Cloud Operations Center (COC)

Getting Started

Issue 01

Date 2025-07-28

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Creating an Application and a Model

This section describes how to use COC to quickly manage your resources and applications on the application and resource management page, including synchronizing resources, creating applications and modeling, and performing operations on a UniAgent. The procedure is as follows:

1. **Preparations**: Sign up for a HUAWEI ID, complete real-name authentication, and enable COC.
2. **Synchronize resources**. Obtain resources in all regions to which the current user belongs and synchronize the resources to COC.
3. **Create an application and model the associations between the application and resources.** This feature facilitates resource management by service logic unit.
4. **Perform operations on a UniAgent**. Install, upgrade, and uninstall a UniAgent on the corresponding node.

Preparations

1. Sign up for a HUAWEI ID and complete real-name authentication.

   Before using COC, **sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication**.

   If you already have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Enable COC.

   Upon your first login, **enable COC** first.

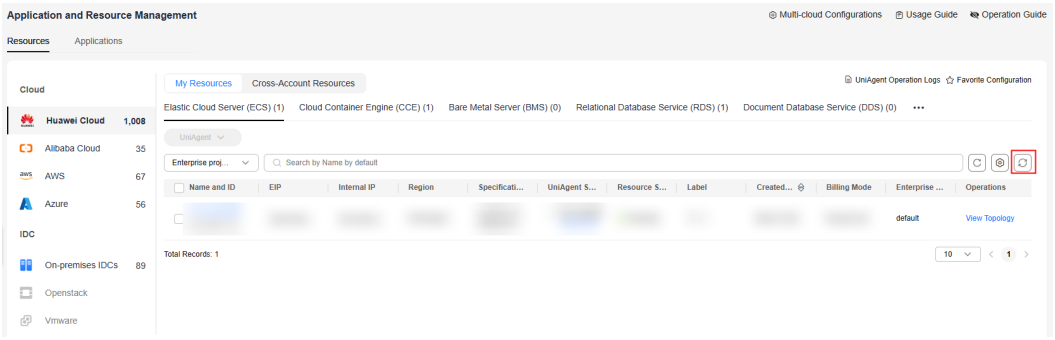
   If you have enabled COC, skip this step.

Synchronizing Resources

Step 1 Log in to **COC**.

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

Figure 1-1 Synchronizing resources



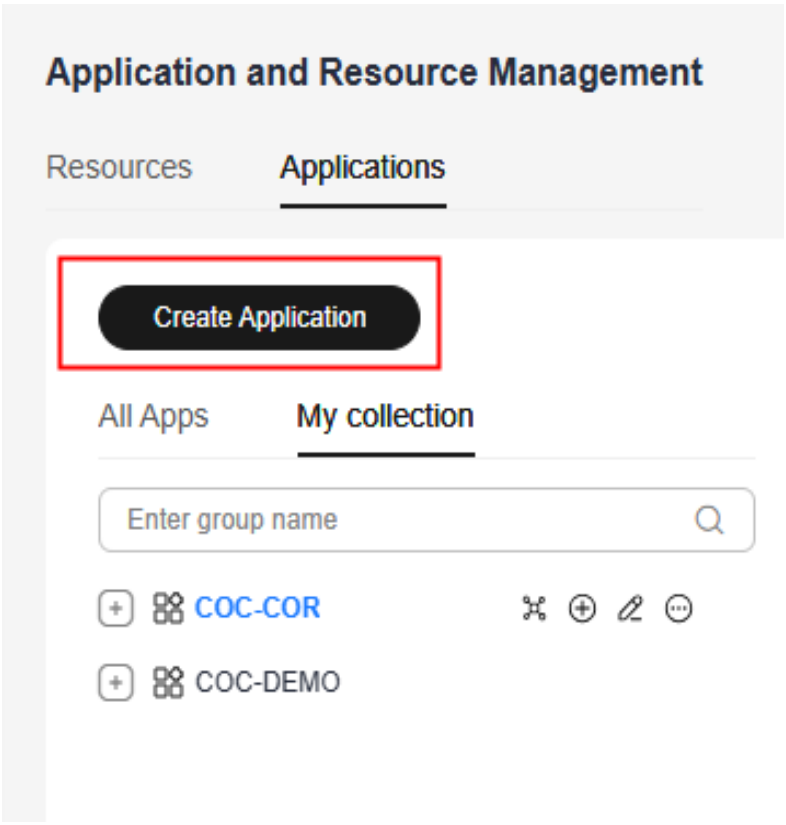
----End

Creating an Application and a Model

Step 1 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 2 Click the **Applications** tab. On the displayed tab page, click **Create Application**.

Figure 1-2 Creating an application

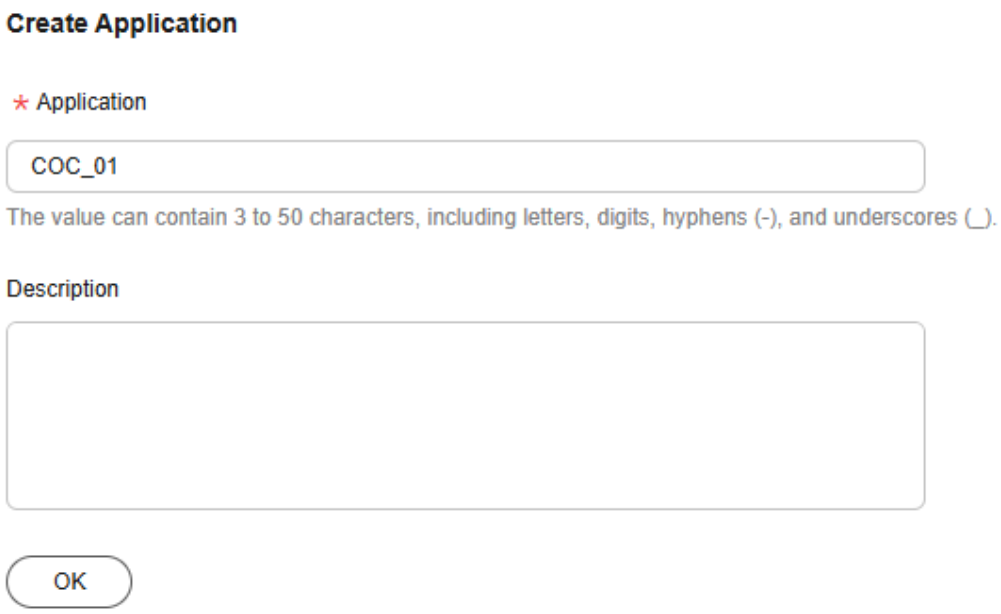


Step 3 Set **Application Structure Type** to **Lightweight**.

Step 4 Specify **Application** and **Description**. For example, set the application name to **COC_01**.

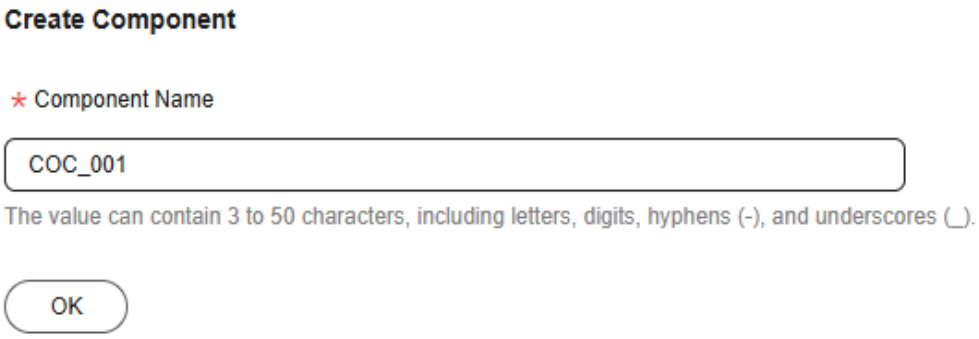
Step 5 Click **OK**.

Figure 1-3 Creating an application



Step 6 Specify the component name, for example, **COC_001**, and click **OK**.

