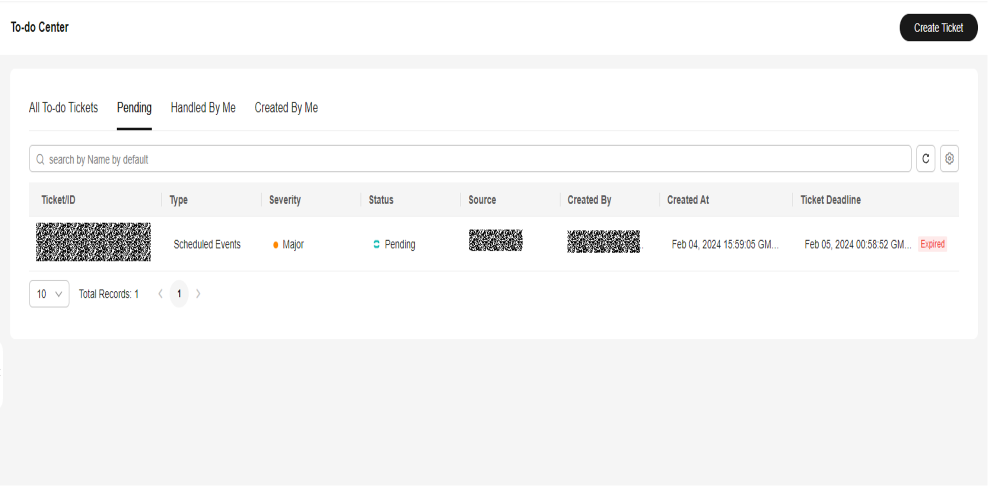
----End

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**.

Figure 9-18 Viewing the to-do center list



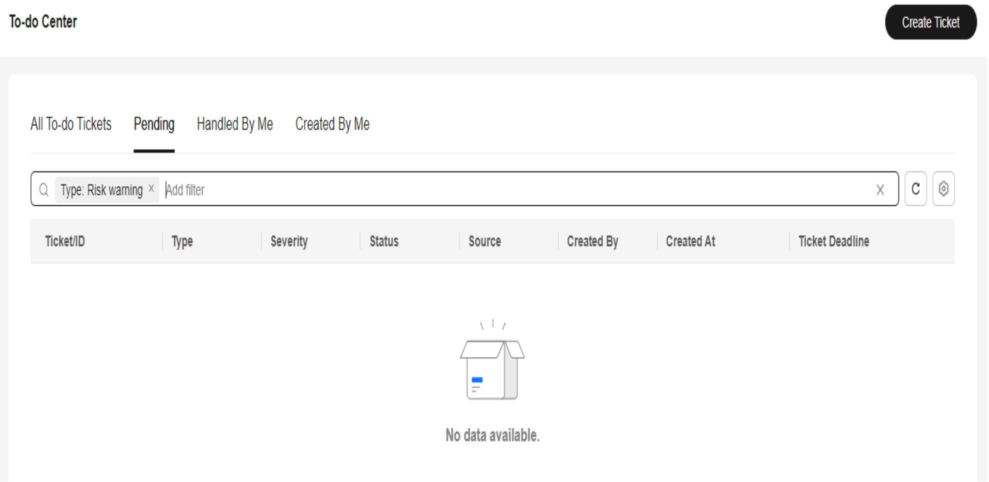
To-do Center

Ticket/ID	Type	Severity	Status	Source	Created By	Created At	Ticket Deadline
[redacted]	Scheduled Events	● Major	Pending	[redacted]	[redacted]	Feb 04, 2024 15:59:05 GM...	Feb 05, 2024 00:58:52 GM... Expired

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 refresh icon next to the search box to refresh the data and set the fields to be displayed in the list.

Figure 9-19 Adding search criteria



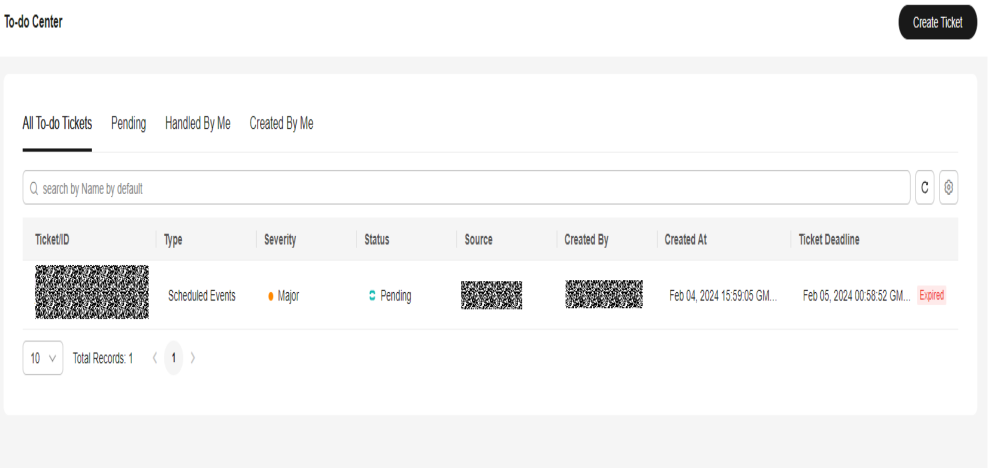
To-do Center

Ticket/ID	Type	Severity	Status	Source	Created By	Created At	Ticket Deadline

No data available.

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



To-do Center

Create Ticket

All To-do Tickets | Pending | Handled By Me | Created By Me

search by Name by default

Ticket/ID	Type	Severity	Status	Source	Created By	Created At	Ticket Deadline
[redacted]	Scheduled Events	● Major	Pending	[redacted]	[redacted]	Feb 04, 2024 15:59:05 GM...	Feb 05, 2024 00:58:52 GM... Expired

10 | Total Records: 1 | 1

NOTE

An user can only view the tickets related to itself on the **All To-do Tickets** tab page.

----End

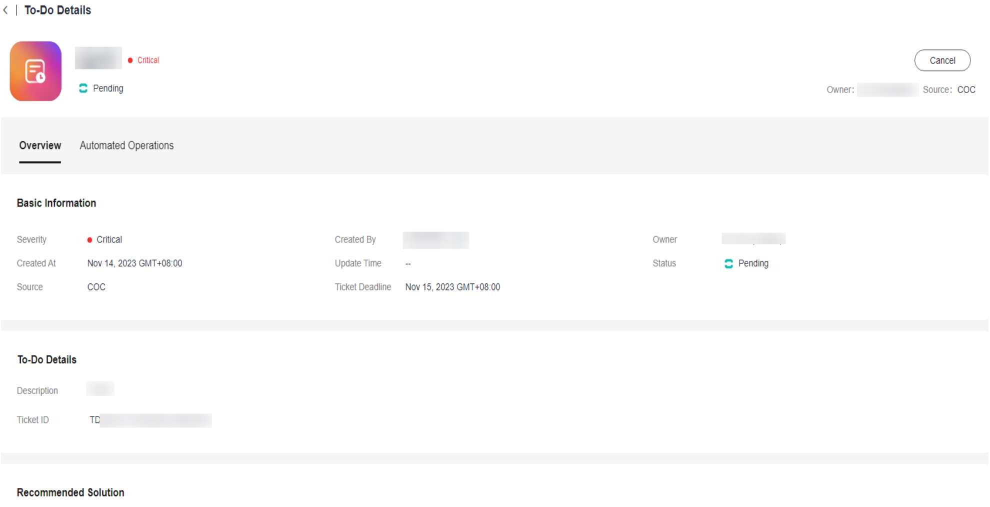
Viewing Pending Tickets

Step 1 Log in to **COC**.

Step 2 In the navigation pane on the left, choose **Task Management** > **To-do Center**.

Step 3 Click a to-do ticket name in the list to go to the ticket details page.

Figure 9-21 To-do ticket details



To-Do Details

[redacted] ● Critical

Pending

Cancel

Owner: [redacted] Source: COC

Overview | Automated Operations

Basic Information

Severity: ● Critical
Created At: Nov 14, 2023 GMT+08:00
Source: COC
Created By: [redacted]
Update Time: --
Ticket Deadline: Nov 15, 2023 GMT+08:00
Owner: [redacted]
Status: Pending

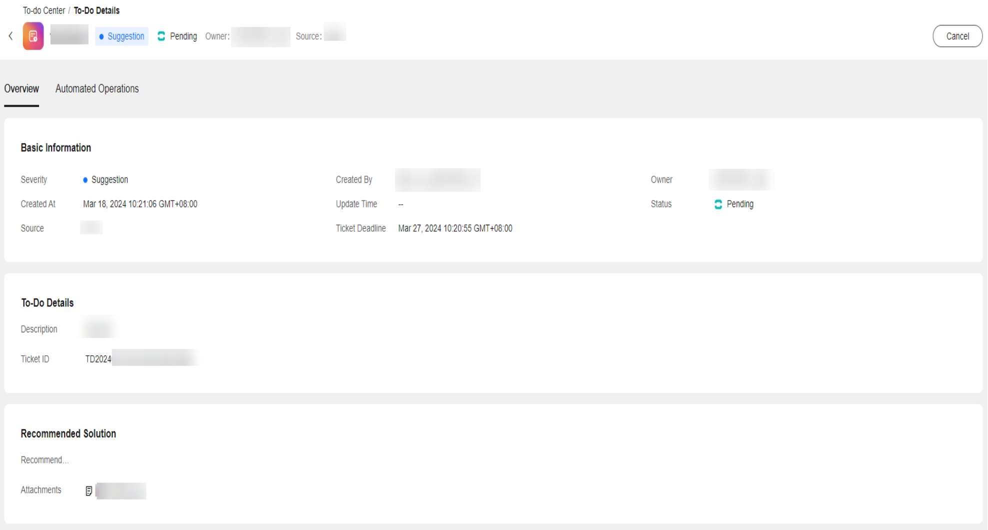
To-Do Details

Description: [redacted]
Ticket ID: TD[redacted]

Recommended Solution

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

Figure 9-22 Downloading an attachment



To-do Center / **To-Do Details**

[redacted] ● Suggestion Pending Owner: [redacted] Source: [redacted]

Basic Information

Severity: ● Suggestion
Created At: Mar 18, 2024 10:21:06 GMT+08:00
Source: [redacted]
Created By: [redacted]
Update Time: --
Ticket Deadline: Mar 27, 2024 10:20:55 GMT+08:00
Owner: [redacted]
Status: Pending

To-Do Details

Description: [redacted]
Ticket ID: TD2024[redacted]

Recommended Solution

Recommend...
Attachments: [redacted]

NOTE

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

----End

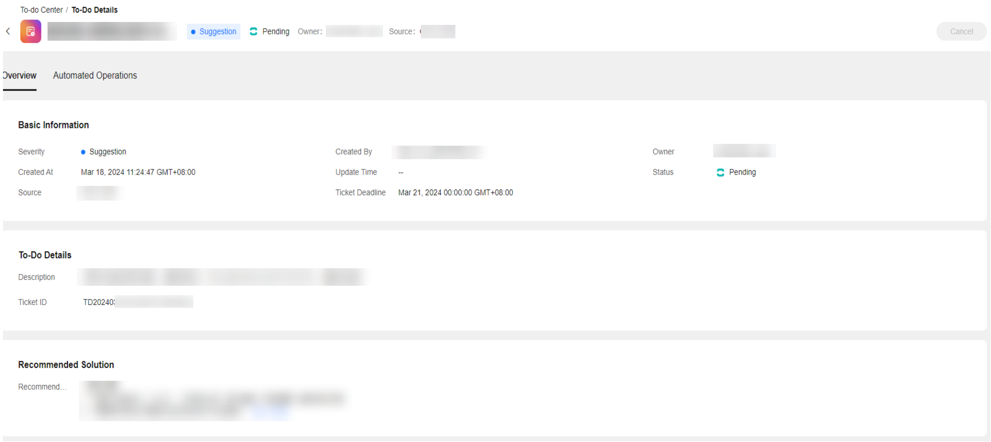
Handling To-do Tickets

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Task Management** > **To-do Center**. 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



To-do Center / **To-Do Details**

[redacted] ● Suggestion Pending Owner: [redacted] Source: [redacted]

Basic Information

Severity: ● Suggestion
Created At: Mar 18, 2024 11:24:47 GMT+08:00
Source: [redacted]
Created By: [redacted]
Update Time: --
Ticket Deadline: Mar 21, 2024 00:00:00 GMT+08:00
Owner: [redacted]
Status: Pending

To-Do Details

Description: [redacted]
Ticket ID: TD20240[redacted]

Recommended Solution

Recommend... [redacted]

NOTE

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

----End

Canceling a To-Do Ticket

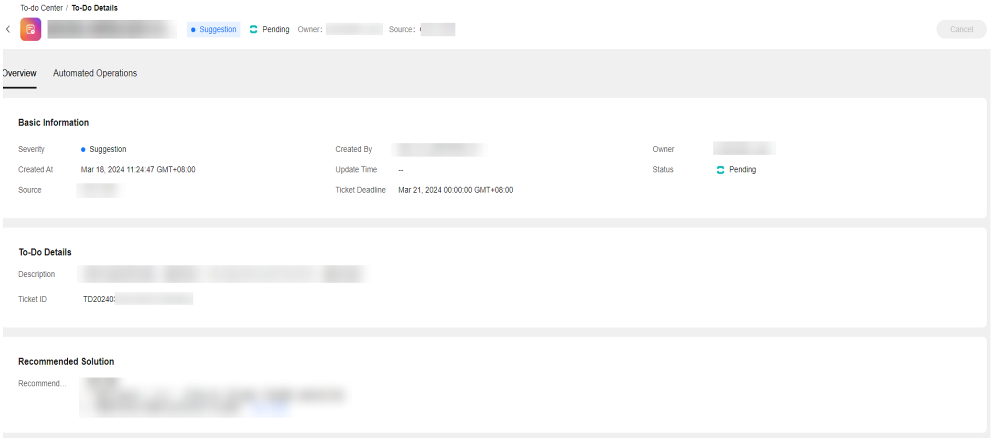
Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Task Management** > **To-do Center**. Click the **Created by Me** tab.

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 and enter the cancellation reason.

Figure 9-24 Canceling a to-do task



To-do Center / To-Do Details

[redacted] ● Suggestion Pending Owner: [redacted] Source: [redacted]

Cancel

Overview Automated Operations

Basic Information

Severity ● Suggestion

Created At Mar 18, 2024 11:24:47 GMT+08:00

Source [redacted]

Created By [redacted]

Update Time --

Ticket Deadline Mar 21, 2024 00:00:00 GMT+08:00

Owner [redacted]

Status Pending

To-Do Details

Description [redacted]

Ticket ID TD20240[redacted]

Recommended Solution

Recommend... [redacted]

NOTE

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

----End

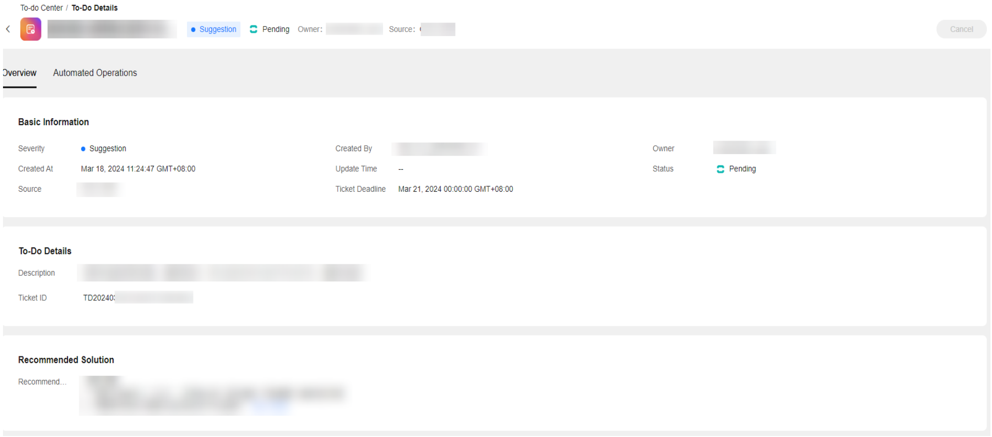
Closing a To-do Ticket

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Task Management** > **To-do Center**. Click the **Handled by Me** tab.

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



Owner:

Source:

Basic Information

Severity	● Suggestion	Created By		Owner	
Created At	Mar 18, 2024 11:24:47 GMT+08:00	Update Time	--	Status	Pending
Source		Ticket Deadline	Mar 21, 2024 00:00:00 GMT+08:00		

To-Do Details

Description

Ticket ID TD20240

Recommended Solution

Recommend...

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

You can centrally O&M engineer personnel on COC using this feature. 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 personnel management page, you can manually select users you want to edit, delete, and configure subscription information for.
- If you edit the information of an existing user, the system background creates a corresponding subscription mode after you specify a communication method, such as mobile number, email address, WeCom, DingTalk, or Lark.
- 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

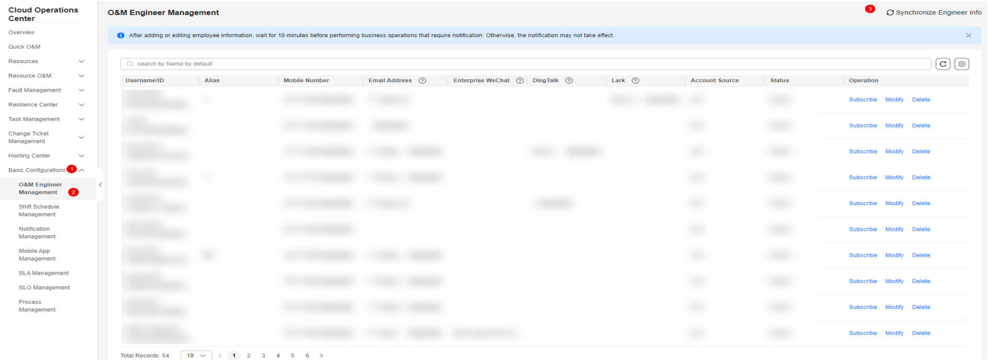
This section describes how to use the **O&M Engineer Management** module.

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

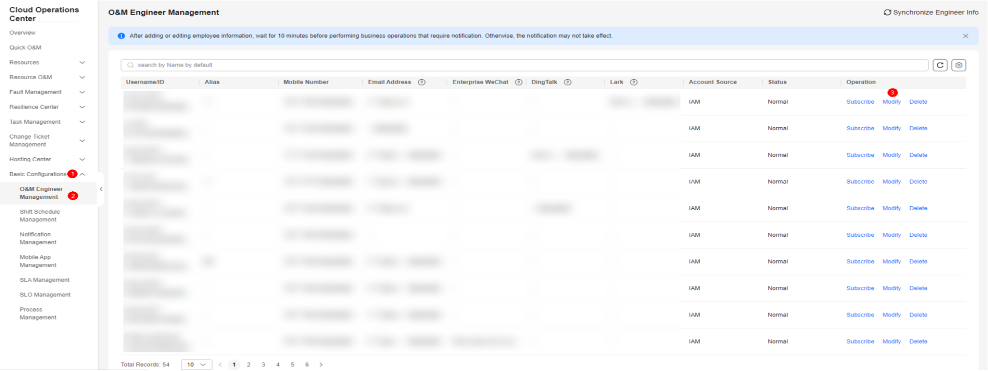
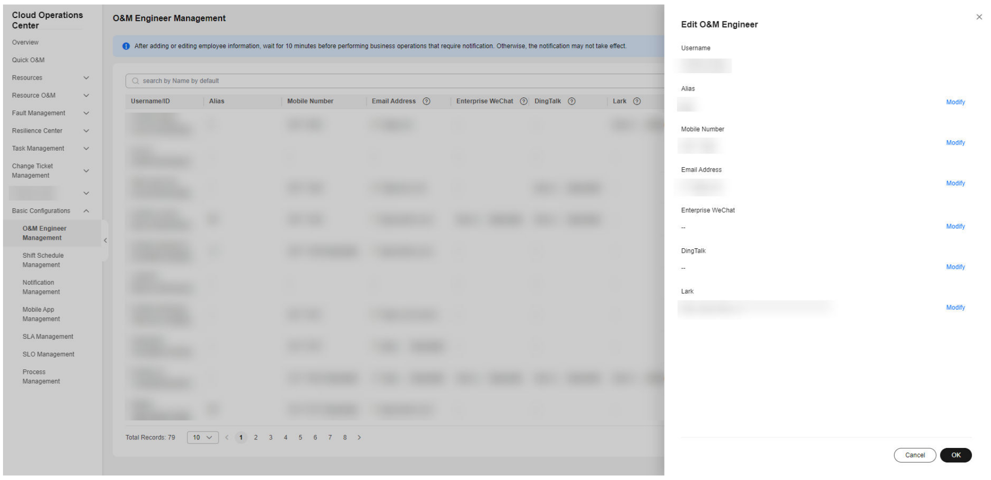


Figure 10-3 Modifying details



- **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.

