Cloud Operations Center

FAQs

Issue 01

Date 2023-11-30

HUAWEI

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 Product Consulting

1.1 How Do I Configure Permissions for the COC?

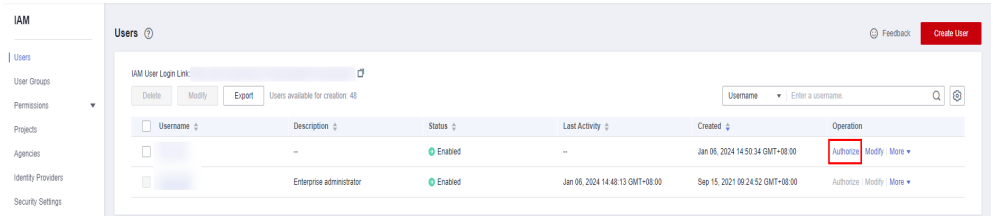
Problem Description

Quickly configuring permissions for COC is required.

Solutions

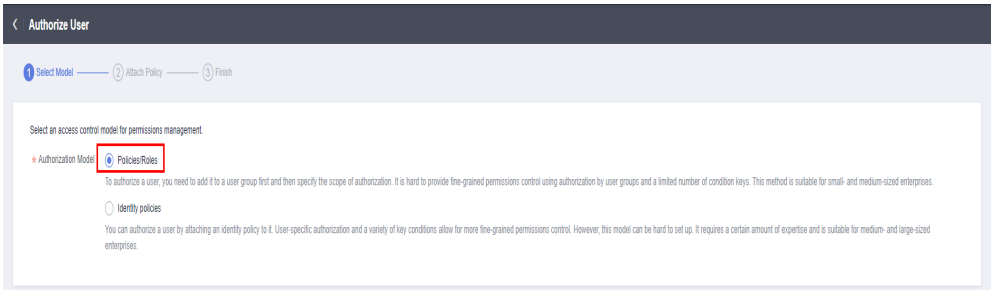
1. Log in to the IAM console as an administrator.
2. In the user list, click **Authorize** in the row that contains the target user.

Figure 1-1 Authorizing an IAM user



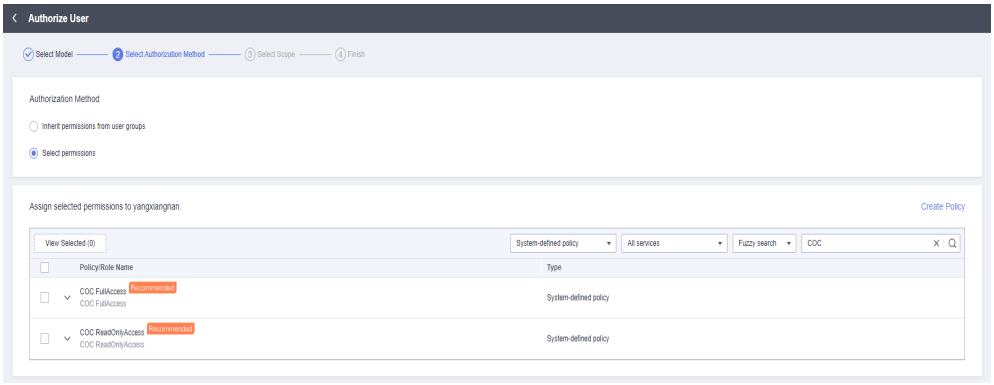
3. Set **Authorization Model** to **RBAC**.

Figure 1-2 Selecting an authorization model



4. Select **Grant permissions to the user** (applicable to enterprise projects), and assign the **COC FullAccess** or **COC ReadOnlyAccess** policy to the user as required. For details about the policy, see COC Permissions Management.

Figure 1-3 Granting COC policies

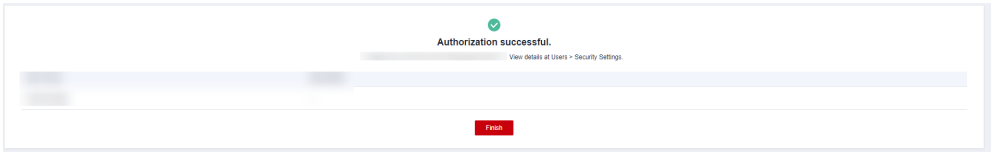


NOTE

If there is a group that has been assigned permissions of COC, you can select the button for inheriting the policies of the selected user group. For details, see IAM User Authorization.

