Cloud Operations Center

# Best Practices

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2023-11-30 |

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

## Notice

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

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

**Huawei Cloud Computing Technologies Co., Ltd.**

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

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

# Contents

# 1 Standardized Fault Management

## Scenario

The incident handling process of a certain intelligent customer service O&M engineer is inefficient due to the lack of standardized accident handling procedures, clear fault recovery joint collaboration teams, and contingency plans. Similar fault scenarios repeatedly occur, no O&M experience is accumulated, and deterministic fault scenarios cannot be automatically restored. There are multiple severities of alarms, but the processing of alarms lacks standardized procedures and is relatively slow. It is necessary to establish a standardized incident process to achieve standardized processing.

## Solution

End-to-end incident handling process: Clearly define standardized incident handling procedures, achieve multi-operational collaboration through WarRoom requests, and improve incident handling efficiency through response plans.

COC helps users manage alarms uniformly by setting up incident forwarding rules to convert raw alarms into incident or alarm tickets. When a raw alarm matches the incident forwarding rules, an incident/alarm is created, and the corresponding owner is notified according to the scheduling management. The owner can handle the alarm or convert it into an incident. After locating and restoring the issue, the alarm is cleared. If the alarm cannot be cleared, it can be escalated to an incident or handled through WarRoom requests. This creates a standardized alarm handling process to avoid abnormal alarm handling.

The standardized incident handling process includes the following steps:

1. Integrate and manage access to raw alarm data.
2. Configure incident forwarding rules to clean and process alarms.
3. Configure notification templates, select notification objects and methods in the notification management according to the notification scenario.
4. Handle or convert alarms in the integrated alarm system.
5. The incident center handles alarms that are converted into incidents, which can be forwarded, escalated, deescalated, or handled through WarRoom requests.

## Prerequisites

An application group has been created on the application management page.

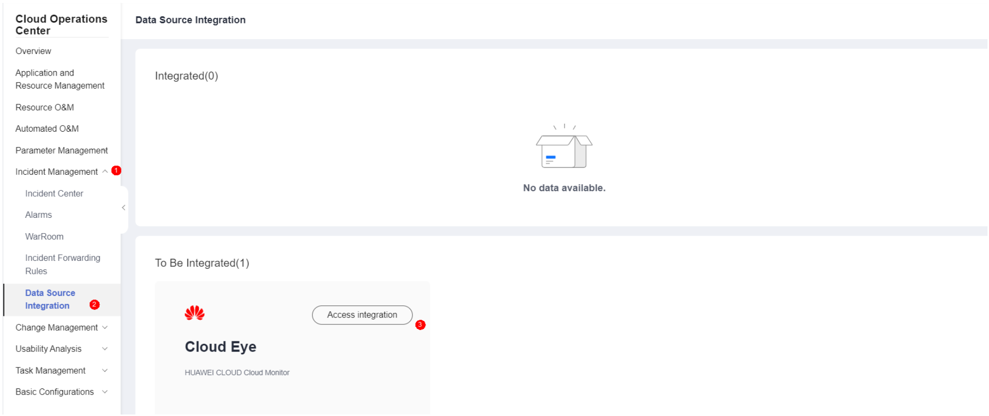
Personnel information has been added on the personnel management page.

A shift has been created on the scheduling management page.

## Step 1: Integrate and Manage Access to Raw Alarm Data

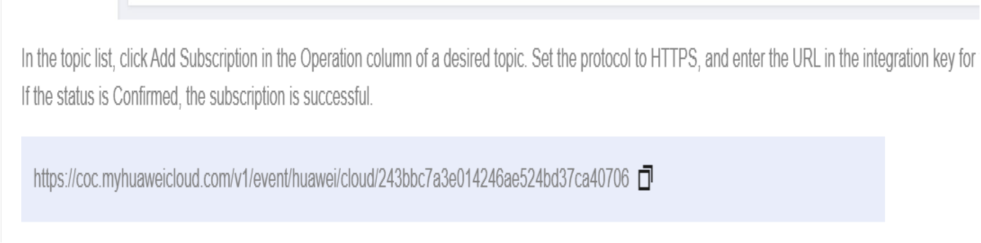
1. Log in to COC.
2. In the navigation tree on the left, choose **Incident Management** > **Data Source Integration**.
3. On the displayed page, select the data source to be accessed based on service requirements and click **Access integration**.

**Figure 1-1** Clicking Access integration



4. On the displayed page, copy the endpoint URL.

**Figure 1-2** Endpoint URL



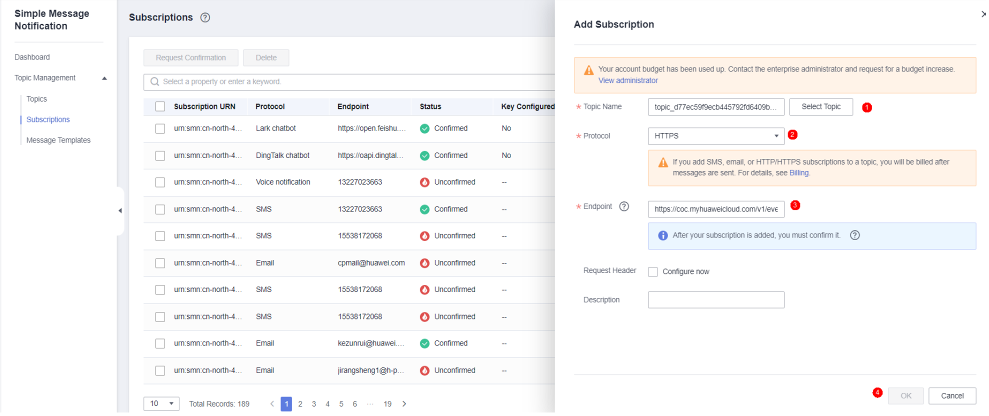
In the topic list, click Add Subscription in the Operation column of a desired topic. Set the protocol to HTTPS, and enter the URL in the integration key for

If the status is Confirmed, the subscription is successful.

https://coc.myhuaweicloud.com/v1/event/huawei/cloud/243bbc7a3e014246ae524bd37ca40706

5. Switch to the SMN console. In the navigation pane on the left, choose **Topic Management** > **Subscriptions**. On the displayed page, locate a desired description and click **Add Subscription** in the **Operation** column. In the displayed dialog box, click **Select Topic** to select a topic for **Topic Name**, set **Protocol** to **HTTPS**, paste the copied endpoint URL to **Endpoint**, and click **OK**.

**Figure 1-3** Add Subscription



Simple Message Notification

Dashboard

Topic Management

Topics

Subscriptions

Message Templates

Subscriptions

Request Confirmation | Delete

Select a property or enter a keyword.

| ☐ | Subscription URN | Protocol | Endpoint | Status | Key Configured |
|---|---|---|---|---|---|
| ☐ | urn:smn:cn-north-4... | Lark chatbot | https://open.feishu.... | Confirmed | No |
| ☐ | urn:smn:cn-north-4... | DingTalk chatbot | https://oapi.dingtal... | Confirmed | No |
| ☐ | urn:smn:cn-north-4... | Voice notification | 13227023663 | Unconfirmed | -- |
| ☐ | urn:smn:cn-north-4... | SMS | 13227023663 | Confirmed | -- |
| ☐ | urn:smn:cn-north-4... | SMS | 15538172068 | Unconfirmed | -- |
| ☐ | urn:smn:cn-north-4... | Email | cpmail@huawei.com | Unconfirmed | -- |
| ☐ | urn:smn:cn-north-4... | SMS | 15538172068 | Unconfirmed | -- |
| ☐ | urn:smn:cn-north-4... | SMS | 15538172068 | Unconfirmed | -- |
| ☐ | urn:smn:cn-north-4... | Email | kezunrui@huawei.... | Confirmed | -- |
| ☐ | urn:smn:cn-north-4... | Email | jirangsheng1@h-p... | Unconfirmed | -- |

10 Total Records: 189 < 1 2 3 4 5 6 ··· 19 >

Add Subscription

Your account budget has been used up. Contact the enterprise administrator and request for a budget increase. View administrator

* Topic Name: topic_d77ec59f9ecb445792fd6409b... Select Topic

* Protocol: HTTPS

If you add SMS, email, or HTTP/HTTPS subscriptions to a topic, you will be billed after messages are sent. For details, see Billing.

* Endpoint: https://coc.myhuaweicloud.com/v1/eve

After your subscription is added, you must confirm it.

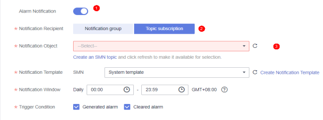
Request Header: ☐ Configure now

Description:

OK | Cancel

6. Log in to the Cloud Eye console. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**. On the displayed page, click **Create Alarm Rule**, enable **Alarm Notification**, and select **Topic subscription** for **Notification Recipient**.

**Figure 1-4** Creating an alarm



Alarm Notification

* Notification Recipient: Notification group | Topic subscription

* Notification Object: --Select--

Create an SMN topic and click refresh to make it available for selection.

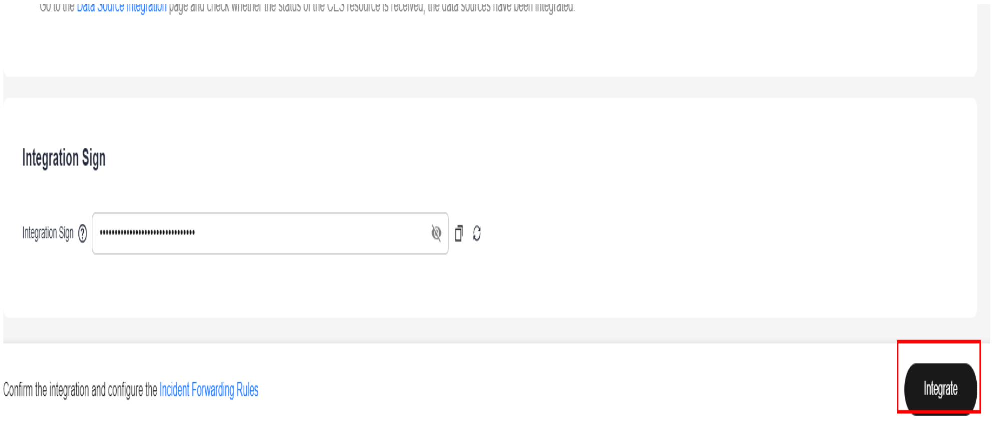
* Notification Template: SMN System template Create Notification Template

* Notification Window: Daily 00:00 - 23:59 GMT+08:00

* Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

7. Return to COC, confirm the integration, and click **Integrate**.

**Figure 1-5** Clicking Integrate



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

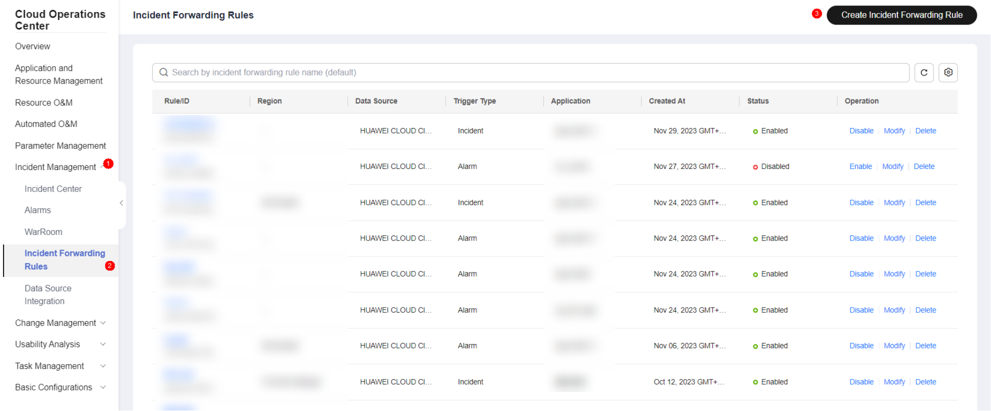
Integration Sign: ••••••••••••••••••••••••••••••

Confirm the integration and configure the Incident Forwarding Rules

## Step 2: Create a Forwarding Rule to Clean Raw Alarm Data

1. Log in to COC.
2. In the navigation pane on the left, choose **Incident Management** > **Incident Forwarding Rules**.
3. In the upper part of the list, click **Create Incident Forwarding Rule**.

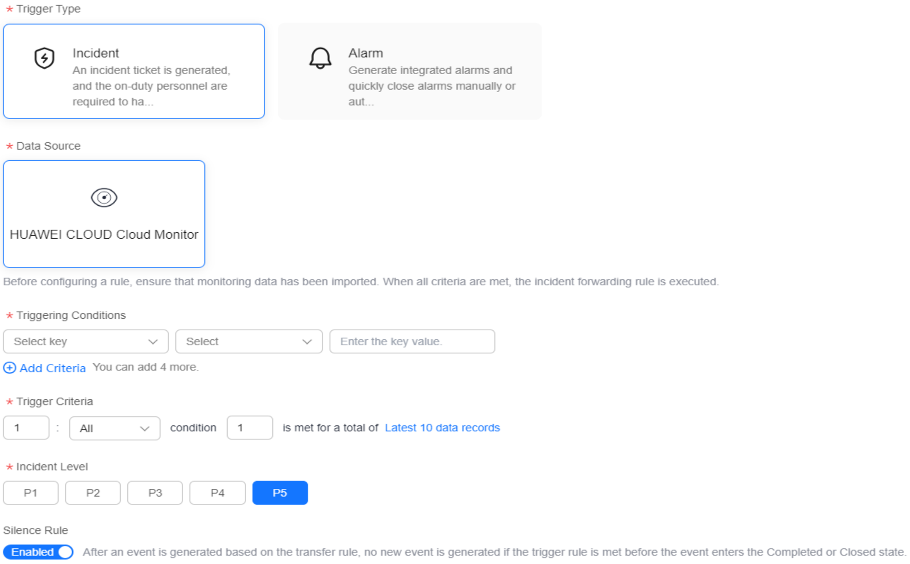
**Figure 1-6** Creating a forwarding rule



| Rule/ID | Region | Data Source | Trigger Type | Application | Created At | Status | Operation |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Incident | [redacted] | Nov 29, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Alarm | [redacted] | Nov 27, 2023 GMT+... | Disabled | Enable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Incident | [redacted] | Nov 24, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Alarm | [redacted] | Nov 24, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Alarm | [redacted] | Nov 24, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Alarm | [redacted] | Nov 24, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Alarm | [redacted] | Nov 06, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |
| [redacted] | [redacted] | HUAWEI CLOUD Cl... | Incident | [redacted] | Oct 12, 2023 GMT+... | Enabled | Disable \| Modify \| Delete |

4. Enter basic information such as the rule name and application name as prompted.
5. In the **Trigger Rules** area, select a trigger type, select a monitoring source for **Data Source**, and set triggering conditions and trigger criteria.

**Figure 1-7** Trigger criteria



* Trigger Type

Incident
An incident ticket is generated, and the on-duty personnel are required to ha...

Alarm
Generate integrated alarms and quickly close alarms manually or aut...

* Data Source

HUAWEI CLOUD Cloud Monitor

Before configuring a rule, ensure that monitoring data has been imported. When all criteria are met, the incident forwarding rule is executed.

* 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

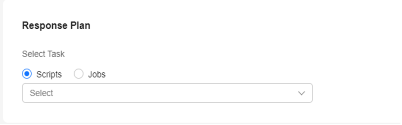
P1 P2 P3 P4 P5

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.

6. You can configure a response plan for the corresponding incident or alarm in the forwarding rule. You can select scripts or jobs.

**Figure 1-8** Response plan



Response Plan

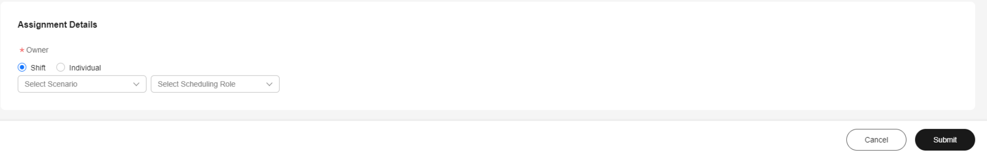
Select Task

● Scripts ○ Jobs

Select

7. In the **Assignment Details** area, select an owner and click **Submit**.

**Figure 1-9** Assignment Details area



Assignment Details

* Owner

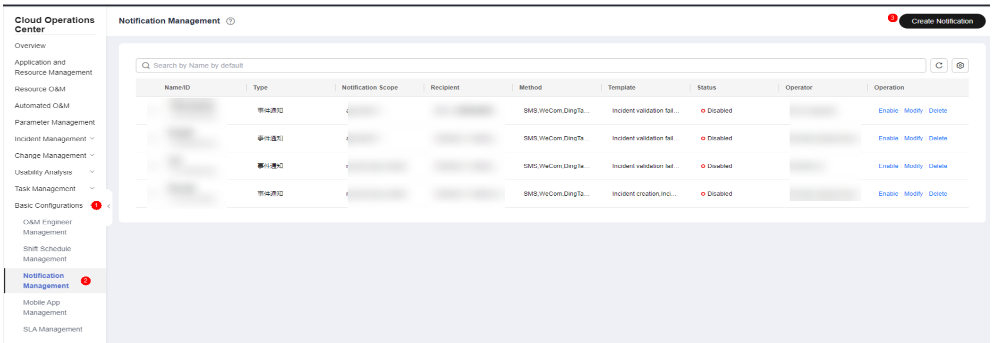
● Shift ○ Individual

Select Scenario | Select Scheduling Role

## Step 3: Configure the Notification Scenario, Recipient, and Method

1. Log in to COC.
2. In the navigation pane on the left, choose **Basic Configurations** > **Notification Management**. On the displayed page, click **Create Notification**.

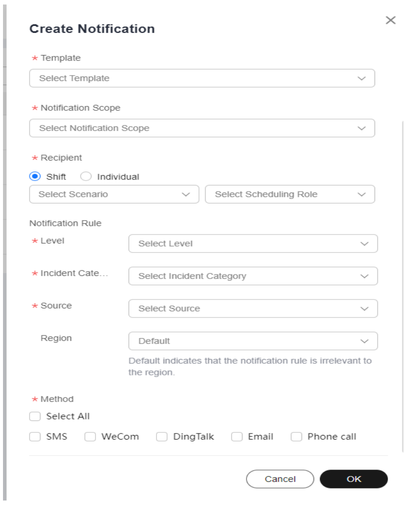
**Figure 1-10** Clicking Create Notification



| Name/ID | Type | Notification Scope | Recipient | Method | Template | Status | Operator | Operation |
|---|---|---|---|---|---|---|---|---|
| [redacted] | 事件通知 | [redacted] | [redacted] | SMS,WeCom,DingTa... | Incident validation fail... | ○ Disabled | [redacted] | Enable \| Modify \| Delete |
| [redacted] | 事件通知 | [redacted] | [redacted] | SMS,WeCom,DingTa... | Incident validation fail... | ○ Disabled | [redacted] | Enable \| Modify \| Delete |
| [redacted] | 事件通知 | [redacted] | [redacted] | SMS,WeCom,DingTa... | Incident validation fail... | ○ Disabled | [redacted] | Enable \| Modify \| Delete |
| [redacted] | 事件通知 | [redacted] | [redacted] | SMS,WeCom,DingTa... | Incident creation,Inci... | ○ Disabled | [redacted] | Enable \| Modify \| Delete |

3. In the displayed dialog box, set the parameters based on **Table 1-1** and click **OK**.

**Figure 1-11** Clicking OK



Create Notification

* Template: Select Template

* Notification Scope: Select Notification Scope

* Recipient: ● Shift ○ Individual

Select Scenario | Select Scheduling Role

Notification Rule

* Level: Select Level

* Incident Cate...: Select Incident Category

* Source: Select Source

Region: Default

Default indicates that the notification rule is irrelevant to the region.

* Method

□ Select All

□ SMS □ WeCom □ DingTalk □ Email □ Phone call

**Table 1-1** Notification parameters

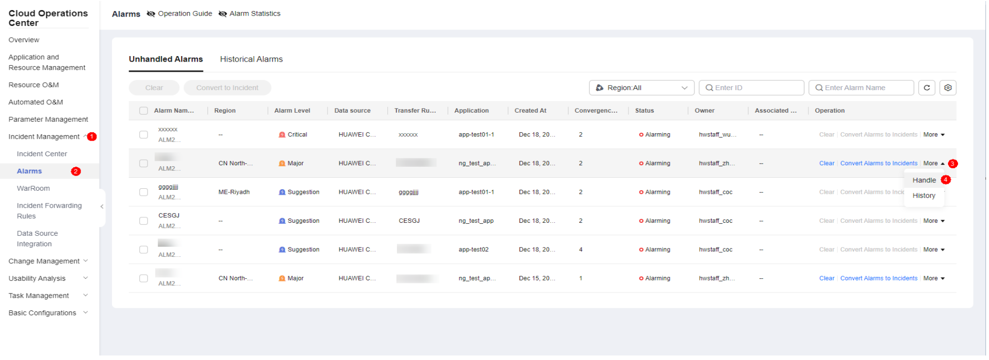
| Parameter | Mandatory | Radio Button/Checkbox | Description |
|---|---|---|---|
| Name | Yes | / | Name of a notification instance. Fuzzy search can be performed based on the notification name. |
| Type | Yes | Radio button | Level-1 category of incident notifications, which is classified by application type. |
| Template | Yes | Checkbox | Notification content template, which is built in the system. The template list varies depending on the notification type. After a template is selected, the template is displayed when you hover the cursor over it. |
| Notification Scope | Yes | Checkbox | When you select a service, such as Service A, and the incident ticket also indicates Service A without considering other matching rules, the subscription instance will take effect and notifications will be sent based on that subscription instance. |
| Recipient | Yes | If you select **Shift**, you can select a single scenario and multiple roles. If you select **Individual**, you can select multiple users. | Recipient who receives notifications. When set to **Shift**, the notification module will automatically retrieve a list of personnel under the current schedule and send notifications to the corresponding individuals. When set to **Individual**, notifications will be sent directly to the corresponding individuals. |

| Parameter | Mandatory | Radio Button/ Checkbox | Description |
|---|---|---|---|
| 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 Incident Levels. |
| Notification Rule - Incident Category | No | Checkbox | Category of an incident ticket. Multiple options are available. |
| 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 |

## Step 4: Handle Alarms

1. Log in to **COC**.
1. In the navigation pane on the left, choose **Incident Management** > **Alarms**.
2. In the alarm list, clear alarms, convert alarms to incidents, handle alarms, and view historical alarms.