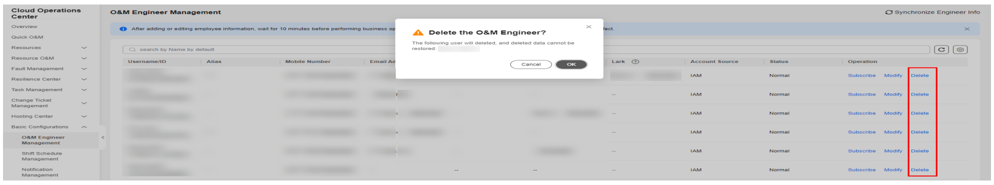
----End

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



Delete the O&M Engineer?

The following user will deleted, and deleted data cannot be restored:

After adding or editing employee information, wait for 10 minutes before performing business op... ...fect.

----End

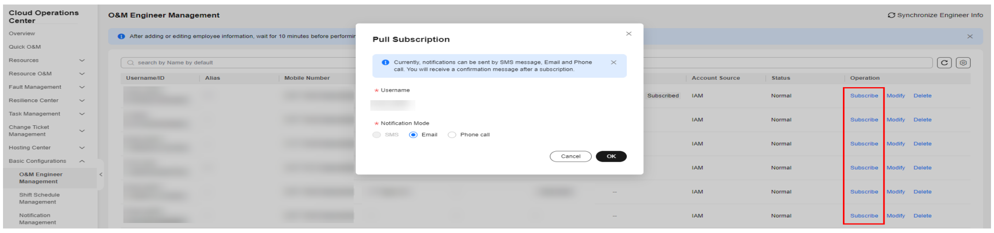
Subscribing to a User

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



Pull Subscription

Currently, notifications can be sent by SMS message, Email and Phone call. You will receive a confirmation message after a subscription.

* Username

* Notification Mode

○ SMS ● Email ○ Phone call

After adding or editing employee information, wait for 10 minutes before performin...

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 **Subscription** 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

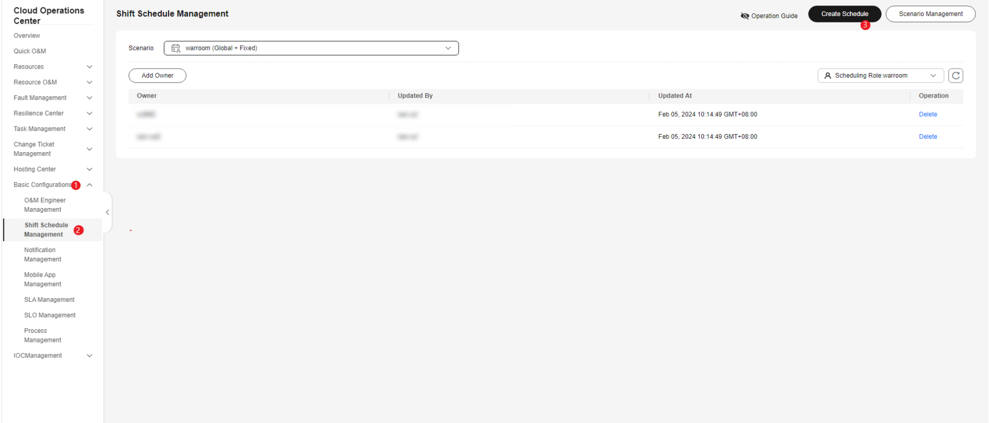
A scheduling scenario role is the minimum unit for setting a schedule. Multiple roles can be created in a scheduling scenario, and each role can be attached to multiple O&M engineers.

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



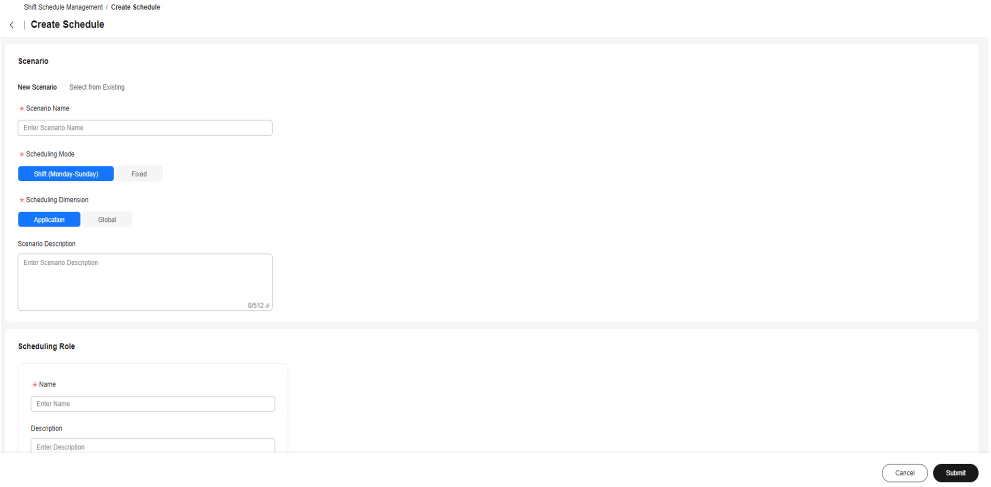
Scenario: warroom (Global + Fixed)

Scheduling Role:warroom

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Feb 05, 2024 10:14:49 GMT+08:00	Delete
[redacted]	[redacted]	Feb 05, 2024 10:14:49 GMT+08:00	Delete

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 scheduling 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 a 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**

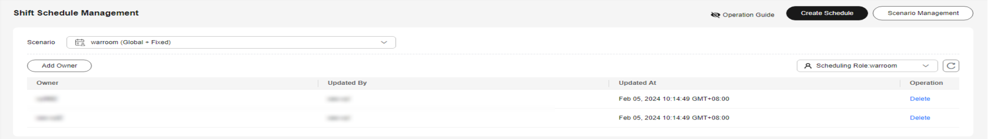
Global Schedule of Fixed Shifts

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



Shift Schedule Management

Scenario: warroom (Global + Fixed)

Scheduling Role:warroom

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Feb 05, 2024 10:14:49 GMT+08:00	Delete
[redacted]	[redacted]	Feb 05, 2024 10:14:49 GMT+08:00	Delete

----End

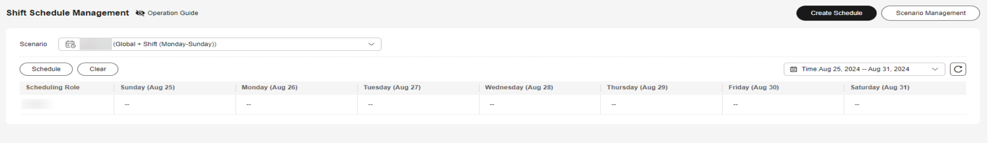
Global Schedule of Rotating Shifts

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



Shift Schedule Management

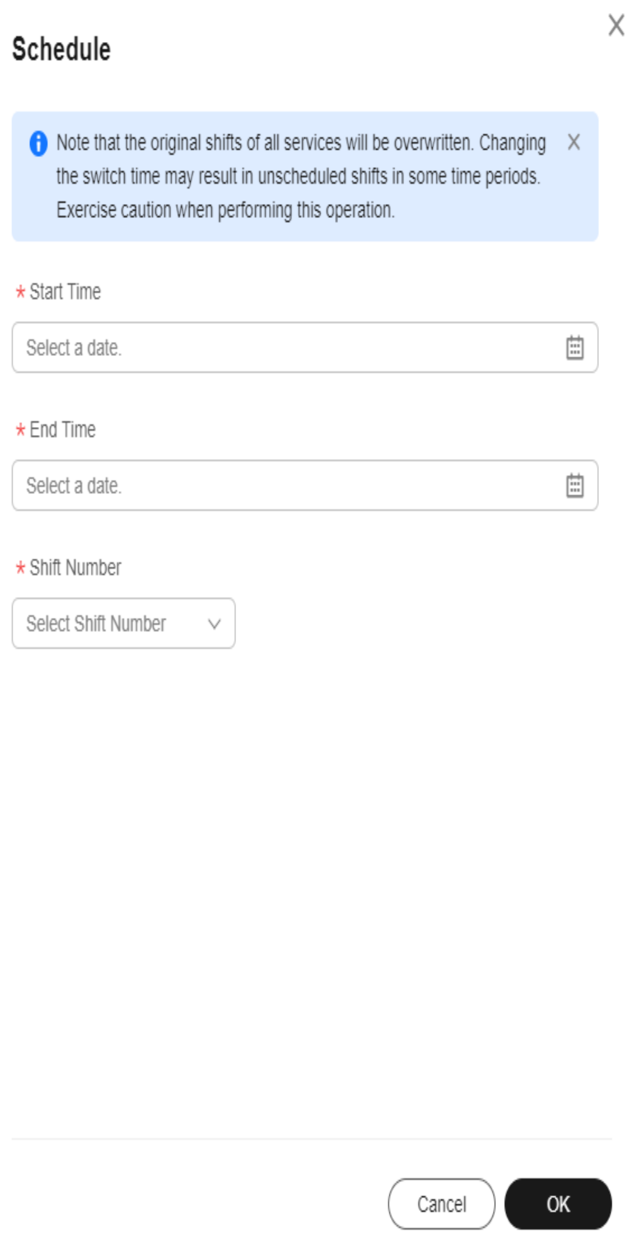
Scenario: [redacted] (Global + Shift (Monday-Sunday))

Time:Aug 25, 2024 -- Aug 31, 2024

Scheduling Role	Sunday (Aug 25)	Monday (Aug 26)	Tuesday (Aug 27)	Wednesday (Aug 28)	Thursday (Aug 29)	Friday (Aug 30)	Saturday (Aug 31)
[redacted]	--	--	--	--	--	--	--

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

Figure 10-10 Adding O&M engineers



Schedule

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

* Start Time

Select a date.

* End Time

Select a date.

* Shift Number

Select Shift Number

- **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

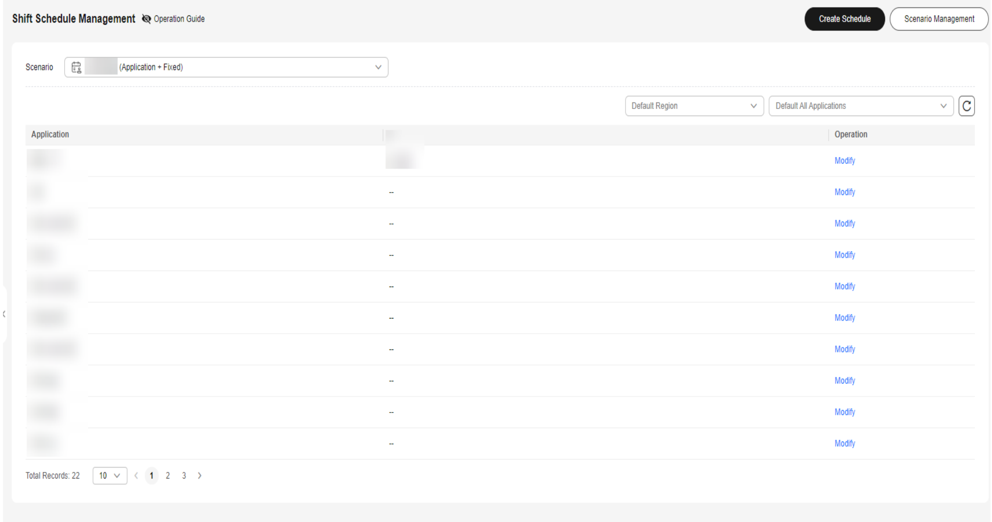
Application scenario: These schedules are applied to specific applications. O&M engineers are fixed in a day.

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

Step 1 Log in to **COC**.

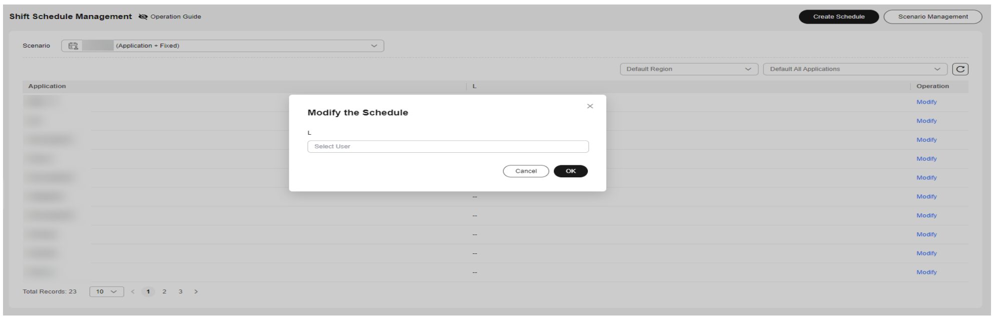
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Shift Schedule Management**. On the displayed page, select a created scenario (**Application + Fixed** is displayed next to the scenario name), region, and application.

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

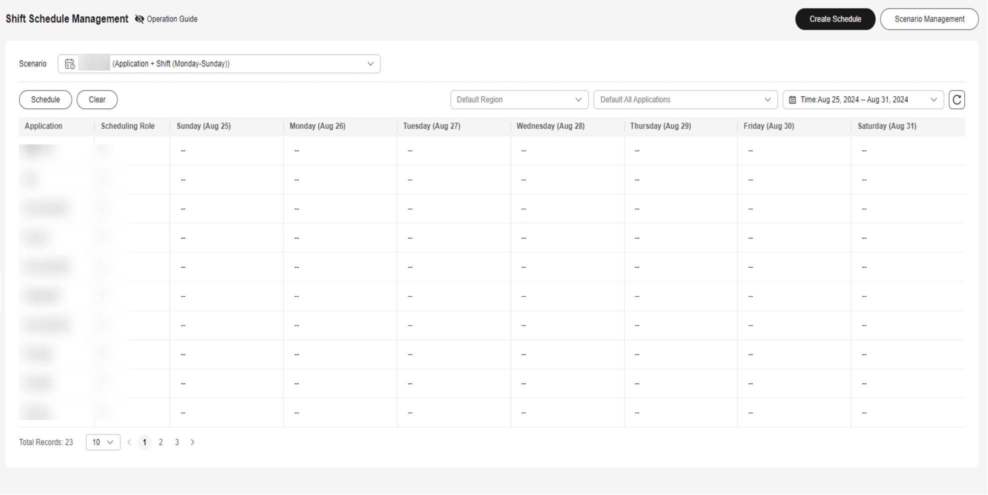
Application scenario: These schedules are applied to specific applications.

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



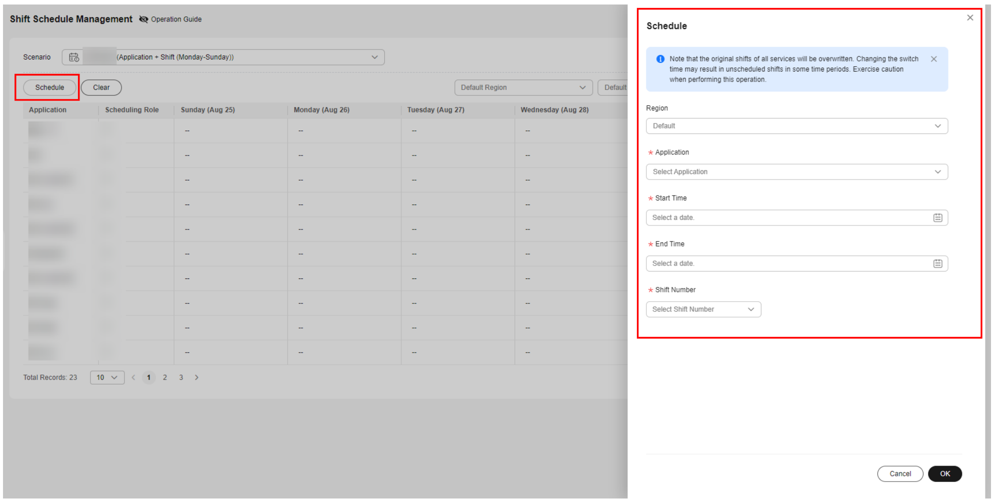
Application	Scheduling Role	Sunday (Aug 25)	Monday (Aug 26)	Tuesday (Aug 27)	Wednesday (Aug 28)	Thursday (Aug 29)	Friday (Aug 30)	Saturday (Aug 31)
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--
[illegible]	[illegible]	--	--	--	--	--	--	--

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



Schedule

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

Region: Default

* Application: Select Application

* Start Time: Select a date.

* End Time: Select a date.

* Shift Number: Select Shift Number

- **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

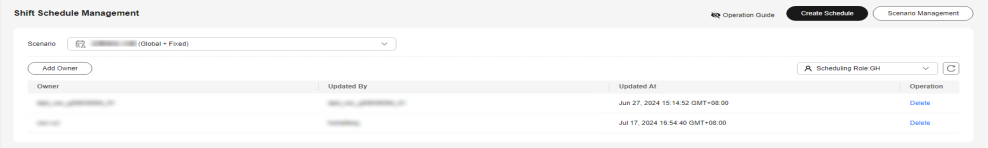
When the engineers in a schedule change, you can modify or delete the information about the changes. The method of changing the engineers varies according to the scenario.

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



Scenario: [redacted] (Global + Fixed)

Scheduling Role:GH

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Jun 27, 2024 15:14:52 GMT+08:00	Delete
[redacted]	[redacted]	Jul 17, 2024 16:54:40 GMT+08:00	Delete

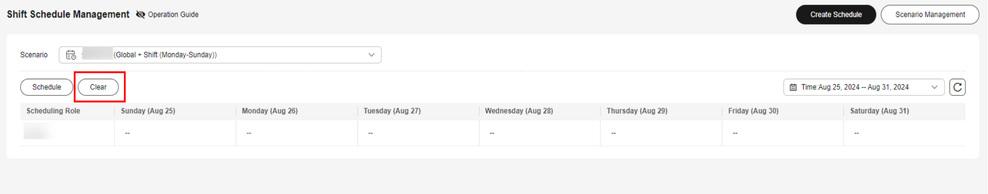
----End

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



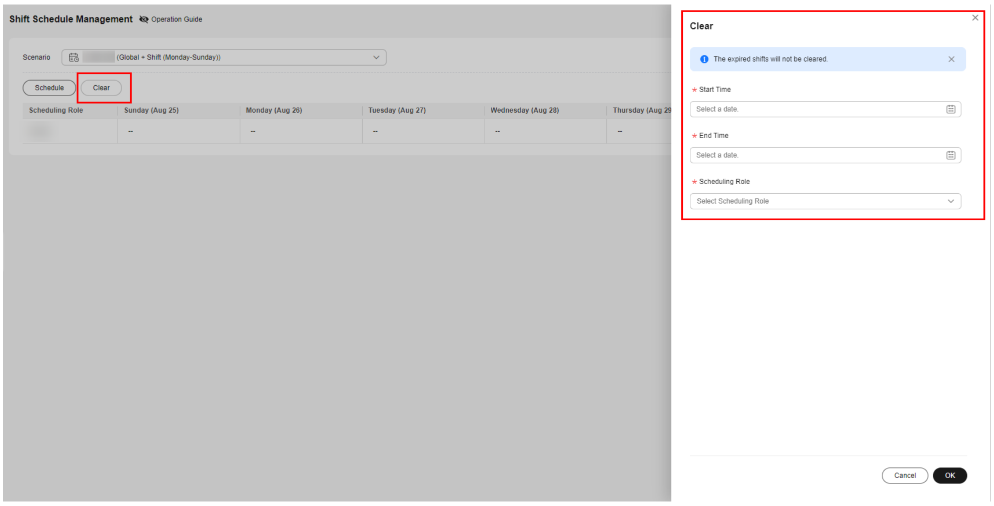
Scenario: [redacted] (Global + Shift (Monday-Sunday))

Time:Aug 25, 2024 -- Aug 31, 2024

Scheduling Role	Sunday (Aug 25)	Monday (Aug 26)	Tuesday (Aug 27)	Wednesday (Aug 28)	Thursday (Aug 29)	Friday (Aug 30)	Saturday (Aug 31)
[redacted]	--	--	--	--	--	--	--

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



Shift Schedule Management Operation Guide

Scenario [redacted] (Global + Shift (Monday-Sunday))

Schedule Clear

Scheduling Role	Sunday (Aug 25)	Monday (Aug 26)	Tuesday (Aug 27)	Wednesday (Aug 28)	Thursday (Aug 29
[redacted]	--	--	--	--	--

Clear

The expired shifts will not be cleared.