Figure 1-4 Creating a component



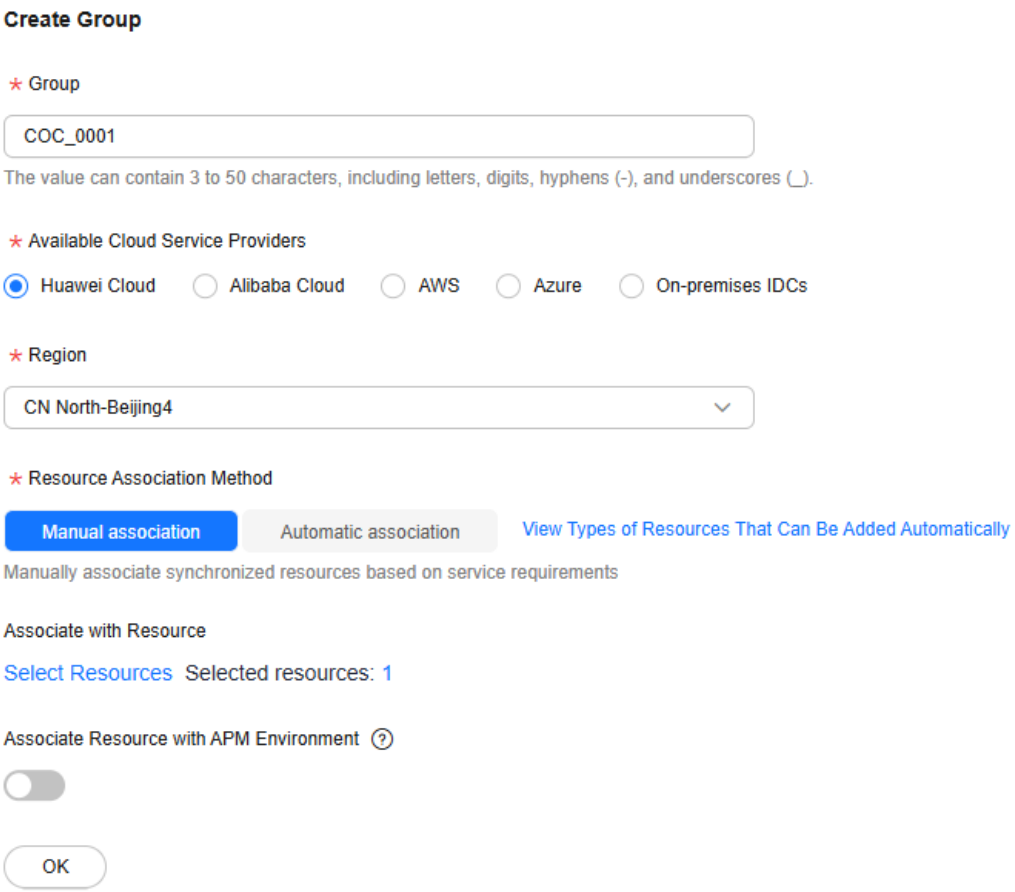
Step 7 Configure the new group by referring to **Table 1-1** and retain the preset values for other parameters.

Table 1-1 Parameters for creating a group

Parameter	Description
Group	Customize a group name based on the naming rule. For example, **COC_0001**.
Available Cloud Service Providers	Select the cloud service provider to which the target instance belongs. Example: **Huawei Cloud**.
Region	Select a region from the drop-down list. For example, **CN North-Beijing4**.

Parameter	Description
Resource Association Method	Select a resource association method. For example, **Manual association**.
Associate with Resource	Manually associate the corresponding resource data with the group.

Figure 1-5 Creating a group



Step 8 Click **OK**.

Step 9 Click **OK** in the lower part of the page to complete the resource modeling.

----End

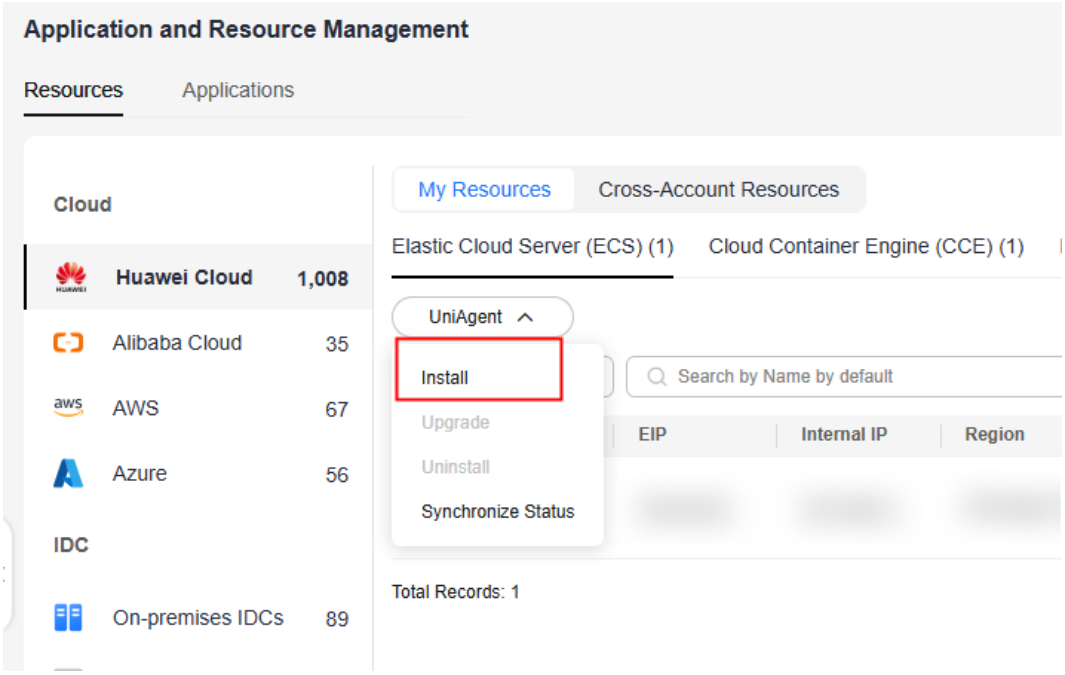
Performing Operations on a UniAgent

Step 1 In the navigation pane, choose **Resources** > **Application and Resource Management**.

Step 2 Click the **Resources** tab. On the **My Resources** tab page, select the specified instances.

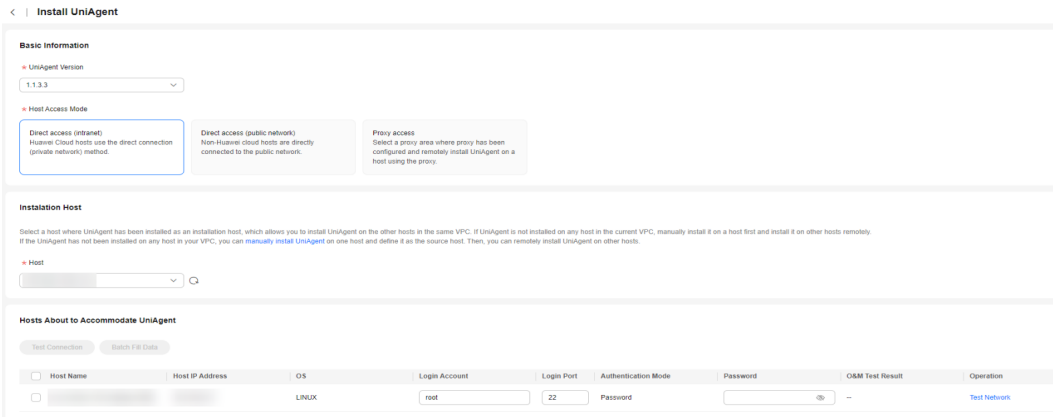
Step 3 Click **UniAgent** and select **Install**.

Figure 1-6 Installing a UniAgent



Step 4 On the displayed **Install UniAgent** page, specify required information and click **OK** to trigger the automated installation process. Wait until the installation is complete.

Figure 1-7 Setting parameters



NOTE

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

----End

2 Creating a Ticket and Notifying the Shift Role

You can manage O&M engineers, schedule shifts, and configure notification rules on COC.

- You can centrally manage O&M engineers on COC using this feature. You can manage users of the current tenant on the **O&M Engineer Management** page. The basic user data on the **O&M Engineer Management** page is synchronized from Identity and Access Management (IAM) and is used by multiple basic functional modules in creating to-do tasks, performing scheduled O&M, managing notifications, managing incidents, and more.
- You can manage O&M engineers centrally, from multiple dimensions, in different forms, or based on your other custom requirements. You can also create shift scheduling scenarios and roles and add members to the scenarios and roles as required.
- The notification management module allows you to create notification subscription instances that contain notification scenarios and matching rules. When an O&M ticket is generated, the notification module first matches the ticket with notification rules and scenarios, then parses the O&M engineers to be notified, the notification content, and notification method, and finally sends the notification messages.

The preceding basic configurations can be applied to incident ticket processes, issue ticket processes, O&M owners, review scenarios, and notifications.

This section uses the creation of an issue ticket and notification to the schedule role as an example to describe how to set basic configurations for O&M.

Operation Process

1. **Preparations**: Sign up for a HUAWEI ID, complete real-name authentication, and enable COC.
2. **Synchronizing O&M engineer information**: Synchronize users and basic information under the current Huawei Cloud account.
3. **Creating shift scenarios and roles**: Create incident, change, and issue ticket execution scenarios, and set shift roles as owners to realize O&M engineer management.