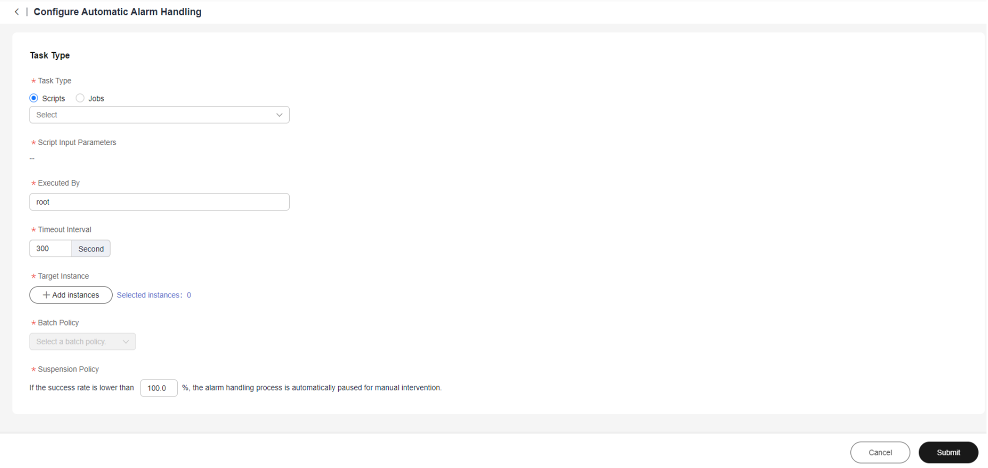
**Figure 1-12** Alarm list



| Alarm Nam... | Region | Alarm Level | Data source | Transfer Ru... | Application | Created At | Convergenc... | Status | Owner | Associated ... | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| xxxxxx<br>ALM2... | -- | Critical | HUAWEI C... | xxxxxx | app-test01-1 | Dec 18, 20... | 2 | Alarming | hwstaff_wu... | -- | Clear \| Convert Alarms to Incidents \| More |
| [redacted]<br>ALM2... | CN North-... | Major | HUAWEI C... | [redacted] | ng_test_ap... | Dec 18, 20... | 2 | Alarming | hwstaff_zh... | -- | Clear \| Convert Alarms to Incidents \| More |
| ggggjjjj<br>ALM2... | ME-Riyadh | Suggestion | HUAWEI C... | ggggjjjj | app-test01-1 | Dec 18, 20... | 2 | Alarming | hwstaff_coc | -- | Clear \| Convert Alarms to Incic |
| CESGJ<br>ALM2... | -- | Suggestion | HUAWEI C... | CESGJ | ng_test_app | Dec 18, 20... | 2 | Alarming | hwstaff_coc | -- | Clear \| Convert Alarms to Incidents \| More |
| [redacted]<br>ALM2... | -- | Suggestion | HUAWEI C... | [redacted] | app-test02 | Dec 18, 20... | 4 | Alarming | hwstaff_coc | -- | Clear \| Convert Alarms to Incidents \| More |
| [redacted]<br>ALM2... | CN North-... | Major | HUAWEI C... | [redacted] | ng_test_ap... | Dec 15, 20... | 1 | Alarming | hwstaff_zh... | -- | Clear \| Convert Alarms to Incidents \| More |

3. On the automatic alarm handling page, you can select scripts or jobs and select target instances for automatic alarm handing.

**Figure 1-13** Automatic alarm handling



* Task Type

● Scripts ○ Jobs

* Script Input Parameters

--

* Executed By

root

* Timeout Interval

300 Second

* Target Instance

Selected instances: 0

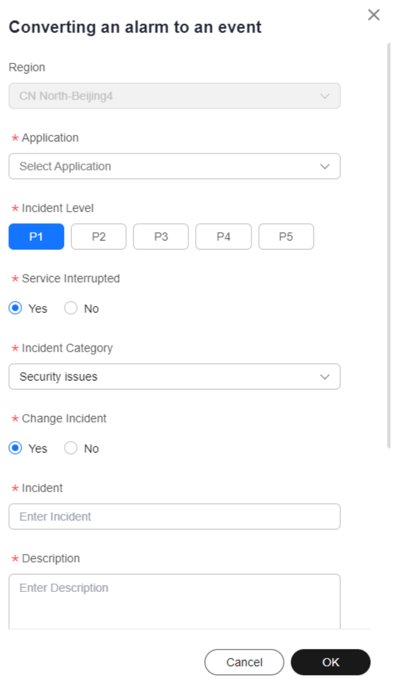
* Batch Policy

* Suspension Policy

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

4. Click **Convert Alarms to Incidents**. In the displayed dialog box, set fields such as **Application**, **Incident Level**, and **Owner**, and click **OK**. The system will send notifications to the owner according to the notification rule.

**Figure 1-14** Converting an alarm to an incident



**Converting an alarm to an event**

Region

CN North-Beijing4

* Application

Select Application

* Incident Level

P1 | P2 | P3 | P4 | P5

* Service Interrupted

● Yes ○ No

* Incident Category

Security issues

* Change Incident

● Yes ○ No

* Incident

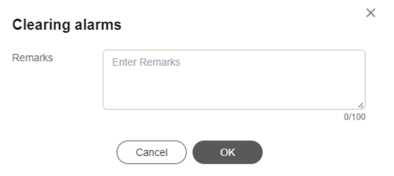
Enter Incident

* Description

Enter Description

5. Click **Clear** to clear the current alarm. The notification alarm is then displayed on the **Historical Alarms** tab.

**Figure 1-15** Clearing alarms



**Clearing alarms**

Remarks

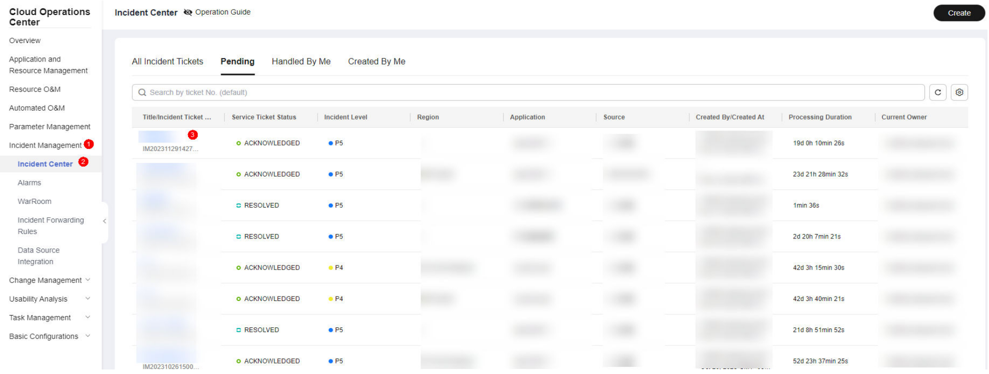
Enter Remarks

0/100

## Step 5: Convert Alarms to Incidents

1. Log in to **COC**.
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 ticket number to access the incident details page.

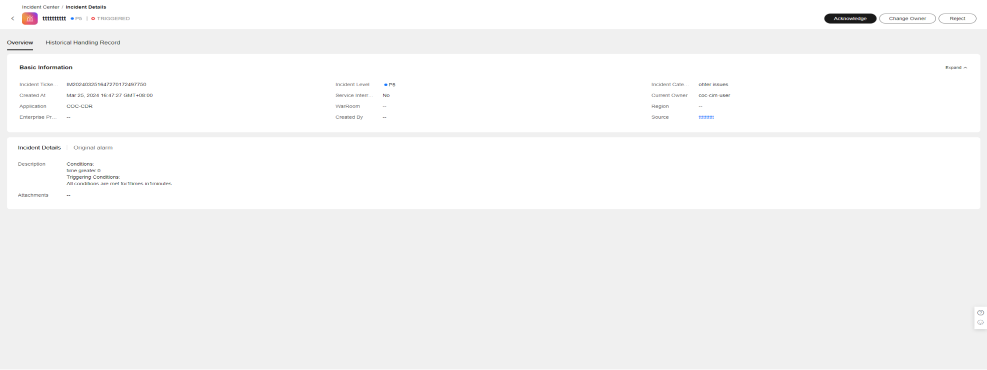
**Figure 1-16** Clicking an incident ticket number



| Title/Incident Ticket ... | Service Ticket Status | Incident Level | Region | Application | Source | Created By/Created At | Processing Duration | Current Owner |
|---|---|---|---|---|---|---|---|---|
| IM202311291427... | ACKNOWLEDGED | P5 | | | | | 19d 0h 10min 26s | |
| | ACKNOWLEDGED | P5 | | | | | 23d 21h 28min 32s | |
| | RESOLVED | P5 | | | | | 1min 36s | |
| | RESOLVED | P5 | | | | | 2d 20h 7min 21s | |
| | ACKNOWLEDGED | P4 | | | | | 42d 3h 15min 30s | |
| | ACKNOWLEDGED | P4 | | | | | 42d 3h 40min 21s | |
| | RESOLVED | P5 | | | | | 21d 8h 51min 52s | |
| IM202310261500... | ACKNOWLEDGED | P5 | | | | | 52d 23h 37min 25s | |

3. Click **Acknowledge**.

**Figure 1-17** Clicking Acknowledge



Basic Information

Incident Ticke... IM202403251647270172497750
Created At Mar 25, 2024 16:47:27 GMT+08:00
Application COC-CDR
Enterprise Pr... --
Incident Level P5
Service Interr... No
WarRoom --
Created By --
Incident Cate... ohter issues
Current Owner coc-cim-user
Region --
Source tttttttttt

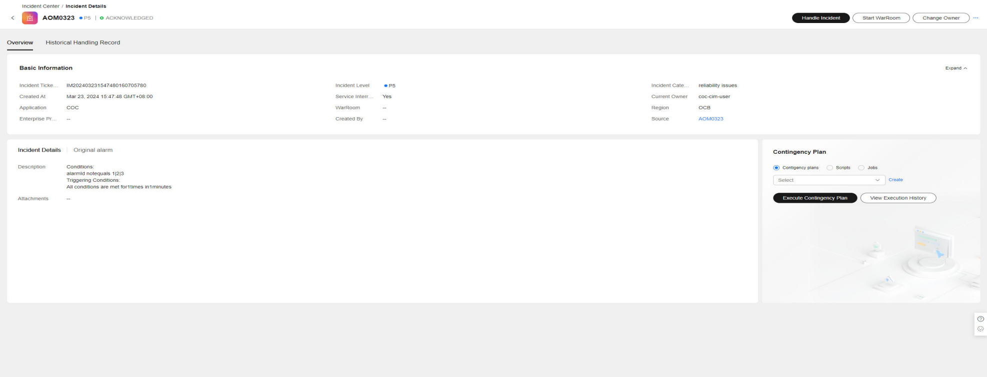
Incident Details | Original alarm

Description Conditions:
time greater 0
Triggering Conditions:
All conditions are met for1times in1minutes

Attachments --

4. Click **Change Owner**.

**Figure 1-18** Clicking Change Owner



Basic Information

Incident Ticke... IM202403231547480160705780
Created At Mar 23, 2024 15:47:48 GMT+08:00
Application COC
Enterprise Pr... --
Incident Level P5
Service Interr... Yes
WarRoom --
Created By --
Incident Cate... reliability issues
Current Owner coc-cim-user
Region OCB
Source AOM0323

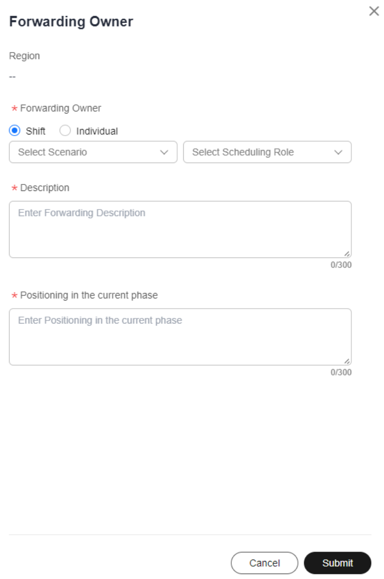
Incident Details | Original alarm

Description Conditions:
alarmId notequals 1|2|3
Triggering Conditions:
All conditions are met for1times in1minutes

Attachments --

5. Enter the forwarding information and click **Submit**.

**Figure 1-19** Entering forwarding information


Forwarding Owner
×
Select Scenario
Select Scheduling Role
Enter Forwarding Description
Enter Positioning in the current phase
Cancel
Submit

Region
--

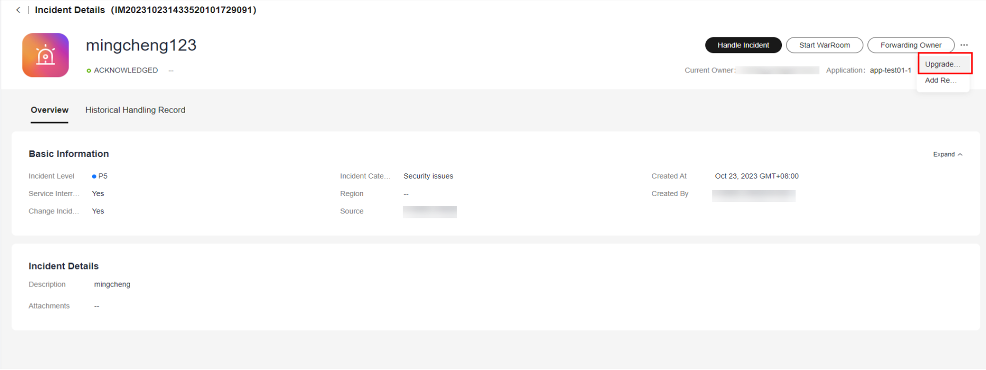
* Forwarding Owner
● Shift ○ Individual

* Description
0/300

* Positioning in the current phase
0/300

6. Click **Upgrade/Downgrade**.

**Figure 1-20** Clicking Upgrade/Downgrade



Incident Details (IM202310231433520101729091)

mingcheng123

ACKNOWLEDGED --

Current Owner: [redacted] Application: app-test01-1

Basic Information

Incident Level P5

Service Interr... Yes

Change Incid... Yes

Incident Cate... Security issues

Region --

Source [redacted]

Created At Oct 23, 2023 GMT+08:00

Created By [redacted]

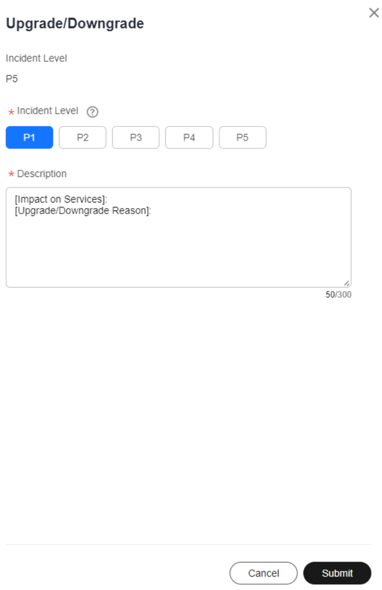
Incident Details

Description mingcheng

Attachments --

7. Enter the upgrade or downgrade information and click **Submit**.

**Figure 1-21** Entering upgrade and downgrade information



Upgrade/Downgrade

Incident Level

P5

* Incident Level

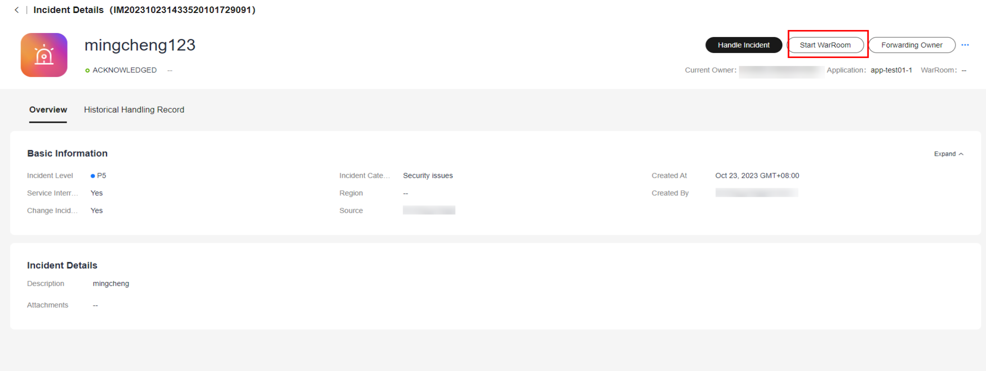
* Description

[Impact on Services]:
[Upgrade/Downgrade Reason]:

50/300

8. Click **Start WarRoom**.

**Figure 1-22** Clicking Start WarRoom



Incident Details (IM202310231433520101729091)

mingcheng123

ACKNOWLEDGED --

Current Owner: [redacted] Application: app-test01-1 WarRoom: --

Basic Information

Incident Level P5

Service Interr... Yes

Change Incid... Yes

Incident Cate... Security issues

Region --

Source [redacted]

Created At Oct 23, 2023 GMT+08:00

Created By [redacted]

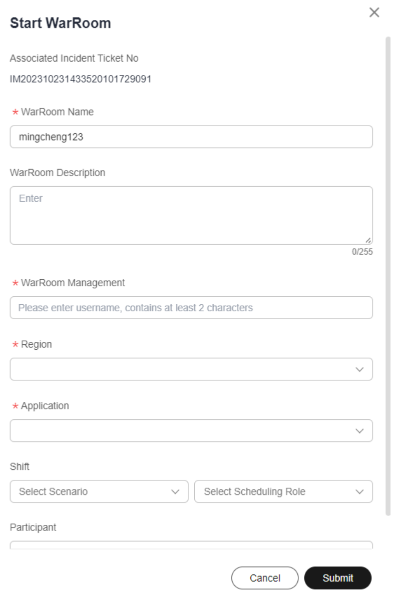
Incident Details

Description mingcheng

Attachments --

9. Enter war room information and click **Submit**.

**Figure 1-23** Entering war room information



Start WarRoom

Associated Incident Ticket No
IM202310231433520101729091

* WarRoom Name
mingcheng123

WarRoom Description
Enter
0/255

* WarRoom Management
Please enter username, contains at least 2 characters

* Region

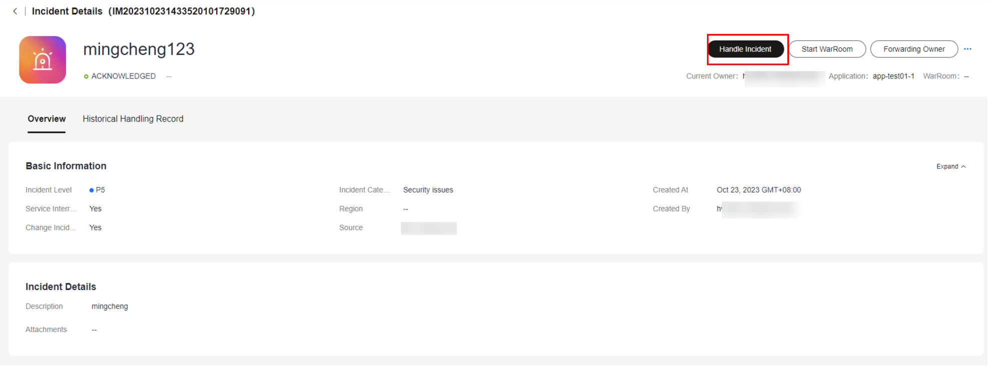
* Application

Shift
Select Scenario | Select Scheduling Role

Participant

10. Click **Handle Incident**.

**Figure 1-24** Clicking Handle Incident



Incident Details (IM202310231433520101729091)

mingcheng123
○ ACKNOWLEDGED --

Current Owner: [redacted] Application: app-test01-1 WarRoom: --

Basic Information

| | | | | | |
|---|---|---|---|---|---|
| Incident Level | ● P5 | Incident Cate... | Security issues | Created At | Oct 23, 2023 GMT+08:00 |
| Service Interr... | Yes | Region | -- | Created By | [redacted] |
| Change Incid... | Yes | Source | [redacted] | | |

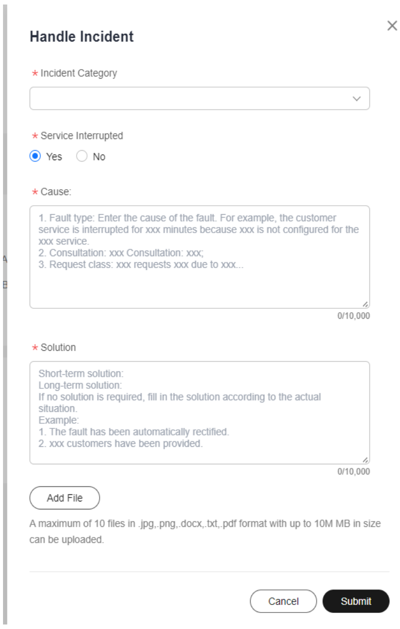
Incident Details

Description mingcheng

Attachments --

11. Enter incident handling information and click **Submit**.

**Figure 1-25** Entering incident handling information



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.