* Start Time

Select a date.

* End Time

Select a date.

* Scheduling Role

Select Scheduling Role

Cancel OK

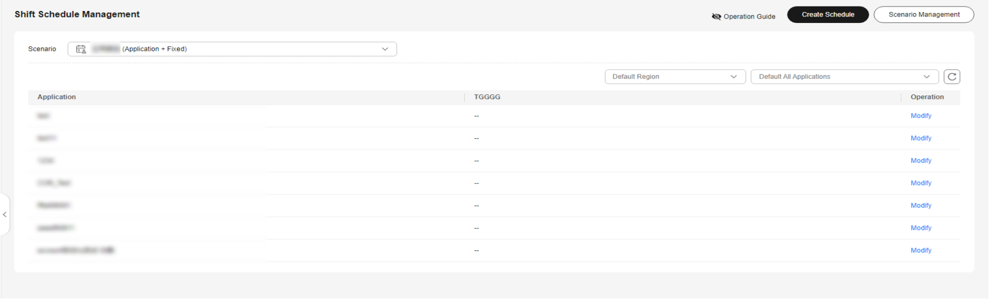
----End

Application-specific Schedule of Fixed Shifts

Step 1 Log in to 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



Shift Schedule Management Operation Guide Create Schedule Scenario Management

Scenario [redacted] (Application + Fixed)

Default Region Default All Applications

Application	TGGGG	Operation
[redacted]	--	Modify
[redacted]	--	Modify
[redacted]	--	Modify
[redacted]	--	Modify
[redacted]	--	Modify
[redacted]	--	Modify
[redacted]	--	Modify

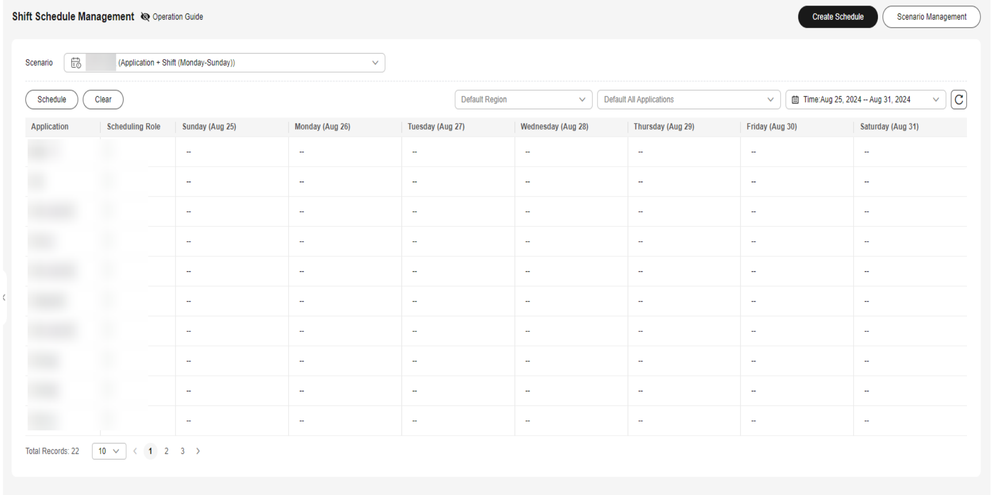
----End

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



Shift Schedule Management · Operation Guide · Create Schedule · Scenario Management

Scenario: [redacted] (Application + Shift (Monday-Sunday))

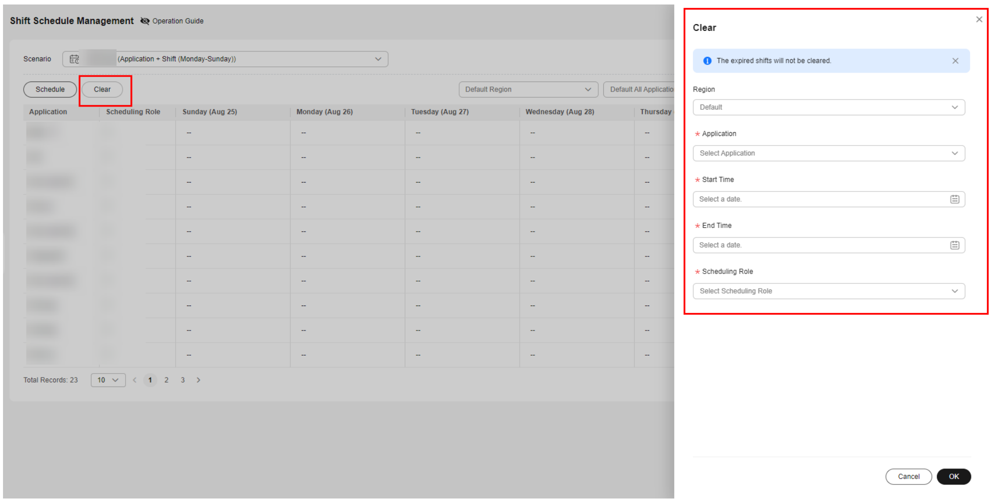
Schedule · Clear · Default Region · Default All Applications · Time:Aug 25, 2024 – Aug 31, 2024

Application	Scheduling Role	Sunday (Aug 25)	Monday (Aug 26)	Tuesday (Aug 27)	Wednesday (Aug 28)	Thursday (Aug 29)	Friday (Aug 30)	Saturday (Aug 31)
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--
[redacted]	[redacted]	--	--	--	--	--	--	--

Total Records: 22 · 10 · 1 2 3

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



Clear

The expired shifts will not be cleared.

Region: Default

* Application: Select Application

* Start Time: Select a date.

* End Time: Select a date.

* Scheduling Role: Select Scheduling Role

Cancel · OK

----End

10.2.2 Managing Scheduling Scenarios

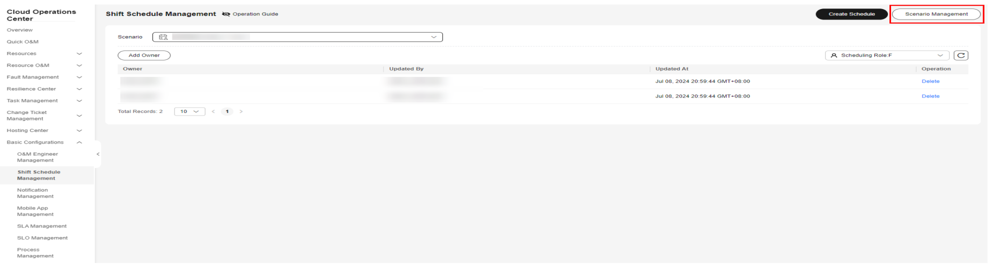
This topic describes how to manage scheduling scenarios and scheduling roles.

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



Scenario [redacted]

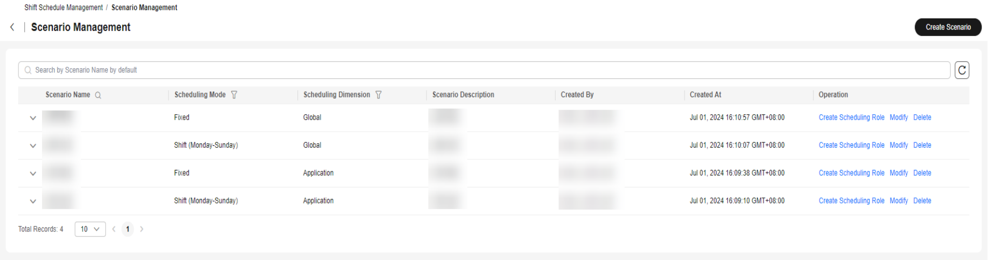
Scheduling Role:F

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete

Total Records: 2 10 < 1 >

Step 3 Click **Create Scenario**.

Figure 10-22 Scenario list

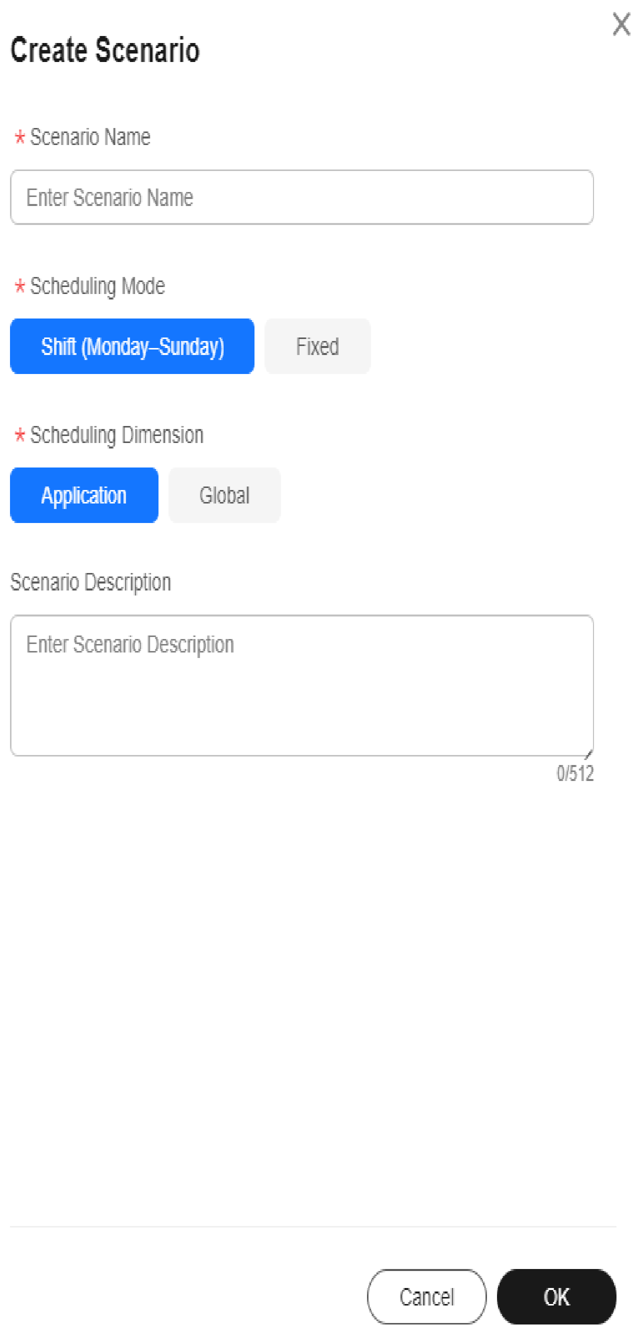

Shift Schedule Management / Scenario Management
Scenario Management
Create Scenario
Search by Scenario Name by default

Scenario Name	Scheduling Mode	Scheduling Dimension	Scenario Description	Created By	Created At	Operation
[redacted]	Fixed	Global	[redacted]	[redacted]	Jul 01, 2024 16:10:57 GMT+08:00	Create Scheduling Role Modify Delete
[redacted]	Shift (Monday-Sunday)	Global	[redacted]	[redacted]	Jul 01, 2024 16:10:07 GMT+08:00	Create Scheduling Role Modify Delete
[redacted]	Fixed	Application	[redacted]	[redacted]	Jul 01, 2024 16:09:38 GMT+08:00	Create Scheduling Role Modify Delete
[redacted]	Shift (Monday-Sunday)	Application	[redacted]	[redacted]	Jul 01, 2024 16:09:10 GMT+08:00	Create Scheduling Role Modify Delete

Total Records: 4 10 < 1 >

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

Figure 10-23 Creating a scheduling scenario



Create Scenario

* Scenario Name

Enter Scenario Name

* Scheduling Mode

Shift (Monday–Sunday) | Fixed

* Scheduling Dimension

Application | Global

Scenario Description

Enter Scenario Description

0/512

- **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.

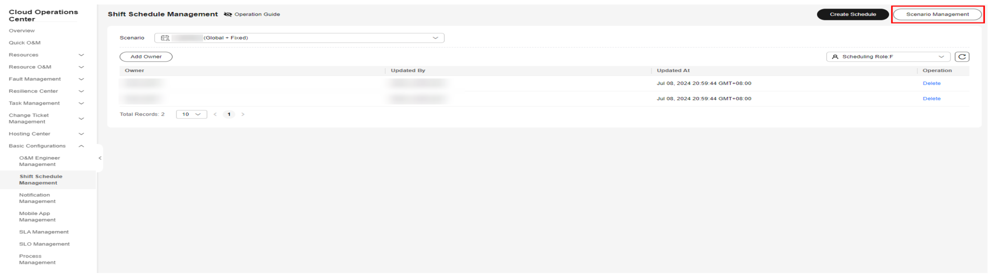
----End

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



Scenario [redacted] (Global + Fixed)

Scheduling Role:F

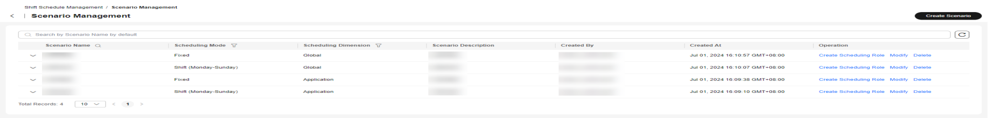
Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete

Total Records: 2 10 < 1 >

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


Shift Schedule Management / Scenario Management
Scenario Management
Create Scenario
Search by Scenario Name by default

	Scenario Name	Scheduling Mode	Scheduling Dimension	Scenario Description	Created By	Created At	Operation
⌄	[redacted]	Fixed	Global	[redacted]	[redacted]	Jul 01, 2024 16:10:57 GMT+08:00	Create Scheduling Role Modify Delete
⌄	[redacted]	Shift (Monday-Sunday)	Global	[redacted]	[redacted]	Jul 01, 2024 16:10:07 GMT+08:00	Create Scheduling Role Modify Delete
⌄	[redacted]	Fixed	Application	[redacted]	[redacted]	Jul 01, 2024 16:09:38 GMT+08:00	Create Scheduling Role Modify Delete
⌄	[redacted]	Shift (Monday-Sunday)	Application	[redacted]	[redacted]	Jul 01, 2024 16:09:10 GMT+08:00	Create Scheduling Role Modify Delete

Total Records: 4 10 < 1 >

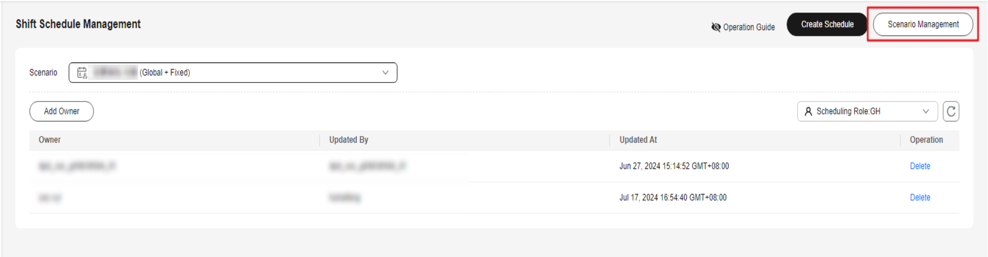
----End

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



Scenario [redacted] (Global + Fixed)

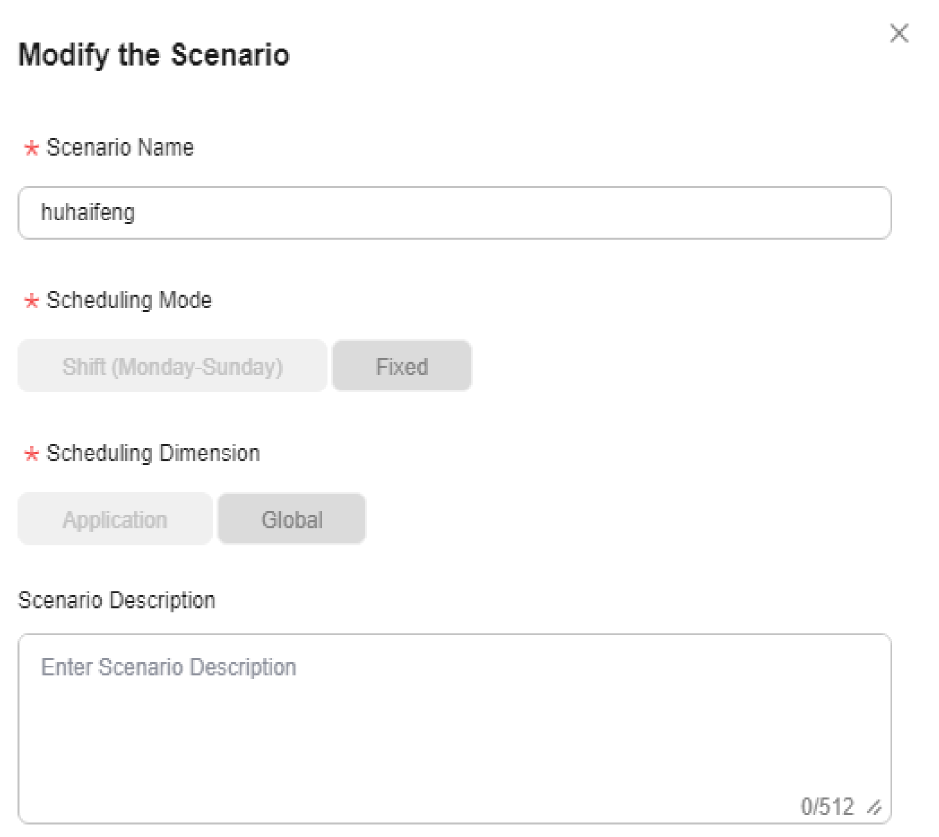
Scheduling Role:GH

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Jun 27, 2024 15:14:52 GMT+08:00	Delete
[redacted]	[redacted]	Jul 17, 2024 16:54:40 GMT+08:00	Delete

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



Modify the Scenario

* Scenario Name

huhaifeng

* Scheduling Mode

Shift (Monday-Sunday) | Fixed

* Scheduling Dimension

Application | Global

Scenario Description

Enter Scenario Description

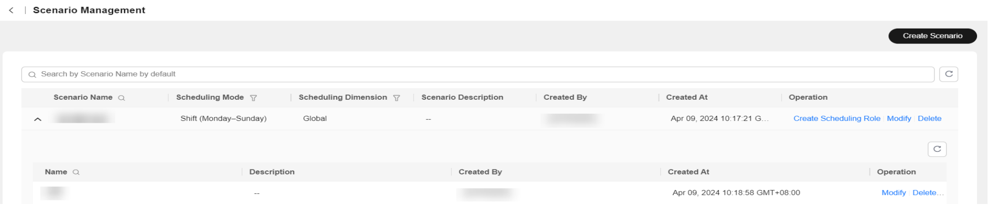
0/512

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



Scenario Management

Create Scenario

Search by Scenario Name by default

Scenario Name	Scheduling Mode	Scheduling Dimension	Scenario Description	Created By	Created At	Operation
[redacted]	Shift (Monday–Sunday)	Global	--	[redacted]	Apr 09, 2024 10:17:21 G...	Create Scheduling Role Modify Delete

Name	Description	Created By	Created At	Operation
[redacted]	--	[redacted]	Apr 09, 2024 10:18:58 GMT+08:00	Modify Delete...