4. **Configuring notification rules**: Create notification rules for scenarios. After a scenario is triggered, notifications are automatically sent to the responsible engineer.
5. **Creating issue tickets**: Create an issue ticket to track the product usage process for issues such as function defects and poor performance. You can configure notification rules on the **Notification Management** module to manage issue tickets.

Preparations

1. Sign up for a HUAWEI ID and complete real-name authentication.

   Before using COC, **sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication**.

   If you already have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Enable COC.

   Upon your first login, **enable COC** first.

   If you have enabled COC, skip this step.

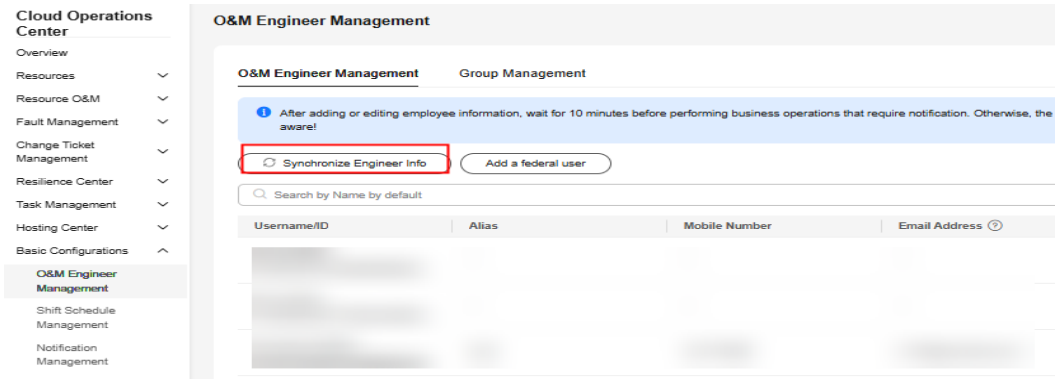
Synchronizing O&M Engineer Information

Step 1 Log in to **COC**.

Step 2 In the navigation pane, choose **Basic Configurations** > **O&M Engineer Management**.

Step 3 Click **Synchronize Engineer Info**.

Figure 2-1 Synchronizing information about O&M engineers



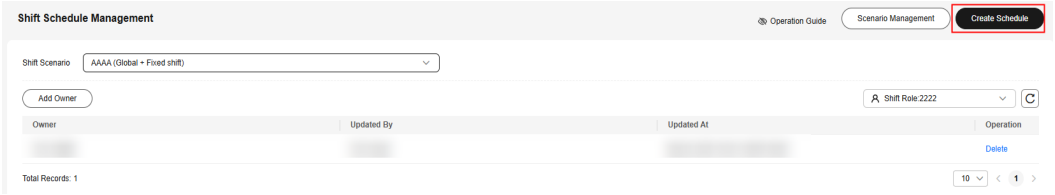
----End

Creating Shift Schedules

Step 1 In the navigation pane, choose **Basic Configurations** > **Shift Schedule Management**.

Step 2 On the shift schedule management page, click **Create Schedule**.

Figure 2-2 Creating a shift schedule



Step 3 On the **Create Schedule** page, configure the shift scenario.

Figure 2-3 Configuring a shift scenario

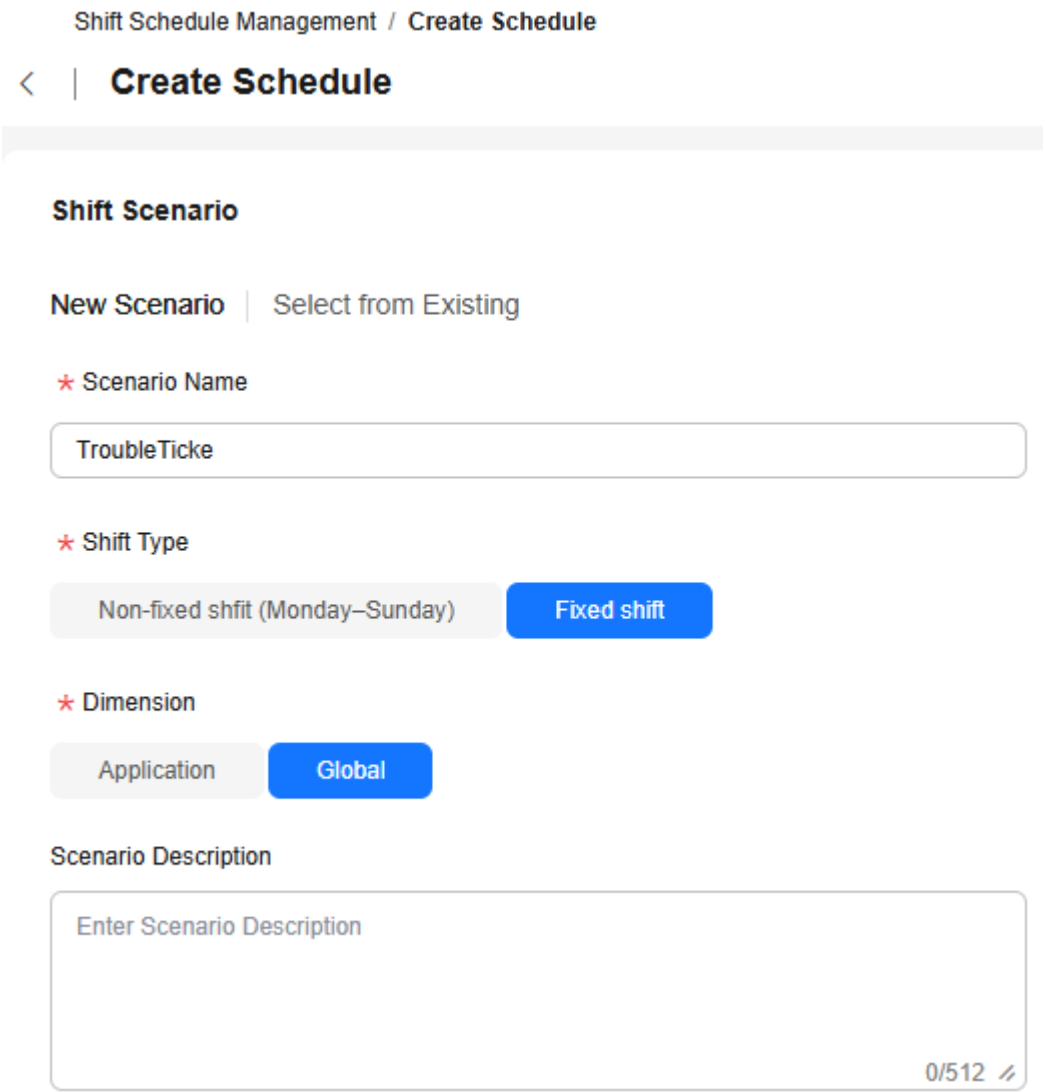


Table 2-1 Parameters for creating a scenario

Parameter	Example Value	Description
Scenario Name	Ticket Handling	Name of a customized shift scenario.

Parameter	Example Value	Description
Shift Type	Fixed Shift	The options are **Non-fixed shift (Monday-Sunday)** and **Fixed shift**. • **Non-fixed shift (Monday–Sunday)**: Engineers work different shifts depending on the schedule. • **Fixed**: Engineers work within fixed working hours.
Scheduling Dimension	Global	The options are **Application** and **Global**. • **Application**: The schedule is created for an application in a specific region (optional). • **Global**: The schedule is globally used regardless of applications.
Scenario Description	-	(Optional) Enter the detailed description of the shift scenario.

Step 4 Set parameters for the shift role and click **OK**.

