Cloud Operations Cente

FAQ

Issue 01

Date 2025-04-02

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?

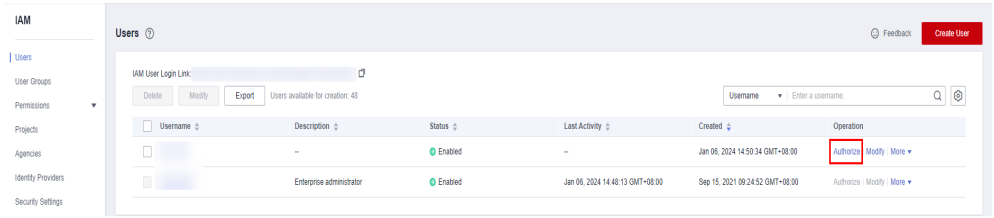
Problem Description

Quickly configuring permissions for COC is required.

Solutions

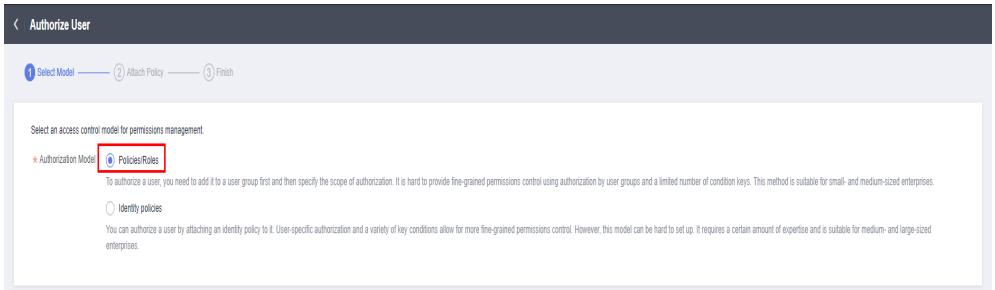
1. Log in to the **IAM console** as an administrator.
2. In the user list, click **Authorize** in the row that contains the target user.

Figure 1-1 Authorizing an IAM user



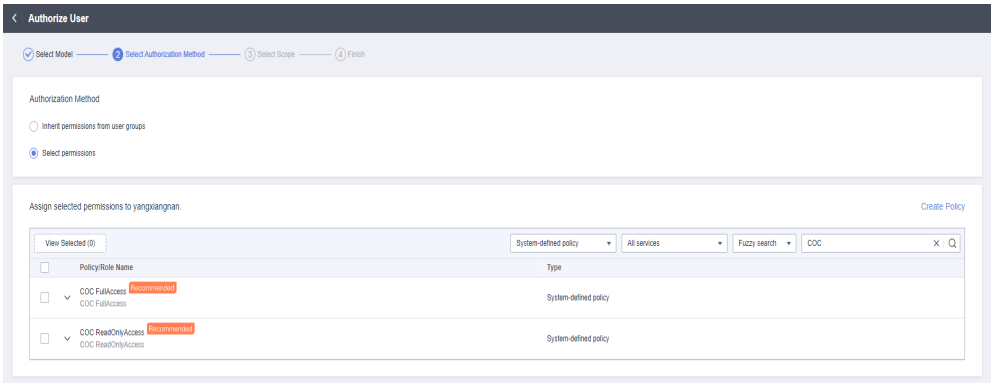
3. Set **Authorization Model** to **RBAC**.