5. Select an authorization scope scheme and specify enterprise project resources.
6. Wait until the authorization is complete.

Figure 1-4 Successful authorization



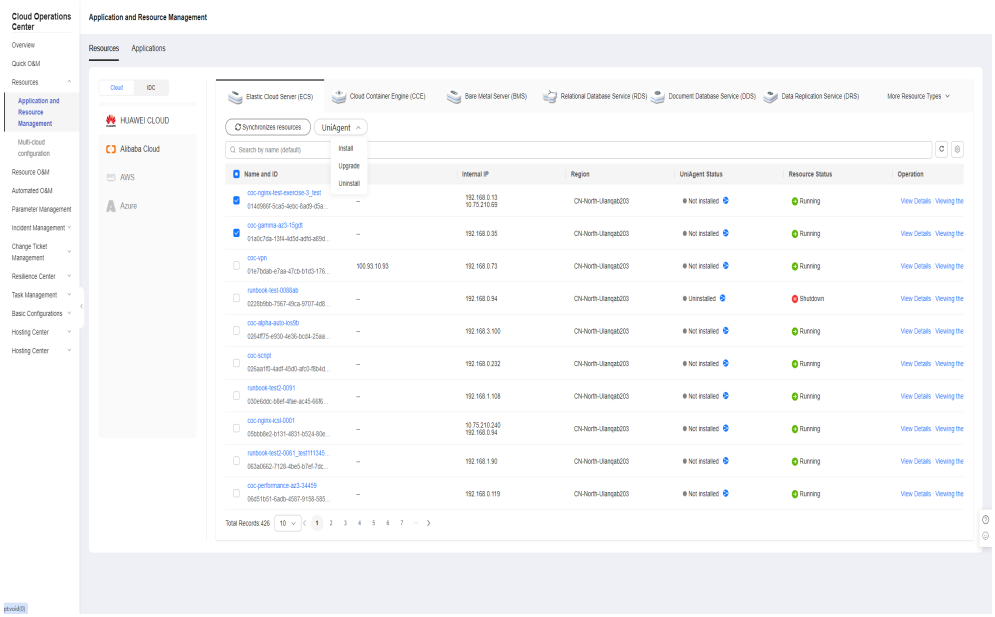
2 CMDB FAQs

2.1 How Do I Install a UniAgent for the First Time?

Step 1 Log in to **COC**.

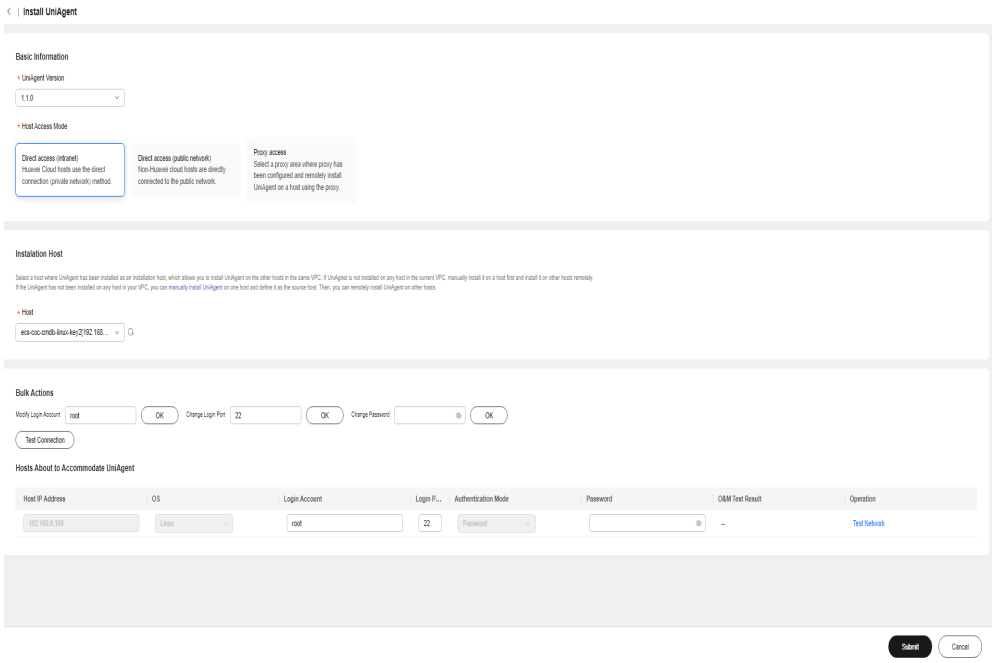
Step 2 In the navigation pane, choose **Application and Resource Management**. On the **Resources** tab page, select a host where no UniAgents have not been installed.