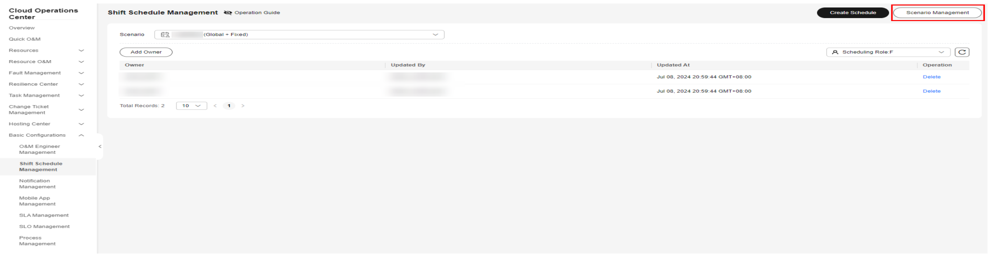
----End

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



Scenario [redacted] (Global + Fixed)

Owner	Updated By	Updated At	Operation
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete
[redacted]	[redacted]	Jul 08, 2024 20:59:44 GMT+08:00	Delete

Total Records: 2 10 < 1 >

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

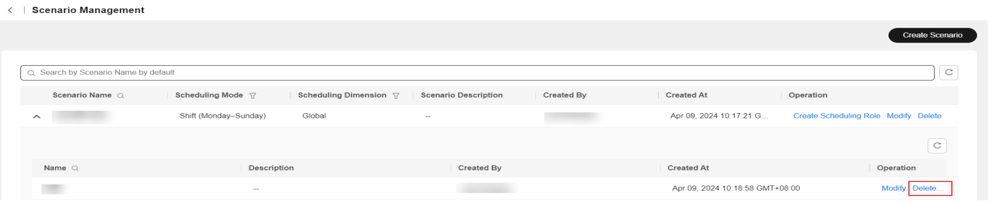
Step 4 In the displayed dialog box, click **OK**.

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



Scenario Name	Scheduling Mode	Scheduling Dimension	Scenario Description	Created By	Created At	Operation
[redacted]	Shift (Monday–Sunday)	Global	--	[redacted]	Apr 09, 2024 10:17:21 G...	Create Scheduling Role Modify Delete

Name	Description	Created By	Created At	Operation
[redacted]	--	[redacted]	Apr 09, 2024 10:18:58 GMT+08:00	Modify Delete...

----End

10.3 Notification Management

Notification Management creates notification rules for users. Notification rules include incident notifications, change notifications, and issue notifications.

When an incident ticket, issue ticket, or change ticket is generated, the notification rule and the information about the incident, issue, or change are matched, then the recipients, the notification content, and notification method are obtained through parsing, and finally the notification messages are sent.

The incident and change notification templates are preset in the system. You can select a notification template as needed.

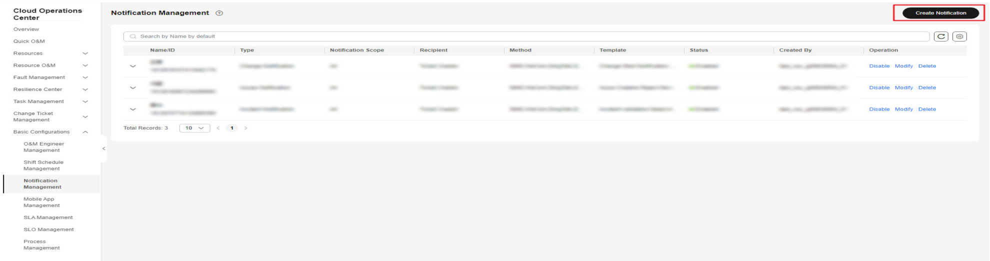
Creating a Notification Rule

Create a notification rule. After an incident, issue, or change ticket matches the corresponding rule, a notification is automatically sent.

Step 1 Log in to **COC**.

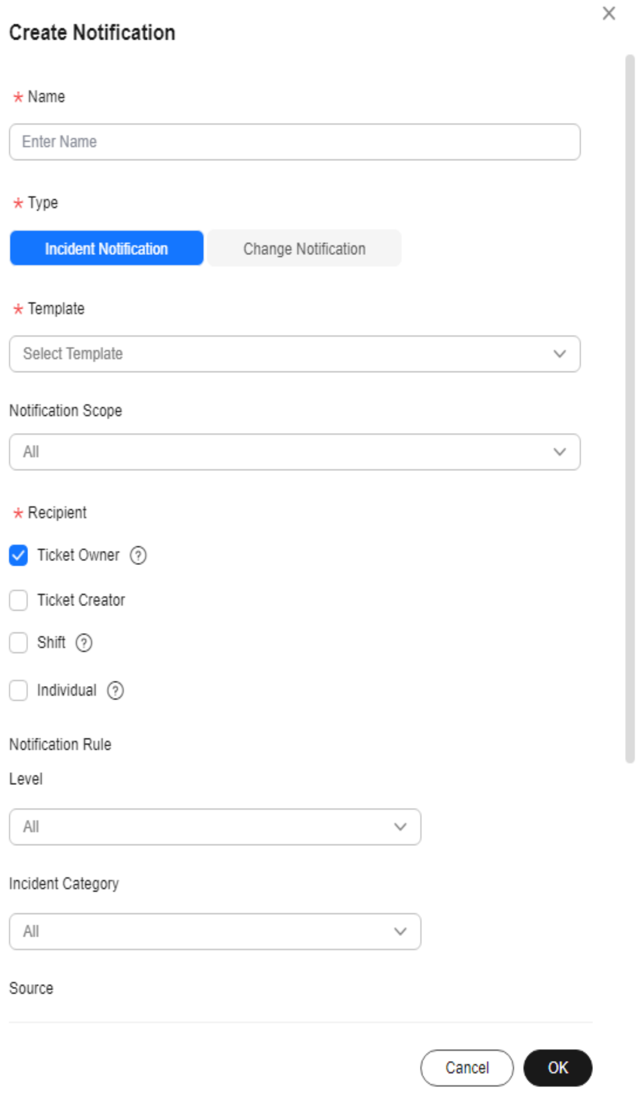
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Notification Management**. On the displayed page, click **Create Notification**.

Figure 10-31 Clicking Create Notification



Step 3 In the displayed dialog box, enter the notification configuration information and click **OK**. **Table 1** described the required parameters.

Figure 10-32 Setting the notification parameters



Create Notification

* Name

Enter Name

* Type

Incident Notification | Change Notification

* Template

Select Template

Notification Scope

All

* Recipient

☑ Ticket Owner

□ Ticket Creator

□ Shift

□ Individual

Notification Rule

Level

All

Incident Category

All

Source

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	Including incident notifications, change notifications, and issue notifications.

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	No	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	No	Checkbox	Category of an incident ticket. Multiple values are available.

Parameter	Mandatory	Radio/ Checkbox	Description
Notification Rule - Source	No	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

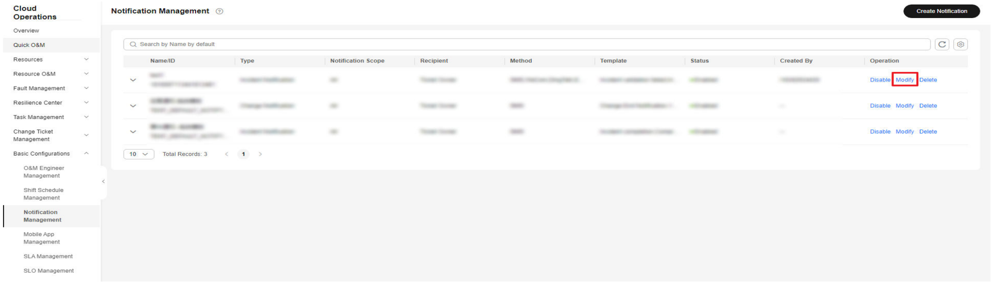
Editing Notifications

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**. Locate the notification to be modified and click **Modify** in the **Operation** column. Modify and save the notification by referring to the **Step 3**.

Figure 10-33 Modifying notifications



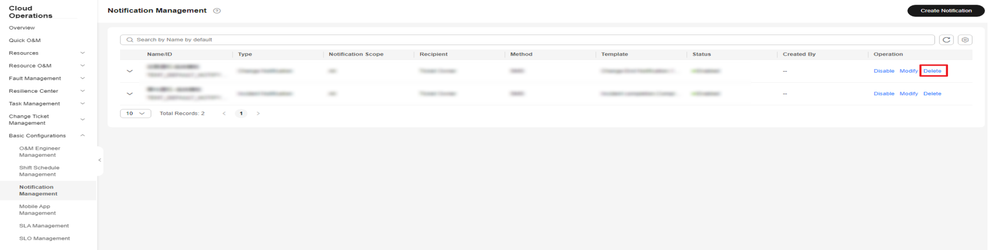
----End

Deleting a Notification

Step 1 Log in to COC.

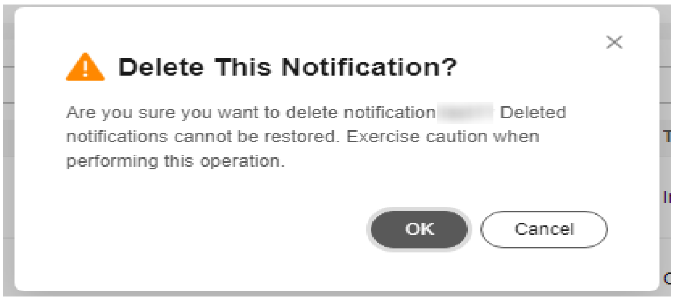
Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Notification Management**. Locate the notification to be deleted and click **Delete** in the **Operation** column.

Figure 10-34 Deleting a notification



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

Figure 10-35 Confirming the deletion



Delete This Notification?

Are you sure you want to delete notification [redacted] Deleted notifications cannot be restored. Exercise caution when performing this operation.

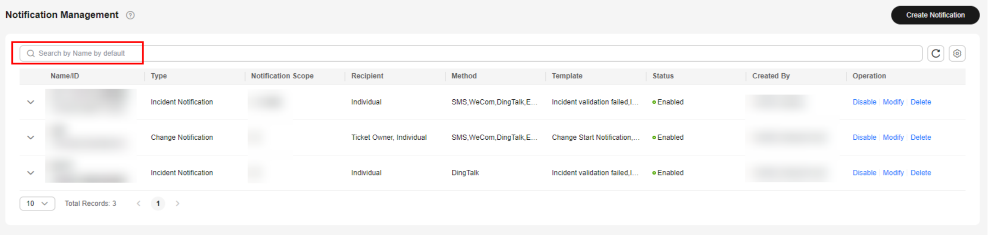
----End

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**. Enter the search criteria in the search box and press **Enter**.

Figure 10-36 Searching for notifications



Notification Management

Search by Name by default

	Name/ID	Type	Notification Scope	Recipient	Method	Template	Status	Created By	Operation
⌄	[redacted]	Incident Notification	[redacted]	Individual	SMS,WeCom,DingTalk,E...	Incident validation failed,I...	● Enabled	[redacted]	Disable Modify Delete
⌄	[redacted]	Change Notification	[redacted]	Ticket Owner, Individual	SMS,WeCom,DingTalk,E...	Change Start Notification,...	● Enabled	[redacted]	Disable Modify Delete
⌄	[redacted]	Incident Notification	[redacted]	Individual	DingTalk	Incident validation failed,I...	● Enabled	[redacted]	Disable Modify Delete

10 ⌄ Total Records: 3 ‹ 1 ›

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.

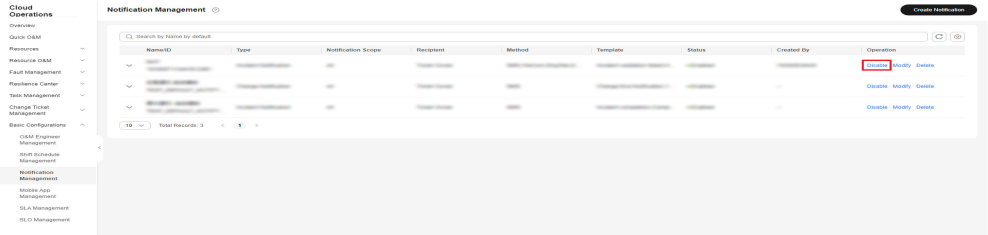
----End

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**. Locate the notification to be enabled or disabled and click **Enable** or **Disable** in the **Operation** column.

Figure 10-37 Enabling/Disabling a Notification



Notification Management

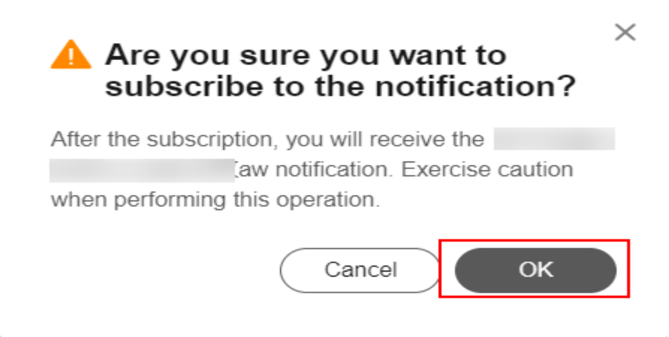
Search by Name by default

	Name/ID	Type	Notification Scope	Recipient	Method	Template	Status	Created By	Operation
⌄	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable Modify Delete
⌄	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Disable Modify Delete
⌄	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	--	Disable Modify Delete

10 ⌄ Total Records: 3 ‹ 1 ›

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

Figure 10-38 Confirming the enabling



Are you sure you want to subscribe to the notification?

After the subscription, you will receive the [redacted] [redacted]aw notification. Exercise caution when performing this operation.

NOTE

The notification instance statuses include **Enabled** (in green) and **Disabled** (in red).

----End

Other Notification Features

The following notification features are not displayed on the page:

1. Notification deduplication

   When an incident ticket or a change ticket triggers multiple notifications, and the recipients or other factors of these notifications are the same, the notification module deduplicates the recipients, ensuring that a recipient receive only one notification when an incident or change ticket is generated.

2. Notification Template Description

   Incident notification template: 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 App Management

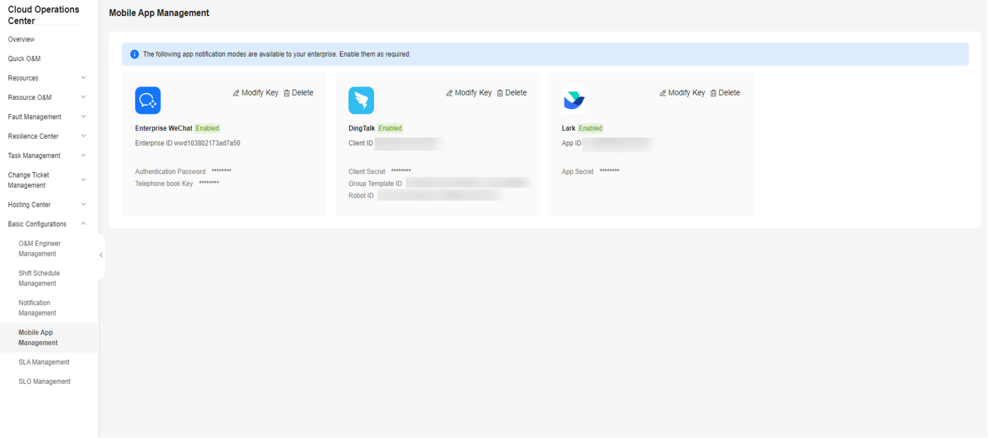
Mobile Application Management is used to manage the enterprise WeChat configuration information required for creating an enterprise WeChat WarRoom.

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



Mobile App Management

The following app notification modes are available to your enterprise. Enable them as required.

Enterprise WeChat Enabled — Modify Key, Delete
Enterprise ID wwd103802173ad7a50
Authentication Password ********
Telephone book Key ********

DingTalk Enabled — Modify Key, Delete
Client ID [redacted]
Client Secret ********
Group Template ID [redacted]
Robot ID [redacted]

Lark Enabled — Modify Key, Delete
App ID [redacted]
App Secret ********

NOTE

Currently, only Enterprise WeChat, DingTalk, and Lark are supported.

----End

Adding a Mobile Application

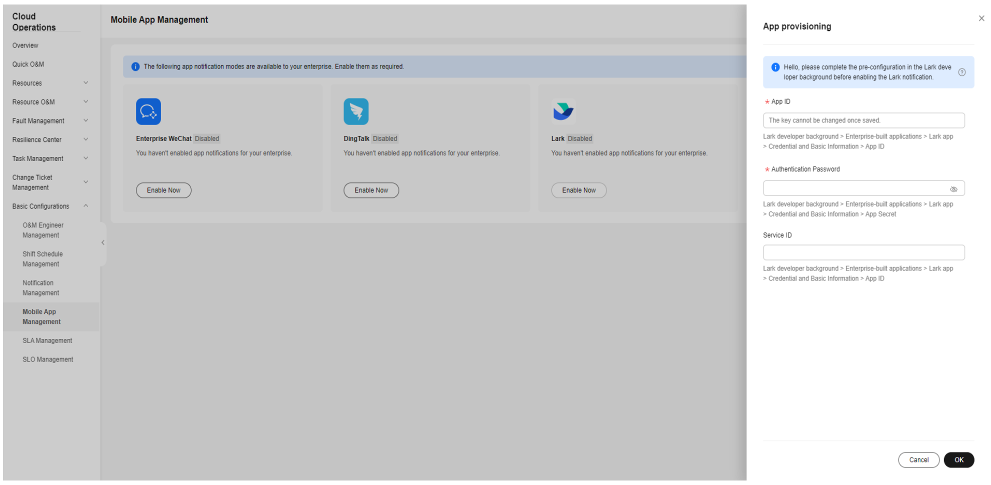
Step 1 Log in to COC.

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 To configure Enterprise WeChat, click **Enable Now** and enter the enterprise WeChat application ID, enterprise key, and address book password. The configuration method is the same for DingTalk enablement and Lark enablement.

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



Mobile App Management

The following app notification modes are available to your enterprise. Enable them as required.

Enterprise WeChat Disabled
You haven't enabled app notifications for your enterprise.

DingTalk Disabled
You haven't enabled app notifications for your enterprise.

Lark Disabled
You haven't enabled app notifications for your enterprise.

App provisioning

Hello, please complete the pre-configuration in the Lark deve loper background before enabling the Lark notification.

* App ID
The key cannot be changed once saved.
Lark developer background > Enterprise-built applications > Lark app > Credential and Basic Information > App ID

* Authentication Password
Lark developer background > Enterprise-built applications > Lark app > Credential and Basic Information > App Secret

Service ID
Lark developer background > Enterprise-built applications > Lark app > Credential and Basic Information > App ID

----End

Changing the Mobile App Key

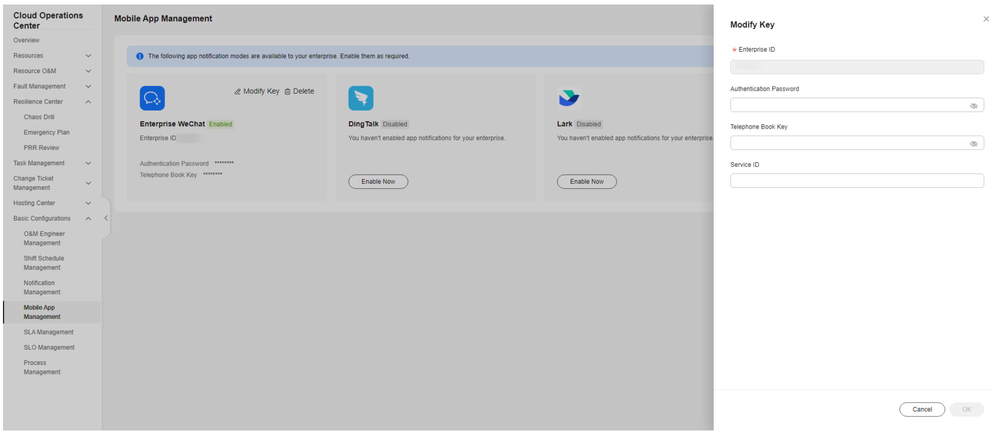
Step 1 Log in to COC.

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

Step 3 Click **Modify Key** and enter the enterprise key and address book key. The same applies to DingTalk and Lark.