0/10,000

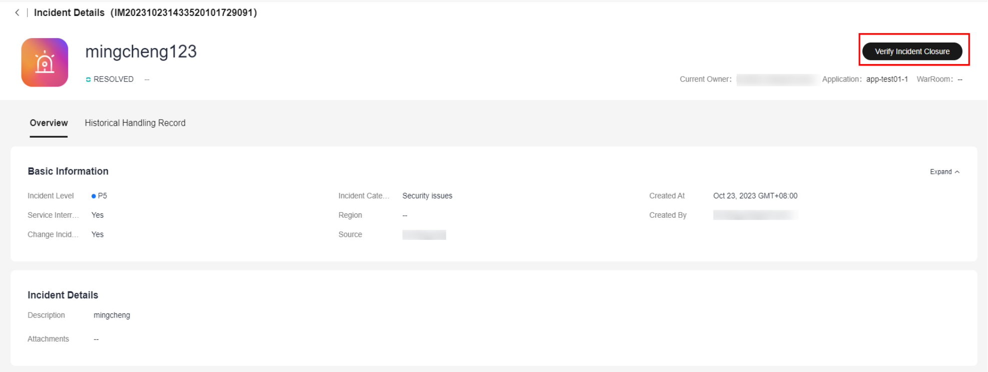
Add File

A maximum of 10 files in .jpg,.png,.docx,.txt,.pdf format with up to 10M MB in size can be uploaded.

Cancel Submit

12. Click **Verify Incident Closure**.

**Figure 1-26** Clicking Verify Incident Closure



Incident Details (IM202310231433520101729091)

mingcheng123

RESOLVED --

Verify Incident Closure

Current Owner: [redacted] Application: app-test01-1 WarRoom: --

Overview Historical Handling Record

Basic Information Expand

Incident Level ● P5 Incident Cate... Security issues Created At Oct 23, 2023 GMT+08:00

Service Interr... Yes Region -- Created By [redacted]

Change Incid... Yes Source [redacted]

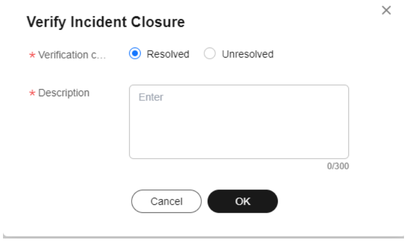
Incident Details

Description mingcheng

Attachments --

13. Enter verification information and click **OK**.

**Figure 1-27** Entering verification information



Verify Incident Closure

* Verification c... ● Resolved ○ Unresolved

* Description Enter

0/300

Cancel OK

# 2 E2E Chaos Engineering

## Scenario

A new application for an e-commerce company has been deployed in the production environment, and they plan to officially launch it for access and traffic. However, their traditional O&M mode is mainly reactive, lacking proactive O&M concepts and tool capabilities. Before the application went live, there was no effective way to identify availability issues, and after it went live, the availability status could not be accurately grasped. The O&M team lacked emergency response capabilities and practical experience. They hope to use chaos engineering to test the application's architectural resilience in the production environment before launching it to ensure that there are no major stability risks during the official launch.

## Solution

Chaos drills drive proactive O&M: Starting from the customer's actual business scenario, we provide end-to-end chaos drill capabilities based on risk analysis, contingency plans, exercise execution, and retrospective improvement.

Fault precipitation mode: We have pioneered a fault scenario analysis method based on a fault-tolerant perspective and have accumulated a library of fault modes from Huawei Cloud SRE's years of experience, which includes over 300 typical fault modes.

- Risk analysis: Analyze the application architecture to identify risks.
- Contingency plan: Designate contingency plans for the identified risks.
- Fault drill: Based on the results of the risk analysis and emergency plans, specify the drill plan and conduct fault drills.
- Review and improvement: After the drill is completed, summarize the drill and output the drill report and improvement items.

## Core Advantages

- Pioneered the FT-FMEA fault scenario analysis method based on a fault-tolerant perspective, gradually incorporating 300+ fault modes.
- Supports multi-dimensional attack scenarios, covering both virtualization and containerization.

- Supports custom attack process orchestration to meet individual customer business needs.

## Prerequisites

An application group has been created on the application management page.

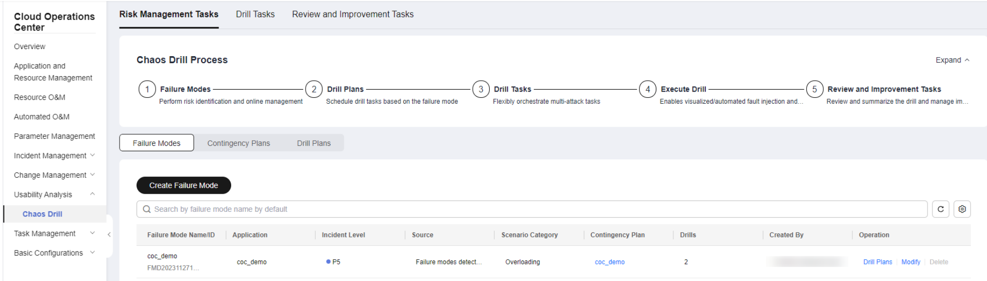
The resources for conducting chaos drills have UniAgent installed. For details, see "Installing the UniAgent".

## Step 1: Failure Mode

Check whether the application to which the target host or container belongs and the incident level are correct.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click **Risk Management Tasks** and then the **Failure Modes** tab.

**Figure 2-1** Failure Modes tab page



Chaos Drill Process

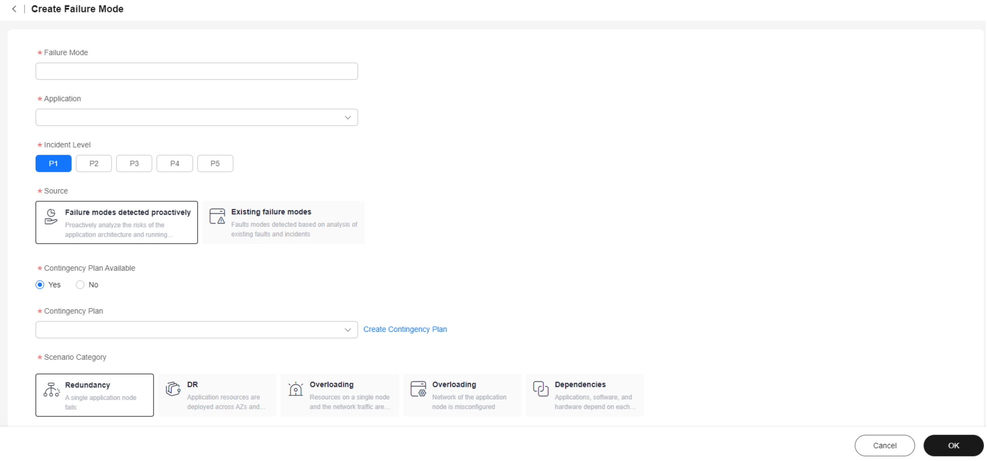
1 Failure Modes: Perform risk identification and online management
2 Drill Plans: Schedule drill tasks based on the failure mode
3 Drill Tasks: Flexibly orchestrate multi-attack tasks
4 Execute Drill: Enables visualized/automated fault injection and...
5 Review and Improvement Tasks: Review and summarize the drill and manage im...

Search by failure mode name by default

| Failure Mode Name/ID | Application | Incident Level | Source | Scenario Category | Contingency Plan | Drills | Created By | Operation |
|---|---|---|---|---|---|---|---|---|
| coc_demo<br>FMD202311271... | coc_demo | ● P5 | Failure modes detect... | Overloading | coc_demo | 2 | [redacted] | Drill Plans \| Modify \| Delete |

3. Enter failure mode information.

**Figure 2-2** Creating a failure mode



* Failure Mode

* 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 AZs and...
- Overloading: Resources on a single node and the network traffic are...
- Overloading: Network of the application node is misconfigured
- Dependencies: Applications, software, and hardware depend on each...

**Table 2-1** Failure mode parameters

| Parameter | Description |
|---|---|
| Failure Mode | Custom failure mode name |
| Application | Application the drill object belongs to |
| Incident Level | See the incident center page. |
| Source | The options are **Failure modes detected proactively** and **Existing failure modes**. |
| Contingency Plan | For details, see the contingency plan section. |
| Scenario Category | Failure scenario. The options are **Redundancy**, **DR**, **Overloading**, **Configuration**, and **Dependencies**. |
| Occurrence Conditions | Possible conditions that cause the failure |

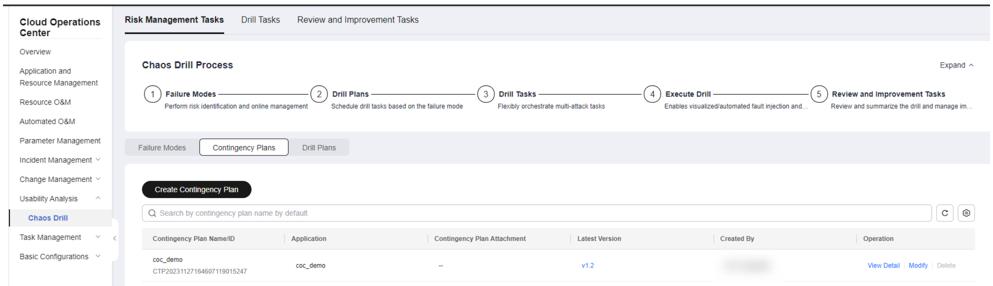
4. Set **Contingency Plan Available**. If you select **Yes**, enter a contingency plan name to search for the plan, select the plan, and click **Save**.

## Step 2: Contingency Plan

Select the application to which the target host, where the fault will be injected, belongs.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click **Risk Management Tasks** and then the **Contingency Plans** tab.

**Figure 2-3** Contingency Plans tab page



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...
5 Review and Improvement Tasks: Review and summarize the drill and manage im...

| Contingency Plan Name/ID | Application | Contingency Plan Attachment | Latest Version | Created By | Operation |
|---|---|---|---|---|---|
| coc_demo<br>CTP20231127164607119015247 | coc_demo | -- | v1.2 | [redacted] | View Detail \| Modify \| Delete |

3. Enter basic information about the contingency plan.

**Figure 2-4** Creating a contingency plan

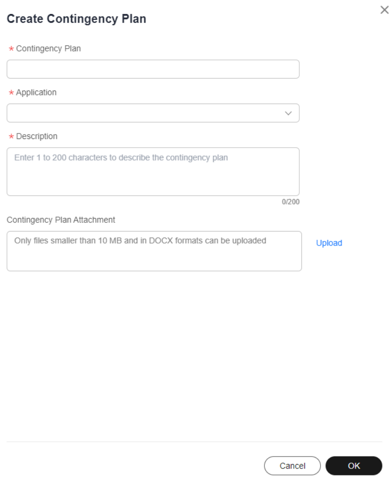

Create Contingency Plan
×
* Contingency Plan
* Application
* Description
Enter 1 to 200 characters to describe the contingency plan
0/200
Contingency Plan Attachment
Only files smaller than 10 MB and in DOCX formats can be uploaded
Upload
Cancel
OK

**Table 2-2** Contingency plan parameters

| Parameter | Description |
|---|---|
| Contingency Plan | Custom contingency plan name |
| Application | Application to which the target host or container belongs |
| Description | Description about the contingency plan |
| Contingency Plan Attachment | Emergency recovery guide for practicing abnormal situations |

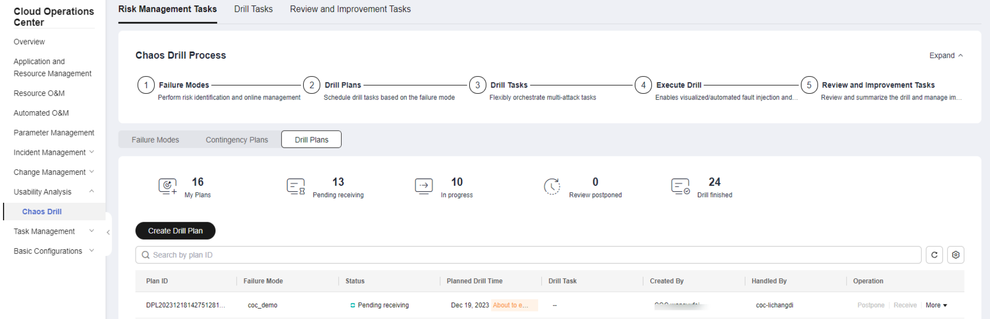
4. During the drill, unexpected abnormal situations may occur, so you should prepare emergency measures in advance and have the emergency recovery guide ready. Click **Upload** to upload it and then click **OK**.

## Step 3: Drill Planning

You can designate an executor to create a drill plan. The executor creates a drill task by receiving a service ticket and associates it with a failure more and region.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click **Risk Management Tasks** and then the **Drill Plans** tab.

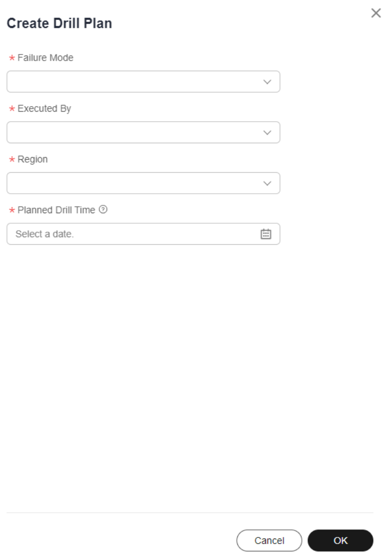
**Figure 2-5** Drill Plans tab page



| Plan ID | Failure Mode | Status | Planned Drill Time | Drill Task | Created By | Handled By | Operation |
|---|---|---|---|---|---|---|---|
| DPL20231218142751281... | coc_demo | Pending receiving | Dec 19, 2023 About to e... | -- | [redacted] | coc-lichangdi | Postpone Receive More |

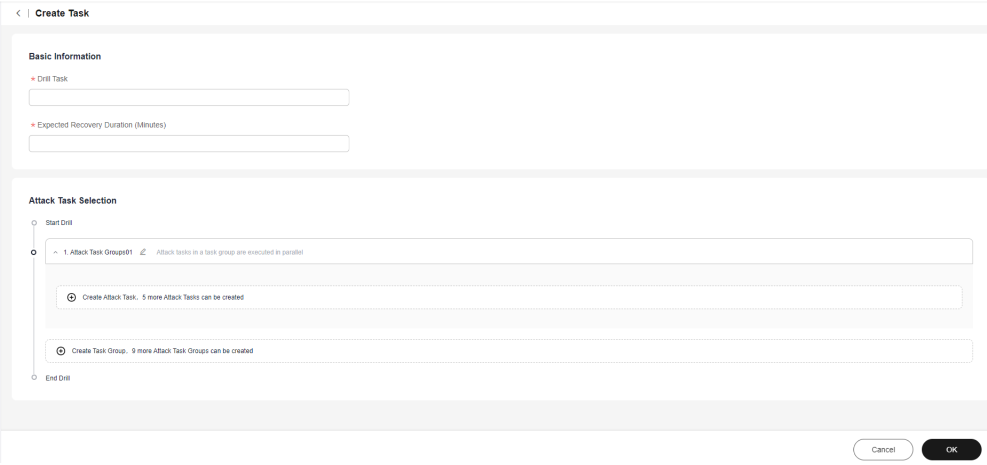
3. Click **Create Drill Plan**. In the displayed dialog box, set **Failure Mode**, **Executed By**, **Region**, and **Planned Drill Time**, and click **OK**.

**Figure 2-6** Creating a drill plan



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

**Figure 2-7** Switching to the page for creating a drill task

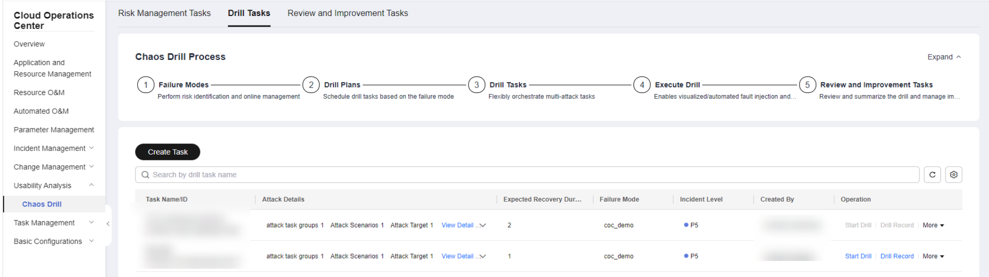

Create Task
Basic Information
* Drill Task
* Expected Recovery Duration (Minutes)
Attack Task Selection
Start Drill
1. Attack Task Groups01
Attack tasks in a task group are executed in parallel
Create Attack Task，5 more Attack Tasks can be created
Create Task Group，9 more Attack Task Groups can be created
End Drill
Cancel
OK

## Step 4: Drill Task

Create a drill task on COC.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click the **Drill Tasks** tab.
3. Click **Create Task**.

**Figure 2-8** Creating a drill task



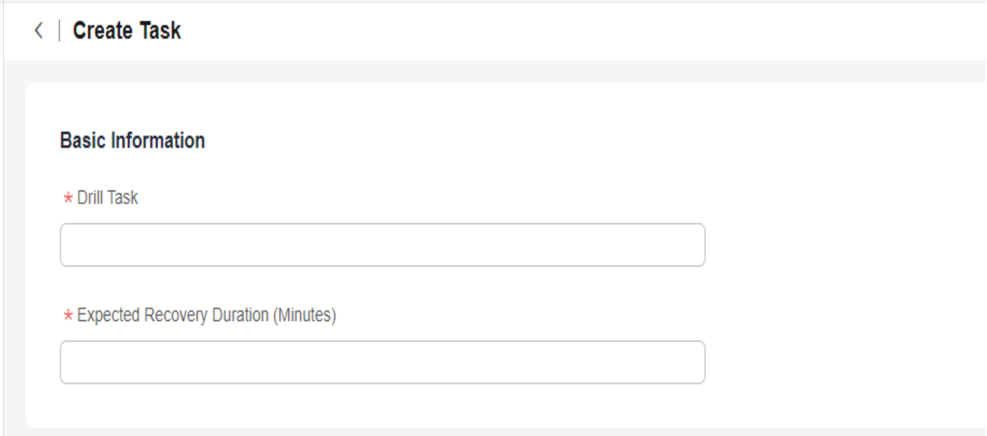
Chaos Drill Process

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...
5 Review and Improvement Tasks — Review and summarize the drill and manage im...

| Task Name/ID | Attack Details | Expected Recovery Dur... | Failure Mode | Incident Level | Created By | Operation |
|---|---|---|---|---|---|---|
| [redacted] | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 2 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |
| [redacted] | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 1 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |

4. Enter basic information about the drill task, including **Drill Task** and **Expected Recovery Duration (Minutes)**.

**Figure 2-9** Basic information

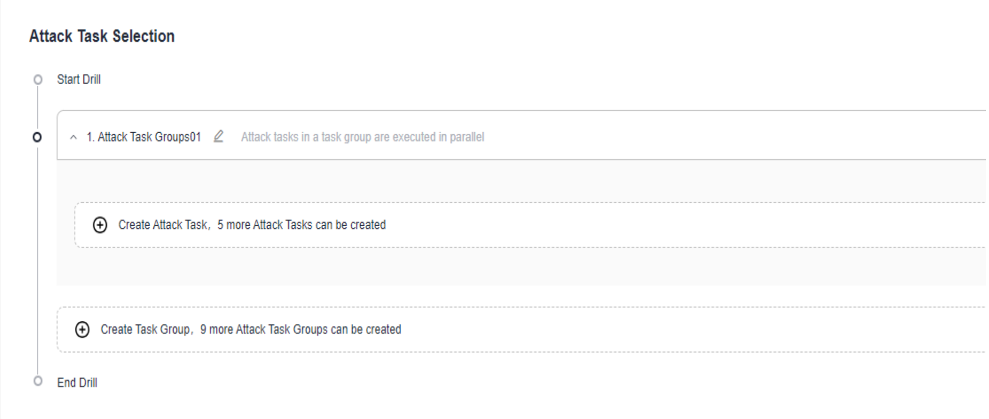


* Drill Task

* Expected Recovery Duration (Minutes)