Figure 2-4 Setting parameters for a shift role

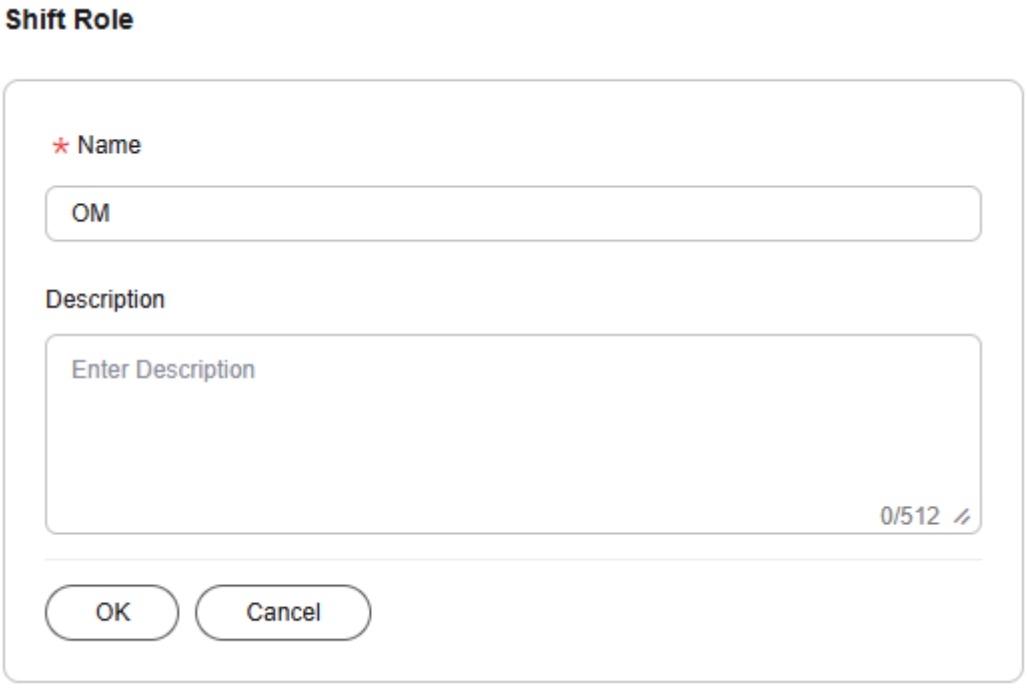
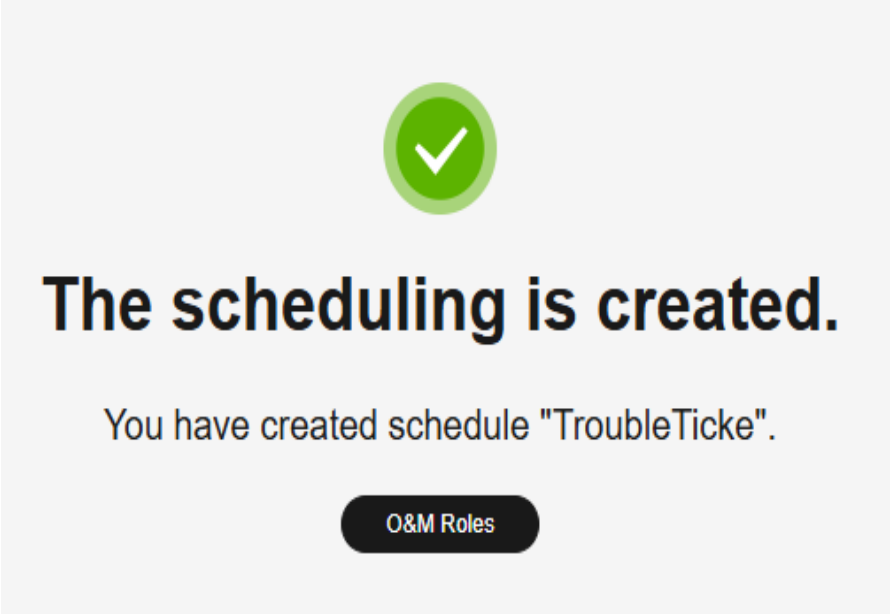


Table 2-2 Parameters for setting a scheduling role.

Parameter	Example Value	Description
Name	O&M	Name of a user-defined role.
Description	-	(Optional) Enter the detailed description of the role.

Step 5 Click **OK**.

Figure 2-5 Completing the schedule creation

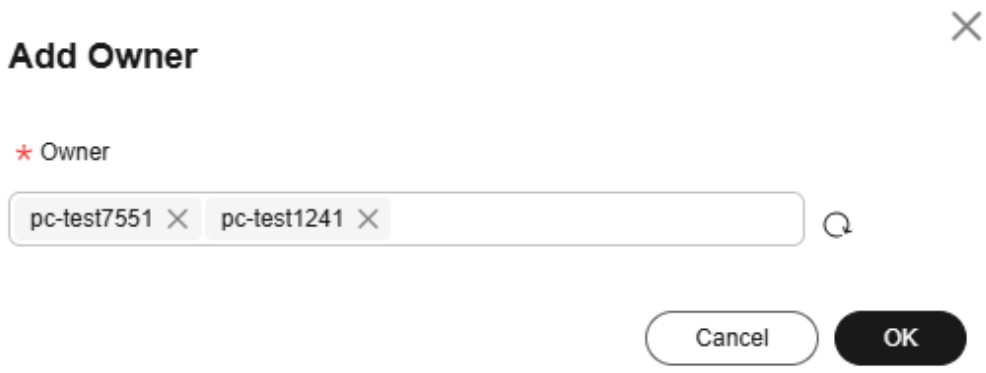


Step 6 Click **O&M Roles** to return to the shift management page.

Step 7 On the displayed page, click **Add Owner** to add owner to the shift schedule.

Step 8 Select a user from the drop-down list. Multiple users can be selected.

Figure 2-6 Adding personnel



Step 9 Click **OK**.

Personnel for scheduling are added.

----End

Configuring Notification Rules

You can create a notification rule. After an incident, issue, or change ticket matches its conditions, a notification is automatically sent.

Step 1 In the navigation pane, choose **Basic Configurations** > **Notification Management**.

Step 2 Click **Create Notification** in the upper right corner.

Step 3 Set basic information.

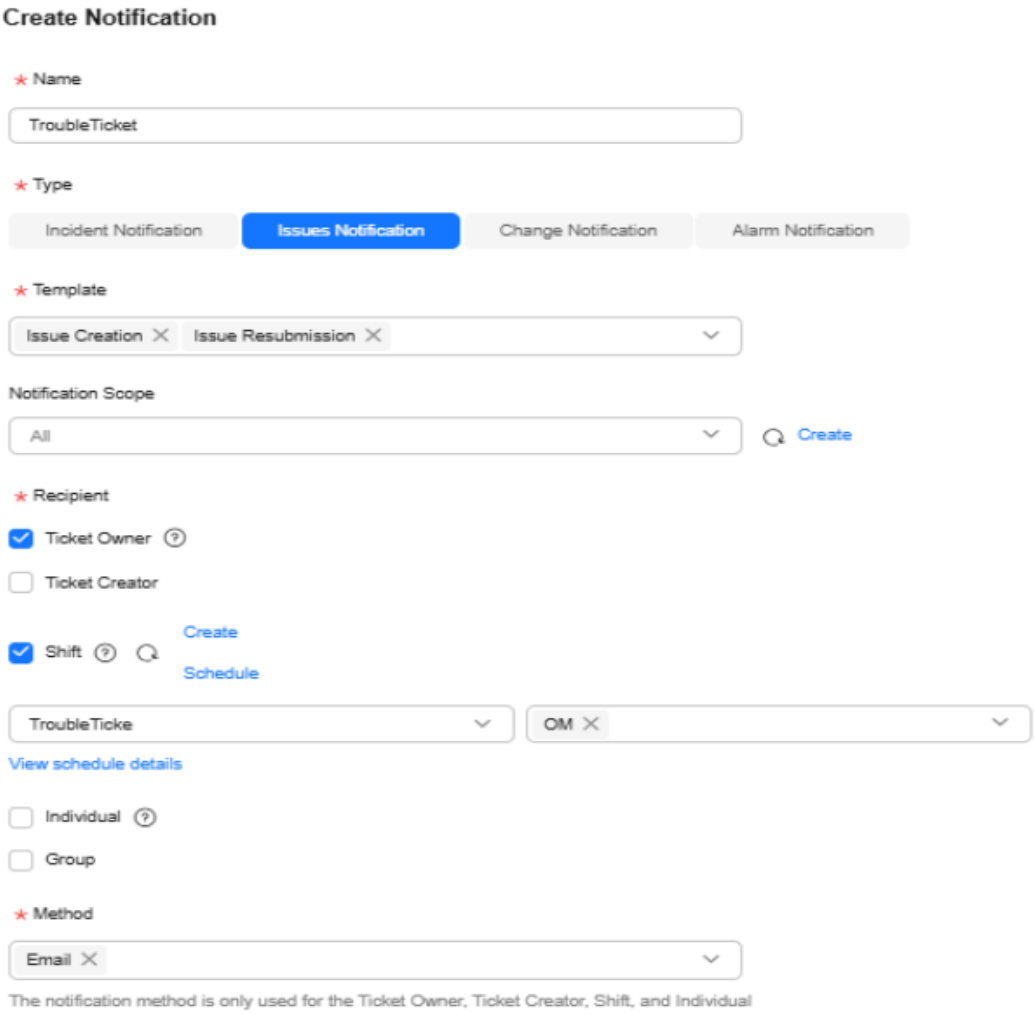
This example describes only the mandatory parameters. Retain the preset values for other parameters. For details about the parameters, see **Notification Management**.