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

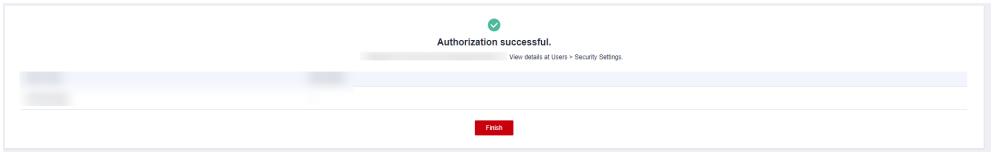


NOTE

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



1.2 How Do I Control Permissions Using Enterprise Projects?

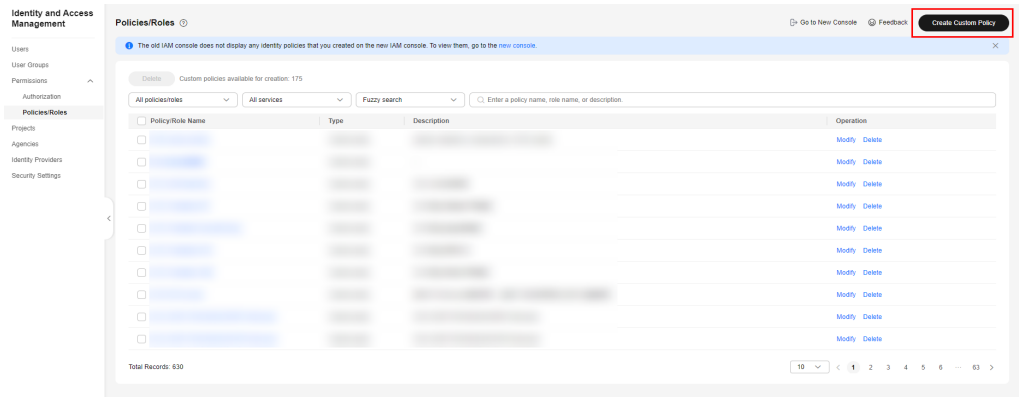
Description

How Do I Control the Permissions of the Cloud O&M Center Through Enterprise Projects?

Solutions

1. Log in to the **IAM console** as an administrator.
2. Choose Permissions > **Policies/Roles** and click **Create Custom Policy**.

Figure 1-5 Creating a custom policy



3. Set the policy content, select **CloudOpsCenter**, and select the operations you want to authorize by enterprise project. Click **OK**.

Figure 1-6 Setting the policy content (1)

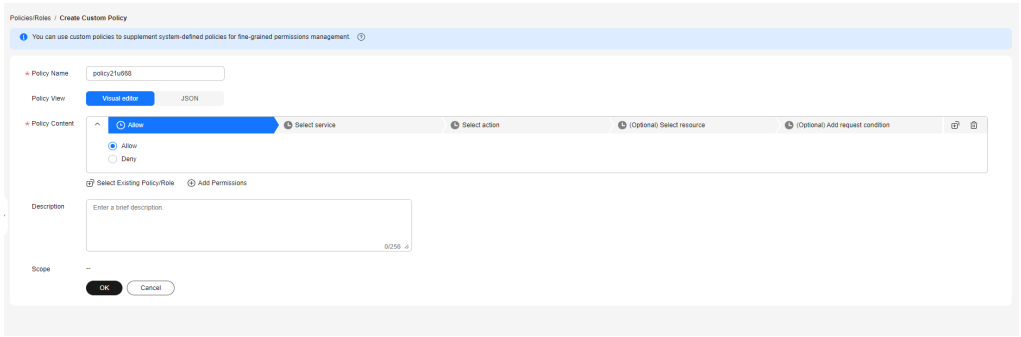


Figure 1-7 Setting the policy content (2)

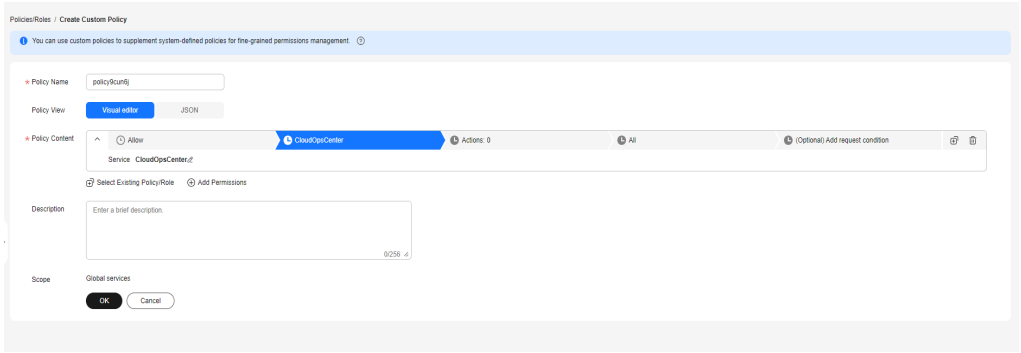
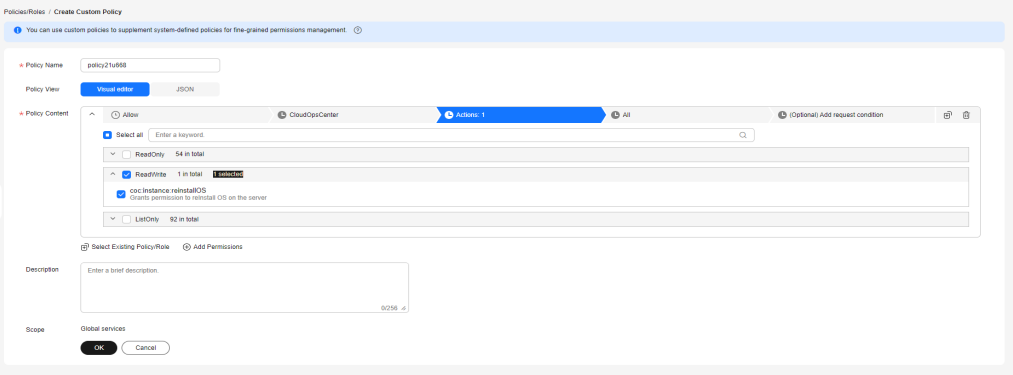


Figure 1-8 Setting the policy content - 3



NOTE

Currently, only some Cloud O&M Center operations can be authorized by enterprise project. For details about how to create custom policies, see **Table 1**.