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 2-10** Selecting an attack task



Attack Task Selection

Start Drill

1. Attack Task Groups01 Attack tasks in a task group are executed in parallel

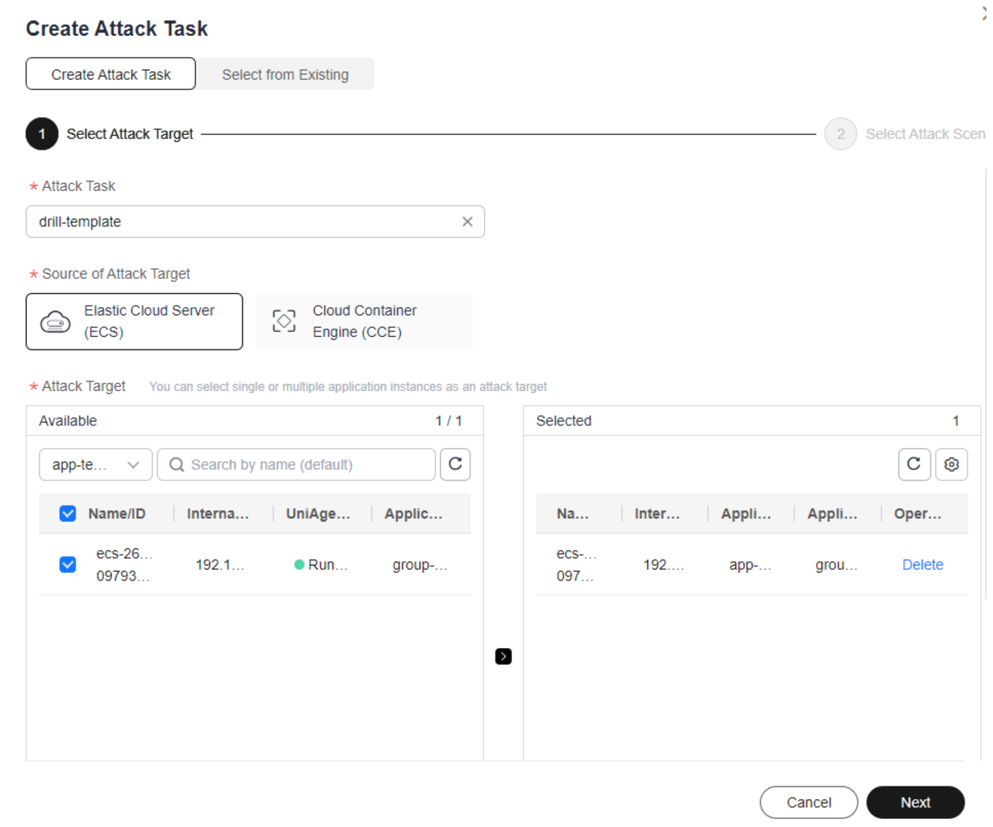
Create Attack Task, 5 more Attack Tasks can be created

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

End Drill

6. On the displayed **Create Attack Task** page, you can select **Create Attack Task** or **Select from Existing**. If you have not created an attack task before, you will need to select **Create Attack Task**. However, if you have created attack tasks previously, you can select **Select from Existing**.
7. Creating an attack task: Select an attack target and then an attack scenario. Different attack targets correspond to different attack scenarios. Enter the attack task name. The attack target source can be **Elastic Cloud Server (ECS)** or **Cloud Container Engine (CCE)**. If you select the former, you will need to select the corresponding server from the list below and click **Next**.

**Figure 2-11** Selecting ECS as the attack target source



Create Attack Task

Create Attack Task | Select from Existing

1 Select Attack Target — 2 Select Attack Scen

* Attack Task

drill-template

* Source of Attack Target

Elastic Cloud Server (ECS) | Cloud Container Engine (CCE)

* Attack Target You can select single or multiple application instances as an attack target

Available 1 / 1

app-te... Search by name (default)

| ☑ Name/ID | Interna... | UniAge... | Applic... |
|---|---|---|---|
| ☑ ecs-26...<br>09793... | 192.1... | ● Run... | group-... |

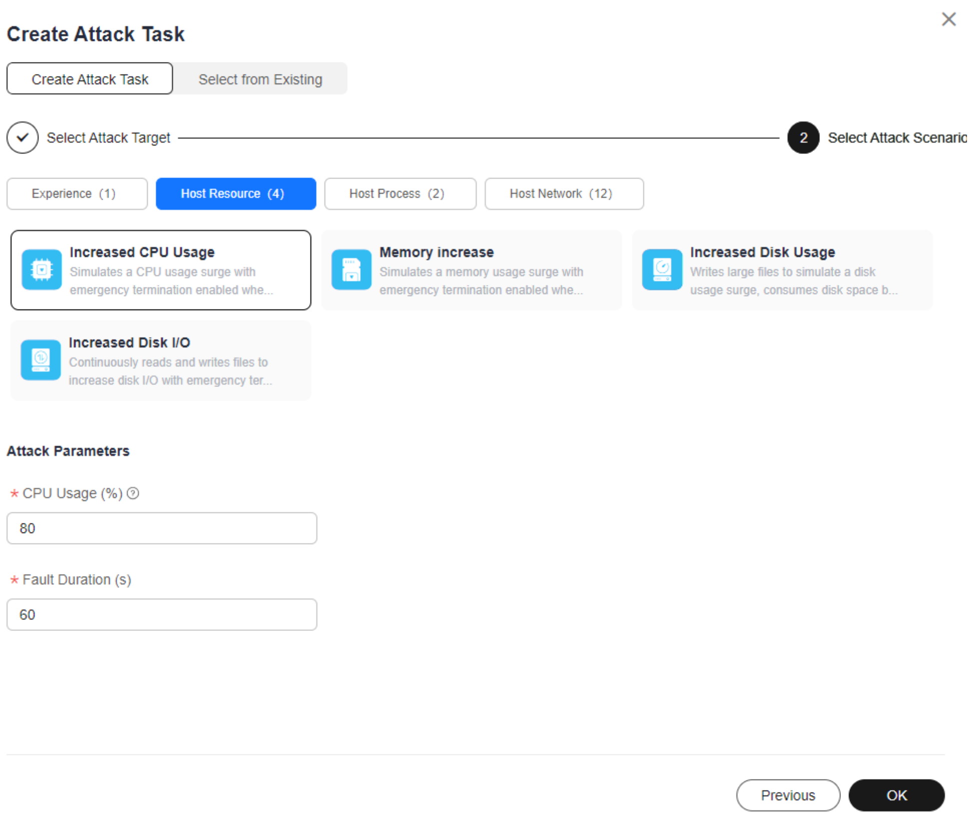
Selected 1

| Na... | Inter... | Appli... | Appli... | Oper... |
|---|---|---|---|---|
| ecs-...<br>097... | 192.... | app-... | grou... | Delete |

Cancel Next

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

**Figure 2-12** ECS attack scenarios



Create Attack Task

Create Attack Task | Select from Existing

✓ Select Attack Target — 2 Select Attack Scenaric

Experience (1) | Host Resource (4) | Host Process (2) | Host Network (12)

**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...

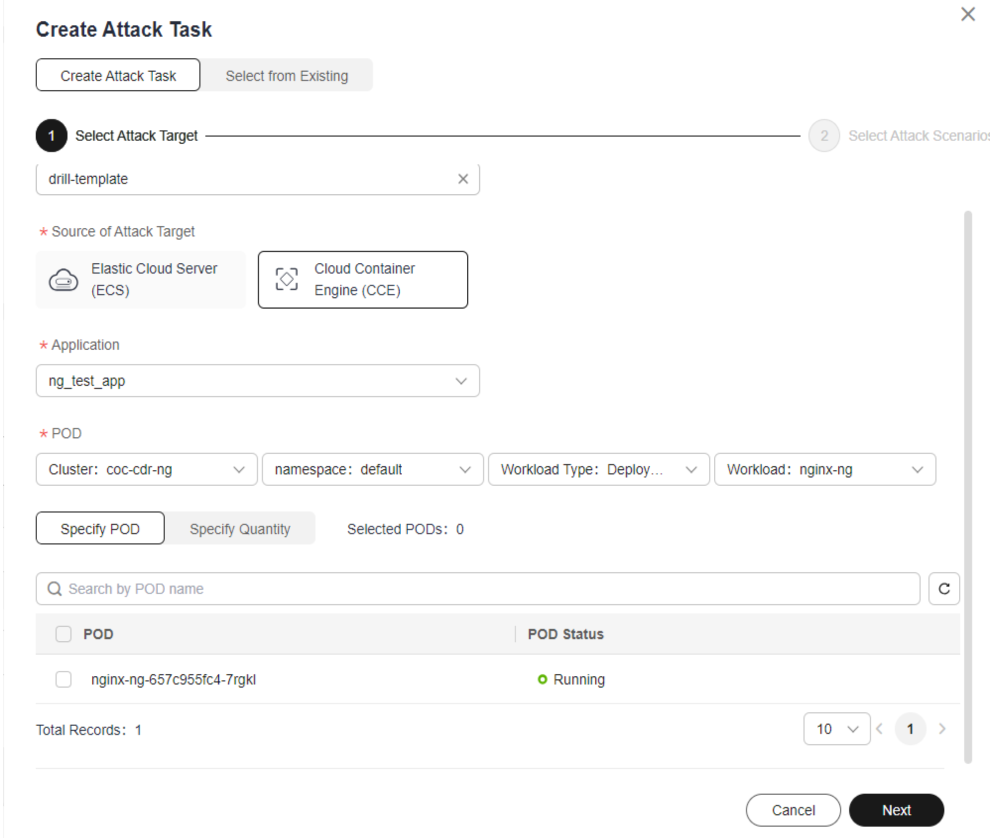
Attack Parameters

* CPU Usage (%): 80

* Fault Duration (s): 60

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

**Figure 2-13** Selecting CCE as the attack target source and specifying a pod



drill-template

* Source of Attack Target

* Application: ng_test_app

* POD

Cluster: coc-cdr-ng

namespace: default

Workload Type: Deploy...

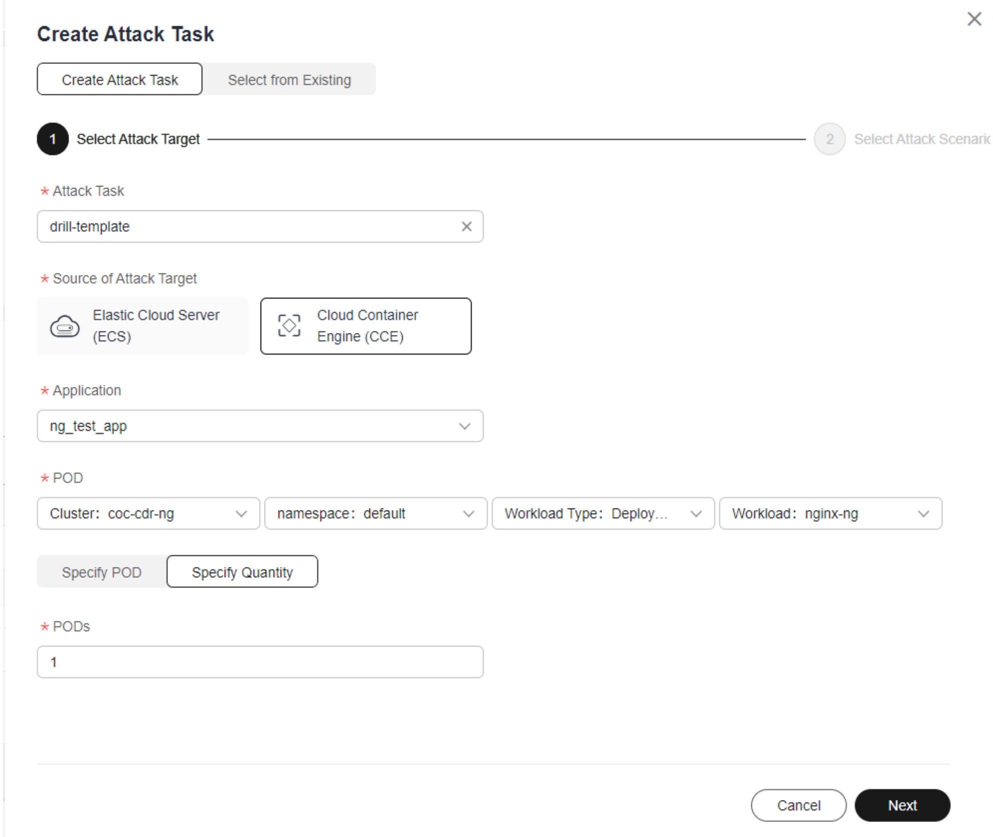
Workload: nginx-ng

Selected PODs: 0

| POD | POD Status |
|---|---|
| nginx-ng-657c955fc4-7rgkl | Running |

Total Records: 1

**Figure 2-14** Selecting CCE as the attack target source and specifying the quantity



Create Attack Task

Create Attack Task | Select from Existing

1 Select Attack Target — 2 Select Attack Scenari

* Attack Task: drill-template

* Source of Attack Target: Elastic Cloud Server (ECS) | Cloud Container Engine (CCE)

* Application: ng_test_app

* POD: Cluster：coc-cdr-ng | namespace：default | Workload Type：Deploy... | Workload：nginx-ng

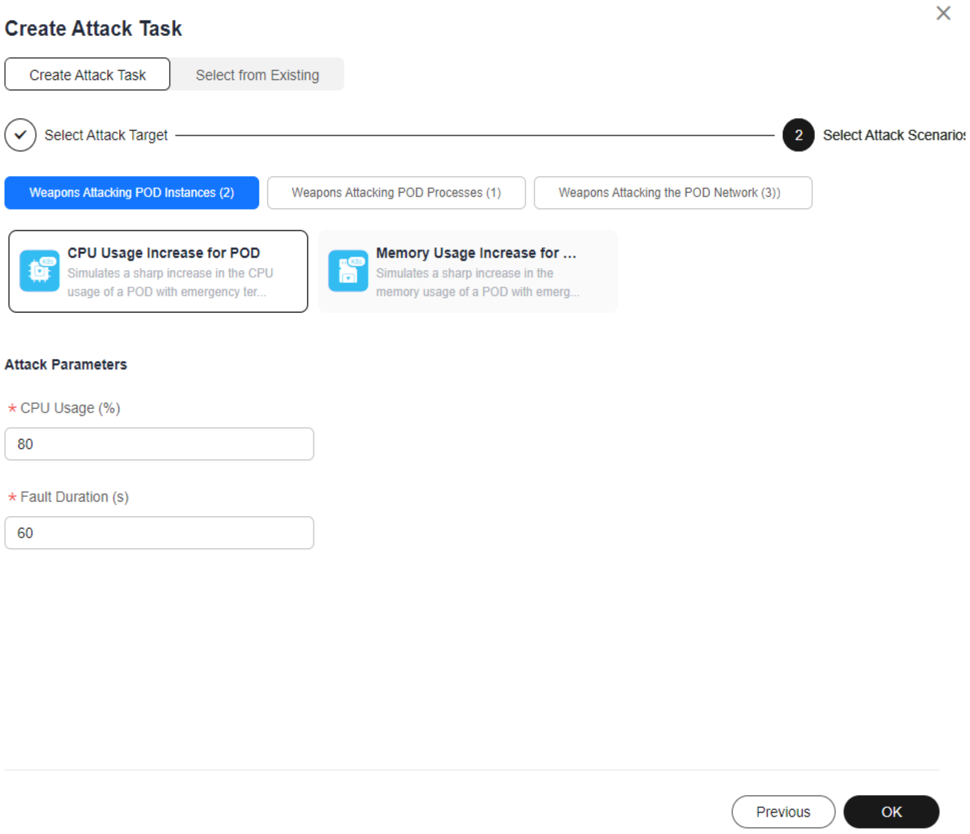
Specify POD | Specify Quantity

* PODs: 1

Cancel | Next

10. 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 2-15** CCE attack scenarios



Create Attack Task

Create Attack Task
Select from Existing
Select Attack Target
2
Select Attack Scenarios
Weapons Attacking POD Instances (2)
Weapons Attacking POD Processes (1)
Weapons Attacking the POD Network (3))

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...

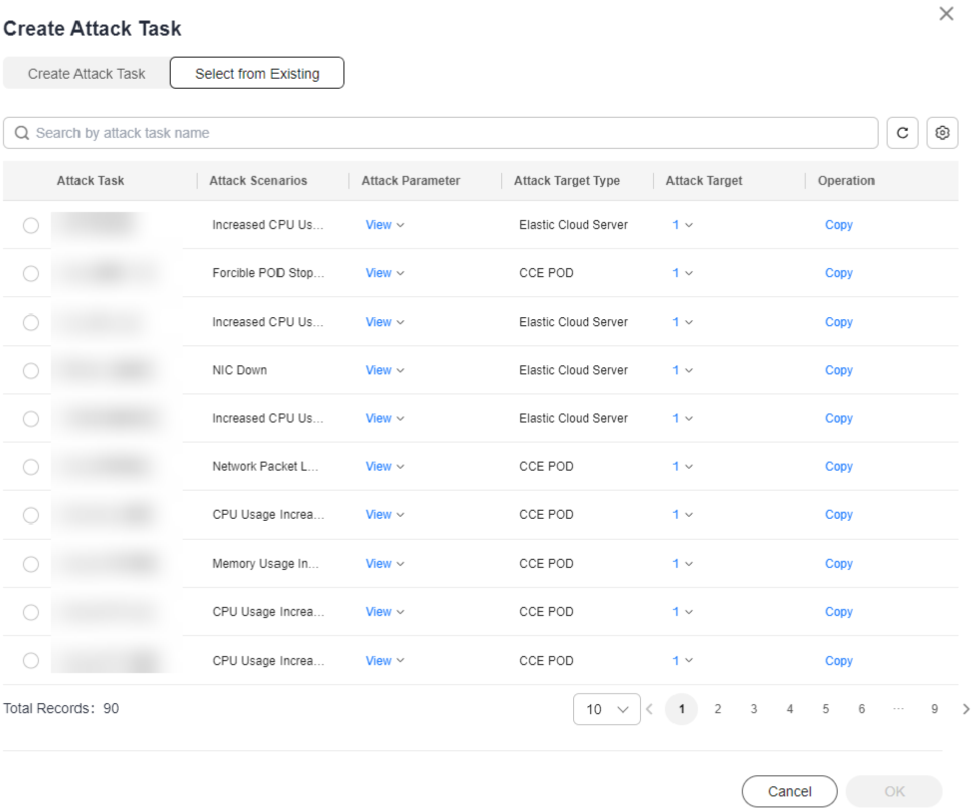
Attack Parameters

* CPU Usage (%)
80

* Fault Duration (s)
60

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

**Figure 2-16** Selecting an existing attack task



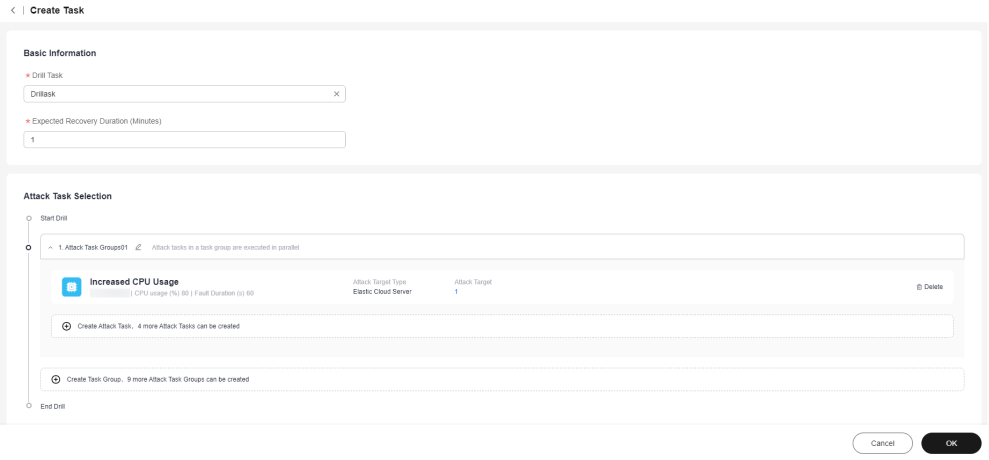
Create Attack Task

| | Attack Task | Attack Scenarios | Attack Parameter | Attack Target Type | Attack Target | Operation |
|---|---|---|---|---|---|---|
| ○ | [redacted] | Increased CPU Us... | View ⌄ | Elastic Cloud Server | 1 ⌄ | Copy |
| ○ | [redacted] | Forcible POD Stop... | View ⌄ | CCE POD | 1 ⌄ | Copy |
| ○ | [redacted] | Increased CPU Us... | View ⌄ | Elastic Cloud Server | 1 ⌄ | Copy |
| ○ | [redacted] | NIC Down | View ⌄ | Elastic Cloud Server | 1 ⌄ | Copy |
| ○ | [redacted] | Increased CPU Us... | View ⌄ | Elastic Cloud Server | 1 ⌄ | Copy |
| ○ | [redacted] | Network Packet L... | View ⌄ | CCE POD | 1 ⌄ | Copy |
| ○ | [redacted] | CPU Usage Increa... | View ⌄ | CCE POD | 1 ⌄ | Copy |
| ○ | [redacted] | Memory Usage In... | View ⌄ | CCE POD | 1 ⌄ | Copy |
| ○ | [redacted] | CPU Usage Increa... | View ⌄ | CCE POD | 1 ⌄ | Copy |
| ○ | [redacted] | CPU Usage Increa... | View ⌄ | CCE POD | 1 ⌄ | Copy |

Total Records: 90

12. Click **OK**. The drill task is created.

**Figure 2-17** Clicking OK



< | Create Task

Basic Information

* Drill Task: Drillask

* Expected Recovery Duration (Minutes): 1

Attack Task Selection

Start Drill

1. Attack Task Groups01 — Attack tasks in a task group are executed in parallel

Increased CPU Usage — | CPU usage (%) 80 | Fault Duration (s) 60 — Attack Target Type: Elastic Cloud Server — Attack Target: 1

Create Attack Task, 4 more Attack Tasks can be created

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

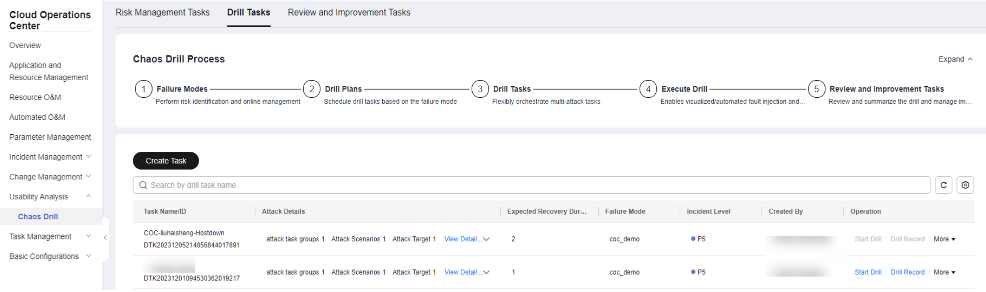
End Drill

## Step 5: Drill Report

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

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click the **Drill Tasks** tab.