Figure 2-1 Installing a UniAgent



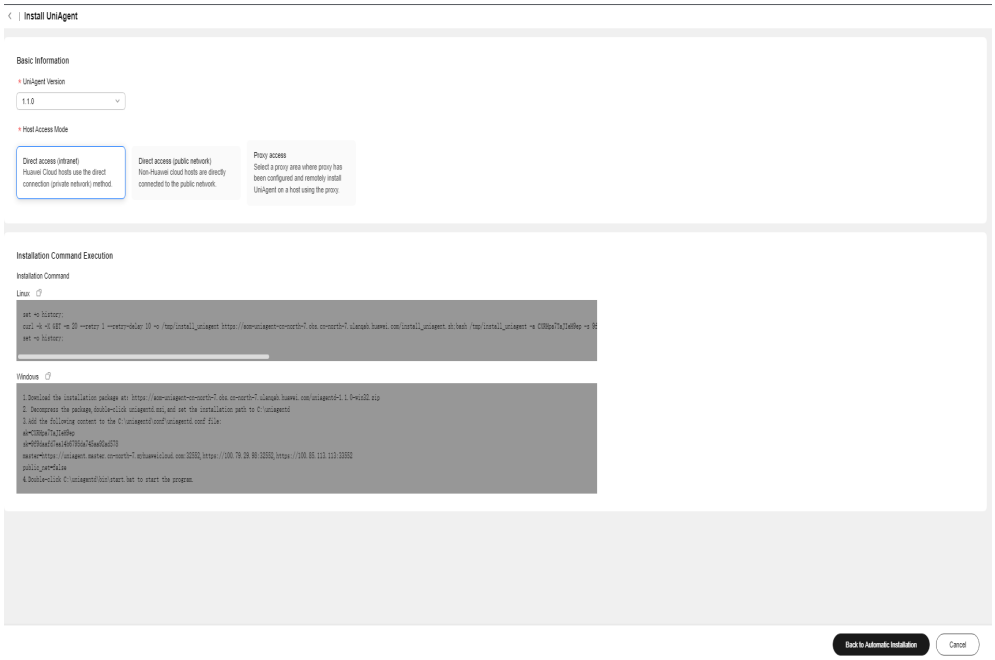
Step 3 On the UniAgent installation page that is displayed, click **Manual installation**.

Figure 2-2 UniAgent installation page



Step 4 Run the installation command on the page to manually install the UniAgent.

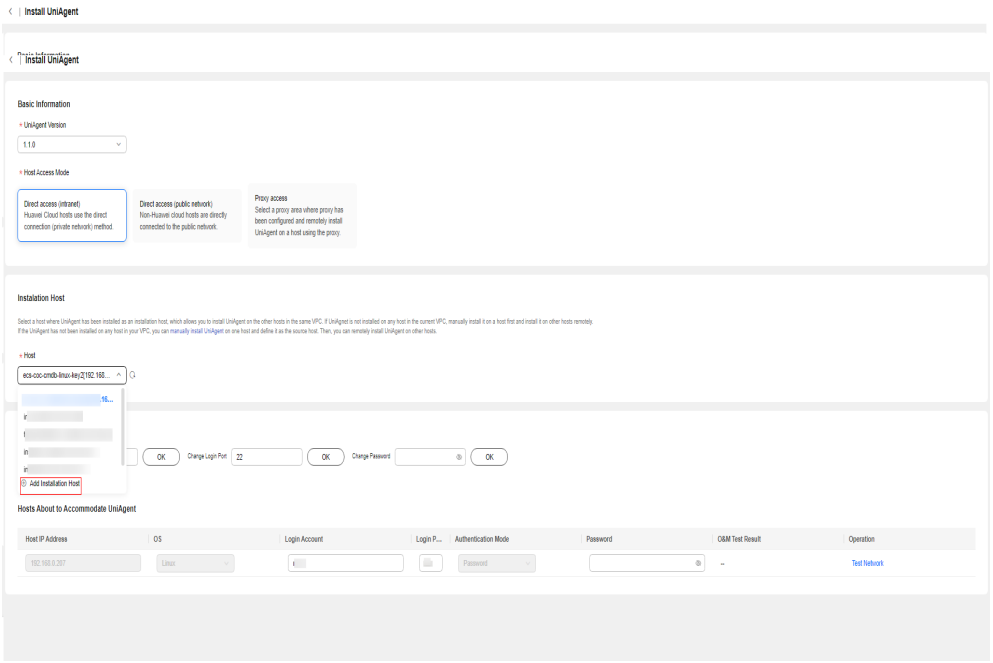
Figure 2-3 Manually installing a UniAgent



Step 5 Click **Return to Automatic Installation**.