Table 2-3 Parameters for creating a notification

Parameter	Example Value	Description
Name	Trouble ticket	Notification name that you can customize.
Type	Select **Issue Notification**.	The options are **Incident notification**, **Issue notification**, **Change notification**, and **Alarm notification**.
Template	Select **Issue creation** and **Issue resubmission**.	Select a notification template from the drop-down list. Multiple templates can be selected. Notification content templates are preset by the system. The template list varies depending on the notification type. After a template is selected, the notification template details are displayed.

Parameter	Example Value	Description
Recipient	Select **Shift** and select the shift scenario and shift role set in **Creating Shift Schedules** from the drop-down list.	The options are **Ticket owner**, **Ticket creator**, **Shift**, **Individual**, and **Group**. Multiple options can be selected at a time. Set the objects to be notified and send notifications to the corresponding recipients. • **Ticket creator**: This parameter is not required if you need to notify users of an alarm. • **Shift**: Select a scenario and role from the drop-down lists based on the configured values. • **Individual**: Select an individual that you want to notify. • **Group**: Select a group you want to send notifications to and specify target group members as the recipients. You can also specify the service ticket owner as the recipient. If you do not specify the service ticket owner or other group members as the recipients, all of them in the group will be selected by default.
Method	Select **Email**.	You can select **All**, **SMS**, **Phone Call**, **Lark**, **WeCom**, **DingTalk**, or **Email**. Multiple options can be selected. WeCom, Lark, and DingTalk need to be configured in **Mobile App Management**.

Figure 2-7 Creating a notification



Step 4 Click **OK**.

----End

Creating Issue Tickets

You can create a notification rule. After an incident, issue, or change ticket matches its conditions, a notification is automatically sent.

Step 1 In the navigation pane on the left, choose **Fault Management** > **Issues**.

Step 2 Click **Create Issue Ticket** in the upper right corner.

Step 3 Set basic information.

This example describes only the mandatory parameters. Retain the preset values for other parameters. For details about the parameters, see **Notification Management**.

Table 2-4 Parameter description

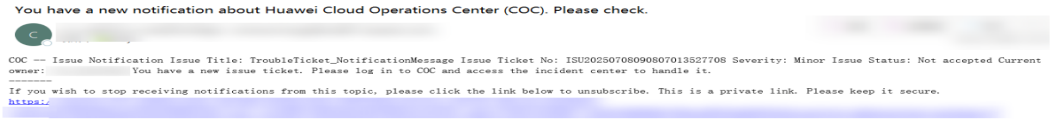
Parameter	Example Value	Description
Issue Title	Issue ticket_Notification	Customize the issue title.
Symptom	-	Description of the issue symptoms and impacts on the live network.
Enterprise Project	default	Select an enterprise project from the drop-down list.
Issue Source	Proactively detected by O&M personnel	Optional The options are **incident**, **alarms**, **WarRoom**, and **Proactive O&M discovery**. Select the source of the issue. If you select **incident**, **alarms**, or **WarRoom**, you need to associate the corresponding service ticket.
Issue Application	test	Select the issue application from the drop-down list.
Severity	Minor	The value can be **Critical**, **Major**, **Minor**, or **Prompts**. • **Critical**: The system or application breaks down, stops, or suspends, causing data loss. Main functions are unavailable, or the module or related modules are abnormal. • **Major**: Some main functions of the system are unavailable, data cannot be saved, and secondary functions of the system are unavailable. The fault is limited to the module. As a result, the module functions are invalid or the module exits abnormally. • **Minor**: Secondary functions are not completely implemented but are not affected, for example, the prompt information is inaccurate, the user interface is poor, the operation time is long, and some module functions are invalid. • **Prompts**: Minor software defects that cause inconvenience or trouble to operators but do not affect the operation and execution of functions.
Type of Issue	This does not affect service functions of the FusionCube.	Select the issue type from the drop-down list.

Parameter	Example Value	Description
Owner	Select **Shift** and select the shift scenario and shift role set in **Creating Shift Schedules** from the drop-down list.	The value can be **Shift** or **Individual**. • **Shift**: Select a scenario and role from the drop-down lists based on the configured values. • **Individual**: Select an owner.

Step 4 Click **OK**.

The ticket status is **Not accepted**, and the shift role will receive a notification for accepting the ticket.

Figure 2-8 Notification for accepting a ticket



----End

3 Restarting an ECS by Executing a Job

Scenarios

COC is a secure and efficient O&M platform, offering one-stop, AI-powered solutions for all your centralized O&M needs. The job management function of COC allows you to customize jobs and execute jobs on target VMs. You can use this function to perform operations on target instances, which can be ECSs or BMSs currently.

This section describes how to restart an ECS on COC.

Operation Process

Procedure	Description
Prepare for the task.	You need to sign up for a HUAWEI ID, complete real-name authentication, and enable COC.
Step 1: Synchronize resources.	This task obtains resources in all regions to which the current user belongs and synchronizes the resources to COC.
Step 2: Install a UniAgent.	You can install an UniAgent on each desired node for information exchange between COC, lower-layer services, and hosts.
Step 3: Execute a job.	On COC, you can enjoy automated job execution on ECSs.

Preparations

1. Sign up for a HUAWEI ID and complete real-name authentication.

   Before using COC, **sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication**.

   If you already have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Enable COC.

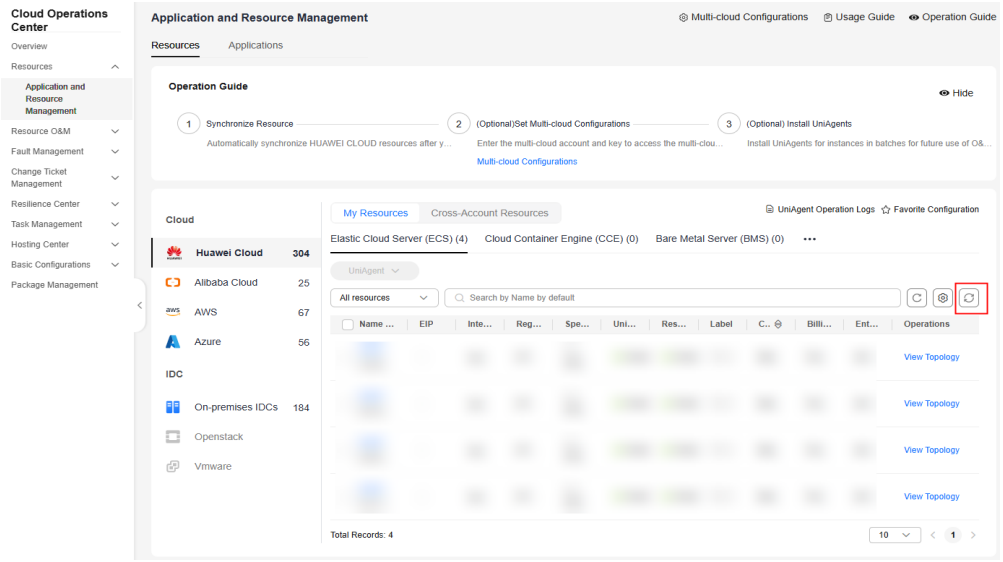
Upon your first login, **enable COC** first.

If you have enabled COC, skip this step.

Step 1: Synchronize Resources.

1. Log in to **COC**.
2. In the navigation pane, choose **Resources** > **Application and Resource Management**.
3. Click  to synchronize resources.

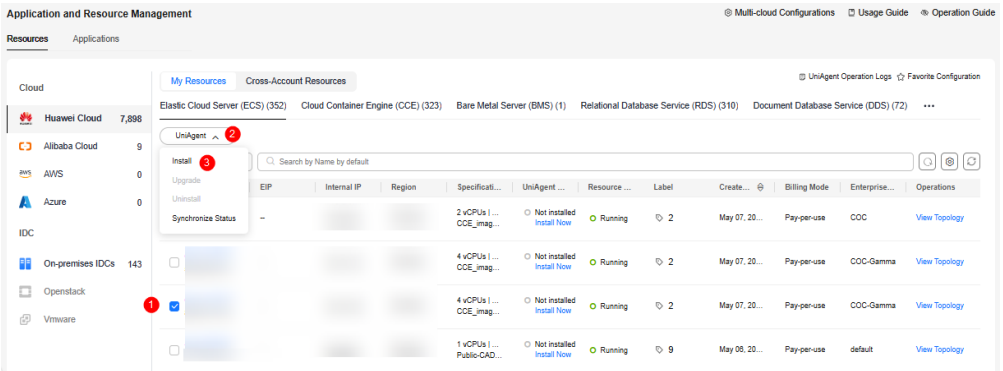
Figure 3-1 Synchronizing resources



Step 2: Install a UniAgent.