**Figure 2-18** Drill task list



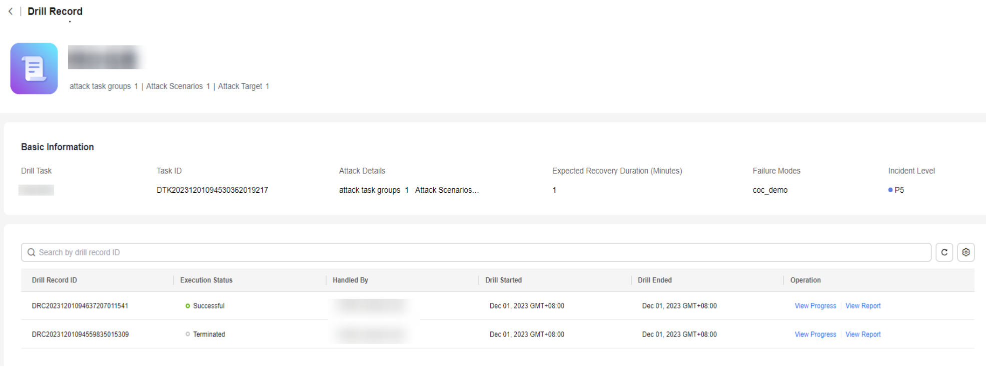
Chaos Drill Process

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...
5. Review and Improvement Tasks: Review and summarize the drill and manage im...

| Task Name/ID | Attack Details | Expected Recovery Dur... | Failure Mode | Incident Level | Created By | Operation |
|---|---|---|---|---|---|---|
| COC-liuhaisheng-Hostdown<br>DTK20231205214856844017891 | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 2 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |
| [redacted]<br>DTK20231201094530362019217 | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 1 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |

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

**Figure 2-19** Drill record list



[redacted]

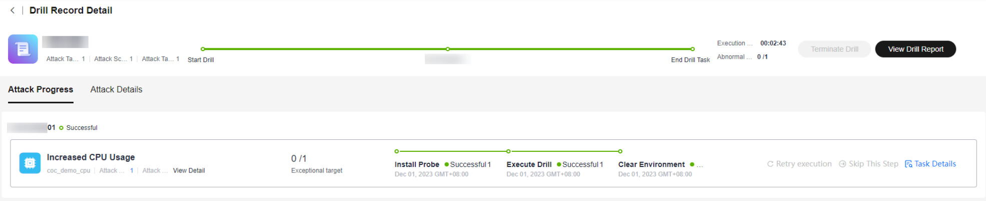
attack task groups 1 | Attack Scenarios 1 | Attack Target 1

Basic Information

| Drill Task | Task ID | Attack Details | Expected Recovery Duration (Minutes) | Failure Modes | Incident Level |
|---|---|---|---|---|---|
| [redacted] | DTK20231201094530362019217 | attack task groups 1 Attack Scenarios... | 1 | coc_demo | ● P5 |

| Drill Record ID | Execution Status | Handled By | Drill Started | Drill Ended | Operation |
|---|---|---|---|---|---|
| DRC20231201094637207011541 | ○ Successful | [redacted] | Dec 01, 2023 GMT+08:00 | Dec 01, 2023 GMT+08:00 | View Progress \| View Report |
| DRC20231201094559835015309 | ○ Terminated | [redacted] | Dec 01, 2023 GMT+08:00 | Dec 01, 2023 GMT+08:00 | View Progress \| View Report |

**Figure 2-20** Drill Record Detail page



[redacted]

Execution ... 00:02:43
Abnormal ... 0 /1

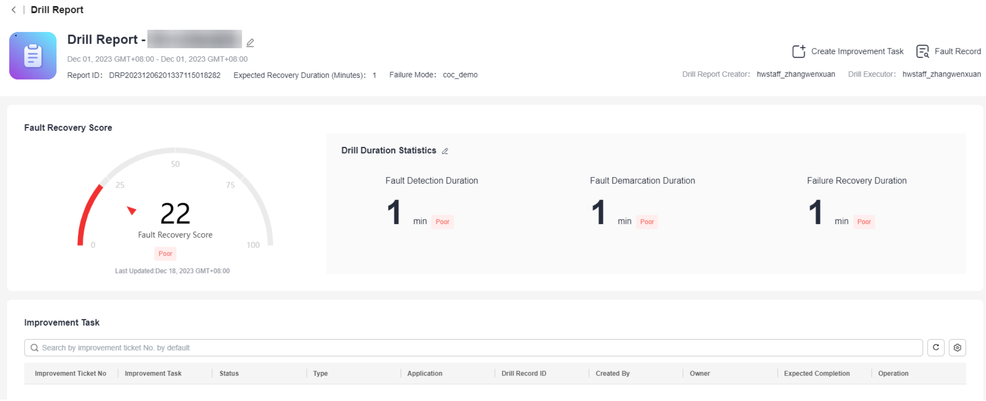
[redacted]01 ○ Successful

Increased CPU Usage
coc_demo_cpu | Attack ... 1 | Attack ... View Detail
0 /1 Exceptional target

Install Probe ● Successful 1 Dec 01, 2023 GMT+08:00
Execute Drill ● Successful 1 Dec 01, 2023 GMT+08:00
Clear Environment ● ... Dec 01, 2023 GMT+08:00

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

**Figure 2-21** Drill report details



Drill Report - [redacted]

Dec 01, 2023 GMT+08:00 - Dec 01, 2023 GMT+08:00

Report ID: DRP20231206201337115018282 Expected Recovery Duration (Minutes): 1 Failure Mode: coc_demo

Drill Report Creator: hwstaff_zhangwenxuan Drill Executor: hwstaff_zhangwenxuan

Fault Recovery Score

22 Fault Recovery Score Poor

Last Updated:Dec 18, 2023 GMT+08:00

Drill Duration Statistics

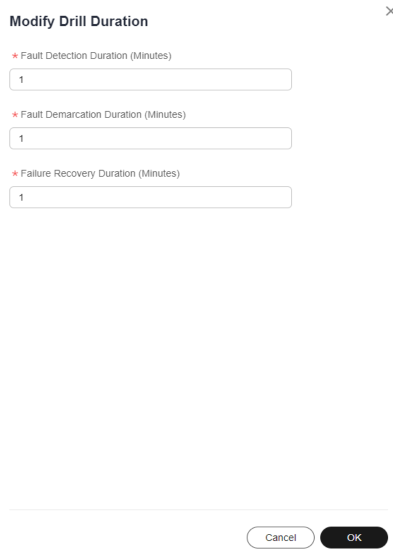
| Fault Detection Duration | Fault Demarcation Duration | Failure Recovery Duration |
|---|---|---|
| 1 min Poor | 1 min Poor | 1 min Poor |

Improvement Task

| Improvement Ticket No | Improvement Task | Status | Type | Application | Drill Record ID | Created By | Owner | Expected Completion | Operation |
|---|---|---|---|---|---|---|---|---|---|

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

**Figure 2-22** Modify Drill Duration



**Modify Drill Duration**

* Fault Detection Duration (Minutes)
1

* Fault Demarcation Duration (Minutes)
1

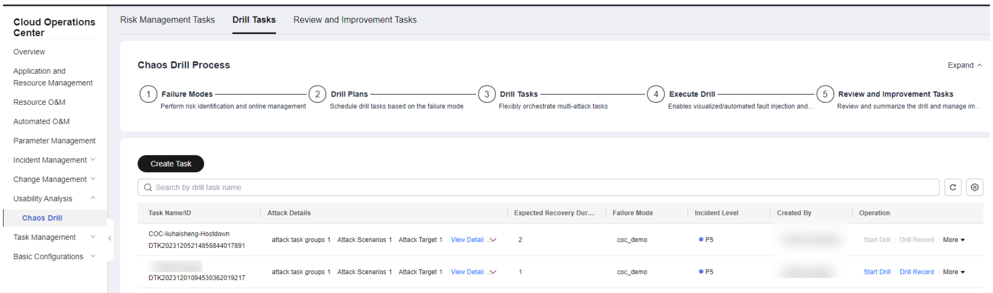
* Failure Recovery Duration (Minutes)
1

## Step 6: Review and Improvement

Once you have created a drill report, you can include suggestions for improvement.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**. On the displayed page, click the **Drill Tasks** tab.

**Figure 2-23** Drill task list



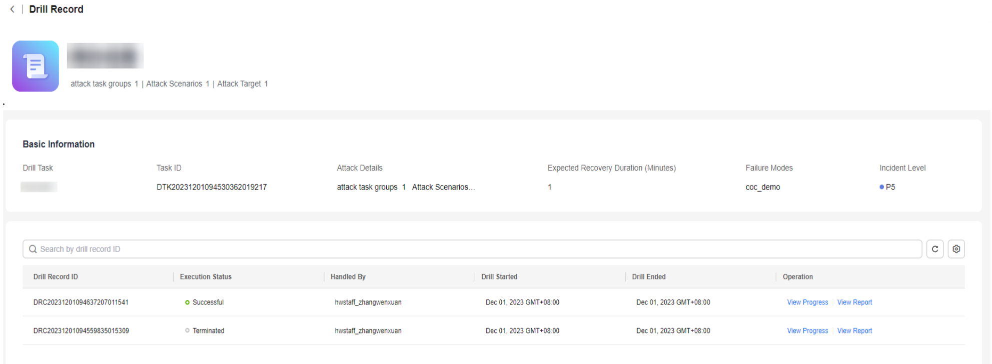
**Chaos Drill Process**

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...
5 **Review and Improvement Tasks** Review and summarize the drill and manage im...

| Task Name/ID | Attack Details | Expected Recovery Dur... | Failure Mode | Incident Level | Created By | Operation |
|---|---|---|---|---|---|---|
| COC-liuhaisheng-Hostdown<br>DTK20231205214856844017891 | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 2 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |
| [redacted]<br>DTK20231201094530362019217 | attack task groups 1 Attack Scenarios 1 Attack Target 1 View Detail ... | 1 | coc_demo | ● P5 | [redacted] | Start Drill \| Drill Record \| More ▾ |

3. Click **Drill Record**.
4. Access the drill record list and click **View Report** or **Create Report**.

**Figure 2-24** Drill record list



< | Drill Record

[redacted]

attack task groups 1 | Attack Scenarios 1 | Attack Target 1

Basic Information

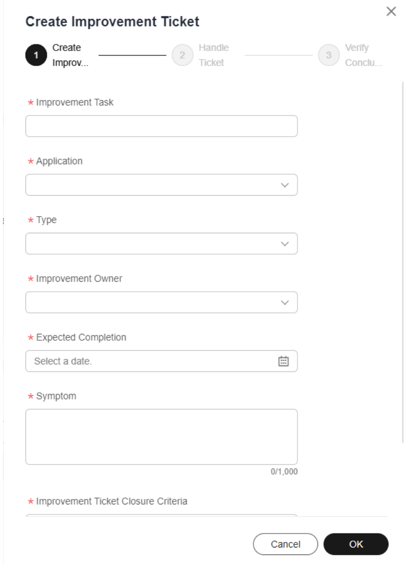
| Drill Task | Task ID | Attack Details | Expected Recovery Duration (Minutes) | Failure Modes | Incident Level |
|---|---|---|---|---|---|
| [redacted] | DTK20231201094530362019217 | attack task groups 1 Attack Scenarios... | 1 | coc_demo | ● P5 |

Search by drill record ID

| Drill Record ID | Execution Status | Handled By | Drill Started | Drill Ended | Operation |
|---|---|---|---|---|---|
| DRC20231201094637207011541 | ○ Successful | hwstaff_zhangwenxuan | Dec 01, 2023 GMT+08:00 | Dec 01, 2023 GMT+08:00 | View Progress \| View Report |
| DRC20231201094559835015309 | ○ Terminated | hwstaff_zhangwenxuan | Dec 01, 2023 GMT+08:00 | Dec 01, 2023 GMT+08:00 | View Progress \| View Report |

5. Access the drill report details page, click **Create Improvement Ticket** on the right, and enter information about the improvement ticket.

**Figure 2-25** Creating an improvement ticket



Create Improvement Ticket

1 Create Improv... — 2 Handle Ticket — 3 Verify Conclu...

* Improvement Task

* Application

* Type

* Improvement Owner

* Expected Completion

Select a date.

* Symptom

0/1,000

* Improvement Ticket Closure Criteria

**Table 2-3** Improvement ticket parameters

| Parameter | Description |
|---|---|
| Improvement Task | Improvement task name |
| Application | Application the improvement task belongs to |
| Type | Type of the improvement task |
| Improvement Owner | Owner of the improvement task |
| Expected Completion | Expected completion time of the improvement task |
| Symptom | Symptom |

| Parameter | Description |
|---|---|
| Improvement Ticket Closure Criteria | Criteria for the closure of the improvement ticket |

# 3 One-Stop Resource O&M

## Scenario

An O&M engineer at an e-commerce company noticed that compliance issues with cloud resources were prominent in their daily work, particularly with regards to OS compliance risks. This raised concerns among customers about the security and compliance of the OS on the cloud. It was necessary to periodically check the compliance of the host OS patches to avoid vulnerabilities caused by missing patches, which could lead to business losses. There was no unified OS compliance management or self-closed loop tool on the cloud, making it difficult to fix compliance issues or seek help from Huawei. The goal was to automate the scanning of OS patches and promptly fix patch vulnerabilities to ensure compliance with host OS patches.

## Solution

Governance: Provide automated and scheduled OS compliance inspections, with an out-of-the-box experience while retaining customer customization capabilities. This allows for the timely detection of OS compliance issues and the output of compliance reports.

O&M: Trigger patch repairs based on compliance reports, and ensure full coverage of OS compliance through incremental iterations, closing the loop on OS compliance issues within the SLA.

Patch management: COC offers OS patch management capabilities, supporting scanning and fixing patches for Linux OSs like Huawei Cloud EulerOS, CentOS, and EulerOS, in ECS node and CCE cluster scenarios. COC scans host OS patches based on the rules in patch baselines and provides compliance reports. It has three common patch baselines and allows you to customize patch baselines to meet your specific needs. You can customize patch installation rules, patch compliance levels, and exceptional patches.

Patch management allows you to:

1. Create patch baselines based on the OS and its corresponding patch scan baselines.
2. Scan patches for resources based on scan baselines.
3. Check the summary for scan compliance once the scan is completed.

4. Fix patches for uncompliant resources.

Scheduled O&M: COC offers automatic O&M capabilities, including script management, job management, and scheduled O&M.

- Script management: COC provides public scripts and allows you to create custom scripts. Three types of scripts are supported: shell, python, and bat.
- Job management: You can orchestrate cloud service APIs, public jobs, custom jobs, and job controls into custom jobs.
- Scheduled O&M: Scheduled O&M can execute specific scripts or jobs on certain instances as scheduled or periodically.

## Core Advantages

- Dynamic identification: OS compliance risks are dynamically identified.
- Automatic resource discovery and management
- Safe production: During O&M operations, automatic batching and blast radius assessment are conducted.
- Automatic warning: SMS, email, and WeChat are utilized to automatically send notifications.

## Prerequisites

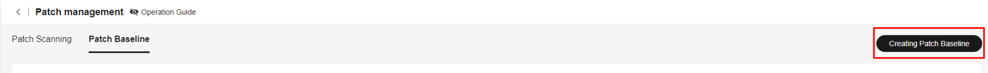
UniAgent has been installed on the server for automatic O&M. For details, see "Installing the UniAgent".

## Step 1: Create a Patch Baseline

Create a patch baseline on COC.

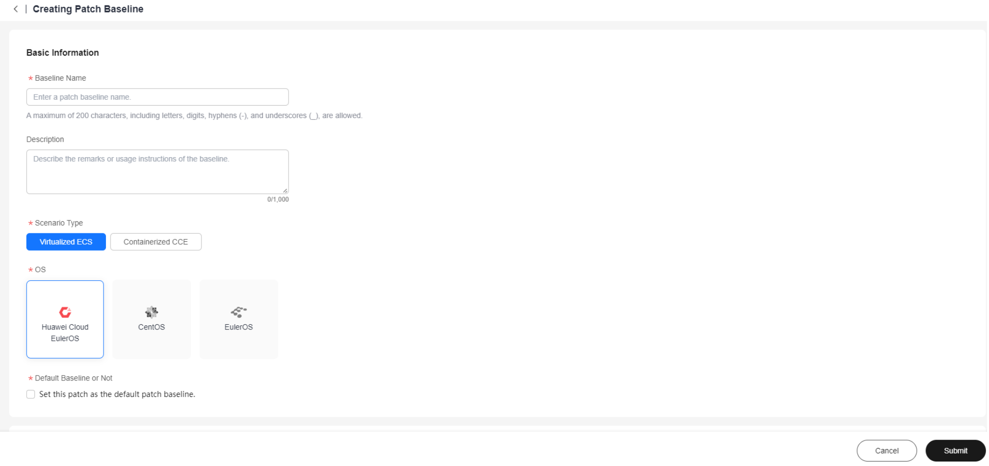
1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resource O&M** > **Resource O&M** > **Patch Management**.
3. Click **Creating Patch Baseline**.

**Figure 3-1** Clicking Creating Patch Baseline



4. Fill in patch baseline information.

**Figure 3-2** Setting patch baseline parameters



Creating 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

Virtualized ECS | Containerized CCE

* OS

Huawei Cloud EulerOS | CentOS | EulerOS

* Default Baseline or Not

□ Set this patch as the default patch baseline.