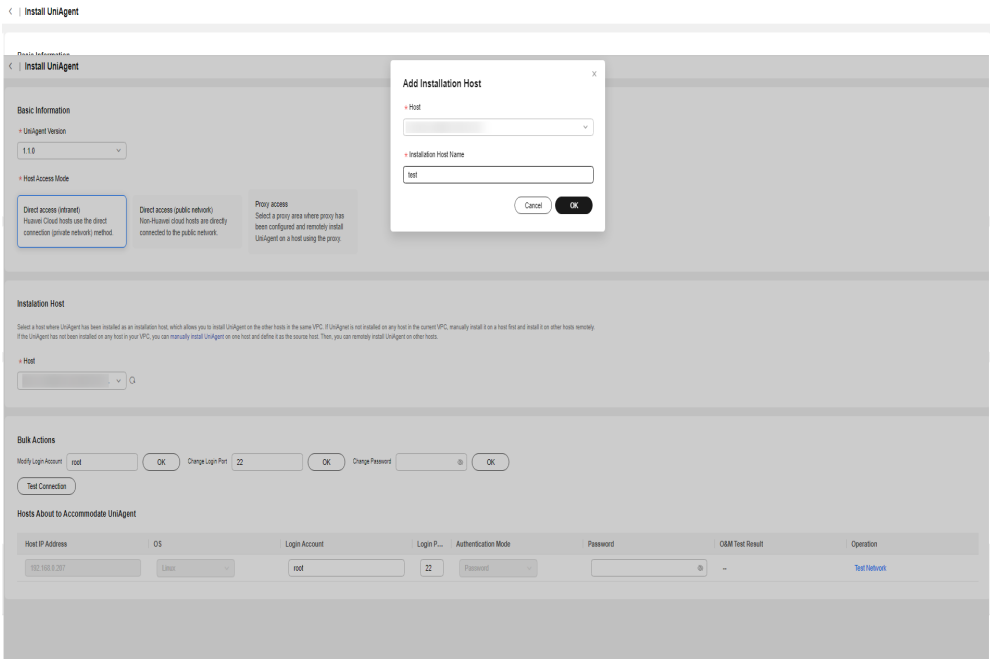
Step 6 Click **Add Installation Host** to set the host where the UniAgent is installed as the installation host.

Figure 2-4 Configuring an installation host



Step 7 In the displayed dialog box, enter the information about the installation host and click **OK**.

Figure 2-5 Selecting an installation host



----End

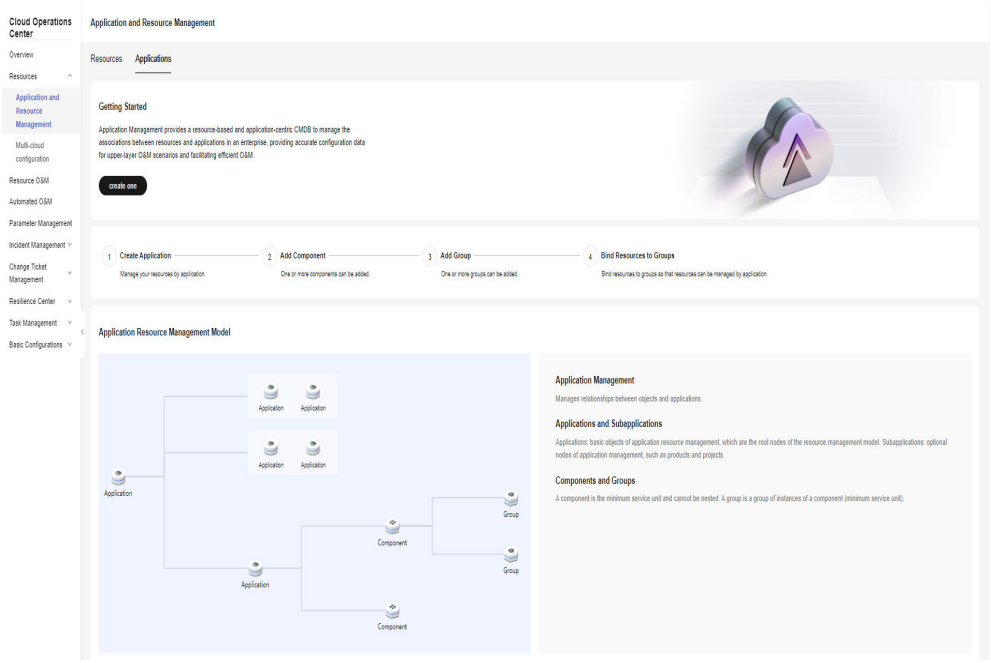
2.2 What Can I Do If Resources Cannot Be Queried on the Resource Management Page?