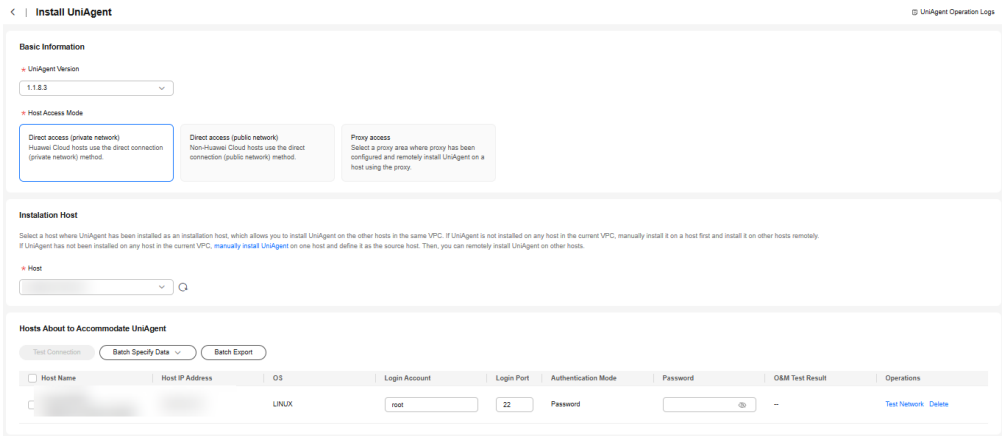
1. Access the **Resources** tab page, select the target ECSs and choose **UniAgent** > **Install**.

Figure 3-2 Installing a UniAgent



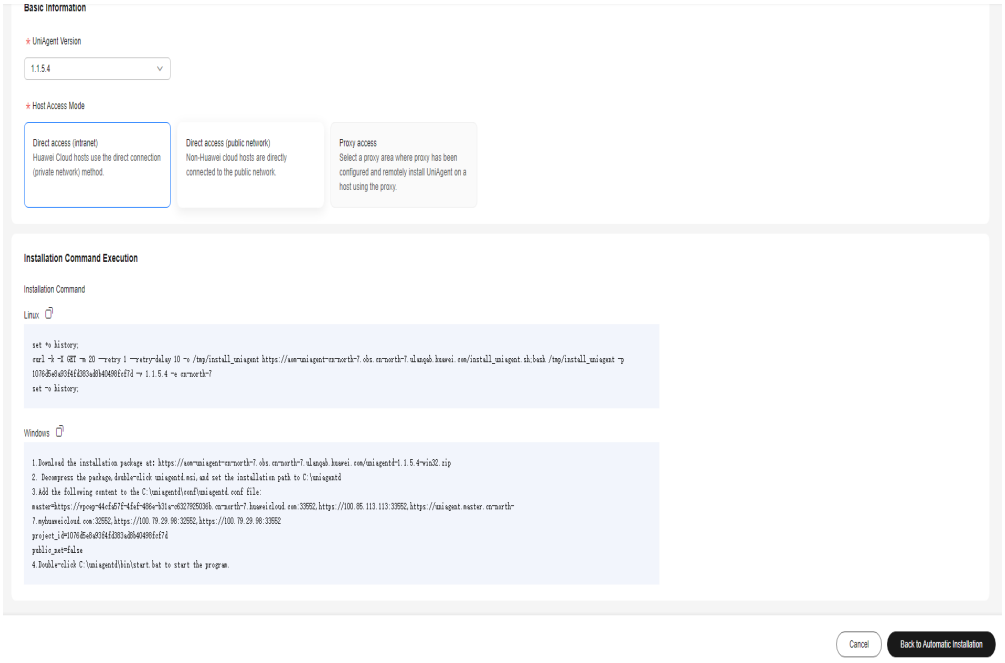
2. Click **manually install UniAgent**. The page for manually installing the UniAgent is displayed.

Figure 3-3 UniAgent installation page



3. Run the installation command on the page to manually install the UniAgent.

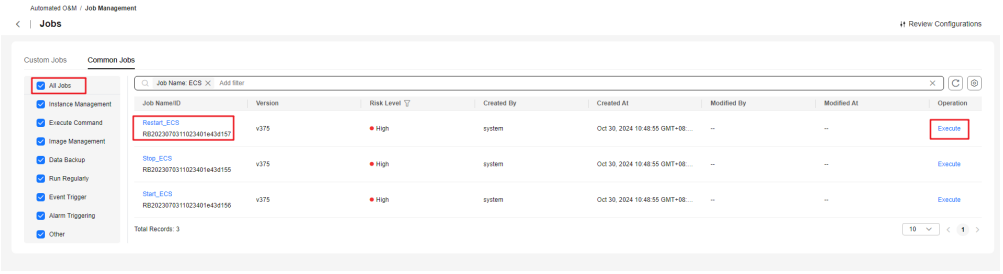
Figure 3-4 Manually installing a UniAgent



Step 3: Execute a Job.

1. In the navigation pane on the left, choose **Resource O&M** > **Automated O&M**.
2. In the Routine O&M area, click **Jobs**.
3. Click the **Public Jobs** tab.
4. Select **All Jobs**, locate the ECS restart job, and click **Execute**.

Figure 3-5 Selecting a job to execute



5. Set execution type and basic information.

Figure 3-6 Parameters in the execution type and basic information areas

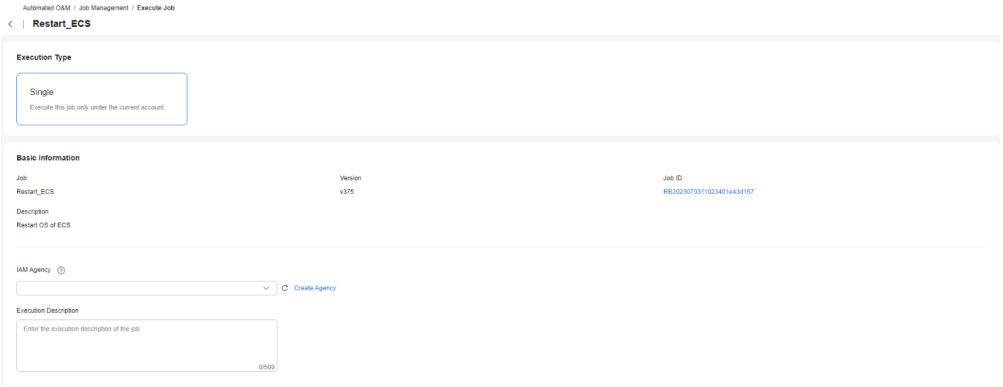


Table 3-1 Parameters in the execution type and basic information areas

Parameter	Example Value	Description
Execution Type	Single	Select the scope of the jobs to be executed.
IAM Agency	**ServiceLinkedAgencyForCOC**	Scope of permissions that can be used by COC to execute jobs.

6. Set the execution content.

Figure 3-7 Parameters in the Execution Content area

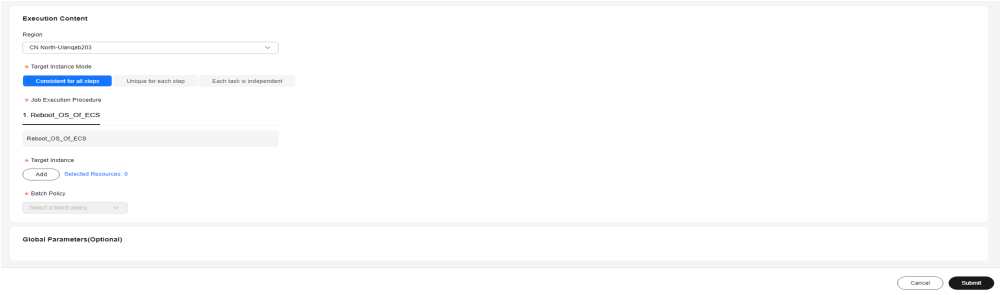


Table 3-2 Parameters in the Execution Content area

Parameter	Example Value	Description
Region	**CN North-Beijing4**	Select the region in which the target instance is located.
Target Instance Mode	Consistent for all steps	Select the execution mode for job steps and target instances.
Target Instance	N/A	Select the target instance to execute the job.
Batch Policy	No Batch	Batch execution policy of the target instance.

7. Click **Submit**.
8. Confirm the job configurations and click **OK**. The service ticket details page is displayed.
9. Refresh the page and view the job execution status.

4 Performing a Fault Drill of Increasing the CPU Usage

Scenarios

COC is a secure and efficient O&M platform, offering one-stop, AI-powered solutions for all your centralized O&M needs. You can configure drill templates and attack templates to perform fault drills on physical machines, VMs, or CCE containers in the chaos drill function module. You can also manage failure modes. You can select a target instance to execute fault drills.