NOTE

**Table 3-1** describes the OS installation rule.

**Table 3-2** describes the custom installation rule.

**Table 3-1** OS installation rule

| Type | Option | Description |
|---|---|---|
| Product | All<br>Huawei Cloud EulerOS 1.1<br>Huawei Cloud EulerOS 2.0 | Product for which you want to scan patches. Only the patches of the selected product are scanned and fixed. |
| Category | All<br>Security<br>Bugfix<br>Enhancement<br>Recommended<br>Newpackage | Category of patches. Only the patches of the selected category are scanned and fixed. |
| Severity | All<br>Critical<br>Important<br>Moderate<br>Low<br>None | Severity level of patches. Only the patches of the selected severity are scanned and fixed. |

| Type | Option | Description |
|---|---|---|
| Compliance Reporting | Unspecified<br>Critical<br>High<br>Medium<br>Low<br>Suggestion | Level at which patches that meet the patch baseline are displayed in the compliance report |
| Install Non-Security Patches | None | If you select this option, patches with vulnerabilities will not be upgraded during patch fix. |
| Exceptional Patches | None | Approved patches and rejected patches can be in the following formats:<br>1. Complete software package name: *example*-**1.0.0-1.r1.hce2.x86_64**<br>2. Software package names that contain a single wildcard: *example*-**1.0.0*.x86_64** |

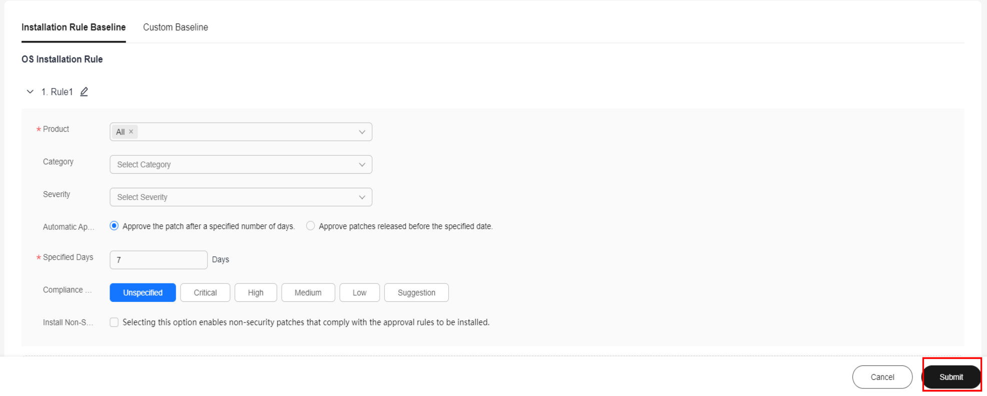
**Table 3-2** Custom installation rule

| Type | Option | Description |
|---|---|---|
| Product | All<br>Huawei Cloud EulerOS 1.1<br>Huawei Cloud EulerOS 2.0 | Product for which you want to scan patches. Only the patches of the selected product are scanned and fixed. |
| Compliance Reporting | Unspecified<br>Critical<br>High<br>Medium<br>Low<br>Suggestion | Level at which patches that meet the patch baseline are displayed in the compliance report |

| Type | Option | Description |
|---|---|---|
| Baseline Patch | None | You can customize the version and release number of baseline patches, and only the patches that match the custom baseline patch can be scanned and installed.<br>1. You can upload a maximum of 1,000 base patches for a single baseline.<br>2. The patch name can contain a maximum of 200 characters. Only letters, digits, underscores (_), hyphens (-), periods (.), asterisks (*), and plus signs (+) are allowed.<br>3. The second column data consists of a version number (consisting of letters, digits, underscores, periods, and colons) and a release number (consisting of letters, digits, underscores, and periods), each supporting a maximum of 50 characters and separated by a hyphen (-). |

5. Click **Submit**.

**Figure 3-3** Creating a custom patch baseline



Installation Rule Baseline | Custom Baseline

OS Installation Rule

1. Rule1

- * Product: All ×
- Category: Select Category
- Severity: Select Severity
- Automatic Ap...: ● Approve the patch after a specified number of days. ○ Approve patches released before the specified date.
- * Specified Days: 7 Days
- Compliance ...: Unspecified | Critical | High | Medium | Low | Suggestion
- Install Non-S...: □ Selecting this option enables non-security patches that comply with the approval rules to be installed.

Cancel | Submit

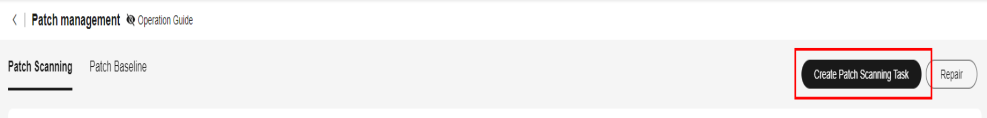
## Step 2: Scan Patches

Patch scan allows you to scan patches on the target ECS or CCE instance for compliance. It scans against the compliance report based on the selected default baseline, instance, and batch execution policy.

If an instance cannot be selected, check whether its UniUniAgent status is normal or whether the OS is supported by COC's patch management.

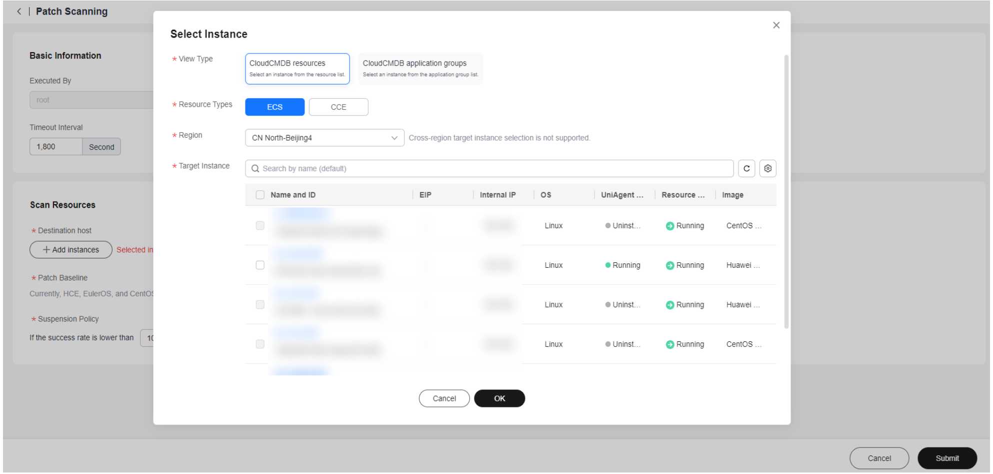
1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resource O&M** > **Resource O&M** > **Patch Management**.
3. Click **Create Patch Scanning Task**.

**Figure 3-4** Clicking Create Patch Scanning Task



4. Click **Add Instances**.

**Figure 3-5** Selecting instances



Patch Scanning

Basic Information

- Executed By: root
- Timeout Interval: 1,800 Second

Scan Resources

- * Destination host: + Add instances Selected in
- * Patch Baseline: Currently, HCE, EulerOS, and CentOS
- * Suspension Policy: If the success rate is lower than 10

Select Instance

- * 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 | CCE
- * Region: CN North-Beijing4 — Cross-region target instance selection is not supported.
- * Target Instance: Search by name (default)

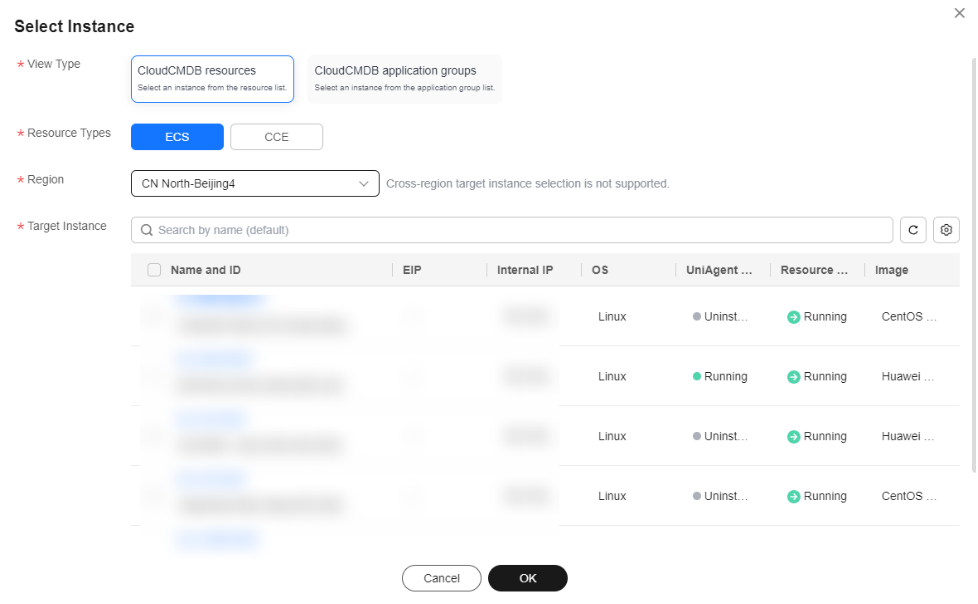
| □ | Name and ID | EIP | Internal IP | OS | UniAgent ... | Resource ... | Image |
|---|---|---|---|---|---|---|---|
| □ | [redacted] | [redacted] | [redacted] | Linux | Uninst... | Running | CentOS ... |
| □ | [redacted] | [redacted] | [redacted] | Linux | Running | Running | Huawei ... |
| □ | [redacted] | [redacted] | [redacted] | Linux | Uninst... | Running | Huawei ... |
| □ | [redacted] | [redacted] | [redacted] | Linux | Uninst... | Running | CentOS ... |

Cancel | OK

Cancel | Submit

5. Select the ECSs or CCE instances to scan.

**Figure 3-6** Selecting the ECSs

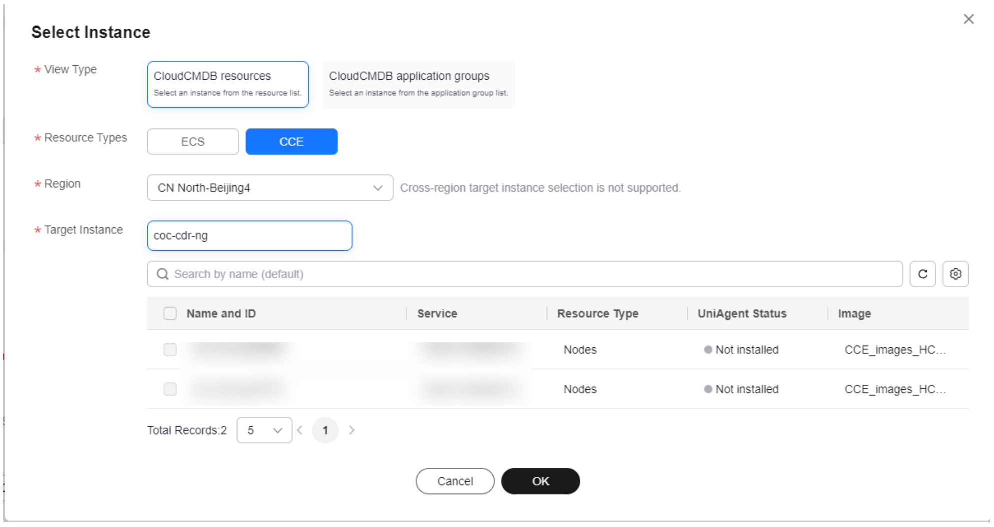


Select Instance

* 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 | CCE
* Region: CN North-Beijing4 — Cross-region target instance selection is not supported.
* Target Instance: Search by name (default)

| Name and ID | EIP | Internal IP | OS | UniAgent ... | Resource ... | Image |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | Linux | ● Uninst... | Running | CentOS ... |
| [redacted] | [redacted] | [redacted] | Linux | ● Running | Running | Huawei ... |
| [redacted] | [redacted] | [redacted] | Linux | ● Uninst... | Running | Huawei ... |
| [redacted] | [redacted] | [redacted] | Linux | ● Uninst... | Running | CentOS ... |

**Figure 3-7** Selecting the CCE instances



Select Instance

* 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 | CCE
* Region: CN North-Beijing4 — Cross-region target instance selection is not supported.
* Target Instance: coc-cdr-ng

Search by name (default)

| Name and ID | Service | Resource Type | UniAgent Status | Image |
|---|---|---|---|---|
| [redacted] | [redacted] | Nodes | ● Not installed | CCE_images_HC... |
| [redacted] | [redacted] | Nodes | ● Not installed | CCE_images_HC... |

Total Records:2 5 < 1 >

6. Set **Batch Policy**.

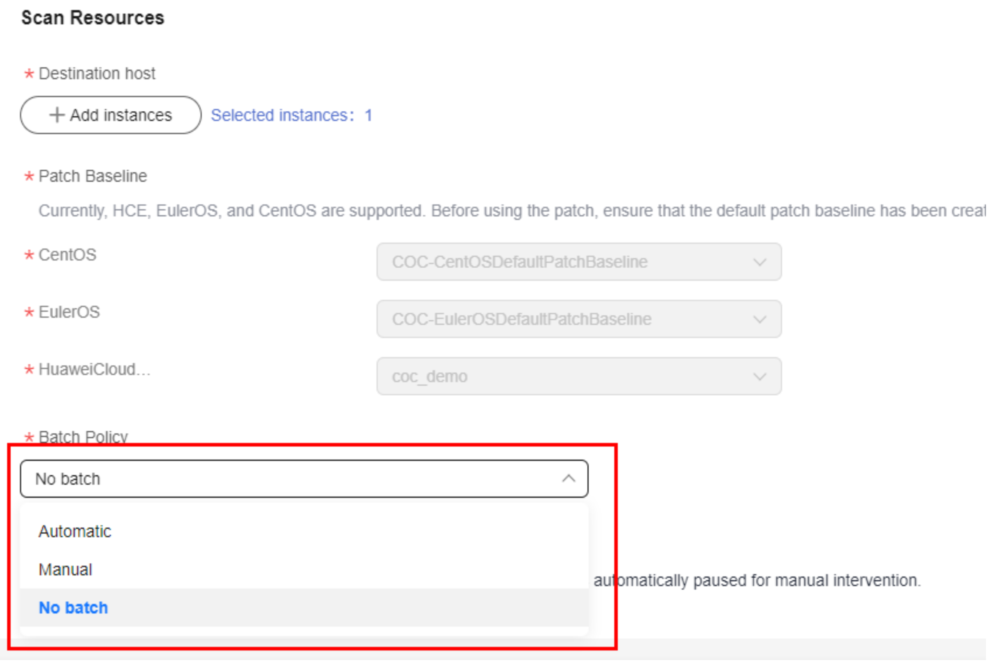
   Batch policy:

   – **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 3-8** Selecting a batch policy



Scan Resources

* Destination host

Selected instances： 1

* Patch Baseline

Currently, HCE, EulerOS, and CentOS are supported. Before using the patch, ensure that the default patch baseline has been creat

* CentOS: COC-CentOSDefaultPatchBaseline

* EulerOS: COC-EulerOSDefaultPatchBaseline

* HuaweiCloud...: coc_demo

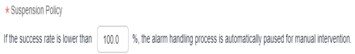
* Batch Policy: No batch

au tomatically paused for manual intervention.

7. Set **Suspension Policy**.

   Suspension threshold: You can set a suspension threshold to determine the execution success rate. Once the number of failed servers reaches the number calculated based on the threshold, the service ticket status will become abnormal and the patch scan will cease.

   **Figure 3-9** Suspension policy

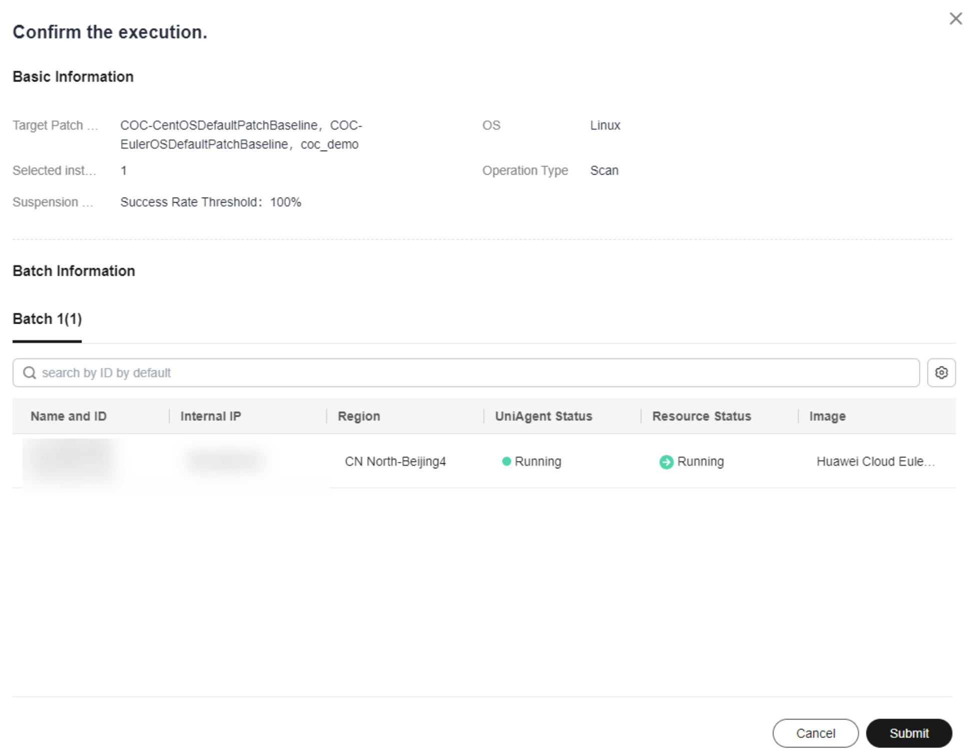
   

   * Suspension Policy

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

8. Click **Submit**.

**Figure 3-10** Execution confirmation page



**Confirm the execution.**

**Basic Information**

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

**Batch Information**

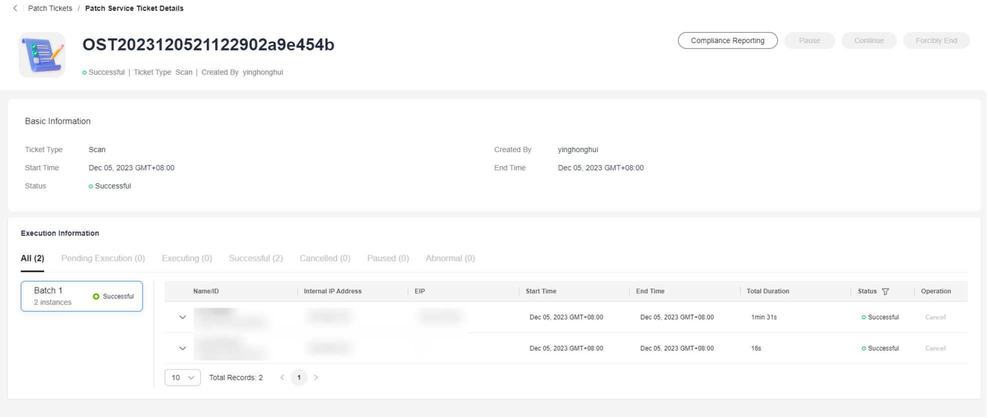
**Batch 1(1)**

search by ID by default

| Name and ID | Internal IP | Region | UniAgent Status | Resource Status | Image |
|---|---|---|---|---|---|
| [redacted] | [redacted] | CN North-Beijing4 | ● Running | Running | Huawei Cloud Eule... |

9. Confirm the execution information. If the information is correct, click **OK**.
10. Once the service ticket is executed, click **Compliance Reporting**. On the displayed page, check the ECS compliance status in the **Compliance Reporting List** area.

**Figure 3-11** Service ticket details



OST2023120521122902a9e454b

○ Successful | Ticket Type Scan | Created By yinghonghui

Basic Information

|  |  |  |  |
|---|---|---|---|
| Ticket Type | Scan | Created By | yinghonghui |
| Start Time | Dec 05, 2023 GMT+08:00 | End Time | Dec 05, 2023 GMT+08:00 |
| Status | ○ Successful |  |  |

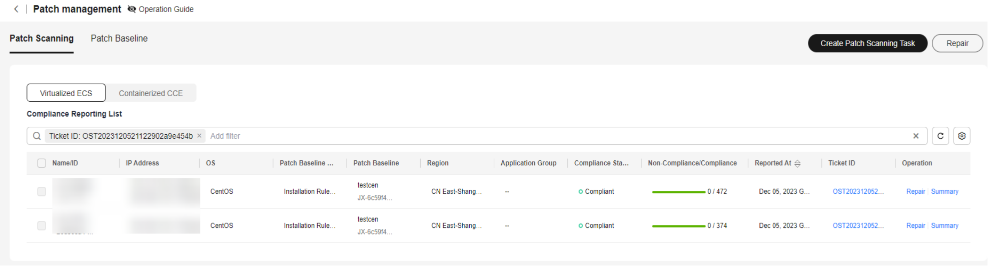
**Execution Information**

Batch 1
2 instances
○ Successful

| Name/ID | Internal IP Address | EIP | Start Time | End Time | Total Duration | Status | Operation |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | Dec 05, 2023 GMT+08:00 | Dec 05, 2023 GMT+08:00 | 1min 31s | ○ Successful | Cancel |
| [redacted] | [redacted] | [redacted] | Dec 05, 2023 GMT+08:00 | Dec 05, 2023 GMT+08:00 | 16s | ○ Successful | Cancel |

10 Total Records: 2 < 1 >

**Figure 3-12** Compliance report list



| Name/ID | IP Address | OS | Patch Baseline ... | Patch Baseline | Region | Application Group | Compliance Sta... | Non-Compliance/Compliance | Reported At | Ticket ID | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | CentOS | Installation Rule... | testcen<br>JX-6c59f4... | CN East-Shang... | -- | Compliant | 0 / 472 | Dec 05, 2023 G... | OST202312052... | Repair Summary |
| [redacted] | [redacted] | CentOS | Installation Rule... | testcen<br>JX-6c59f4... | CN East-Shang... | -- | Compliant | 0 / 374 | Dec 05, 2023 G... | OST202312052... | Repair Summary |

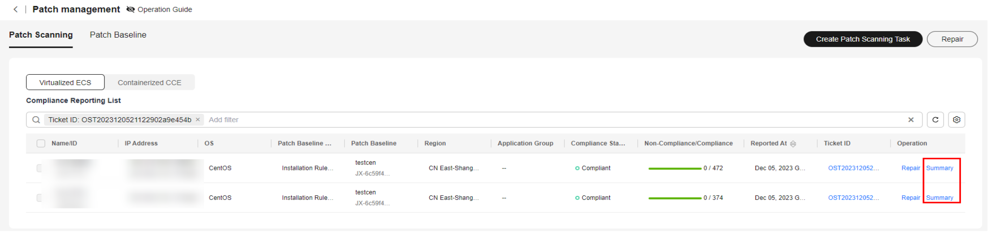
## Step 3: View the Patch Compliance Report

After patch compliance scanning or remediation, you can click the compliance report summary details to view patch details on the instance.