Synchronize resources on the resource management page. For details, see Synchronizing Resources.

2.3 How Can I Find the Description About Application Management Layers?

If you have not created any application, you can find the description about the application management layers on the **Applications** page, as shown in **Figure 2-6**. Once you create an application, the application management layer description will not be displayed any more.

Figure 2-6 Description of application management layers



3 FAQs About Resource O&M

3.1 What Can I Do If the Patch Baselines Do Not Take Effect?

Before using the patch management, scanning, or repair feature, ensure that the created patch baselines have been set as the default baselines and the application scenarios are correct.

3.2 What Are the Differences Between the Installation Rule Baselines And User-defined Baselines?

Installation rule baselines provides the capability of filtering patch baselines based on the basic information about the corresponding patch packages. If an installation rule baseline is used, non-compliant patches will be upgraded to the latest version for reparation.

User-defined baselines provides the capability of customizing patch package names and versions for baseline filtering. If you use a user-defined baseline, non-compliant patches will be repaired and upgraded to the version specified.

3.3 What Can I Do If Exception all mirrors were tried Is Recorded in the Patch Service Ticket Log?

Generally, the error message is reported when network faults occur. Check whether the network connectivity between the node and patch sources configured on the node is normal or whether the network of the node is normal.

3.4 Why Can't I Select a Node?

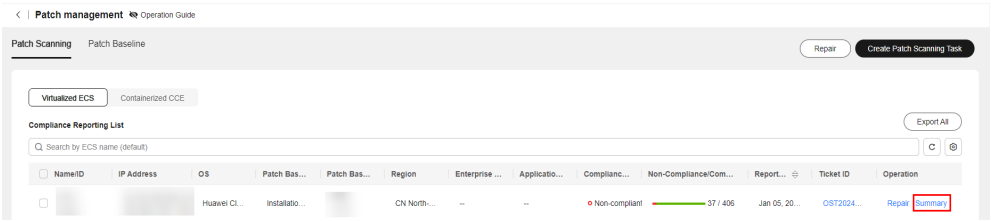
Check whether the node is in the normal state: the resource status is **Running** and the UniAgent status is **Running**.

For details about how to install a UniAgent, see Installing a UniAgent.

3.5 What Can I Do If the Compliance Report Still Reports Non-compliance for a Patch After the Patch Has Been Rpaired?

Step 1 Click the button for viewing the summary of the compliance report that reports non-compliance.

Figure 3-1 Viewing the compliance report summary



Step 2 View the status of the non-compliant patch and view different solutions based on the compliance status.

Table 3-1 Solutions for different compliance statuses

Non-compliance Status	Solution
Failed	View the log of the patch service ticket that generates the compliance report and rectify the fault based on the failure log.
Installed-to be restarted	A newly installed patch can only take effect after the host is restarted. Therefore, you need to restart the host.
Rejected	If a patch is rejected in the patch baseline, the compliance report shows that the patch is rejected. To cancel the rejection, edit the corresponding baseline in the patch baseline.

----End

4 Automation FAQs

4.1 How to Perform Manage Selected Parameters in the Parameter Repository and Selected Host Instances Across Regions?

Ensure that the regions selected for the host instances must be the same as that selected for the parameter repository.