Step 4 Click **OK**. If a message indicating the modification succeeded is displayed in the upper right corner, the modification is successful.

Figure 10-41 Changing a key



The following app notification modes are available to your enterprise. Enable them as required.

Enterprise ID [redacted]

Authentication Password ********

Telephone Book Key ********

You haven't enabled app notifications for your enterprise.

You haven't enabled app notifications for your enterprise.

* Enterprise ID [redacted]

Authentication Password

Telephone Book Key

Service ID

----End

Deleting a Mobile Application

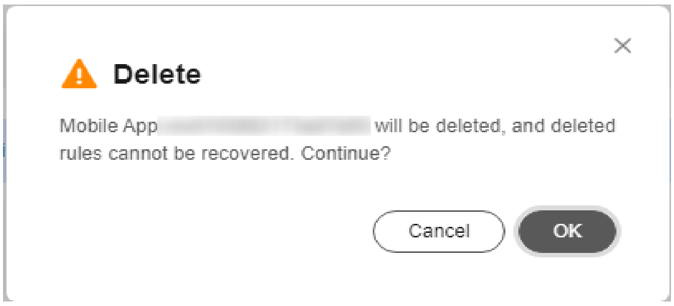
Step 1 Log in to COC.

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 10-42 Deleting a mobile application



Mobile App [redacted] will be deleted, and deleted rules cannot be recovered. Continue?

----End

10.5 SLA Management

Service Level Agreement (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.

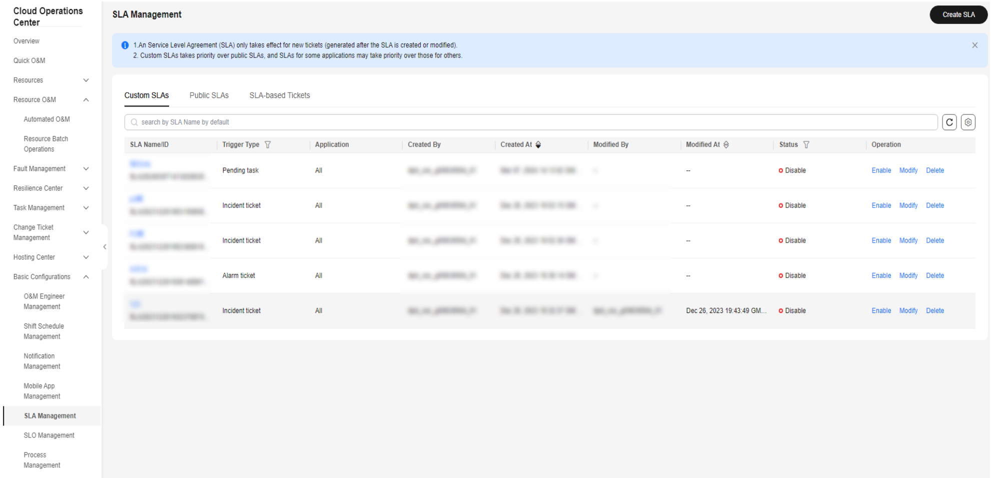
Querying a Custom SLA

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 SLAs** tab to view the custom SLA list.

Figure 10-43 SLA list



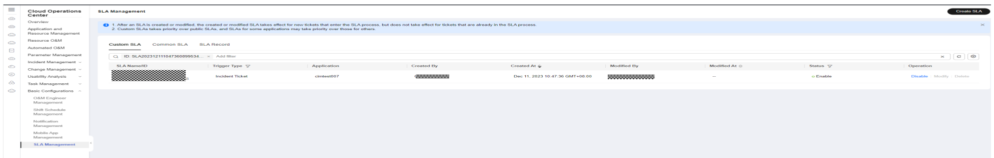
SLA Management

1.An Service Level Agreement (SLA) only takes effect for new tickets (generated after the SLA is created or modified).
2. Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

SLA Name/ID	Trigger Type	Application	Created By	Created At	Modified By	Modified At	Status	Operation
[redacted]	Pending task	All	[redacted]	[redacted]	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Alarm ticket	All	[redacted]	[redacted]	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	[redacted]	Dec 26, 2023 19:43:49 GM...	Disable	Enable Modify Delete

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 10-44 Filtering SLA rules



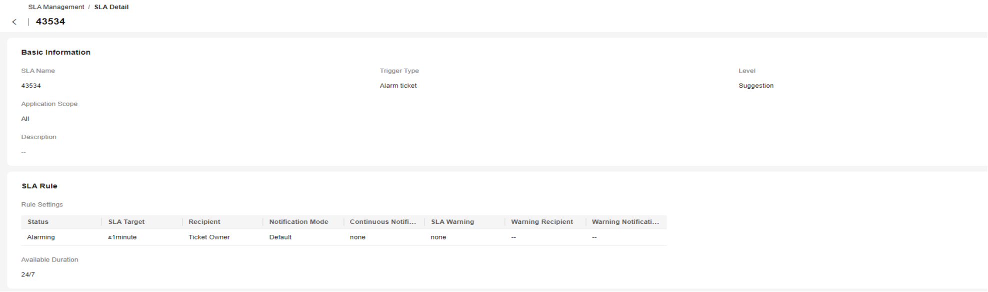
SLA Management

1. After an SLA is created or modified, the created or modified SLA takes effect for new tickets that enter the SLA process, but does not take effect for tickets that are already in the SLA process.
2. Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

SLA Name/ID	Trigger Type	Application	Created By	Created At	Modified By	Modified At	Status	Operation
[redacted]	Incident Ticket	cimtest007	[redacted]	Dec 11, 2023 10:47:36 GMT+08:00	[redacted]	--	Enable	Disable Modify Delete

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

Figure 10-45 Viewing SLA details



Basic Information

SLA Name: 43534

Trigger Type: Alarm ticket

Level: Suggestion

Application Scope: All

Description: --

SLA Rule

Rule Settings

Status	SLA Target	Recipient	Notification Mode	Continuous Notifi...	SLA Warning	Warning Recipient	Warning Notificati...
Alarming	≤1minute	Ticket Owner	Default	none	none	--	--

Available Duration: 24/7

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

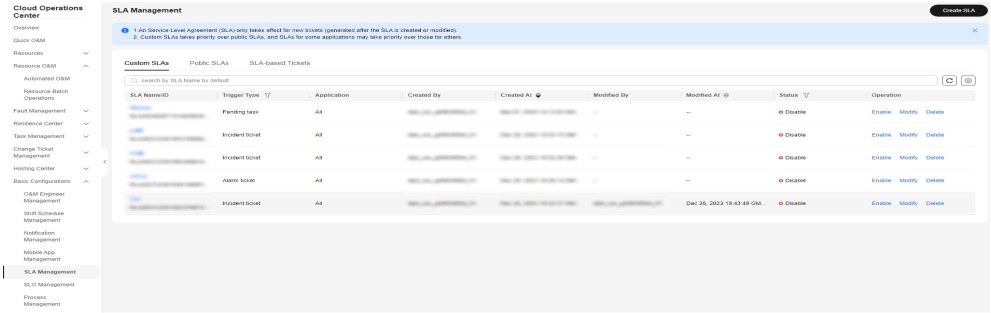
Creating a Custom SLA

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 SLAs** tab.

Figure 10-46 Querying the SLA List

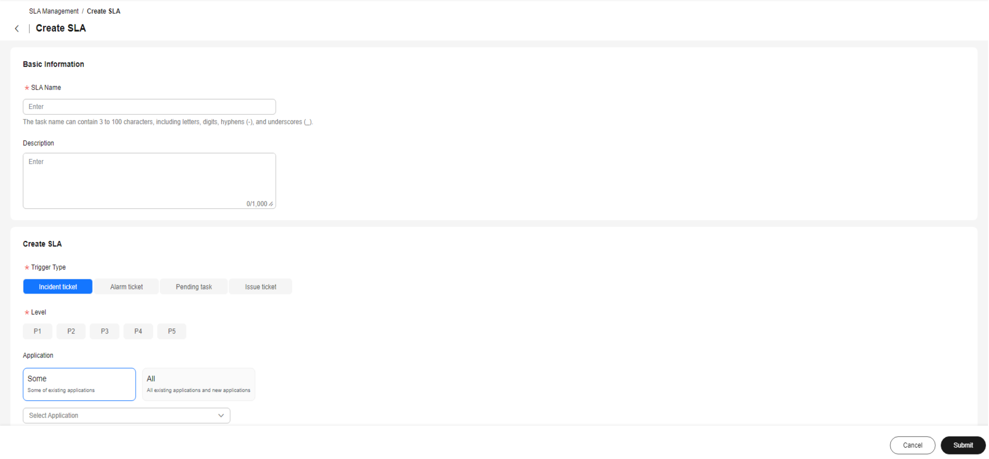


1.An Service Level Agreement (SLA) only takes effect for new tickets (generated after the SLA is created or modified).
2. Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

SLA Name/ID	Trigger Type	Application	Created By	Created At	Modified By	Modified At	Status	Operation
[redacted]	Pending task	All	[redacted]	[redacted]	--	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	--	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	--	--	Disable	Enable Modify Delete
[redacted]	Alarm ticket	All	[redacted]	[redacted]	--	--	Disable	Enable Modify Delete
[redacted]	Incident ticket	All	[redacted]	[redacted]	[redacted]	Dec 26, 2023 19:43:49 GM...	Disable	Enable Modify Delete

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

Figure 10-47 Creating a custom SLA



SLA Management / Create SLA

Create SLA

Basic Information

* SLA Name

Enter

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

Description

Enter

0/1,000

Create SLA

* Trigger Type

Incident ticket | Alarm ticket | Pending task | Issue ticket

* Level

P1 | P2 | P3 | P4 | P5

Application

Some
Some of existing applications

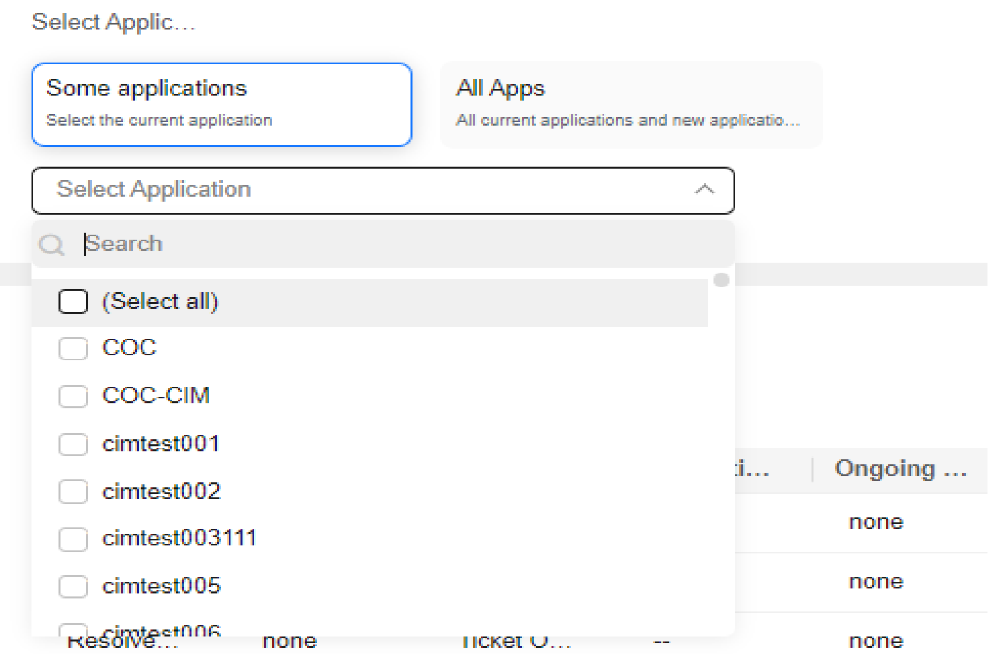
All
All existing applications and new applications

Select Application

Cancel | Submit

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 10-48 Selecting applications



Select Applic...

Some applications
Select the current application

All Apps
All current applications and new applicatio...

Select Application

Search

□ (Select all)
□ COC
□ COC-CIM
□ cimtest001
□ cimtest002
□ cimtest003111
□ cimtest005
□ cimtest006

Table 10-2 Description

Parameter	Description
SLA Name	Mandatory The value can contain 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).

Parameter	Description
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 ● Pending task ● Issue ticket
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 pending task, the levels include: ● Critical ● Major ● Minor ● Suggestion When the trigger type is issue ticket, the levels include: ● Critical ● Major ● Minor ● Suggestion
Application	Options: ● Some ● All

Step 6 In the **SLA Rule** table, locate a target rule, Click **Modify** in **Operation** column.

Step 7 Set **SLA Target**, **Recipient**, and **Notification Mode** in the dialog box that is displayed.

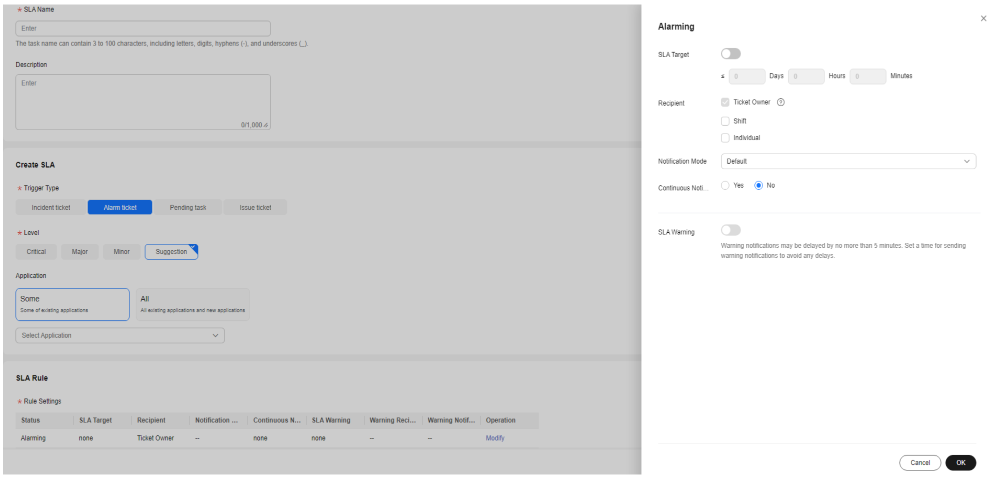
Table 10-3 Parameter description

Parameter	Description
Status	When **Trigger Type** is set to **Incident ticket**, the status types are as follows: ● Pending handling ● Handling ● Resolved and pending verification When **Trigger Type** is set to **Alarm ticket**, the status types are as follows: ● Alarming When **Trigger Type** is set to **Pending task**, the status types are as follows: ● Pending handling ● Handling When **Trigger Type** is set to **Issue ticket**, the status types are as follows: ● Pending handling ● Locating the solution ● To be implemented on the live network ● To be verified
SLA Target	**SLA Target** can be enabled. After it is enabled, a maximum of seven days can be set.
Recipient	**Recipient** is classified into the following types: ● Ticket Owner ● Shift ● Individual **Ticket Owner** is selected by default.

Parameter	Description
Notification Mode	Notification mode. The options are as follows: ● Default ● SMS ● Enterprise WeChat ● DingTalk ● Email ● Lark ● No notification

Step 8 Click **OK**.

Figure 10-49 Configure an SLA Rule



* SLA Name: Enter

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

Description: Enter 0/1,000

Create SLA

* Trigger Type: Incident ticket [✓ Alarm ticket] Pending task Issue ticket

* Level: Critical Major Minor [✓ Suggestion]

Application: [✓ Some — Some of existing applications] All — All existing applications and new applications

Select Application

SLA Rule

* Rule Settings

Status	SLA Target	Recipient	Notification ...	Continuous N...	SLA Warning	Warning Reci...	Warning Notif...	Operation
Alarming	none	Ticket Owner	--	none	none	--	--	Modify

Alarming

SLA Target: ≤ 0 Days 0 Hours 0 Minutes

Recipient: ☑ Ticket Owner ☐ Shift ☐ Individual

Notification Mode: Default

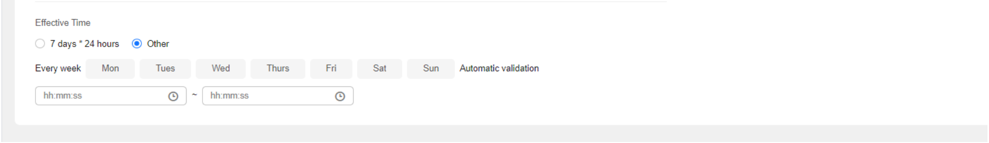
Continuous Noti...: ○ Yes ● No

SLA Warning

Warning notifications may be delayed by no more than 5 minutes. Set a time for sending warning notifications to avoid any delays.

Step 9 By default, **Available Duration** is set to **24/7**. 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 10-50 Setting available duration



Effective Time

○ 7 days * 24 hours ● Other

Every week: Mon Tues Wed Thurs Fri Sat Sun Automatic validation

hh:mm:ss ~ hh:mm:ss

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

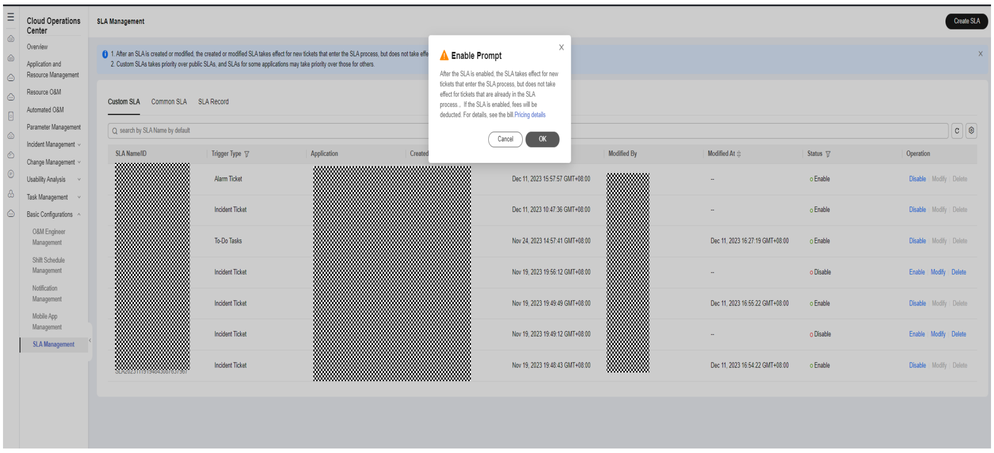
Enabling or Disabling a Custom SLA

Step 1 Log in to COC.

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

Step 3 Locate an SLA record, click **Enable** or **Disable** in the **Operation** column on the right. In the displayed dialog box, click **OK**.