This section describes how to use COC to perform a fault drill on an ECS to increase the CPU usage.

Operation Process

Procedure	Description
Prepare for the task.	You need to sign up for a HUAWEI ID, complete real-name authentication, and enable COC.
Step 1: Synchronize resources.	This task obtains resources in all regions to which the current user belongs and synchronizes the resources to COC.
Step 2: Create an Application.	An application enables you to manage the relationship between applications and cloud resources, and provides unified and timely resource environment management services for follow-up resource monitoring and automated O&M.
Step 3: Create a drill task.	Drill tasks preset drill solutions for resources and enable flexible orchestration of multiple attack tasks for fault injection.
Step 4: Start the Drill.	Automatic fault injection will start based on the created drill task once you start a drill task.

Preparations

1. Sign up for a HUAWEI ID and complete real-name authentication.

   Before using COC, **sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication**.

   If you already have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Enable COC.

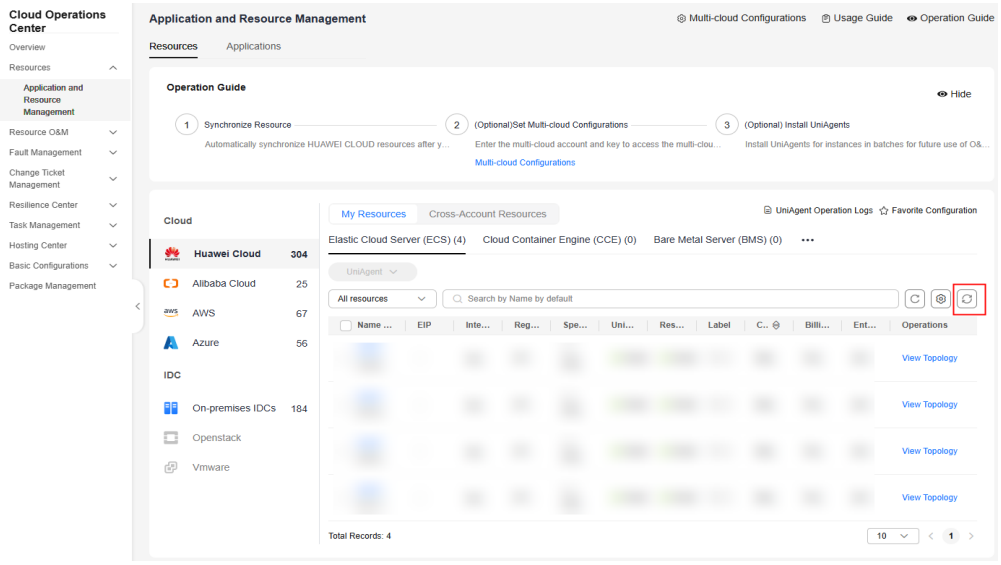
   Upon your first login, **enable COC** first.

   If you have enabled COC, skip this step.

Step 1: Synchronize Resources.

1. Log in to **COC**.
2. In the navigation pane, choose **Resources** > **Application and Resource Management**.
3. Click  to synchronize resources.

Figure 4-1 Synchronizing resources



Step 2: Create an Application.

1. In the navigation pane, choose **Resources** > **Application and Resource Management**.
2. Click the **Applications** tab.
3. Click **Create Application**.
4. Configure the application structure type.

Figure 4-2 Parameters for configuring the application structure type

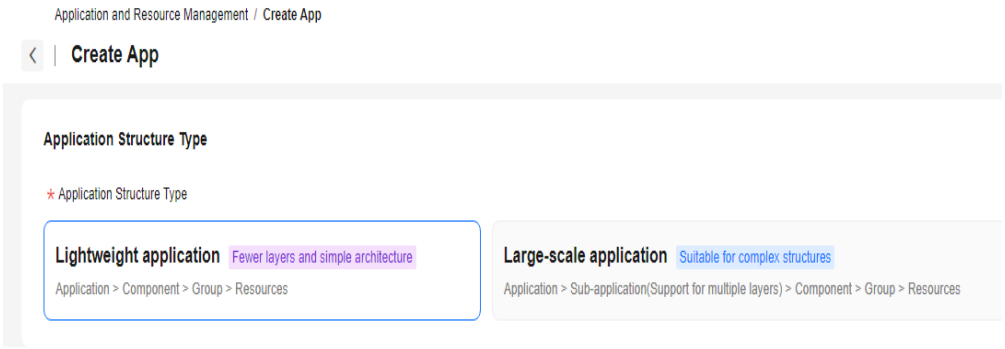


Table 4-1 Parameters for configuring the application structure type

Parameter	Example Value	Description
Application Structure Type	Lightweight application	Select a value based on the complexity of the application structure.

5. Configure the application structure.

Figure 4-3 Parameters for configuring the application structure

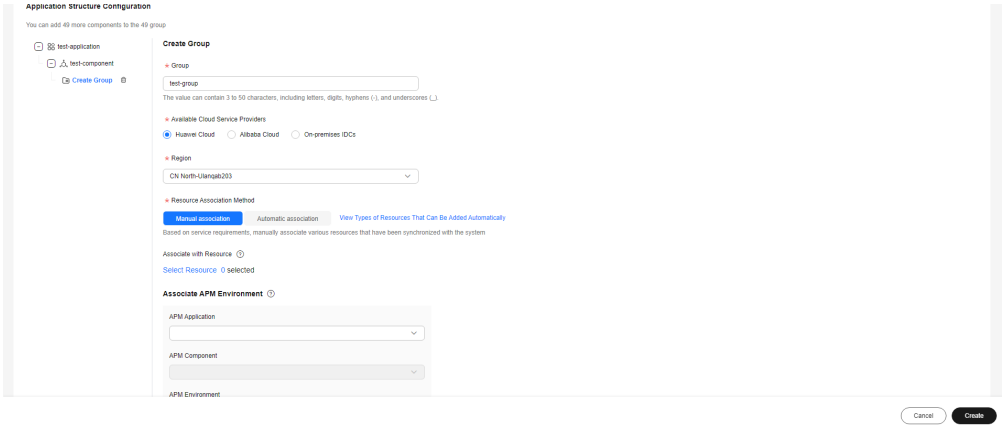


Table 4-2 Parameters in the Application Structure Configuration area

Parameter	Example Value	Description
Application	test-application	Customize an application name based on the naming rule. Click **OK**.
Component	test-component	Customize the component name based on the naming rule. Click **OK**.
Group	test-group	Customize a group name based on the naming rule.

Parameter	Example Value	Description
Available Cloud Service Providers	Huawei Cloud	Select the cloud service provider to which the target instance belongs.
Region	CN North-Beijing4	Select the region in which the target instance is located.
Resource Association Method	Manual association	Select a resource association method.
Associate with Resource	N/A	Select the target instance to execute the chaos drill. Click **OK**.

6. Click **OK**.

Step 3: Create a Drill Task.

1. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**.
2. Click the **Drill Tasks** tab.
3. Click **Create Task**.
4. Configure basic information.

Figure 4-4 Parameters for configuring the basic information

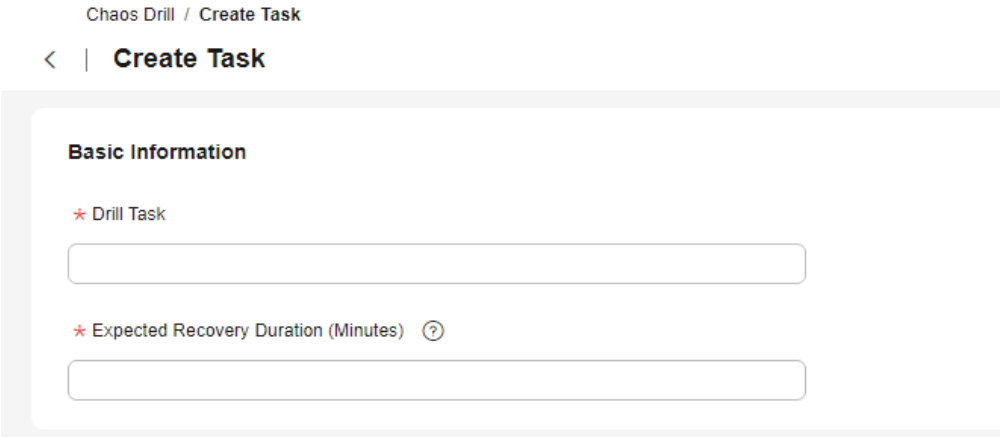


Table 4-3 Basic information parameters

Parameter	Example Value	Description
Drill Task	**test-drill**	Customize the drill task name based on the naming rules.

