

Cloud Operations Center

Getting Started

Issue 01
Date 2023-11-30



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

| | |
|--|-----------|
| 1 Account Application and Authorization..... | 1 |
| 2 Modeling Associations Between Applications and Resources..... | 3 |
| 3 Basic O&M Configurations..... | 7 |
| 4 Practices..... | 11 |
| 5 Change History | 12 |

1 Account Application and Authorization

Before using COC, ensure that you have a HUAWEI ID or an IAM user that can access COC for accessing COC. This section describes how to sign up for a HUAWEI ID, enable Huawei Cloud services, and completing real-name authentication, or create an IAM user and grant permissions to the user.

Signing up for a HUAWEI ID, Enabling Huawei Cloud, and Completing Real-Name Authentication

Perform the following operations to sign up for a HUAWEI ID, enable Huawei Cloud, and complete real-name authentication. If you already have a HUAWEI ID, skip this part.

1. Visit [Huawei Cloud](#) and click **Sign Up**.
2. Sign up for a HUAWEI ID as prompted. For details, see [Registering a HUAWEI ID and Enabling Huawei Cloud Services](#).
3. Complete real-name authentication.
 - If your account is an individual account, see [Individual Real-Name Authentication](#).
 - If your account is an enterprise account, see [Enterprise Real-Name Authentication](#).

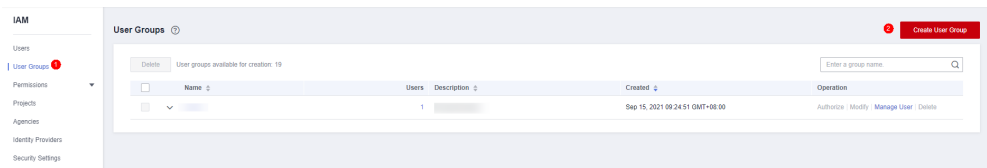
Creating an IAM User

You can use your account to create IAM users to ensure the security of accounts and resources. For more information about IAM users, see [Creating an IAM User](#). This part describes how to create an IAM user with the COC access permission. If you do not need to use any IAM users, skip this part.

1. Visit [Huawei Cloud](#), and log in to the management console using an account and its password.
2. Hover your cursor over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
3. [Create a user group and assign permissions](#) to it.

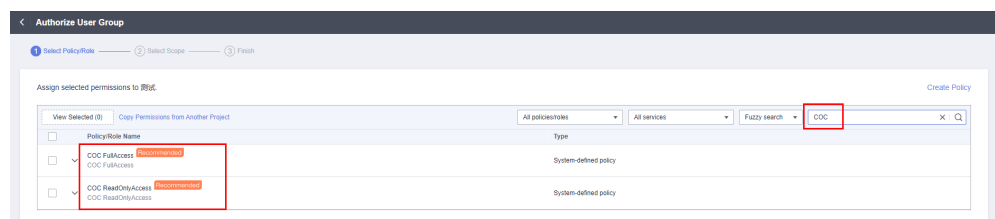
In the navigation pane, choose **User Groups**. On the displayed page, click **Create User Group**. In the displayed dialog box, enter the user group name and description and submit the configurations.

Figure 1-1 Creating a user group



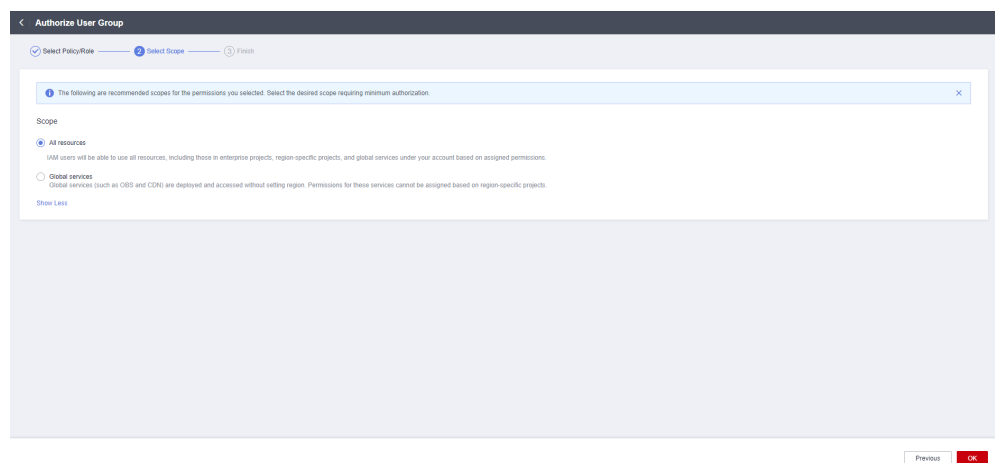
4. Locate the user group you created, and click **Authorize** in the **Operation** column. On the displayed page, enter **COC** in the search box in the upper right corner to search for policies and select the permissions you want to grant to the user group. For details about COC permissions, see [Permissions Management](#).