The patch compliance report will only retain the most recent scan or remediation record.

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Resource O&M** > **Resource O&M** > **Patch Management**.

**Figure 3-13** Clicking Summary in the Operation column



| Name/ID | IP Address | OS | Patch Baseline ... | Patch Baseline | Region | Application Group | Compliance Sta... | Non-Compliance/Compliance | Reported At | Ticket ID | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | CentOS | Installation Rule... | testcen<br>JX-6c59f4... | CN East-Shang... | -- | Compliant | 0 / 472 | Dec 05, 2023 G... | OST202312052... | Repair Summary |
| [redacted] | [redacted] | CentOS | Installation Rule... | testcen<br>JX-6c59f4... | CN East-Shang... | -- | Compliant | 0 / 374 | Dec 05, 2023 G... | OST202312052... | Repair Summary |

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:

   Compliant (Installed): The patch complies with the patch baseline, has been installed on an ECS instance, and no update is available.

   Compliant (Installed-other): The patch is not compliant with the patch baseline but has been installed on an ECS instance.

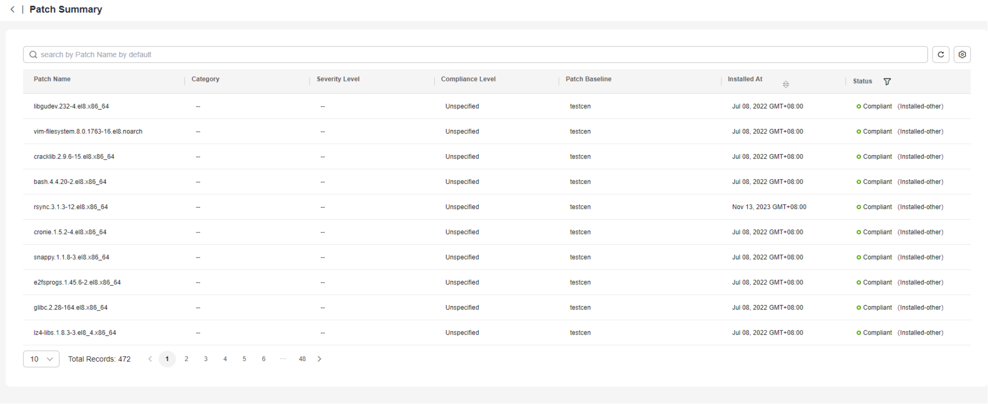
   Noncompliant (Installed-to be restarted): The patch has been repaired, and can take effect only after the ECS instance is restarted.

   Noncompliant (InstalledRejected): The rejected patches defined in the exceptional patches of a patch baseline. This patch will not be repaired even if it is compliant with the patch baseline.

   Noncompliant (Missing): The patch meets the baseline but has not been installed.

   Noncompliant (Failed): The patch failed to be repaired.

**Figure 3-14** Patch compliance report summary



Patch Summary

search by Patch Name by default

| Patch Name | Category | Severity Level | Compliance Level | Patch Baseline | Installed At | Status |
|---|---|---|---|---|---|---|
| libgudev.232-4.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| vim-filesystem.8.0.1763-16.el8.noarch | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| cracklib.2.9.6-15.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| bash.4.4.20-2.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| rsync.3.1.3-12.el8.x86_64 | -- | -- | Unspecified | testcen | Nov 13, 2023 GMT+08:00 | Compliant (Installed-other) |
| cronie.1.5.2-4.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| snappy.1.1.8-3.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| e2fsprogs.1.45.6-2.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| glibc.2.28-164.el8.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |
| lz4-libs.1.8.3-3.el8_4.x86_64 | -- | -- | Unspecified | testcen | Jul 08, 2022 GMT+08:00 | Compliant (Installed-other) |

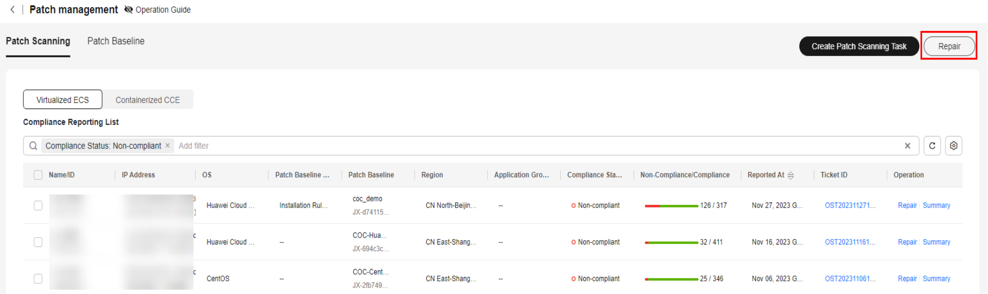
10 Total Records: 472 < 1 2 3 4 5 6 ··· 48 >

## Step 4: Install the Patch

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

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

**Figure 3-15** Selecting the target instances



Compliance Reporting List

Compliance Status: Non-compliant × Add filter

| Name/ID | IP Address | OS | Patch Baseline ... | Patch Baseline | Region | Application Gro... | Compliance Sta... | Non-Compliance/Compliance | Reported At | Ticket ID | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | Huawei Cloud ... | Installation Rul... | coc_demo<br>JX-d74115... | CN North-Beijin... | -- | Non-compliant | 126 / 317 | Nov 27, 2023 G... | OST202311271... | Repair \| Summary |
| [redacted] | [redacted] | Huawei Cloud ... | -- | COC-Hua...<br>JX-694c3c... | CN East-Shang... | -- | Non-compliant | 32 / 411 | Nov 16, 2023 G... | OST202311161... | Repair \| Summary |
| [redacted] | [redacted] | CentOS | -- | COC-Cent...<br>JX-2fb749... | CN East-Shang... | -- | Non-compliant | 25 / 346 | Nov 06, 2023 G... | OST202311061... | Repair \| Summary |

4. Set **Batch Policy**.

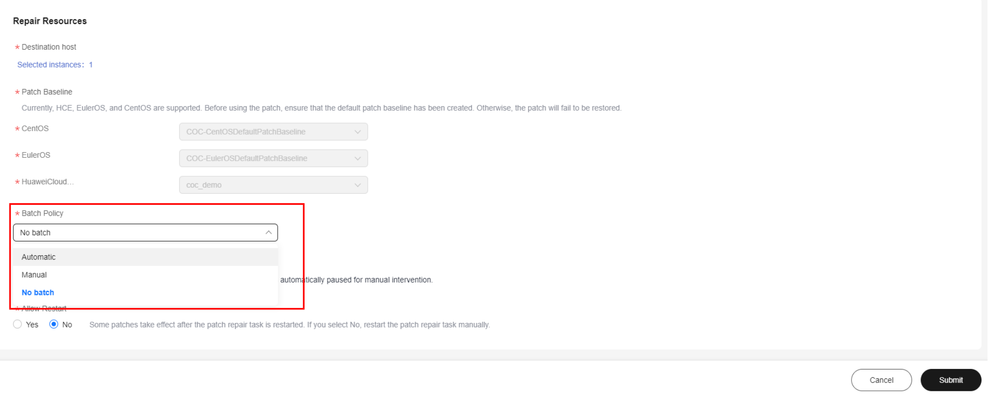
   Batch policy:

   – **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 3-16** Selecting a batch policy



Repair Resources

* Destination host

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_demo

* Batch Policy: No batch

Automatic
Manual
No batch

automatically paused for manual intervention.

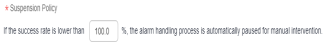
* Allow Restart

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

5. Set **Suspension Policy**.

   Suspension threshold: You can set a suspension threshold to determine the execution success rate. Once the number of failed servers reaches the number calculated based on the threshold, the service ticket status will become abnormal and the patch scan will cease.

   **Figure 3-17** Suspension policy

   * Suspension Policy

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

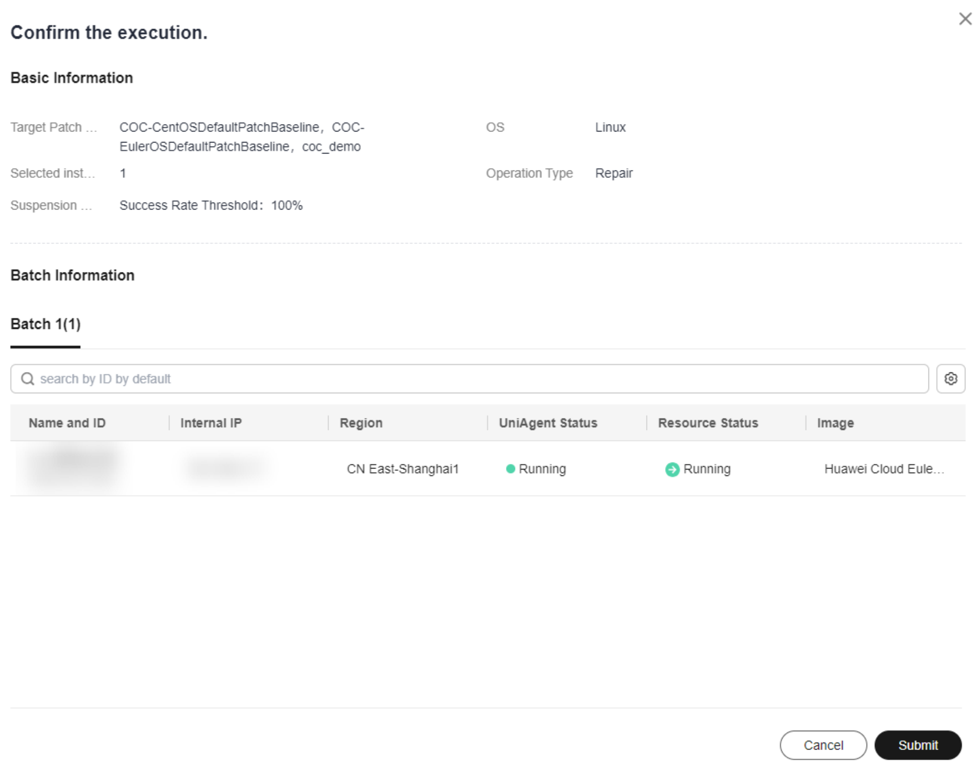
6. Set whether to allow restart.

   NOTE

   Some patches require a restart to take effect. If you choose not to restart, you will need to schedule a restart at a later time.

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

**Figure 3-18** Execution information page



Confirm the execution.

Basic Information

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

Batch Information

Batch 1(1)

search by ID by default

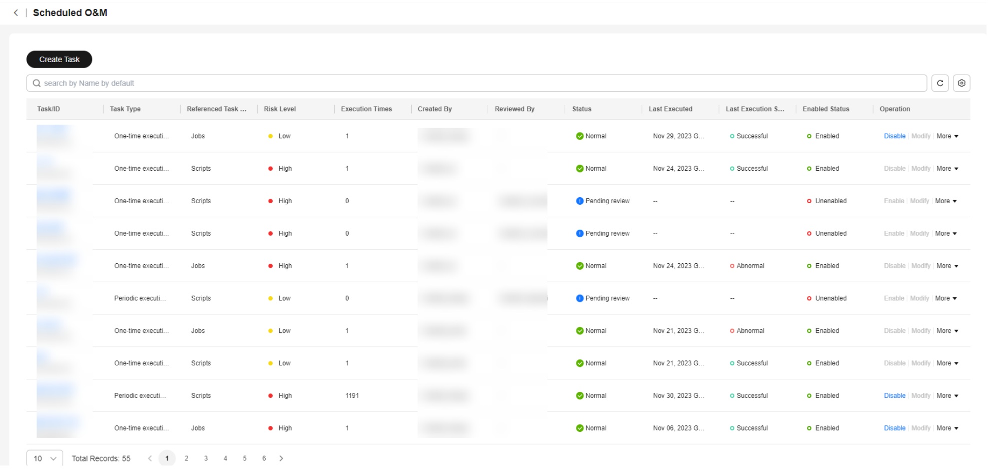
| Name and ID | Internal IP | Region | UniAgent Status | Resource Status | Image |
|---|---|---|---|---|---|
| [redacted] | [redacted] | CN East-Shanghai1 | ● Running | Running | Huawei Cloud Eule... |

## Step 5: Create a Scheduled O&M Task

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

1. Log in to **COC**.
2. In the navigation pane on the left, choose **Automated O&M** > **Scheduled O&M**.

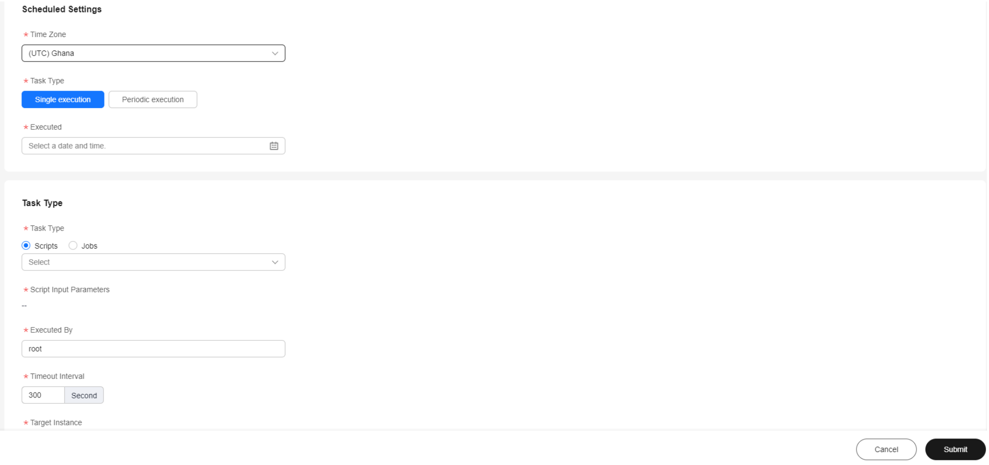
**Figure 3-19** Listing scheduled O&M tasks



| Task/ID | Task Type | Referenced Task ... | Risk Level | Execution Times | Created By | Reviewed By | Status | Last Executed | Last Execution S... | Enabled Status | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | One-time executi... | Jobs | ● Low | 1 | [redacted] | | Normal | Nov 29, 2023 G... | ○ Successful | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Scripts | ● High | 1 | [redacted] | | Normal | Nov 24, 2023 G... | ○ Successful | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Scripts | ● High | 0 | [redacted] | [redacted] | Pending review | -- | -- | ○ Unenabled | Enable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Scripts | ● High | 0 | [redacted] | [redacted] | Pending review | -- | -- | ○ Unenabled | Enable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Jobs | ● High | 1 | [redacted] | | Normal | Nov 24, 2023 G... | ○ Abnormal | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | Periodic executi... | Scripts | ● Low | 0 | [redacted] | [redacted] | Pending review | -- | -- | ○ Unenabled | Enable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Jobs | ● Low | 1 | [redacted] | | Normal | Nov 21, 2023 G... | ○ Abnormal | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Scripts | ● Low | 1 | [redacted] | | Normal | Nov 21, 2023 G... | ○ Successful | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | Periodic executi... | Scripts | ● High | 1191 | [redacted] | | Normal | Nov 30, 2023 G... | ○ Successful | ○ Enabled | Disable \| Modify \| More ▾ |
| [redacted] | One-time executi... | Jobs | ● High | 1 | [redacted] | | Normal | Nov 06, 2023 G... | ○ Successful | ○ Enabled | Disable \| Modify \| More ▾ |

3. Click **Create Task**.

**Figure 3-20** Modifying a scheduled task



Scheduled Settings

* Time Zone
(UTC) Ghana

* Task Type
Single execution | Periodic execution

* Executed
Select a date and time.

Task Type

* Task Type
● Scripts ○ Jobs
Select

* Script Input Parameters
--

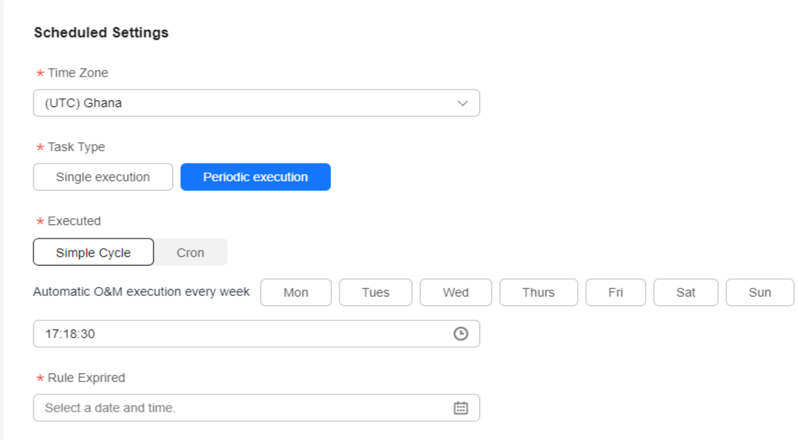
* Executed By
root

* Timeout Interval
300 Second

* Target Instance

4. Enter basic information about the scheduled task. 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.

**Figure 3-21** Scheduled Settings



Scheduled Settings

* Time Zone
(UTC) Ghana

* Task Type
Single execution | Periodic execution

* Executed
Simple Cycle | Cron

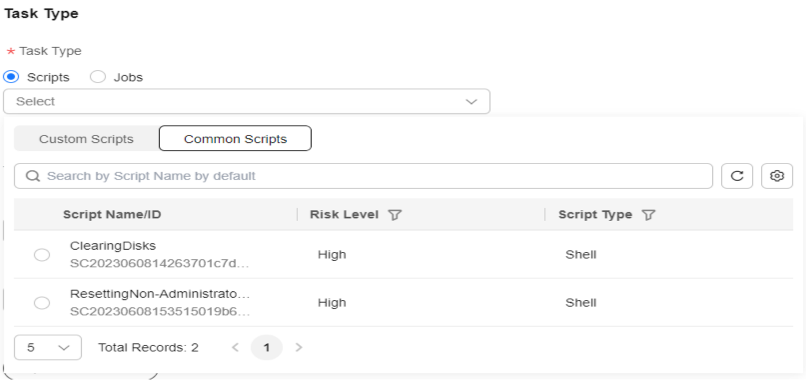
Automatic O&M execution every week Mon Tues Wed Thurs Fri Sat Sun

17:18:30

* Rule Expired
Select a date and time.

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

**Figure 3-22** Task Type



Task Type

* Task Type
● Scripts ○ Jobs
Select

Custom Scripts | Common Scripts

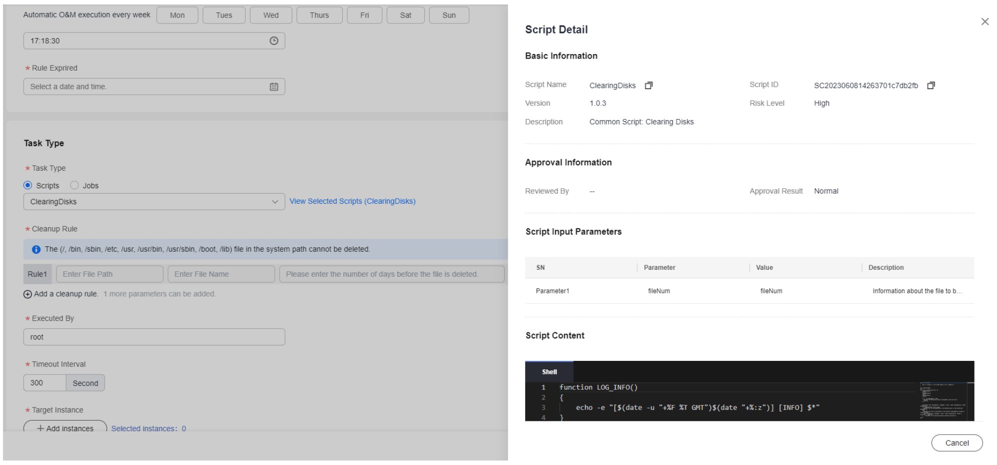
Search by Script Name by default

| | Script Name/ID | Risk Level | Script Type |
|---|---|---|---|
| ○ | ClearingDisks<br>SC2023060814263701c7d... | High | Shell |
| ○ | ResettingNon-Administrato...<br>SC20230608153515019b6... | High | Shell |

5 Total Records: 2 < 1 >

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

**Figure 3-23** Script Details



Automatic O&M execution every week: Mon, Tues, Wed, Thurs, Fri, Sat, Sun

17:18:30

* Rule Exprired: Select a date and time.

**Task Type**

* Task Type: ● Scripts ○ Jobs

ClearingDisks — View Selected Scripts (ClearingDisks)

* Cleanup Rule

The (/, /bin, /sbin, /etc, /usr, /usr/bin, /usr/sbin, /boot, /lib) file in the system path cannot be deleted.

Rule1 | Enter File Path | Enter File Name | Please enter the number of days before the file is deleted.

Add a cleanup rule. 1 more parameters can be added.