Parameter	Example Value	Description
Expected Recovery Duration (Minutes)	**3**	Expected time from fault occurrence to fault recovery

5. Click **Add Attack Task**. The **Create Attack Task** drawer is displayed.
6. Configure required parameters on the **Create Attack Task** page and click **Next**.

Figure 4-5 Parameters for creating an attack task

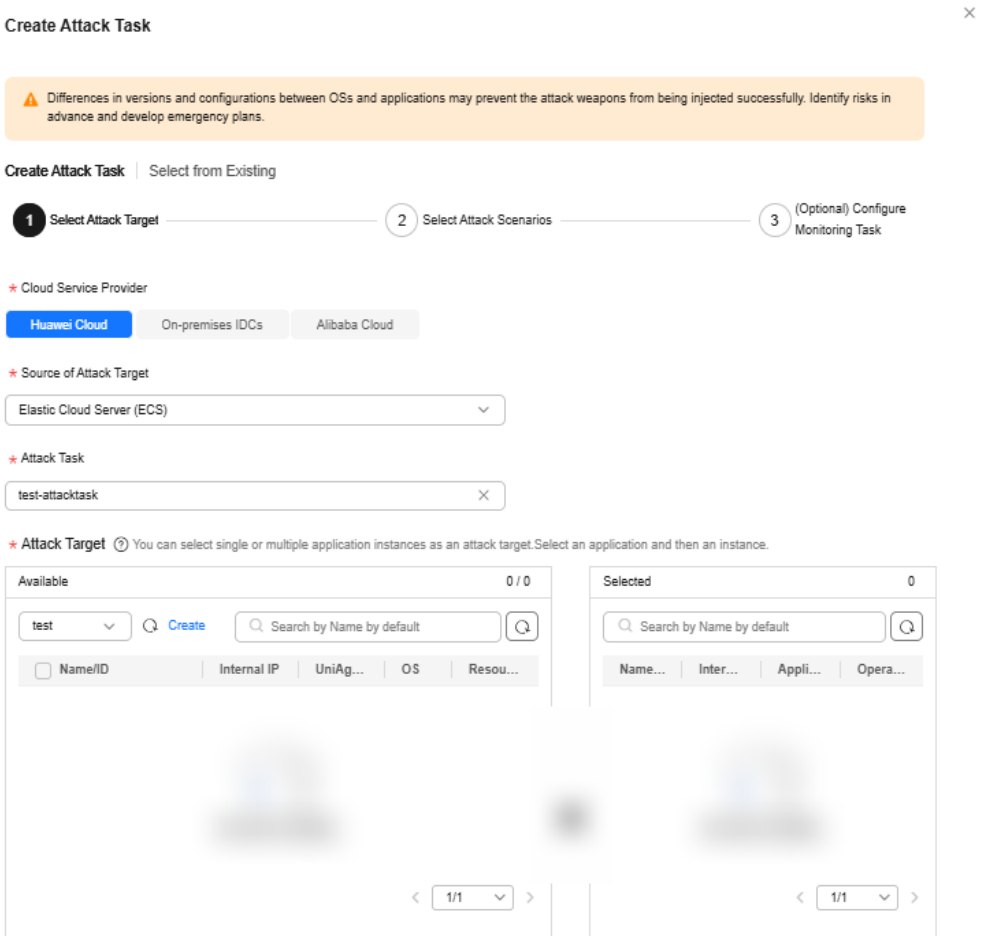


Table 4-4 Parameters for creating an attack task

Parameter	Example Value	Description
Available Cloud Service Providers	Huawei Cloud	Select a cloud vendor type.

Parameter	Example Value	Description
Source of Attack Target	Elastic Cloud Server (ECS)	Select the source of the target instance.
Attack Task	**test-attacktask**	Customize the name of the attack task based on the naming rule.
Attack Target	N/A	Select a target instance.

7. Set parameters in the **Select Attack Scenarios** step and click **Next**.

Figure 4-6 Parameters for selecting an attack scenario

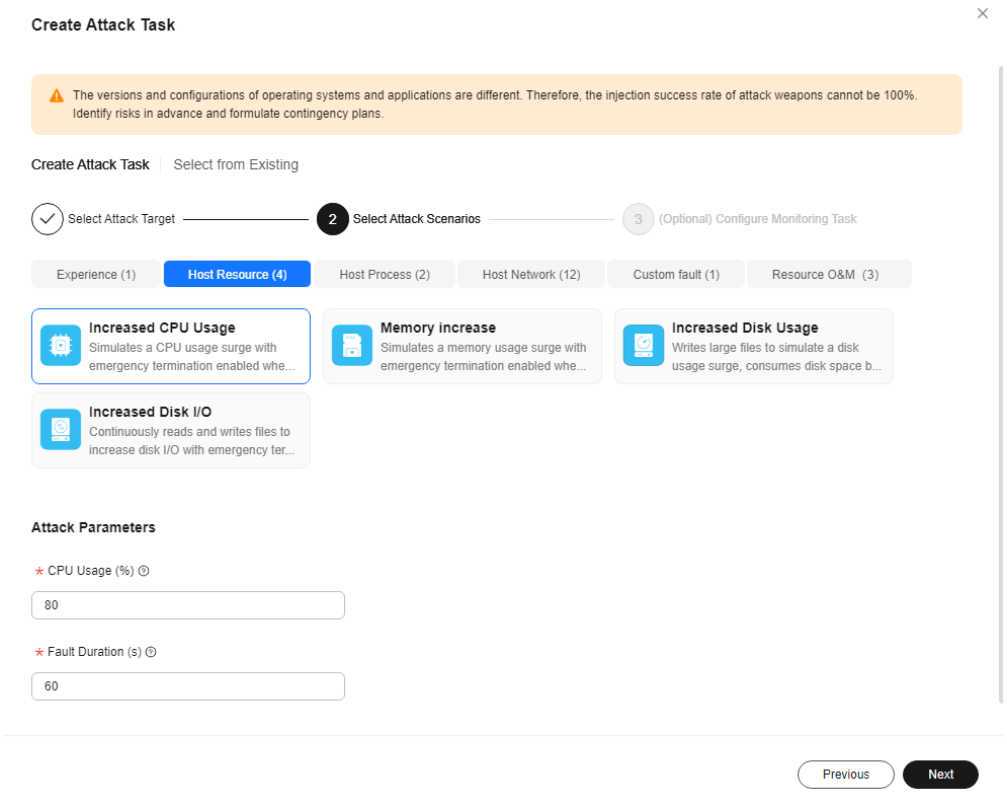


Table 4-5 Parameters for selecting an attack scenario

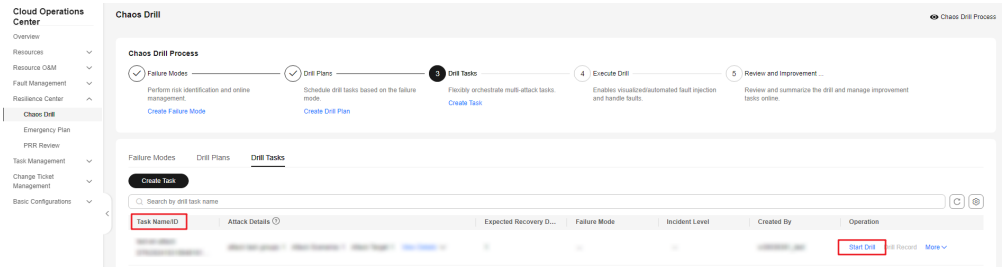
Parameter	Example Value	Description
Attack Type	Host Resource	Attack scenarios are classified based on attack scenario types.
Attack Scenario	Increased CPU Usage	Customize the name of the attack task based on the naming rule.
Attack Parameters	CPU Usage (%): 80 Fault Duration (s): 60	Configure attack parameters based on attack scenarios.

8. Click **Finish**.
9. Click **OK**.

Step 4: Start the Drill.

1. In the navigation pane on the left, choose **Resilience Center** > **Chaos Drills**.
2. Click the **Drill Tasks** tab.
3. Locate the drill task created in **Step 3** and click **Start Drill** in the **Operation** column.

Figure 4-7 Starting a drill task



4. Click **OK**.
5. Check the attack progress and details. After the drill is complete, click **Create Drill Report** in the upper right corner to create a drill report.

5 Practices for Beginners

After completing basic operations such as account registration and authorization, application resource modeling, and basic O&M configurations, you can use a series of common practices provided by COC based on your service requirements.

Table 5-1 Common best practices

Practice	Description
Standardized Fault Management	It is necessary to establish a standardized incident handling process.
E2E Chaos Engineering	You can perform chaos drills on your systems and verify and improve the system availability based on the drill results.
One-Stop Resource O&M	You can check the compliance of host OS patches to prevent service loss caused by missing OS patches.