Figure 1-2 Selecting a policy



5. In the step for configuring the minimum authorization scope, select an authorization schema and click **OK** in the lower right corner.

Figure 1-3 Setting the minimum authorization scope



6. **Create an IAM user and add it to the user group.**
Create a user and add it to the user group authorized with COC permissions in [Step 3](#).

Obtaining Access Keys (AK/SK)

Access keys are identity credentials used to call APIs. The account administrator and IAM users can only use their own access keys to call APIs or perform authentication. For details about how to obtain the access keys, see [Access Keys](#).

2 Modeling Associations Between Applications and Resources

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. **Synchronize resources.** Obtain resource data in all regions to which the current user belongs and synchronizes the data to COC.
2. **Create an application and model the associations between the application and resources.** This feature facilitates resource management by service logic unit.
3. **Perform operations on a UniAgent.** Install, upgrade, and uninstall a UniAgent on the corresponding node.

Synchronizing Resources

Step 1 Log in to COC.


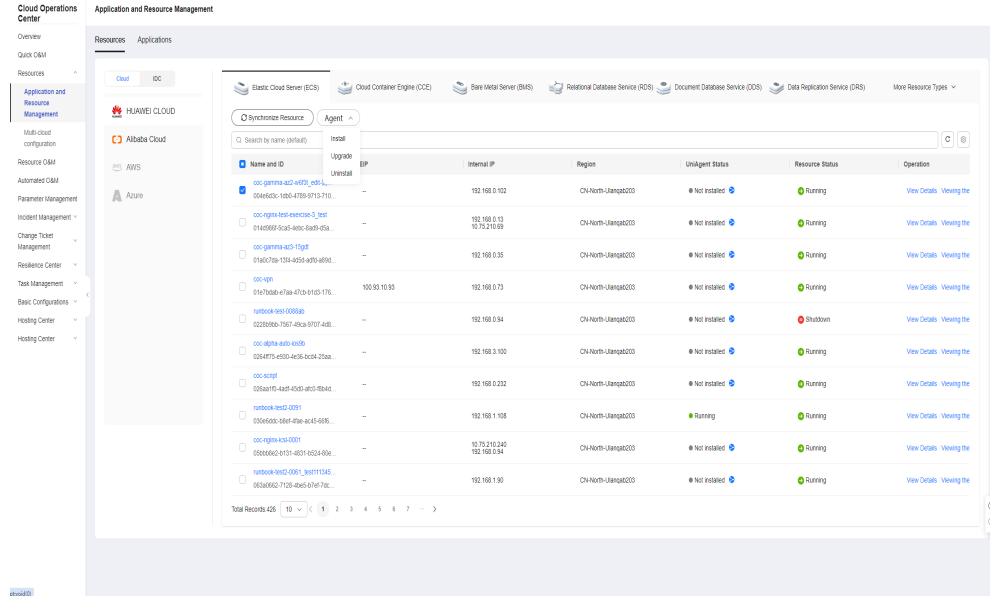
Step 2 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Resources** tab page, click  to synchronize resources.

Figure 2-1 Synchronizing resources

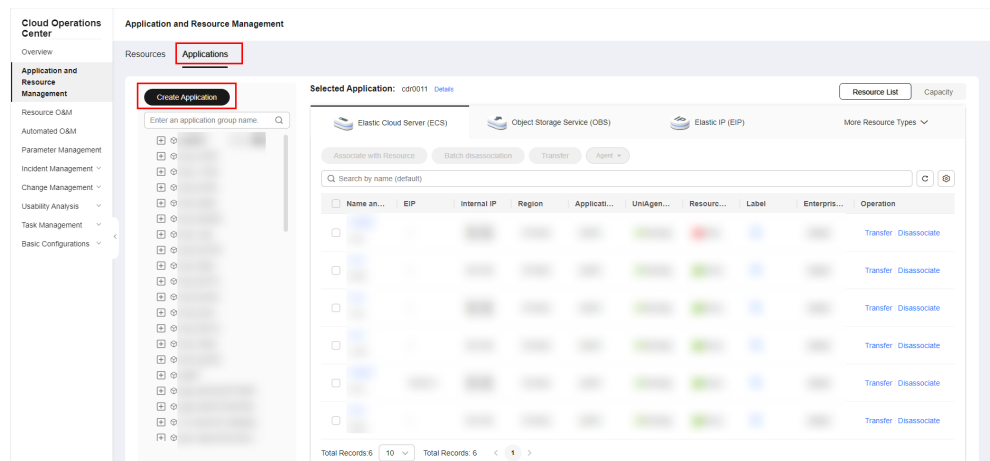


----End

Creating an Application and Creating a Model

Step 1 In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the displayed **Applications** tab page, click **Create Application** to synchronize resources.