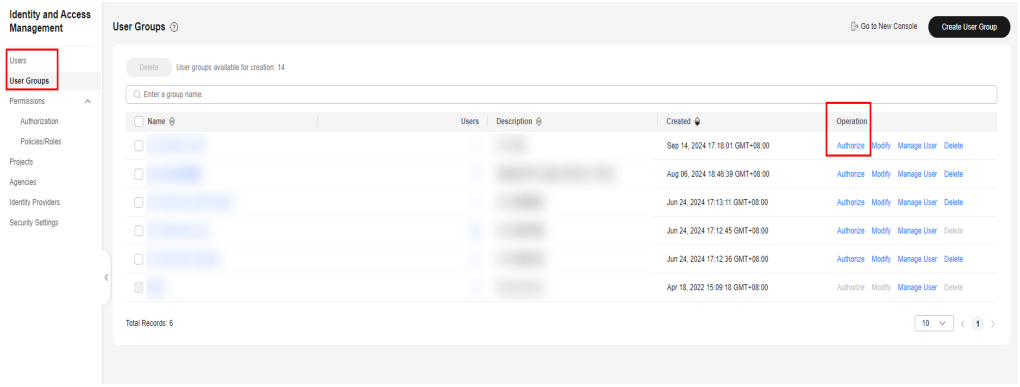
Table 1-1 Operations that can be authorized by enterprise project

Operation	Description
coc:instance:reinstallOS	Grants permission to reinstall the ECS OS.
coc:instance:changeOS	Grants permission to change the ECS OS.
coc:instance:start	Grants permission to start an ECS.
coc:instance:reboot	Grants permission to restart an ECS.
coc:instance:stop	Grants permission to stop an ECS.
coc:instance:startRDSInstance	Grants permission to enable an RDS DB instance.
coc:instance:stopRDSInstance	Grants permission to stop an RDS DB instance.
coc:instance:restartRDSInstance	Grants permission to reboot an RDS DB instance.
coc:instance:scanOSCompliance	Grants the permission to scan server OS patches.
coc:instance:installPatches	Grants permission to install patches for an ECS.
coc:instance:executeDocument	Grants permission to execute documents on an ECS.
coc:schedule:create	Grants permission to create a scheduled task list.

Operation	Description
coc:schedule:update	Grants permission to update a scheduled task.

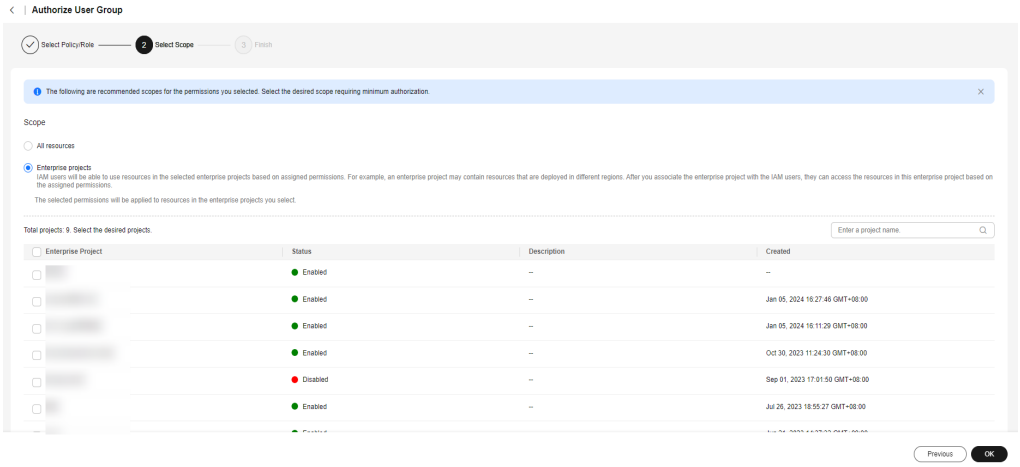
4. The administrator selects a user or user group for authorization.

Figure 1-9 Select an object for authorization.



5. Select the custom policy created in step 3. When setting the minimum authorization scope, specify enterprise project resources.