Figure 10-51 Enabling or disabling an SLA



1. After an SLA is created or modified, the created or modified SLA takes effect for new tickets that enter the SLA process, but does not take effe
2. Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

Enable Prompt

After the SLA is enabled, the SLA takes effect for new tickets that enter the SLA process, but does not take effect for tickets that are already in the SLA process. , If the SLA is enabled, fees will be deducted. For details, see the bill.Pricing details

Cancel OK

SLA Name/ID	Trigger Type	Application	Created		Modified By	Modified At	Status	Operation
[redacted]	Alarm Ticket	[redacted]	[redacted]	Dec 11, 2023 15:57:57 GMT+08:00	[redacted]	--	Enable	Disable | Modify | Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Dec 11, 2023 10:47:36 GMT+08:00	[redacted]	--	Enable	Disable | Modify | Delete
[redacted]	To-Do Tasks	[redacted]	[redacted]	Nov 24, 2023 14:57:41 GMT+08:00	[redacted]	Dec 11, 2023 16:27:19 GMT+08:00	Enable	Disable | Modify | Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:56:12 GMT+08:00	[redacted]	--	Disable	Enable | Modify | Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:49:49 GMT+08:00	[redacted]	Dec 11, 2023 16:55:22 GMT+08:00	Enable	Disable | Modify | Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:49:12 GMT+08:00	[redacted]	--	Disable	Enable | Modify | Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:48:43 GMT+08:00	[redacted]	Dec 11, 2023 16:54:22 GMT+08:00	Enable	Disable | Modify | Delete

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

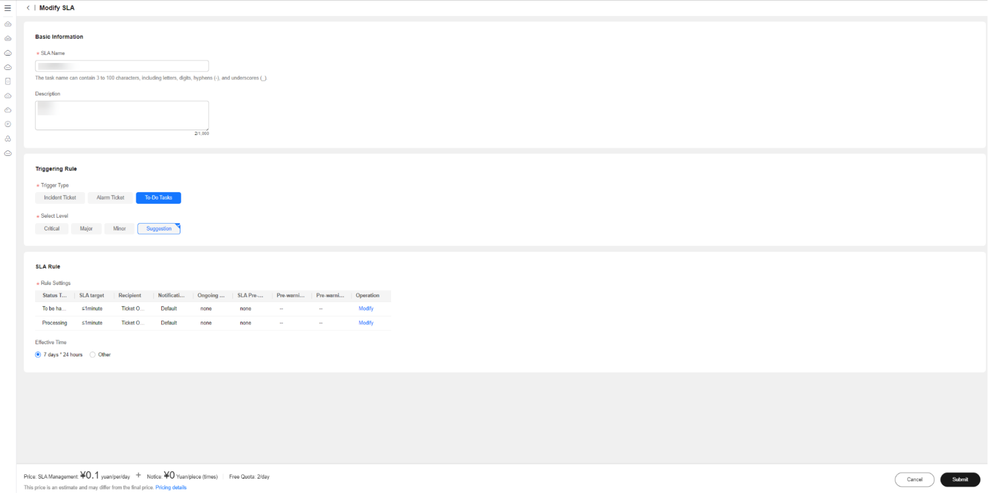
Modifying SLA

Step 1 Log in to COC.

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

Step 3 Locate an SLA data record from the list and click **Modify** in the **Operation** column. The SLA basic information is displayed.

Figure 10-52 SLA details



Basic Information

* SLA Name

[redacted]

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

Description

[redacted]

2/1,000

Triggering Rule

* Trigger Type

Incident Ticket | Alarm Ticket | To-Do Tasks

* Select Level

Critical | Major | Minor | Suggestion

SLA Rule

* Rule Settings

Status T...	SLA target	Recipient	Notificati...	Ongoing ...	SLA Pre-...	Pre-warni...	Pre-warni...	Operation
To be ha...	≤1minute	Ticket O...	Default	none	none	--	--	Modify
Processing	≤1minute	Ticket O...	Default	none	none	--	--	Modify

Effective Time

● 7 days * 24 hours ○ Other

Price: SLA Management: ¥0.1 yuan/per/day + Notice: ¥0 Yuan/piece (times) | Free Quota: 2/day

This price is an estimate and may differ from the final price. Pricing details

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

NOTE

- Only custom SLAs in the **Disable** 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

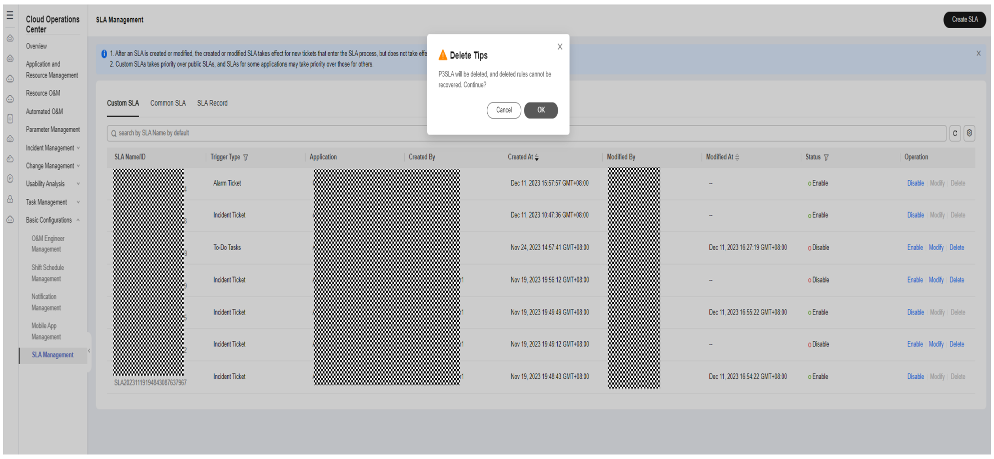
Deleting SLA

Step 1 Log in to COC.

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

Step 3 Locate an SLA data record from the list and click **Delete** in the **Operation** column. In the displayed dialog box, click **OK**.

Figure 10-53 Deleting SLA



SLA Management

1. After an SLA is created or modified, the created or modified SLA takes effect for new tickets that enter the SLA process, but does not take effe
2. Custom SLAs takes priority over public SLAs, and SLAs for some applications may take priority over those for others.

Delete Tips

P3SLA will be deleted, and deleted rules cannot be recovered. Continue?

search by SLA Name by default

SLA Name/ID	Trigger Type	Application	Created By	Created At	Modified By	Modified At	Status	Operation
[redacted]	Alarm Ticket	[redacted]	[redacted]	Dec 11, 2023 15:57:57 GMT+08:00	[redacted]	--	Enable	Disable Modify Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Dec 11, 2023 10:47:36 GMT+08:00	[redacted]	--	Enable	Disable Modify Delete
[redacted]	To-Do Tasks	[redacted]	[redacted]	Nov 24, 2023 14:57:41 GMT+08:00	[redacted]	Dec 11, 2023 16:27:19 GMT+08:00	Disable	Enable Modify Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:56:12 GMT+08:00	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:49:49 GMT+08:00	[redacted]	Dec 11, 2023 16:55:22 GMT+08:00	Enable	Disable Modify Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:49:12 GMT+08:00	[redacted]	--	Disable	Enable Modify Delete
[redacted]	Incident Ticket	[redacted]	[redacted]	Nov 19, 2023 19:48:43 GMT+08:00	[redacted]	Dec 11, 2023 16:54:22 GMT+08:00	Enable	Disable Modify Delete

NOTE

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

----End

10.5.2 Common SLA

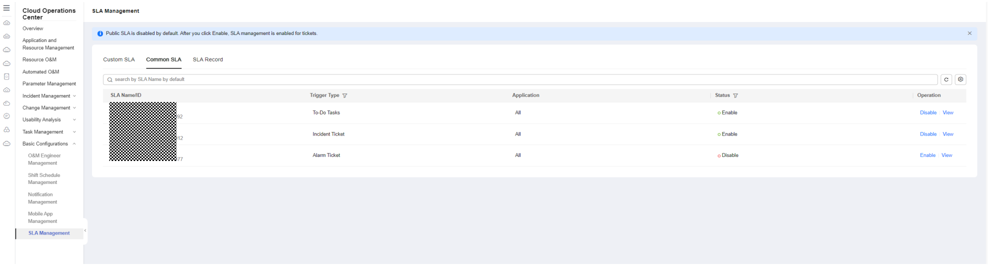
Querying Common SLA

Step 1 Log in to COC.

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

Step 3 Click the **Public SLAs** tab.

Figure 10-54 Viewing the SLA list



SLA Management

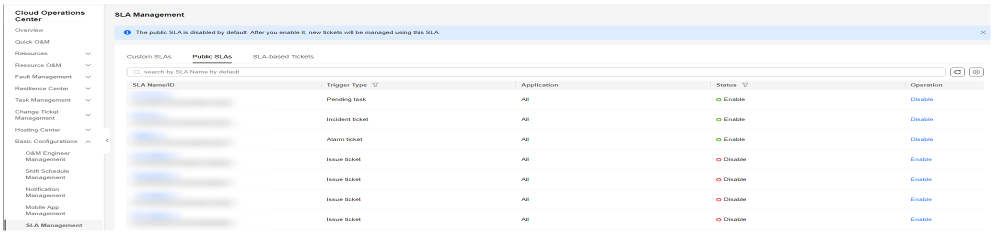
Public SLA is disabled by default. After you click Enable, SLA management is enabled for tickets.

search by SLA Name by default

SLA Name/ID	Trigger Type	Application	Status	Operation
[redacted]	To-Do Tasks	All	○ Enable	Disable View
[redacted]	Incident Ticket	All	○ Enable	Disable View
[redacted]	Alarm Ticket	All	○ Disable	Enable View

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.

Figure 10-55 Searching for a public SLA template



SLA Management

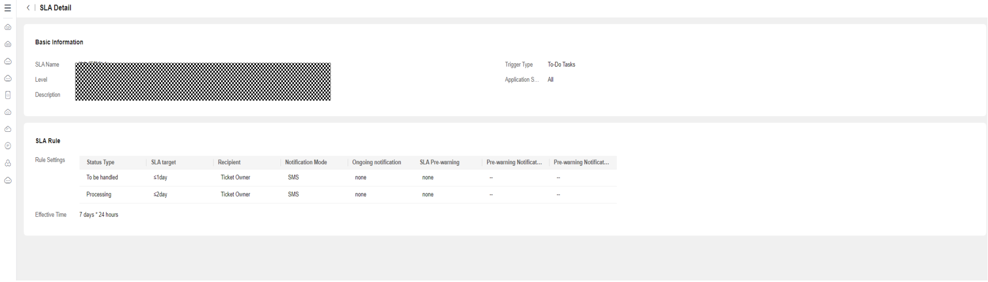
The public SLA is disabled by default. After you enable it, new tickets will be managed using this SLA.

search by SLA Name by default

SLA Name/ID	Trigger Type	Application	Status	Operation
[redacted]	Pending task	All	○ Enable	Disable
[redacted]	Incident ticket	All	○ Enable	Disable
[redacted]	Alarm ticket	All	○ Enable	Disable
[redacted]	Issue ticket	All	○ Disable	Enable
[redacted]	Issue ticket	All	○ Disable	Enable
[redacted]	Issue ticket	All	○ Disable	Enable
[redacted]	Issue ticket	All	○ Disable	Enable

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

Figure 10-56 Viewing public SLA details


SLA Detail

Basic Information

SLA Name [redacted]
Level
Description

Trigger Type To-Do Tasks
Application S... All

SLA Rule

Rule Settings

Status Type	SLA target	Recipient	Notification Mode	Ongoing notification	SLA Pre-warning	Pre-warning Notificat...	Pre-warning Notificat...
To be handled	≤1day	Ticket Owner	SMS	none	none	--	--
Processing	≤2day	Ticket Owner	SMS	none	none	--	--

Effective Time 7 days * 24 hours

NOTE

All users can view the preset common SLA.

----End

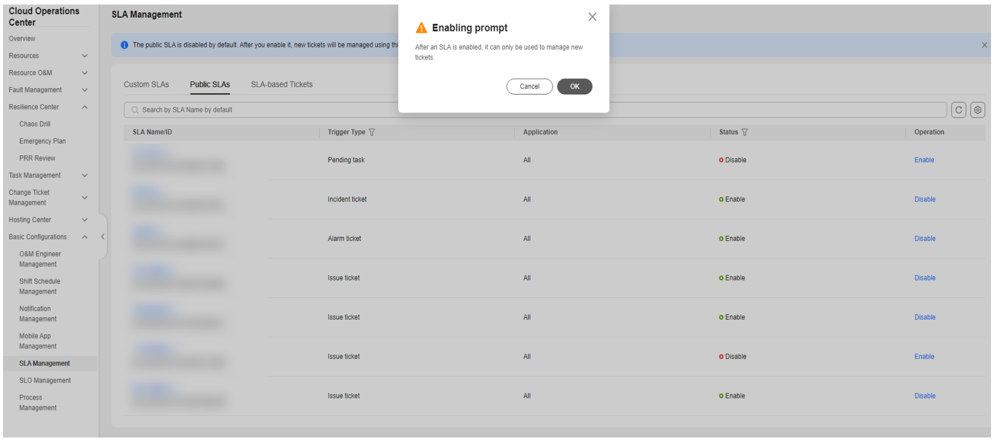
Enabling or Disabling Common SLAs

Step 1 Log in to COC.

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

Step 3 Locate an SLA record, click **Enable** or **Disable** in the **Operation** column on the right. In the displayed dialog box, click **OK**.

Figure 10-57 Enabling or Disabling a public SLA



The public SLA is disabled by default. After you enable it, new tickets will be managed using thi

Enabling prompt

After an SLA is enabled, it can only be used to manage new tickets.

SLA Name/ID	Trigger Type	Application	Status	Operation
[redacted]	Pending task	All	Disable	Enable
[redacted]	Incident ticket	All	Enable	Disable
[redacted]	Alarm ticket	All	Enable	Disable
[redacted]	Issue ticket	All	Enable	Disable
[redacted]	Issue ticket	All	Enable	Disable
[redacted]	Issue ticket	All	Disable	Enable
[redacted]	Issue ticket	All	Enable	Disable

----End

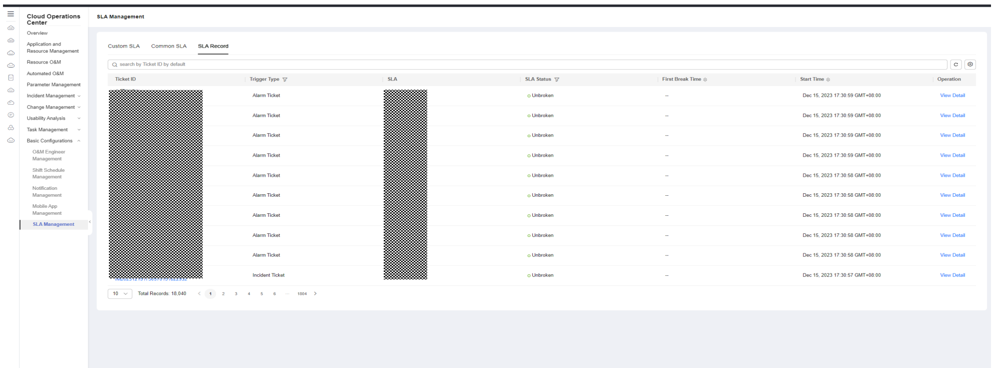
10.5.3 Managing SLA Records

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 10-58 Querying SLA records



Ticket ID	Trigger Type	SLA	SLA Status	First Break Time	Start Time	Operation
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:59 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:59 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:59 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:59 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:58 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:58 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:58 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:58 GMT+08:00	View Detail
[redacted]	Alarm Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:58 GMT+08:00	View Detail
[redacted]	Incident Ticket	[redacted]	Unbroken	--	Dec 15, 2023 17:30:57 GMT+08:00	View Detail

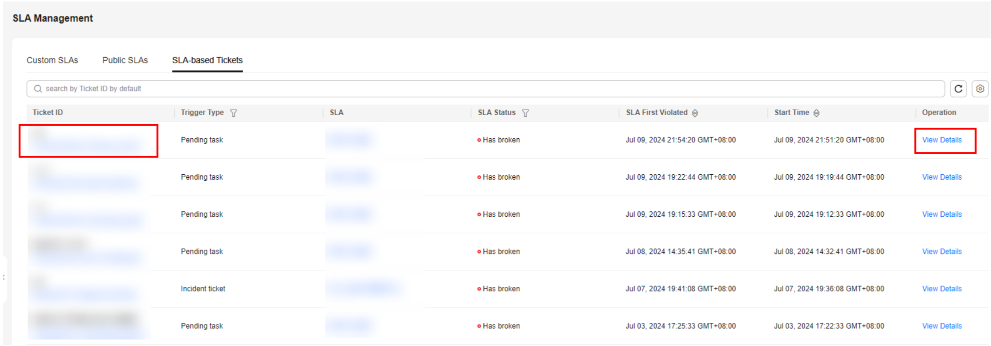
Total Records: 18,040

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 10-59 Querying SLA record details



SLA Management

Custom SLAs | Public SLAs | SLA-based Tickets

search by Ticket ID by default

Ticket ID	Trigger Type	SLA	SLA Status	SLA First Violated	Start Time	Operation
[redacted]	Pending task	[redacted]	● Has broken	Jul 09, 2024 21:54:20 GMT+08:00	Jul 09, 2024 21:51:20 GMT+08:00	View Details
[redacted]	Pending task	[redacted]	● Has broken	Jul 09, 2024 19:22:44 GMT+08:00	Jul 09, 2024 19:19:44 GMT+08:00	View Details
[redacted]	Pending task	[redacted]	● Has broken	Jul 09, 2024 19:15:33 GMT+08:00	Jul 09, 2024 19:12:33 GMT+08:00	View Details
[redacted]	Pending task	[redacted]	● Has broken	Jul 08, 2024 14:35:41 GMT+08:00	Jul 08, 2024 14:32:41 GMT+08:00	View Details
[redacted]	Incident ticket	[redacted]	● Has broken	Jul 07, 2024 19:41:08 GMT+08:00	Jul 07, 2024 19:36:08 GMT+08:00	View Details
[redacted]	Pending task	[redacted]	● Has broken	Jul 03, 2024 17:25:33 GMT+08:00	Jul 03, 2024 17:22:33 GMT+08:00	View 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

Service Level Object (SLO): Currently, SLO management interconnects with functions such as war rooms, fault, and alarm, automatically calculates SLO, and provides data for the SLO dashboard.

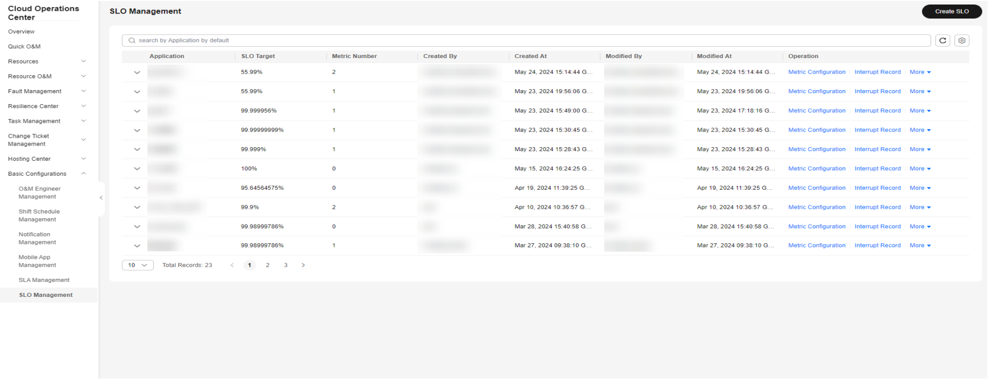
10.6.1 Viewing an SLO

Viewing an SLO

Step 1 Log in to COC.

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

Figure 10-60 SLOs



SLO Management

Create SLO

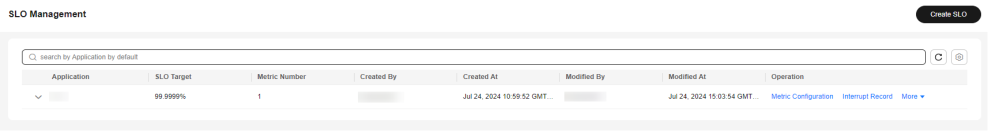
search by Application by default

	Application	SLO Target	Metric Number	Created By	Created At	Modified By	Modified At	Operation
⌄	[redacted]	55.99%	2	[redacted]	May 24, 2024 15:14:44 G...	[redacted]	May 24, 2024 15:14:44 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	55.99%	1	[redacted]	May 23, 2024 19:56:06 G...	[redacted]	May 23, 2024 19:56:06 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.999956%	1	[redacted]	May 23, 2024 15:49:00 G...	[redacted]	May 23, 2024 17:18:16 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.99999999%	1	[redacted]	May 23, 2024 15:30:45 G...	[redacted]	May 23, 2024 15:30:45 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.999%	1	[redacted]	May 23, 2024 15:28:43 G...	[redacted]	May 23, 2024 15:28:43 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	100%	0	[redacted]	May 15, 2024 16:24:25 G...	[redacted]	May 15, 2024 16:24:25 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	95.64564575%	0	[redacted]	Apr 19, 2024 11:39:25 G...	[redacted]	Apr 19, 2024 11:39:25 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.9%	2	[redacted]	Apr 10, 2024 10:36:57 G...	[redacted]	Apr 10, 2024 10:36:57 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.98999786%	0	[redacted]	Mar 28, 2024 15:40:58 G...	[redacted]	Mar 28, 2024 15:40:58 G...	Metric Configuration | Interrupt Record | More ▾
⌄	[redacted]	99.98999786%	1	[redacted]	Mar 27, 2024 09:38:10 G...	[redacted]	Mar 27, 2024 09:38:10 G...	Metric Configuration | Interrupt Record | More ▾

10 ⌄ Total Records: 23 ‹ 1 2 3 ›

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 10-61 Filtering SLOs



SLO Management

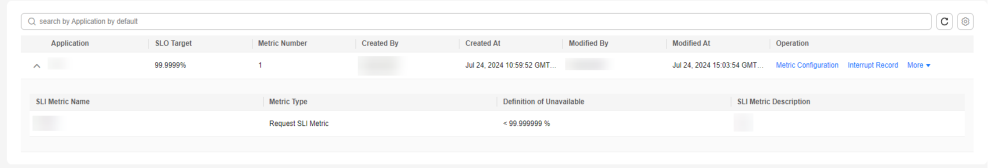
Create SLO

search by Application by default

	Application	SLO Target	Metric Number	Created By	Created At	Modified By	Modified At	Operation
⌄	[redacted]	99.9999%	1	[redacted]	Jul 24, 2024 10:59:52 GMT...	[redacted]	Jul 24, 2024 15:03:54 GMT...	Metric Configuration | Interrupt Record | More ▾

Step 4 Click ⌄ in the list to view details.