Figure 2-2 Creating an application



Step 2 On the **Create Application** page, specify required information and click **Submit**.

Figure 2-3 Configuring required information and creating an application

----End

Performing Operations on a UniAgent

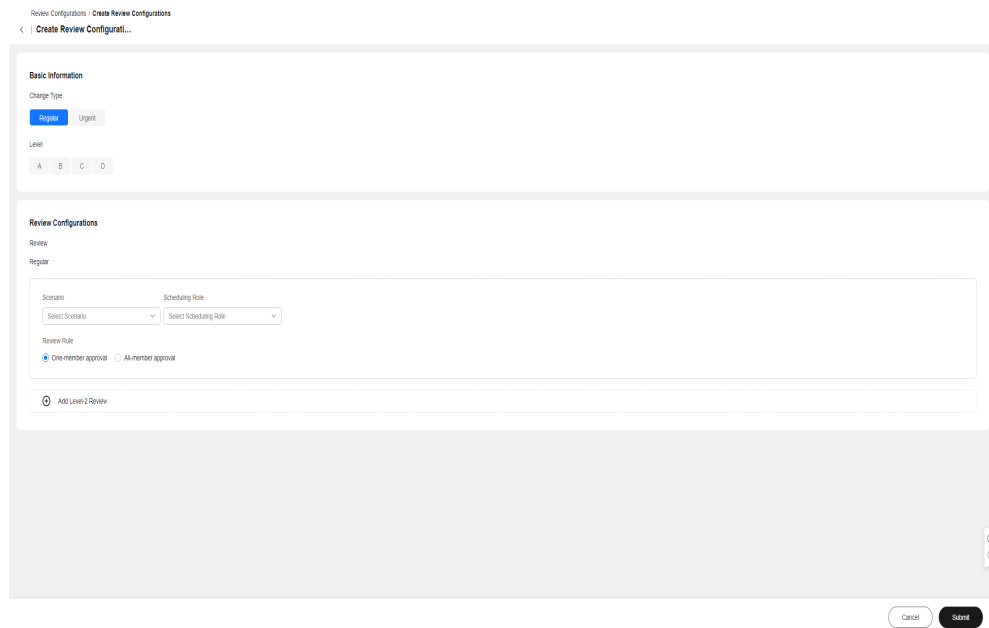
- Step 1** In the navigation pane on the left, choose **Resources > Application and Resource Management**. On the **Resources** tab page, select ECSs for which you want to install a UniAgent and click **UniAgent** and choose **Install**.

Figure 2-4 Installing a UniAgent

| Name and ID | Login | IP | Internal IP | Region | UniAgent Status | Resource Status | Operation |
|--|-------|--------------|--------------------------------|-------------------|-----------------|-----------------|--------------------------|
| ooc-gamma-ac2-w49r-w85l-0046d50c-4204-478b-9713-710... | | | 192.168.0.102 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| ooc-egins-tesl-exercise_3_inst-01468699-5a45-480c-8a09-495a... | | | 192.168.0.113 192.168.0.114 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| ooc-gamma-ac2-15gdt-0146078a-1204-4d50-a870-a89d... | | | 192.168.0.95 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| ooc-egp-0146700ab-e73a9-470b-0145-17f5... | | 100.51.10.33 | 192.168.0.73 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| natbook-nos-0090ab-02280806-7507-40ca-9707-408... | | | 192.168.0.84 | OH North-Ubang203 | Not installed | Shutdown | View Details Viewing the |
| ooc-483ha-w8h-w899-0244715-4050-4e56-4a64-20aa... | | | 192.168.3.100 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| ooc-4c19f-025a11f5-448f-4500-4a03-0ba0... | | | 192.168.0.232 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| natbook-nos-0091-0204650a-054f-47ae-4e43-609c... | | | 192.168.1.108 | OH North-Ubang203 | Running | Running | View Details Viewing the |
| ooc-egins-acc-0200-0202a660-6131-4031-4034-809a... | | | 10.75.210.249 192.168.0.94 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |
| natbook-nos-0091_nos11134d-083a0602-7120-4a20-616f-7ac... | | | 192.168.1.90 | OH North-Ubang203 | Not installed | Running | View Details Viewing the |

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

Figure 2-5 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 the this ECS as the installation node. For details, see [Installing UniAgent for the First Time](#).