Figure 4-1 Parameter repository

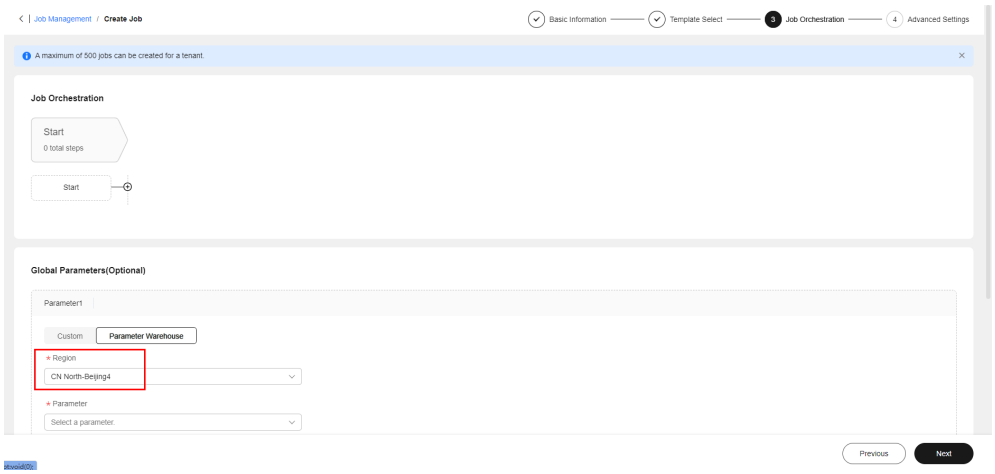
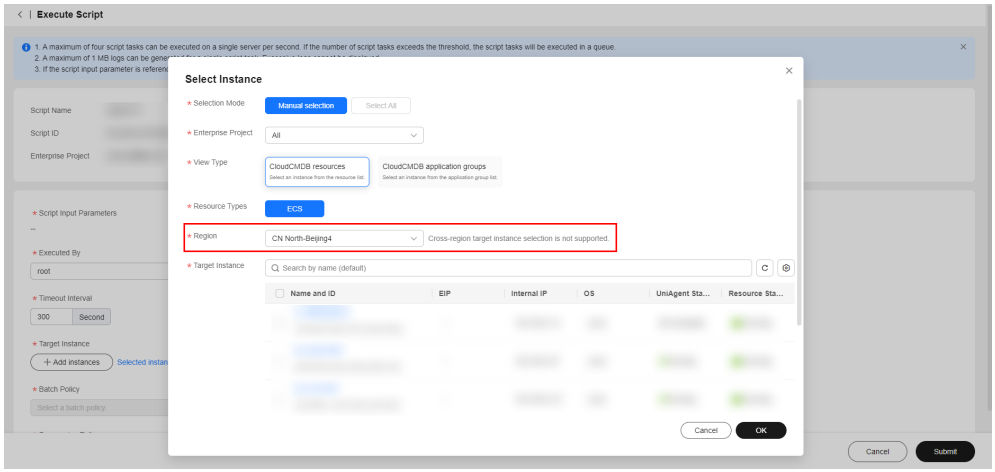


Figure 4-2 Selecting host instances



4.2 Why Can't the Reviewer Receive Notifications?

No notification channel is configured for the reviewer on the **O&M Engineer Management** page.

For details about how to configure a notification channel, see Using O&M Engineer Management.

4.3 Why Is the Input Value of a Customized Script Parameter Invalid?

The value of a customized script parameter must meet the following requirements:

1. The parameter value contains 1 to 1024 characters.
2. The value can contain letters, digits, spaces, and special characters (_-/.*?:",=+@\[{]})
3. Consecutive periods (.) are not allowed.

4.4 Why Cannot I Select an Instance?

A UniAgent must be installed for instances to perform automatic O&M.

For details about how to install a UniAgent, see Installing a UniAgent.

5 FAQs About Parameter Management

5.1 What Are the Permissions Required for Managing Parameters?

Permission design

1. To access the parameter list page, the **coc:parameter:list** permission is required.
2. To obtain parameter details, the **coc:parameter:get** permission is required.
3. To delete a parameter, the operation permission **coc:parameter:delete** is required.
4. To create a parameter, the operation permission **coc:parameter:create** is required.
5. To update a parameter, the operation permission **coc:parameter:update** is required.
6. Resource permissions: **coc:*:*:parameter:***name* (The first asterisk (*) indicates all region IDs, the second asterisk (*) indicates all tenants, and *name* indicates the parameter name. This permission means that you can access a parameter of the specified tenant in a certain region.)