Figure 10-62 SLO details



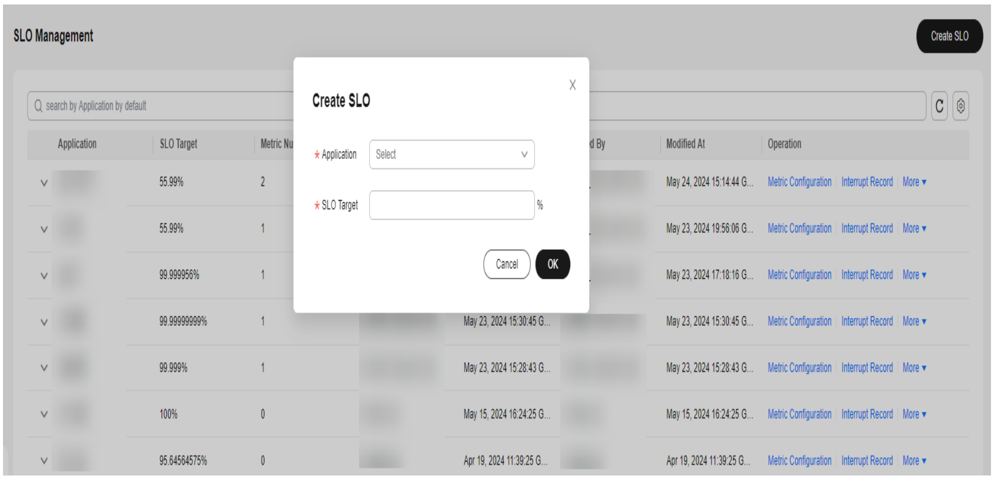
search by Application by default

	Application	SLO Target	Metric Number	Created By	Created At	Modified By	Modified At	Operation
⌃	[redacted]	99.9999%	1	[redacted]	Jul 24, 2024 10:59:52 GMT...	[redacted]	Jul 24, 2024 15:03:54 GMT...	Metric Configuration | Interrupt Record | More ▾

SLI Metric Name	Metric Type	Definition of Unavailable	SLI Metric Description
[redacted]	Request SLI Metric	< 99.999999 %	[redacted]

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

Figure 10-63 Creating an SLO



SLO Management

Create SLO

Create SLO

* Application: Select

* SLO Target: %

Cancel OK

search by Application by default
Application
SLO Target
Metric Nu
By
Modified At
Operation
55.99%
2
May 24, 2024 15:14:44 G...
55.99%
1
May 23, 2024 19:56:06 G...
99.999956%
1
May 23, 2024 17:18:16 G...
99.99999999%
1
May 23, 2024 15:30:45 G...
99.999%
1
May 23, 2024 15:28:43 G...
100%
0
May 15, 2024 16:24:25 G...
95.64564575%
0
Apr 19, 2024 11:39:25 G...
Metric Configuration
Interrupt Record
More ▾

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

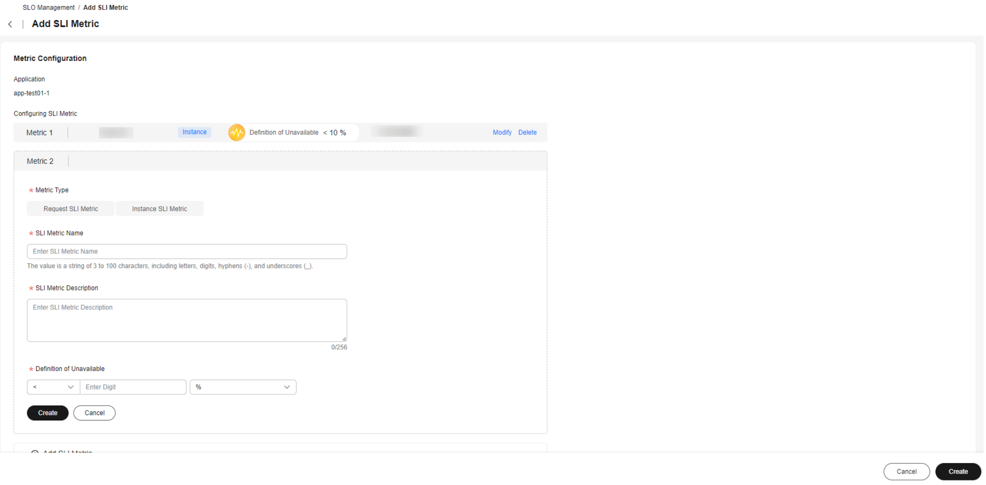
10.6.2 Configuring SLO Metrics

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 10-64 Configuring SLI metrics



SLO Management / Add SLI Metric

Add SLI Metric

Metric Configuration

Application
app-test01-1

Configuring SLI Metric

Metric 1 [redacted] Instance Definition of Unavailable < 10 % [redacted] Modify Delete

Metric 2

* Metric Type
Request SLI Metric | Instance SLI Metric

* SLI Metric Name
Enter SLI Metric Name
The value is a string of 3 to 100 characters, including letters, digits, hyphens (-), and underscores (_).

* SLI Metric Description
Enter SLI Metric Description
0/256

* Definition of Unavailable
< | Enter Digit | %

Create Cancel

Cancel Create

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

----End

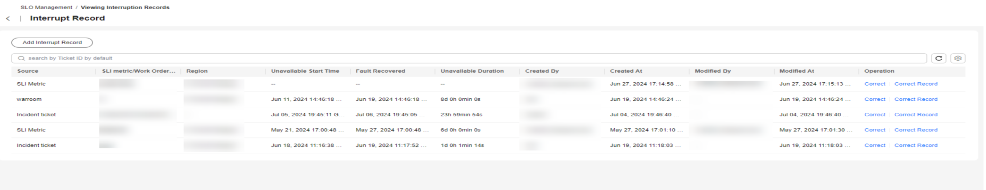
10.6.3 Viewing the SLO Interruption Records

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 10-65 Viewing the SLO interruption records



SLO Management / Viewing Interruption Records

Interrupt Record

Add Interrupt Record

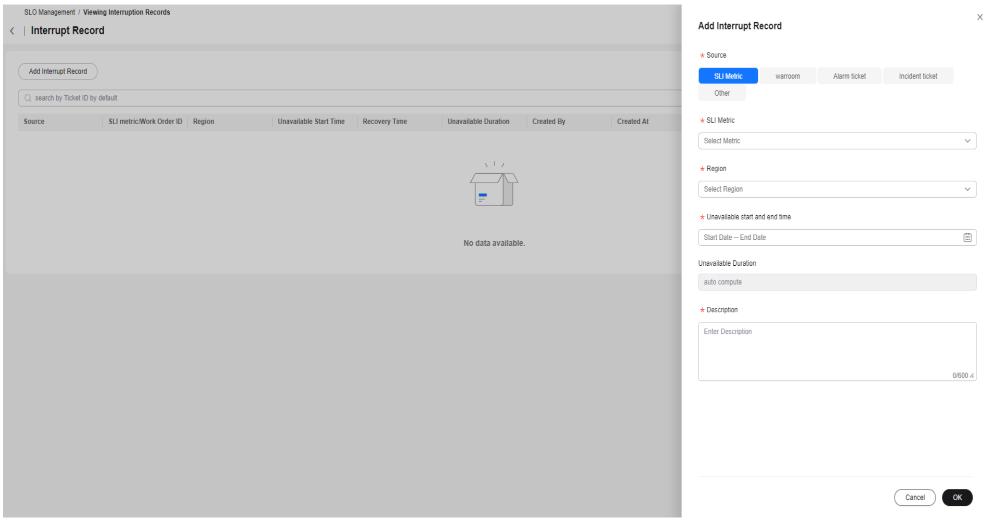
search by Ticket ID by default

Source	SLI metric/Work Order...	Region	Unavailable Start Time	Fault Recovered	Unavailable Duration	Created By	Created At	Modified By	Modified At	Operation
SLI Metric	[redacted]	[redacted]	--	--	--	[redacted]	Jun 27, 2024 17:14:58 ...	[redacted]	Jun 27, 2024 17:15:13 ...	Correct Correct Record
warroom	[redacted]	[redacted]	Jun 11, 2024 14:46:18 ...	Jun 19, 2024 14:46:18 ...	8d 0h 0min 0s	[redacted]	Jun 19, 2024 14:46:24 ...	[redacted]	Jun 19, 2024 14:46:24 ...	Correct Correct Record
Incident ticket	[redacted]	[redacted]	Jul 05, 2024 19:45:11 G...	Jul 06, 2024 19:45:05 ...	23h 59min 54s	[redacted]	Jul 04, 2024 19:46:40 ...	[redacted]	Jul 04, 2024 19:46:40 ...	Correct Correct Record
SLI Metric	[redacted]	[redacted]	May 21, 2024 17:00:48 ...	May 27, 2024 17:00:48 ...	6d 0h 0min 0s	[redacted]	May 27, 2024 17:01:10 ...	[redacted]	May 27, 2024 17:01:30 ...	Correct Correct Record
Incident ticket	[redacted]	[redacted]	Jun 18, 2024 11:16:38 ...	Jun 19, 2024 11:17:52 ...	1d 0h 1min 14s	[redacted]	Jun 19, 2024 11:18:03 ...	[redacted]	Jun 19, 2024 11:18:03 ...	Correct Correct Record

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 10-66 Adding an interrupt record



Source	SLI metric/Work Order ID	Region	Unavailable Start Time	Recovery Time	Unavailable Duration	Created By	Created At

* Source: SLI Metric / warroom / Alarm ticket / Incident ticket / Other

* SLI Metric: Select Metric

* Region: Select Region

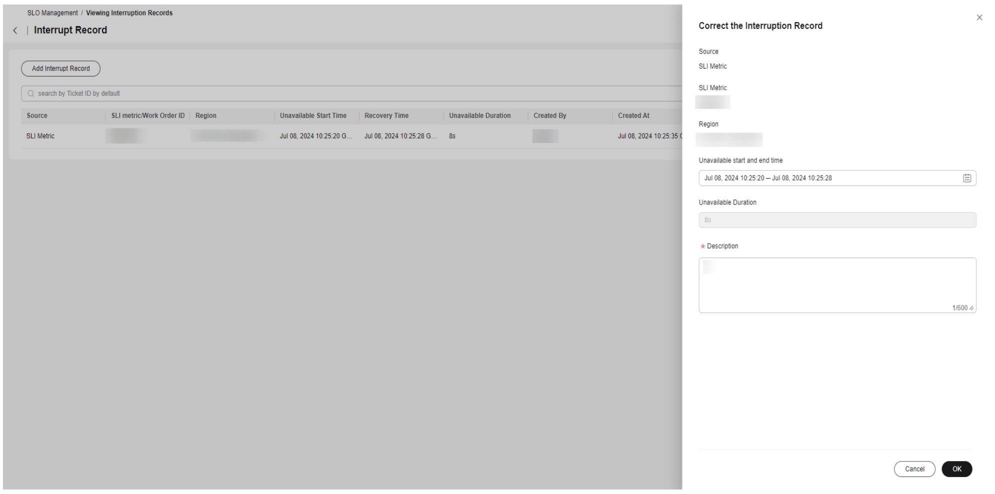
* Unavailable start and end time: Start Date – End Date

Unavailable Duration: auto compute

* Description: Enter Description 0/600

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 10-67 Modifying an interruption record


SLO Management / Viewing Interruption Records
Interrupt Record
Add Interrupt Record
search by Ticket ID by default
Correct the Interruption Record
Cancel
OK

Source	SLI metric/Work Order ID	Region	Unavailable Start Time	Recovery Time	Unavailable Duration	Created By	Created At
SLI Metric	[redacted]	[redacted]	Jul 08, 2024 10:25:20 G...	Jul 08, 2024 10:25:28 G...	8s	[redacted]	Jul 08, 2024 10:25:35 (

Source
SLI Metric

SLI Metric
[redacted]

Region
[redacted]

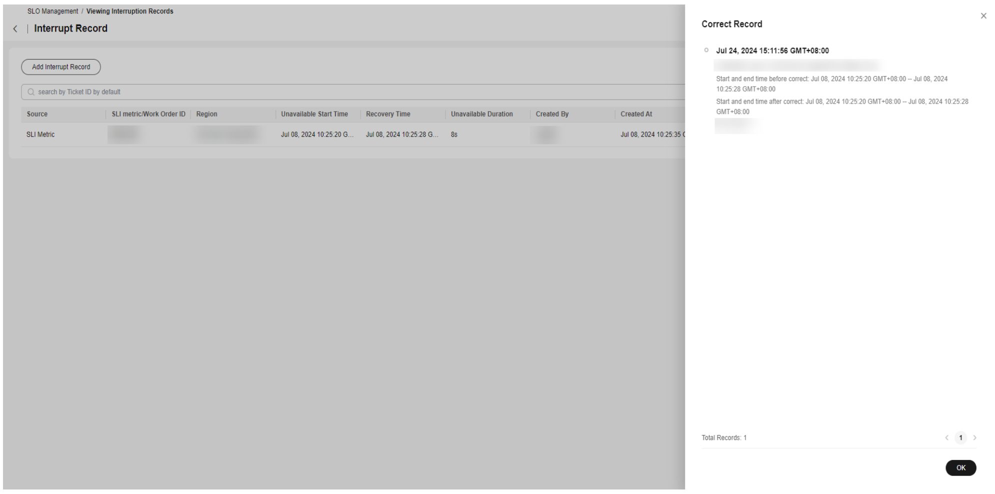
Unavailable start and end time
Jul 08, 2024 10:25:20 – Jul 08, 2024 10:25:28

Unavailable Duration
8s

* Description
[redacted] 1/600

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 10-68 Viewing interrupt modification records



SLO Management / Viewing Interruption Records

Interrupt Record

Add Interrupt Record

search by Ticket ID by default

Source	SLI metric/Work Order ID	Region	Unavailable Start Time	Recovery Time	Unavailable Duration	Created By	Created At
SLI Metric	[redacted]	[redacted]	Jul 08, 2024 10:25:20 G...	Jul 08, 2024 10:25:28 G...	8s	[redacted]	Jul 08, 2024 10:25:35 (

Correct Record

Jul 24, 2024 15:11:56 GMT+08:00

[redacted]

Start and end time before correct: Jul 08, 2024 10:25:20 GMT+08:00 -- Jul 08, 2024 10:25:28 GMT+08:00

Start and end time after correct: Jul 08, 2024 10:25:20 GMT+08:00 -- Jul 08, 2024 10:25:28 GMT+08:00

[redacted]

Total Records: 1

OK

----End

10.7 Process Management

Process management allows you to customize the levels and descriptions of incidents and issues, and configure the escalation, deescalation, and suspension of incidents and issues. Incident and issue levels and categories are developed according to the incident and issue management process

10.7.1 Incident Handling Process

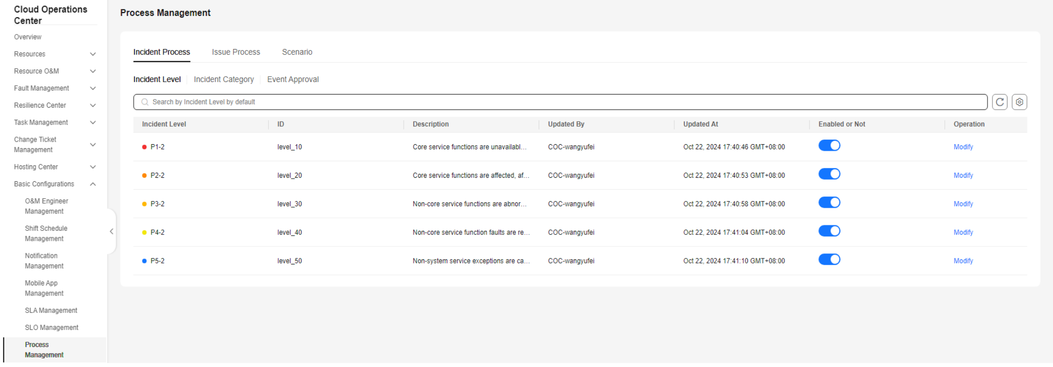
You can modify configurations for incident levels and incident categories and also can configure review for incident degradation and incident suspension.

10.7.1.1 Managing Incident Levels

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**. On the displayed **Incident Process** tab page,click the **Incident Level** tab.

Figure 10-69 Incident level



Process Management

Incident Process | Issue Process | Scenario

Incident Level | Incident Category | Event Approval

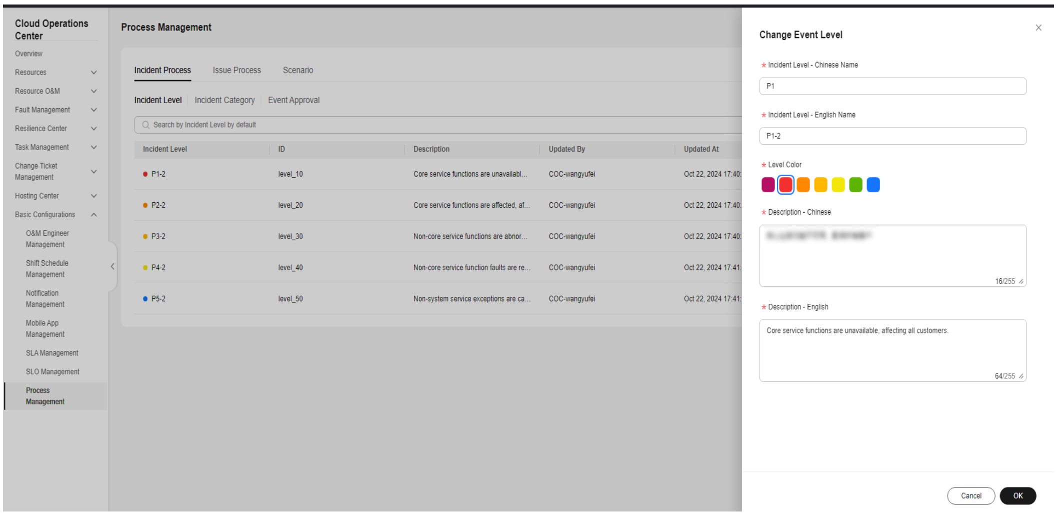
Search by Incident Level by default

Incident Level	ID	Description	Updated By	Updated At	Enabled or Not	Operation
● P1-2	level_10	Core service functions are unavailabl...	COC-wangyufei	Oct 22, 2024 17:40:46 GMT+08:00	●	Modify
● P2-2	level_20	Core service functions are affected, af...	COC-wangyufei	Oct 22, 2024 17:40:53 GMT+08:00	●	Modify
● P3-2	level_30	Non-core service functions are abnor...	COC-wangyufei	Oct 22, 2024 17:40:58 GMT+08:00	●	Modify
● P4-2	level_40	Non-core service function faults are re...	COC-wangyufei	Oct 22, 2024 17:41:04 GMT+08:00	●	Modify
● P5-2	level_50	Non-system service exceptions are ca...	COC-wangyufei	Oct 22, 2024 17:41:10 GMT+08:00	●	Modify

Step 3 Locate the target data records, and click **Edit** in the **Operation** column to modify the incident level and description. If a level does not need to be enabled, you can disable it.