----End

3 Basic O&M Configurations

This section describes how to configure parameters for managing O&M engineers, shift schedules, and notification rules on COC. These are basic O&M configurations and will be used in the incident ticket handling process, configuration of O&M operation owners, review scenarios, and notifications.

- O&M engineer management: Data on this page is the basic user data of COC and is available for authorized users to use the basic functional modules such as to-do task creation, scheduled O&M, notification management, and incident center.
- Shift schedule management: You can manage O&M engineers centrally, from multiple dimensions, in different forms, or based on your other custom requirements.
- Notification management: You can create notification instances that consist of notification scenarios and matching rules. If rule triggering conditions are met, notifications are sent to specified personnel, implementing automatic notifications.

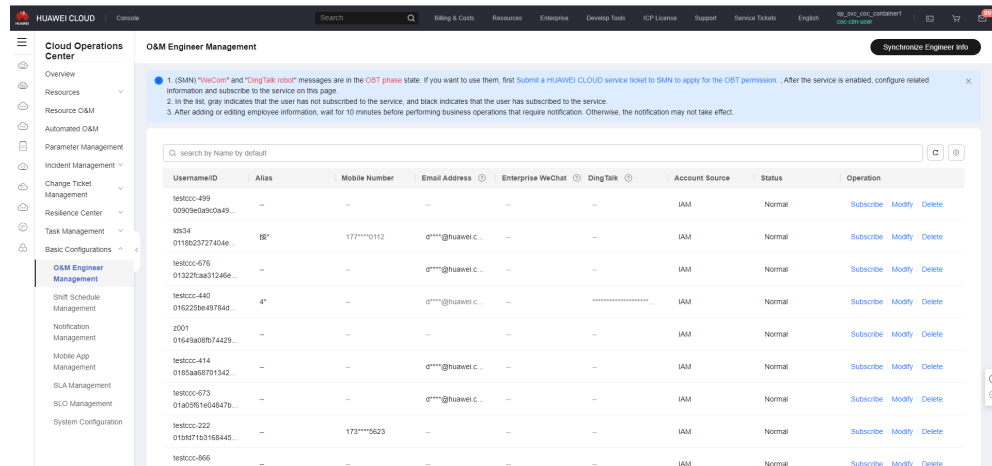
O&M Engineer Management

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. For more about O&M engineer management, see COC O&M Engineer Management.

Step 1 Log in to COC.

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

Figure 3-1 O&M engineer management



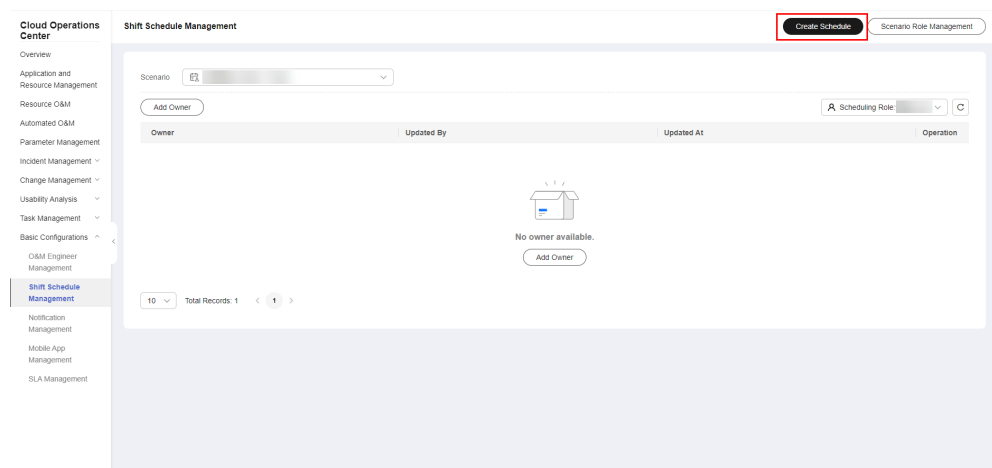
----End

Shift Schedule Management

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.