* Executed By: root

* Timeout Interval: 300 Second

* Target Instance: Add instances Selected instances：0

**Script Detail**

**Basic Information**

Script Name: ClearingDisks
Script ID: SC2023060814263701c7db2fb
Version: 1.0.3
Risk Level: High
Description: Common Script: Clearing Disks

**Approval Information**

Reviewed By: --
Approval Result: Normal

**Script Input Parameters**

| SN | Parameter | Value | Description |
|---|---|---|---|
| Parameter1 | fileNum | fileNum | Information about the file to b... |

**Script Content**

Shell

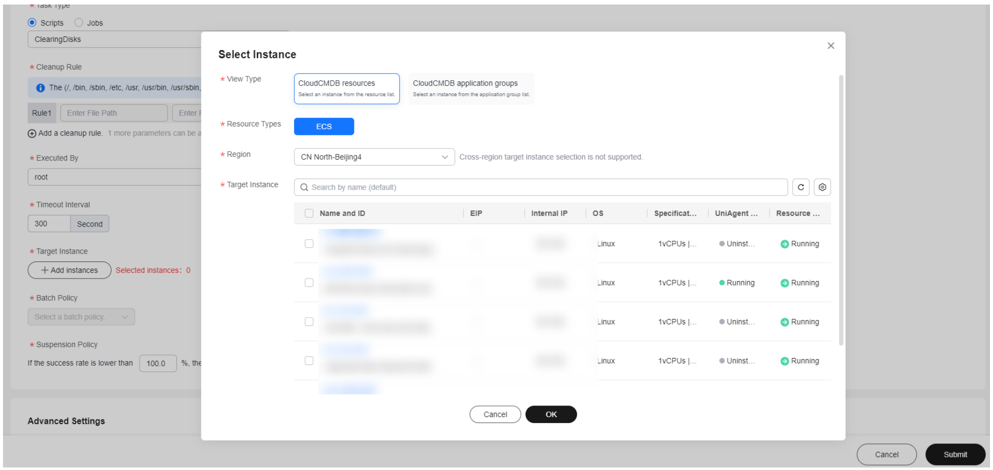
```
function LOG_INFO()
{
    echo -e "[$(date -u "+%F %T GMT")$(date "+%:z")] [INFO] $*"
}
```

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.

Enter the execution user and the timeout interval.

Select an instance and click **Add instances**. The **Select Instance** dialog box is displayed. You can select **CloudCMDB resources** or **CloudCMDB application groups** for **View Type** and search for the target instances based on the resource type and region. Select the check box next to the instance list and click **OK**.

**Figure 3-24** Selecting instances



**Select Instance**

* 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-Beijing4 — Cross-region target instance selection is not supported.

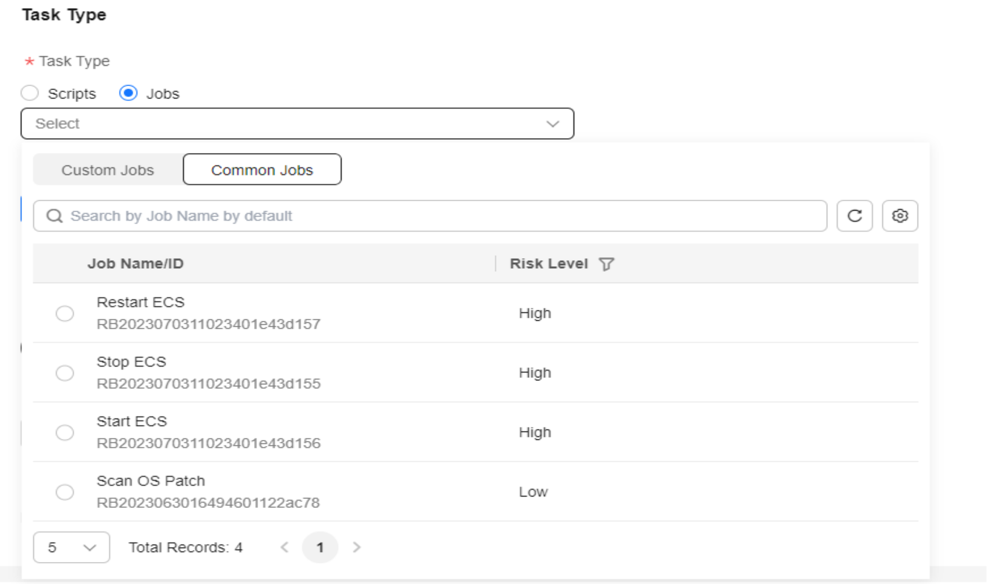
* Target Instance: Search by name (default)

| Name and ID | EIP | Internal IP | OS | Specificat... | UniAgent ... | Resource ... |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | Linux | 1vCPUs \|... | Uninst... | Running |
| [redacted] | [redacted] | [redacted] | Linux | 1vCPUs \|... | Running | Running |
| [redacted] | [redacted] | [redacted] | Linux | 1vCPUs \|... | Uninst... | Running |
| [redacted] | [redacted] | [redacted] | Linux | 1vCPUs \|... | Uninst... | Running |

Select a batch policy and suspension policy.

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

**Figure 3-25** Selecting Jobs



**Task Type**

* Task Type

○ Scripts ● Jobs

Select

Custom Jobs | Common Jobs

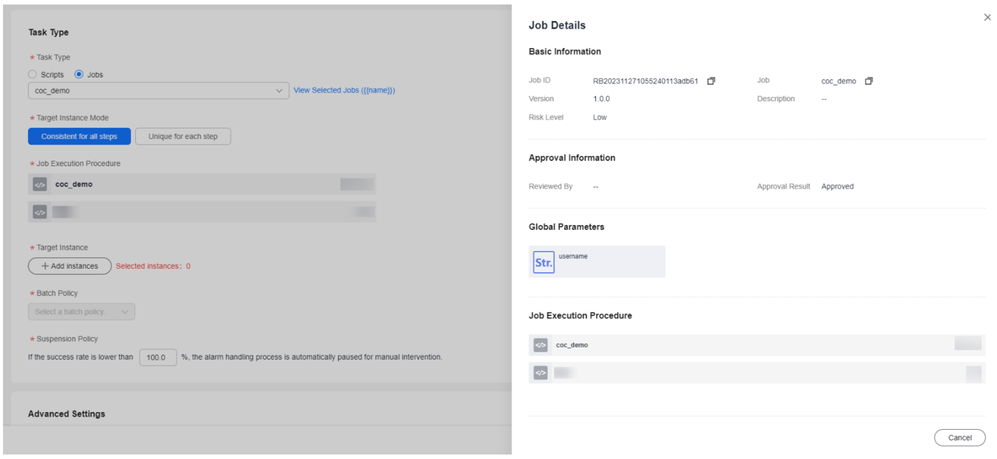
Search by Job Name by default

| Job Name/ID | Risk Level |
|---|---|
| ○ Restart ECS<br>RB2023070311023401e43d157 | High |
| ○ Stop ECS<br>RB2023070311023401e43d155 | High |
| ○ Start ECS<br>RB2023070311023401e43d156 | High |
| ○ Scan OS Patch<br>RB2023063016494601122ac78 | Low |

5 Total Records: 4 < 1 >

Click **View Selected Jobs**. The **Job Details** slide-out is displayed. Click the option in the **Global Parameters** area. The global parameter details are displayed in the level-2 dialog box on the right. Click an option in the **Job Execution Procedure** area. The job step details are displayed in the level-2 dialog box on the right.

**Figure 3-26** Querying job steps



**Task Type**

* Task Type

○ Scripts ● Jobs

coc_demo View Selected Jobs ({{name}})

* Target Instance Mode

Consistent for all steps | Unique for each step

* Job Execution Procedure

coc_demo

* 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.

**Advanced Settings**

**Job Details**

**Basic Information**

| | | | |
|---|---|---|---|
| Job ID | RB202311271055240113adb61 | Job | coc_demo |
| Version | 1.0.0 | Description | -- |
| Risk Level | Low | | |

**Approval Information**

| | | | |
|---|---|---|---|
| Reviewed By | -- | Approval Result | Approved |

**Global Parameters**

Str. username

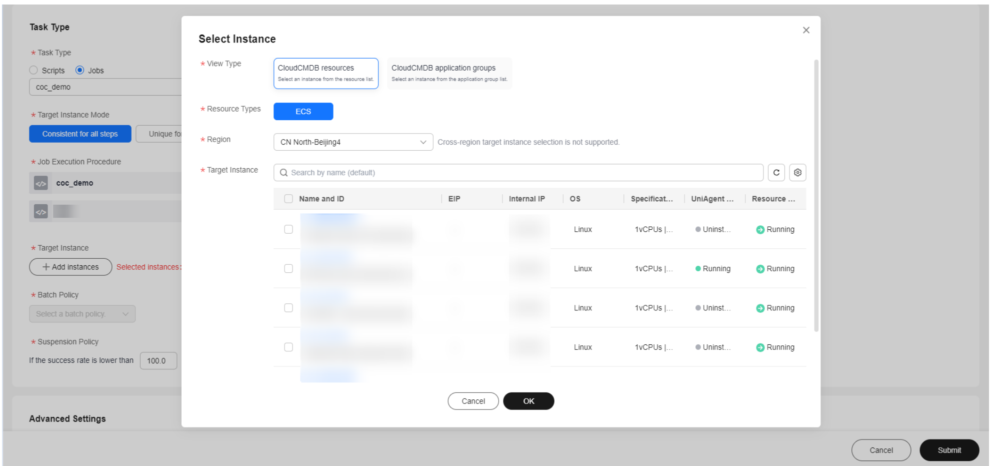
**Job Execution Procedure**

coc_demo

Cancel

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 3-27** Selecting instances



Select Instance

* 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

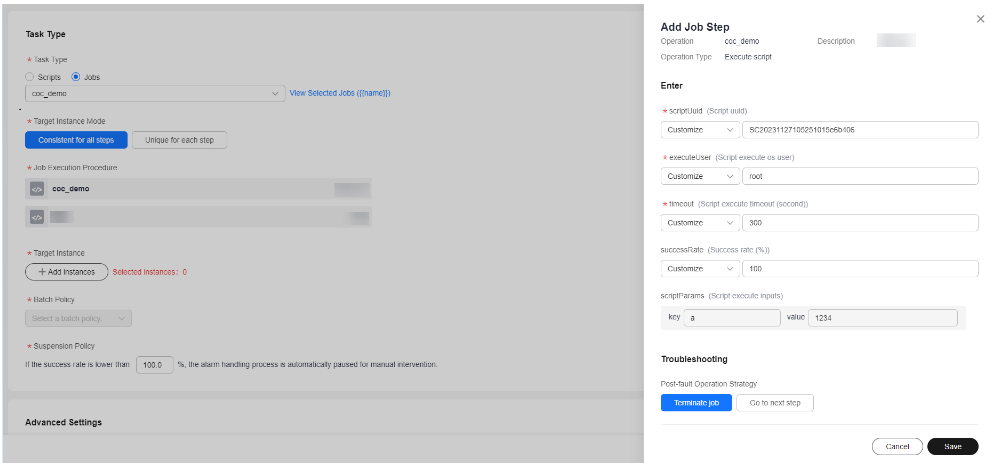
* Region: CN North-Beijing4 — Cross-region target instance selection is not supported.

* Target Instance: Search by name (default)

| □ Name and ID | EIP | Internal IP | OS | Specificat... | UniAgent ... | Resource ... |
|---|---|---|---|---|---|---|
| □ | | | Linux | 1vCPUs \|... | ● Uninst... | Running |
| □ | | | Linux | 1vCPUs \|... | ● Running | Running |
| □ | | | Linux | 1vCPUs \|... | ● Uninst... | Running |
| □ | | | Linux | 1vCPUs \|... | ● Uninst... | Running |

Click the job procedure. The job step details are displayed on the right. Enter the success rate threshold and the temporary continuation strategy, select an exception handling policy, and click **Save** complete the modification.

**Figure 3-28** Editing a job step



Add Job Step

Operation: coc_demo    Description:

Operation Type: Execute script

Enter

* scriptUuid (Script uuid): Customize | SC20231127105251015e6b406

* executeUser (Script execute os user): Customize | root

* timeout (Script execute timeout (second)): Customize | 300

successRate (Success rate (%)): Customize | 100

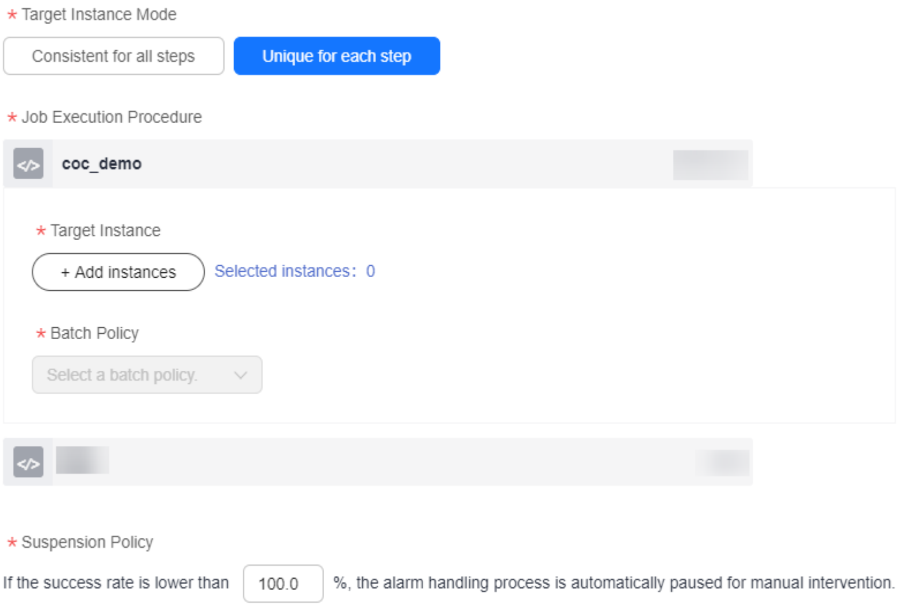
scriptParams (Script execute inputs): key a value 1234

Troubleshooting

Post-fault Operation Strategy: Terminate job | Go to next step

Select an instance and click **Add instances**. The **Select Instance** dialog box is displayed. You can select **CloudCMDB resources** or **CloudCMDB application groups** for **View Type** and search for the target instances based on the resource type and region. Select the check box next to the instance list and click **OK**.

**Figure 3-29** Adding instances



* Target Instance Mode

Consistent for all steps | **Unique for each step**

* Job Execution Procedure

coc_demo

* Target Instance

+ Add instances   Selected instances：0

* Batch Policy

Select a batch policy.

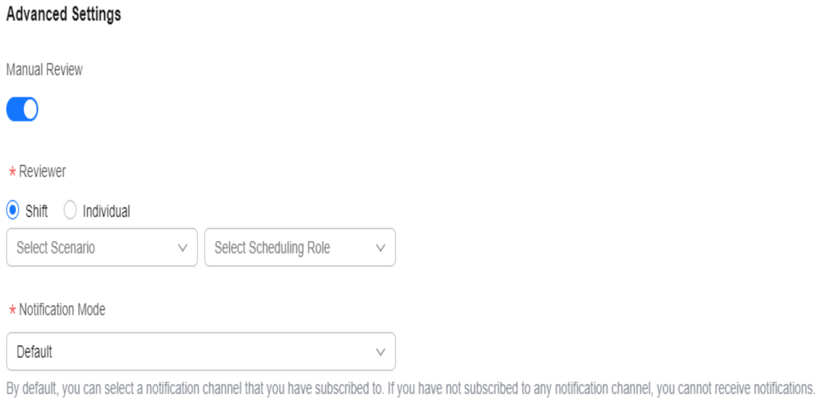
* Suspension Policy

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

Select a batch policy and suspension policy.

7. You can determine whether to select **Manual Review** based on the service requirements.

**Figure 3-30** Enabling manual review



Advanced Settings

Manual Review

* Reviewer

● Shift ○ Individual

Select Scenario | Select Scheduling Role

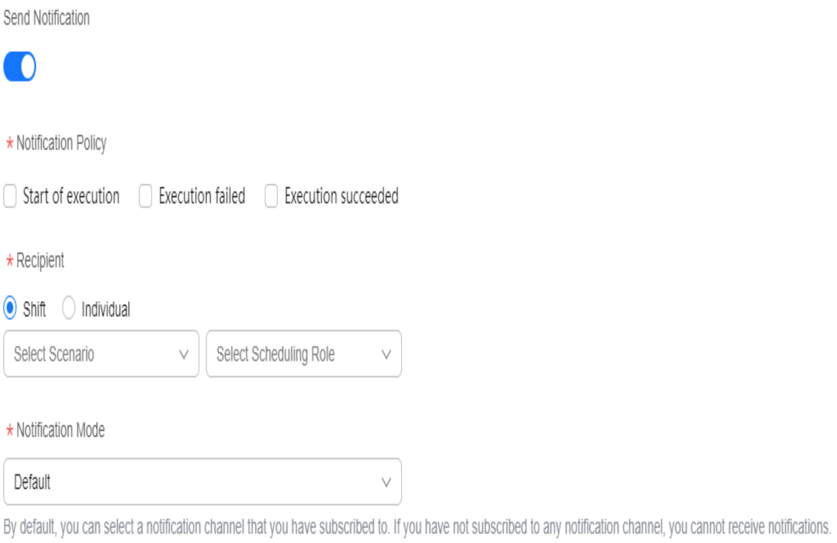
* Notification Mode

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.

8. Determine whether to enable **Send Notification** based on service requirements. If enabled, set **Notification Policy**, **Recipient**, and **Notification Mode**.

**Figure 3-31** Setting notification parameters



Send Notification

* Notification Policy

□ Start of execution □ Execution failed □ Execution succeeded

* Recipient

● Shift ○ Individual

Select Scenario ∨ Select Scheduling Role ∨

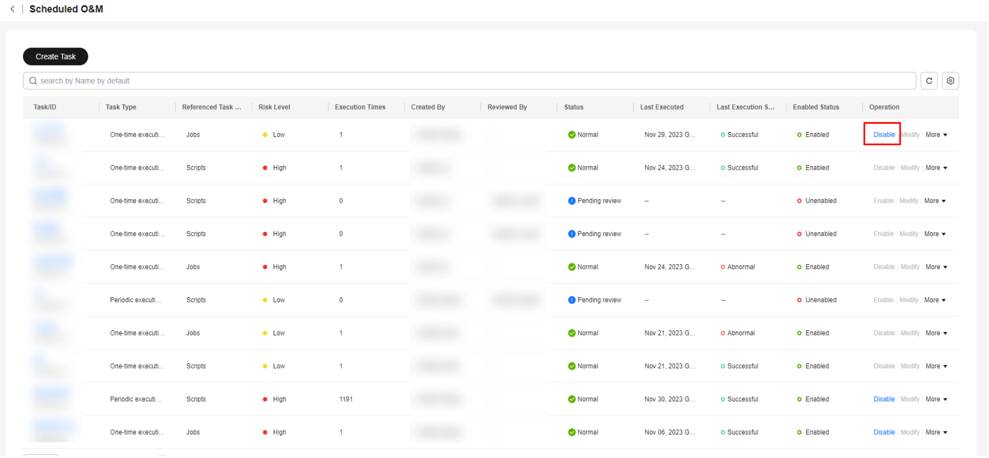
* Notification Mode

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.

9. Click **Submit**.
10. Locate a target task in the list, and click **Enable** or **Disable** in the **Operation** column to enable or disable it.

**Figure 3-32** Checking the task list



Scheduled O&M

| Task/ID | Task Type | Referenced Task ... | Risk Level | Execution Times | Created By | Reviewed By | Status | Last Executed | Last Execution S... | Enabled Status | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | One-time executi... | Jobs | ● Low | 1 | [redacted] | | Normal | Nov 29, 2023 G... | Successful | Enabled | Disable \| Modify \| More |
| [redacted] | One-time executi... | Scripts | ● High | 1 | [redacted] | | Normal | Nov 24, 2023 G... | Successful | Enabled | Disable \| Modify \| More |
| [redacted] | One-time executi... | Scripts | ● High | 0 | [redacted] | [redacted] | Pending review | -- | -- | Unenabled | Enable \| Modify \| More |
| [redacted] | One-time executi... | Scripts | ● High | 0 | [redacted] | [redacted] | Pending review | -- | -- | Unenabled | Enable \| Modify \| More |
| [redacted] | One-time executi... | Jobs | ● High | 1 | [redacted] | | Normal | Nov 24, 2023 G... | Abnormal | Enabled | Disable \| Modify \| More |
| [redacted] | Periodic executi... | Scripts | ● Low | 0 | [redacted] | [redacted] | Pending review | -- | -- | Unenabled | Enable \| Modify \| More |
| [redacted] | One-time executi... | Jobs | ● Low | 1 | [redacted] | | Normal | Nov 21, 2023 G... | Abnormal | Enabled | Disable \| Modify \| More |
| [redacted] | One-time executi... | Scripts | ● Low | 1 | [redacted] | | Normal | Nov 21, 2023 G... | Successful | Enabled | Disable \| Modify \| More |
| [redacted] | Periodic executi... | Scripts | ● High | 1191 | [redacted] | | Normal | Nov 30, 2023 G... | Successful | Enabled | Disable \| Modify \| More |
| [redacted] | One-time executi... | Jobs | ● High | 1 | [redacted] | | Normal | Nov 06, 2023 G... | Successful | Enabled | Disable \| Modify \| More |

# 4 Change History

| Released On | Description |
|---|---|
| 2023-11-30 | This issue is the first official release. |