Step 4 After the modification, you can view the latest incident level list on the **Incidents** page.

Figure 10-70 Editing incident levels and descriptions



Incident Level	ID	Description	Updated By	Updated At
● P1-2	level_10	Core service functions are unavailabl...	COC-wangyufei	Oct 22, 2024 17:40:
● P2-2	level_20	Core service functions are affected, af...	COC-wangyufei	Oct 22, 2024 17:40:
● P3-2	level_30	Non-core service functions are abnor...	COC-wangyufei	Oct 22, 2024 17:40:
● P4-2	level_40	Non-core service function faults are re...	COC-wangyufei	Oct 22, 2024 17:41:
● P5-2	level_50	Non-system service exceptions are ca...	COC-wangyufei	Oct 22, 2024 17:41:

Change Event Level

* Incident Level - Chinese Name: P1

* Incident Level - English Name: P1-2

* Level Color

* Description - Chinese: [redacted] 16/255

* Description - English: Core service functions are unavailable, affecting all customers. 64/255

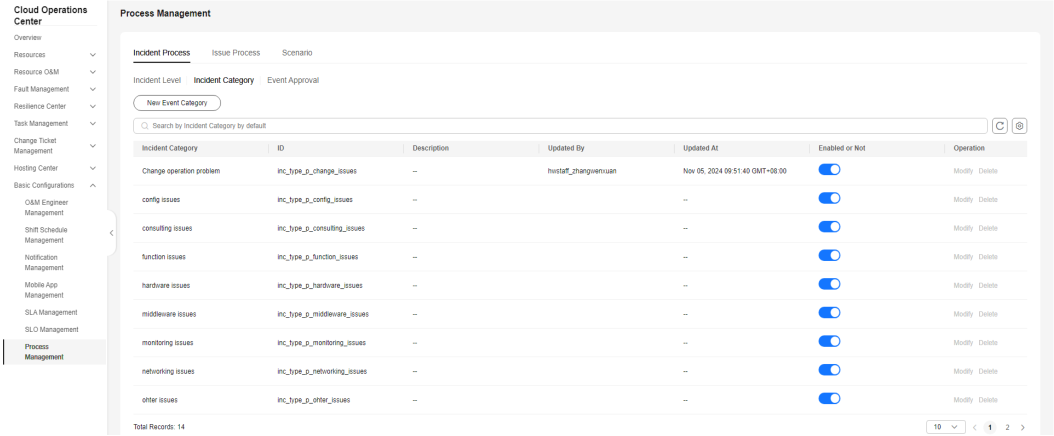
----End

10.7.1.2 Managing Incident Categories

Step 1 Log in to COC.

Step 2 In the navigation pane, choose **Basic Configurations** > **Process Management**. On the displayed page, click **Incident Category**. The incident categories preset in the system are displayed on this page and cannot be edited or deleted.

Figure 10-71 Incident categories

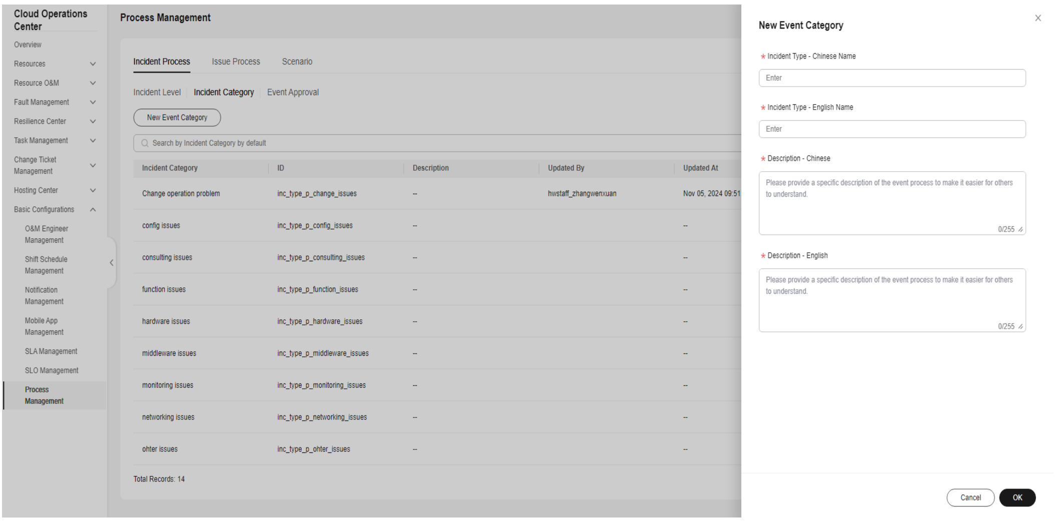


Incident Category	ID	Description	Updated By	Updated At	Enabled or Not	Operation
Change operation problem	inc_type_p_change_issues	--	hwstaff_zhangwenxuan	Nov 05, 2024 09:51:40 GMT+08:00	●	Modify Delete
config issues	inc_type_p_config_issues	--		--	●	Modify Delete
consulting issues	inc_type_p_consulting_issues	--		--	●	Modify Delete
function issues	inc_type_p_function_issues	--		--	●	Modify Delete
hardware issues	inc_type_p_hardware_issues	--		--	●	Modify Delete
middleware issues	inc_type_p_middleware_issues	--		--	●	Modify Delete
monitoring issues	inc_type_p_monitoring_issues	--		--	●	Modify Delete
networking issues	inc_type_p_networking_issues	--		--	●	Modify Delete
ohter issues	inc_type_p_ohter_issues	--		--	●	Modify Delete

Total Records: 14

Step 3 If you do not use a preset incidence category, you can disable it. To add an incident category, click **Create Incident Category**. After the incident category is added, you can view the latest enumerated values of **Incident Category** on the page for creating an incident ticket on the **Incidents** page.

Figure 10-72 Creating an incident category



Process Management

Search by Incident Category by default

Incident Category	ID	Description	Updated By	Updated At
Change operation problem	inc_type_p_change_issues	--	hwstaff_zhangwenxuan	Nov 05, 2024 09:51
config issues	inc_type_p_config_issues	--		--
consulting issues	inc_type_p_consulting_issues	--		--
function issues	inc_type_p_function_issues	--		--
hardware issues	inc_type_p_hardware_issues	--		--
middleware issues	inc_type_p_middleware_issues	--		--
monitoring issues	inc_type_p_monitoring_issues	--		--
networking issues	inc_type_p_networking_issues	--		--
ohter issues	inc_type_p_ohter_issues	--		--

Total Records: 14

New Event Category

* Incident Type - Chinese Name

Enter

* Incident Type - English Name

Enter

* Description - Chinese

Please provide a specific description of the event process to make it easier for others to understand.

0/255

* Description - English

Please provide a specific description of the event process to make it easier for others to understand.

0/255

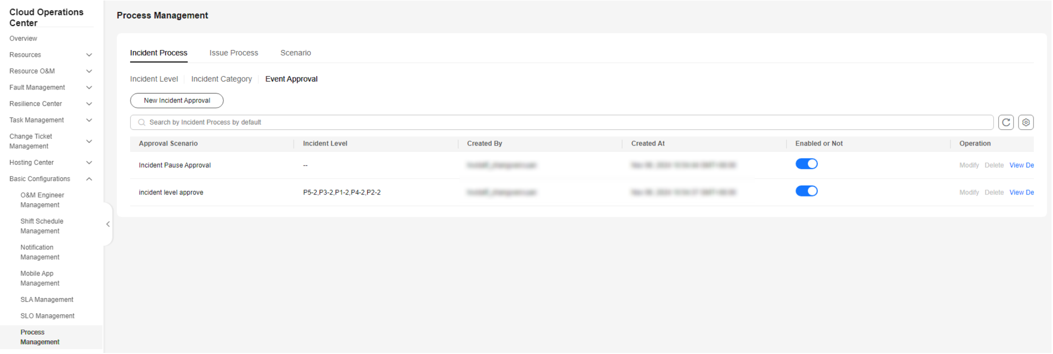
----End

10.7.1.3 Reviewing an Incident

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Basic Configurations** > **Process Management**. Click the **Incident Review** tab under **Incident Process** to configure the incident deescalation and suspension review processes. By default, incident deescalation does not need to be reviewed, and incident suspension is not available.

Figure 10-73 Reviewing an incident



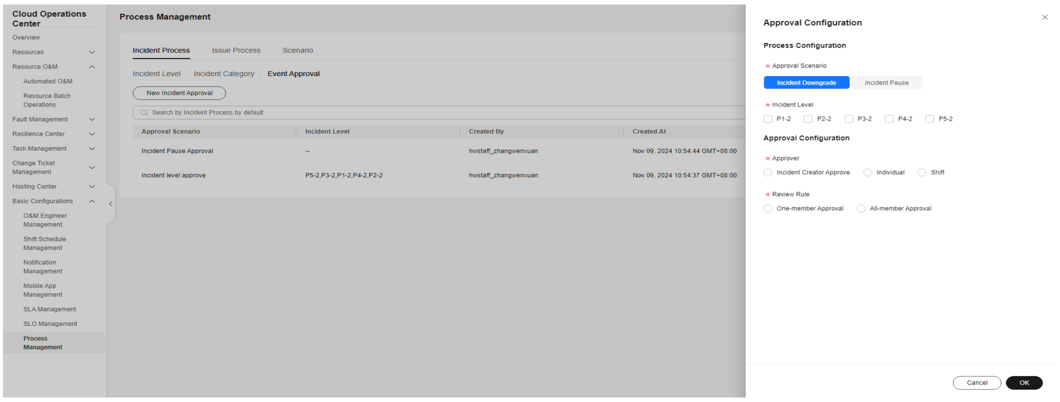
Process Management

Search by Incident Process by default

Approval Scenario	Incident Level	Created By	Created At	Enabled or Not	Operation
Incident Pause Approval	--	[redacted]	[redacted]	●	Modify Delete View De
incident level approve	P5-2,P3-2,P1-2,P4-2,P2-2	[redacted]	[redacted]	●	Modify Delete View De

Step 3 Click **Create Incident Review** to configure the incident deescalation or suspension process, and specify the incident process configurations, incident level, and review configurations.

Figure 10-74 Creating an incident review process



Approval Scenario	Incident Level	Created By	Created At
Incident Pause Approval	--	hwstaff_zhangwenxuan	Nov 09, 2024 10:54:44 GMT+08:00
incident level approve	P5-2,P3-2,P1-2,P4-2,P2-2	hwstaff_zhangwenxuan	Nov 09, 2024 10:54:37 GMT+08:00

Approval Configuration

Process Configuration

* Approval Scenario

Incident Downgrade | Incident Pause

* Incident Level

□ P1-2 □ P2-2 □ P3-2 □ P4-2 □ P5-2

Approval Configuration

* Approver

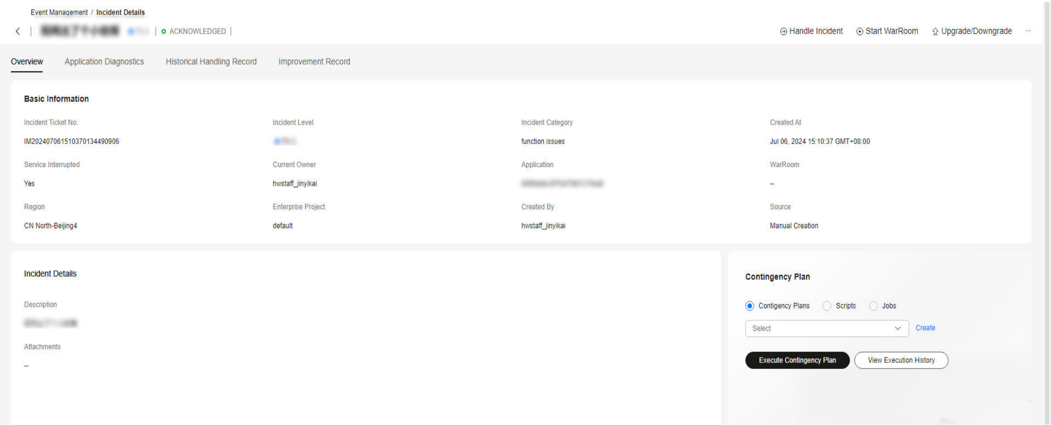
○ Incident Creator Approve ○ Individual ○ Shift

* Review Rule

○ One-member Approval ○ All-member Approval

Step 4 After the configuration is complete, the incident deescalation needs to be reviewed on the incidents processing page. In addition, the incident can be suspended.

Figure 10-75 Incident processing page



Basic Information

Incident Ticket No.	Incident Level	Incident Category	Created At
IM202407061510370134490906	[redacted]	function issues	Jul 06, 2024 15:10:37 GMT+08:00

Service Interrupted	Current Owner	Application	WarRoom
Yes	hwstaff_jinyikai	[redacted]	--

Region	Enterprise Project	Created By	Source
CN North-Beijing4	default	hwstaff_jinyikai	Manual Creation

Incident Details

Description

[redacted]

Attachments

--

Contingency Plan

● Contigency Plans ○ Scripts ○ Jobs

Select

NOTICE

1. The created incident ticket process takes effect only after the incident deescalation and review process configurations take effect.

2. Incidents in the handled state can be escalated, deescalated, or suspended.

3. Before closing an incident, close the escalation, deescalation, and suspension e-flows.

4. Incident escalation does not need to be reviewed.

----End

11 Viewing Logs

COC Operations That Can Be Audited

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

Action	Resource	Trace
Executing actions	Ticket	actionTicket
Creating a service ticket	Ticket	createTicket
Modifying a service ticket	Ticket	updateTicket
Deleting a service ticket	Ticket	deleteTicketInfo
Uploading an attachment	Attachment	uploadFileTicket
Downloading files	Attachment	downloadFileTicket
Updating the integration configuration key	IntegrationConfig	updateIntegrationConfig-Key
Accessing integration	IntegrationConfig	accessIntegrationConfig
Disabling Integration	IntegrationConfig	disableIntegrationConfig
Enabling integration	IntegrationConfig	enableIntegrationConfig
Canceling integration	IntegrationConfig	removeIntegrationConfig
Creating 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

Action	Resource	Trace
Updating a scheduling scenario	ScheduleScene	updateSceneOncall
Creating a shift role	ScheduleRole	createRoleOncall
Updating a shift role	ScheduleRole	updateRoleOncall
Deleting a shift role	ScheduleRole	deleteRoleOncall
Deleting a fixed 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

Action	Resource	Trace
Executing a public job	Job	ExecutePublicRunbook
Operating the job service ticket	Job	OperateJobTicket

Viewing Logs

Step 1 Log in to the management console.

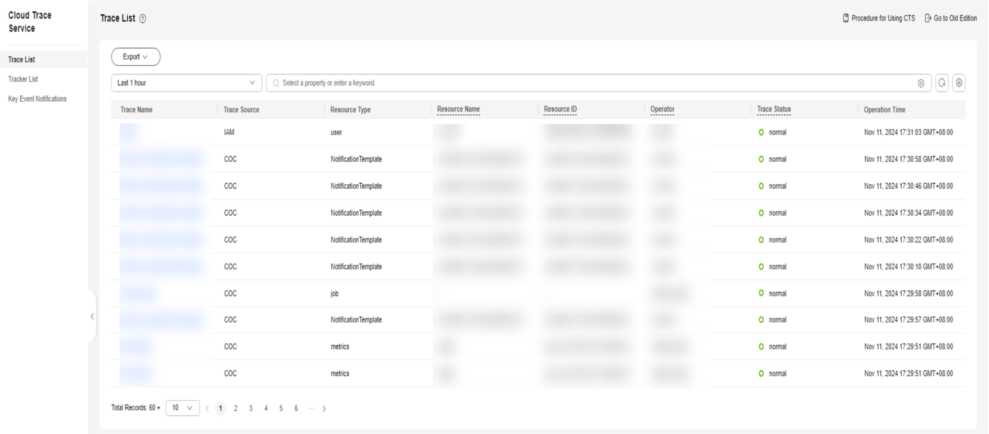
Step 2 In the upper left corner, select a region and project.

Step 3 Click ☰ in the upper left corner. Choose **Management & Governance** > **Cloud Trace Service**.

Step 4 Choose **Trace List** in the navigation pane on the left.

Step 5 Specify filter criteria as needed.

Figure 11-1 CTS events



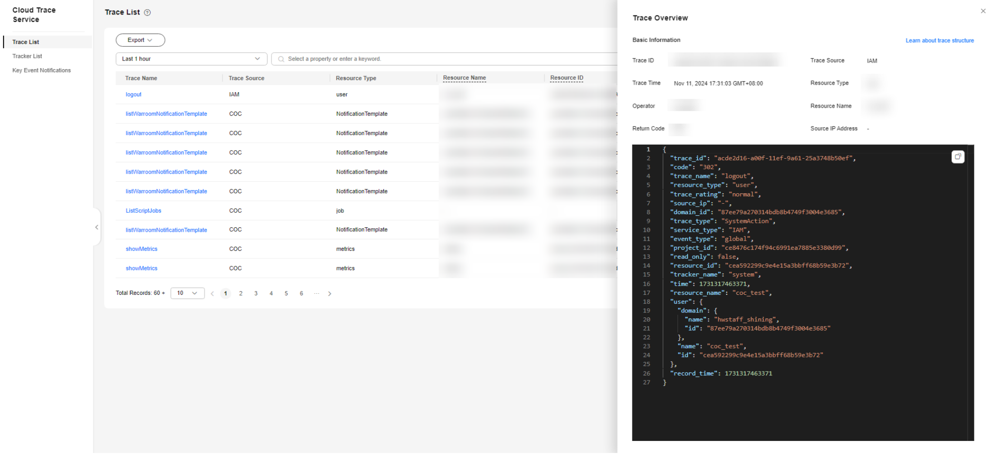
Last 1 hour

Trace Name	Trace Source	Resource Type	Resource Name	Resource ID	Operator	Trace Status	Operation Time
[redacted]	IAM	user	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:31:03 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:58 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:46 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:34 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:22 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:30:10 GMT+08:00
[redacted]	COC	job			[redacted]	normal	Nov 11, 2024 17:29:58 GMT+08:00
[redacted]	COC	NotificationTemplate	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:57 GMT+08:00
[redacted]	COC	metrics	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:51 GMT+08:00
[redacted]	COC	metrics	[redacted]	[redacted]	[redacted]	normal	Nov 11, 2024 17:29:51 GMT+08:00

Total Records: 60 + 10 ‹ 1 2 3 4 5 6 ··· ›

Step 6 Select the trace to be viewed and click the trace name to expand the overview.

Figure 11-2 Trace overview



Trace Name	Trace Source	Resource Type	Resource Name	Resource ID
logout	IAM	user	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
ListScriptJobs	COC	job		
listWarroomNotificationTemplate	COC	NotificationTemplate	[redacted]	[redacted]
showMetrics	COC	metrics	[redacted]	[redacted]
showMetrics	COC	metrics	[redacted]	[redacted]

Trace ID [redacted]

Trace Source IAM

Trace Time Nov 11, 2024 17:31:03 GMT+08:00

Resource Type [redacted]

Operator [redacted]

Resource Name [redacted]

Return Code [redacted]

Source IP Address -

```
{
  "trace_id": "acde2d16-a00f-11ef-9a61-25a3748b50ef",
  "code": "302",
  "trace_name": "logout",
  "resource_type": "user",
  "trace_rating": "normal",
  "source_ip": "-",
  "domain_id": "87ee79a270314bdb8b4749f3004e3685",
  "trace_type": "SystemAction",
  "service_type": "IAM",
  "event_type": "global",
  "project_id": "ce8476c174f94c6991ea7885e3380d99",
  "read_only": false,
  "resource_id": "cea592299c9e4e15a3bbff68b59e3b72",
  "tracker_name": "system",
  "time": 1731317463371,
  "resource_name": "coc_test",
  "user": {
    "domain": {
      "name": "hwstaff_shining",
      "id": "87ee79a270314bdb8b4749f3004e3685"
    },
    "name": "coc_test",
    "id": "cea592299c9e4e15a3bbff68b59e3b72"
  },
  "record_time": 1731317463371
}
```

----End