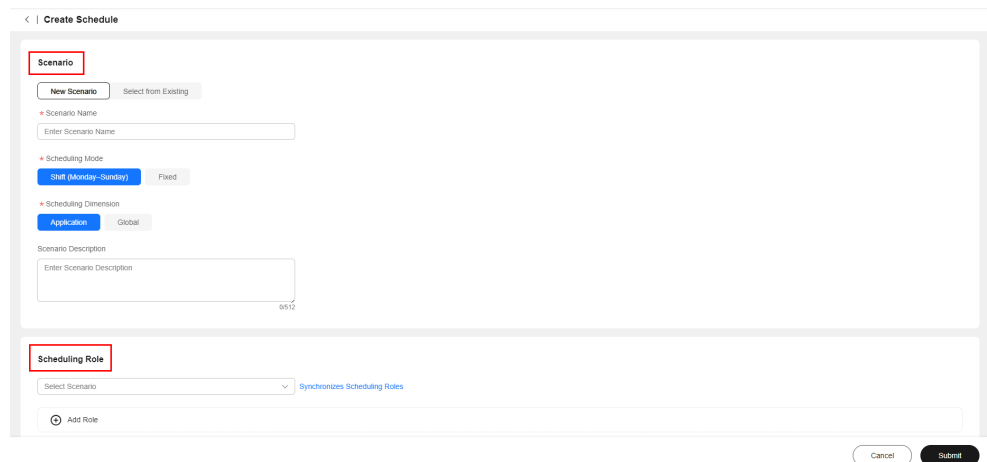
- Step 1** Log in to COC.
- Step 2** In the navigation tree on the left, choose **Basic Configuration > Shift Engineer Management**.
- Step 3** On the shift schedule management page, click **Create Schedule**.

Figure 3-2 Creating a shift schedule



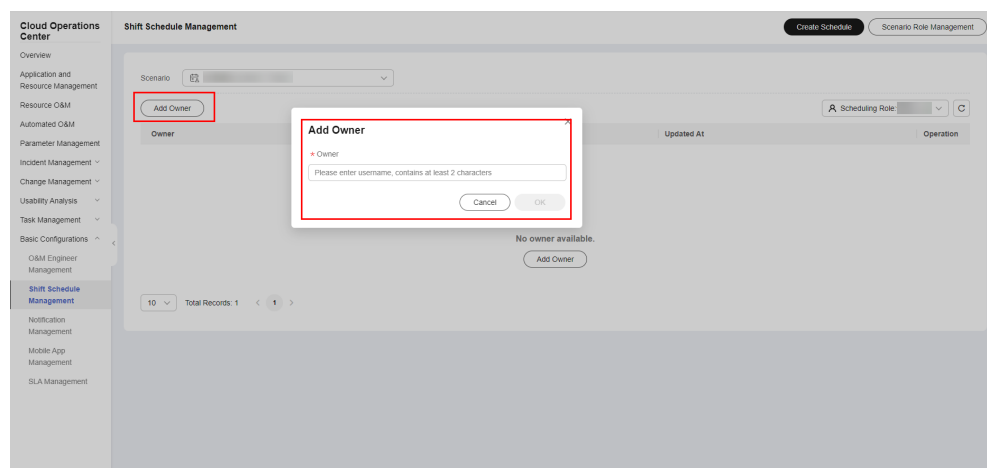
- Step 4** Add or select an existing scheduling scenario and a role.

Figure 3-3 Selecting a scheduling scenario and a role



Step 5 Return to the shift schedule management page, locate the schedule created in the previous step, and click **Add Owner** to configure owner for the schedule.

Figure 3-4 Adding a schedule owner



----End

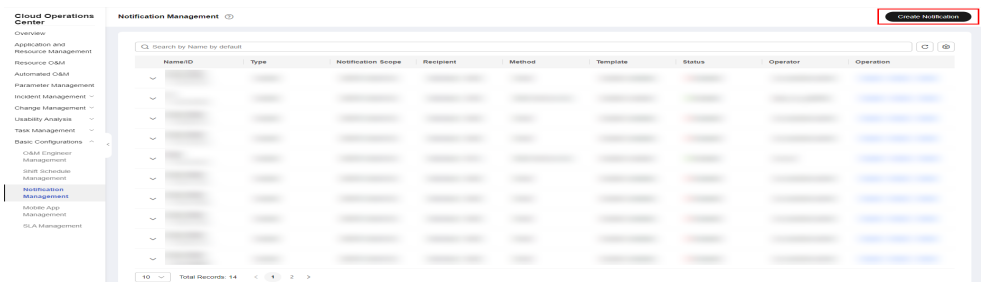
Notification Management

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.

Step 1 Log in to COC.

Step 2 In the navigation pane on the left, choose **Basic Configurations > Notification Management**. On the displayed page, click **Create Notification** in the upper right corner.

Figure 3-5 Creating a notification



Step 3 Specify the required information for creating a notification and click **OK**. For details about terms and notification rules, see COC Notification Management.

----End

4 Practices

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 4-1 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. |

5 Change History

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