Resource permissions determine the data that you can access. Operation permissions are used to perform operations on your resource permissions. Common problems are as follows:

1. If you can access a parameter but cannot access the parameter list page, you do not have the **coc:parameter:list** permission.
2. If you cannot find a specified parameter, check whether you have the permission on the parameter.
3. **coc:service-name:region:account-id:resource-type:resource-path** is the structure of resource permissions. The asterisk (*) indicates all permissions at this level. To add resource permissions, enter information in this format.

6 FAQs About Incident Management

6.1 What Is the Process of Generating an Incident?

There are three methods available: manual incident creation, converting alarms to incidents, or automatically generate an incident based on an incident forwarding rule. The detailed processes of the three operation methods are as follows.

Manually Creating an Incident

Choose **Incident Management** > **Incident Center**. On the displayed page, create an incident ticket. For details, see Creating an Incident Ticket.

Converting an Alarm to an Incident

Choose **Incident Management** > **Alarms** to create an incident ticket. For details, see Converting Alarms to incidents.

Automatically Generating Incidents Based on Forwarding Rules

To automatically generate an incident based on a forwarding rule, perform the following operations:

Step 1 Log in to **COC**.

Step 2 Synchronize engineer information. For details, see O&M Engineer Management.

Step 3 Configure shift schedules and add members to the shift schedules. For details, see Shift Schedule Management.

Step 4 Integrates the monitoring system to automatically report alarm information. For details, see Data Source Integration.

Step 5 Configure a incident forwarding rule to generate incidents based on the rule. For details, see Configuring an Incident Forwarding Rule.

Step 6 To receive incident notifications after an incident is generated, configure the automated notification feature. For details, see Notification Management.

----End

6.2 How Can I Receive an Incident Ticket Notification?

Step 1 Log in to **COC**.

Step 2 Subscribe to notifications on the **O&M Engineer Management** page. For details, see O&M Engineer Management.

Step 3 Configure notification rules on the **Notification Management** page. For details, see Notification Management.

----End

6.3 What is Warroom?

A WarRoom request is a meeting set up to provide guidance for quick service recovery. It supports joint operations of O&M engineers, R&D team, and operations personnel for fault handling. You can initiate a WarRoom request for an incident that has been received. For details, see initiating a WarRoom Request.

For details about how to use WarRoom feature, see WarRoom.

7 Change Center FAQs

7.1 What Are the Differences Between Regular Changes and Emergency Changes?

Conceptual Differences

Regular changes are non-emergency changes that can be requested, evaluated, reviewed, sorted, planned, tested, and implemented using regular procedures.

Emergency changes are unplanned changes that are proposed to meet urgent service requirements when the production environment is unavailable, planned requirements cannot be fulfilled, or changes cannot be evaluated and reviewed in time through regular procedures.

Differences in Review

Review is supported for both regular and urgent changes.

7.2 How Are Change Levels Defined?

Change levels are used to indicate change risks of different severities. Level A indicates the most risky change, followed by level B, level C, and level D.

8 Resilience Center FAQs

8.1 What Is a Chaos Drill?

Chaos drill is a system resilience assurance method. It proactively simulates hardware or software faults in a system and provides optimization policies based on the responses of the system under various pressures. A complete chaos drill includes failure mode analysis in the early stage, fault injection in the middle stage, and review and improvement in the later stage.

8.2 What Are the Available Attack Scenarios ?

Common fault scenarios of the following cloud services can be simulated, Huawei Cloud ECS instances, RDS DB instances, CCE clusters, and PODs. In addition, flexible orchestration and combination of multiple fault scenarios are allowed.

8.3 What Is a Failure Mode?

A failue mode is a category of potential risks faced by cloud applications. Years of failure modes accumulated on Huawei Cloud are preconfigured on the chaos drill platform. The FT-FMEA fault analysis method is used to help you analyze the potential risks of cloud applications.

8.4 What Do Drill Plans Do?

Drill plans help drill management personnel schedule drills for failure modes and manage drill progress. Drill plans check and verify availability of failure modes through drills.

8.5 What Is the Relationship Between a Failure Mode and a Drill Task?

Failure modes are used to evaluate cloud applications and identify risks, which is the prerequisite for chaos drills. Drill tasks combine different attack scenarios and use fault injection to simulate corresponding failure modes.

8.6 What Are Included in a Drill Report?

A drill report includes the basic information about a drill process, service recovery capability score, and review improvement measures. In addition, a drill report can generate review improvement service ticket to ensure that the issues found in the drill can be resolved.

9 FAQs About Basic Configurations

10 Change History

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