Figure 1-10 Granting permissions by enterprise project



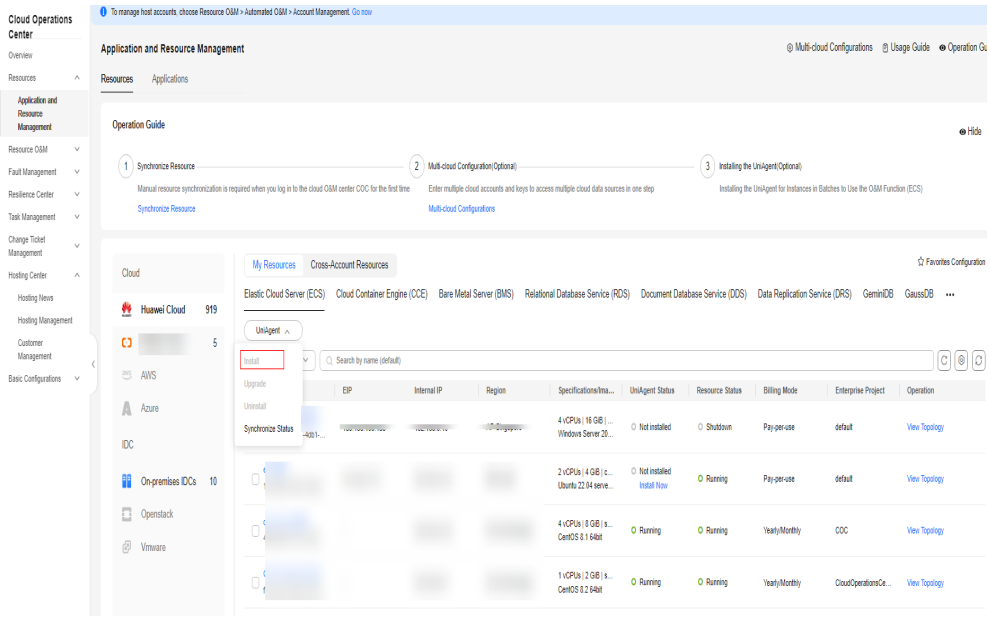
2 Resource Management FAQs

2.1 How Do I Install UniAgent for the First Time?

Step 1 Log in to **COC**.

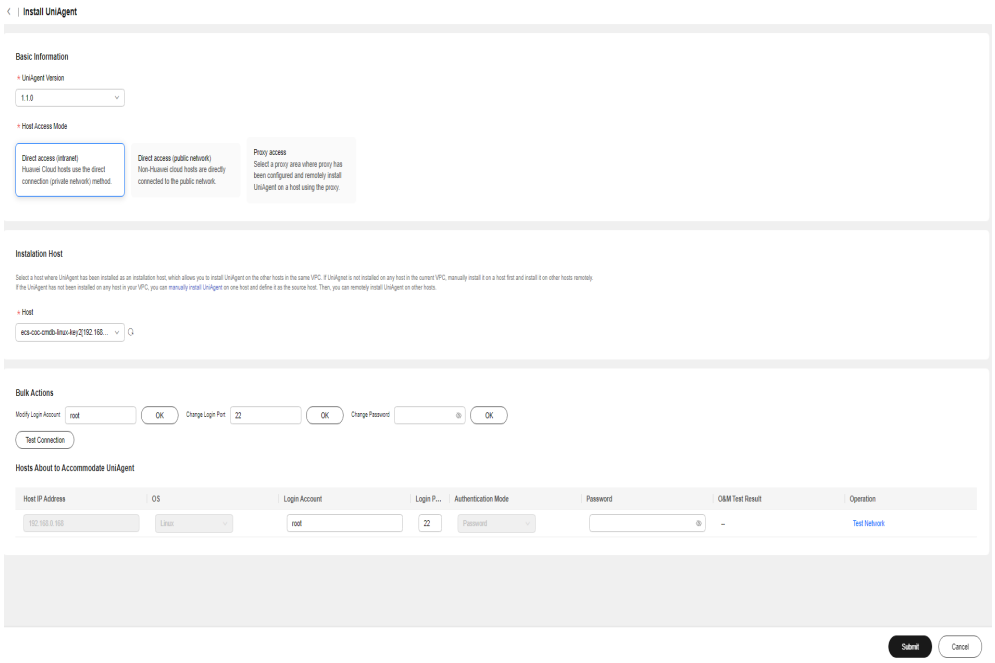
Step 2 In the navigation pane, choose **Application and Resource Management**. On the **Resources** page, select a host where no UniAgents have not been installed.

Figure 2-1 Installing a UniAgent



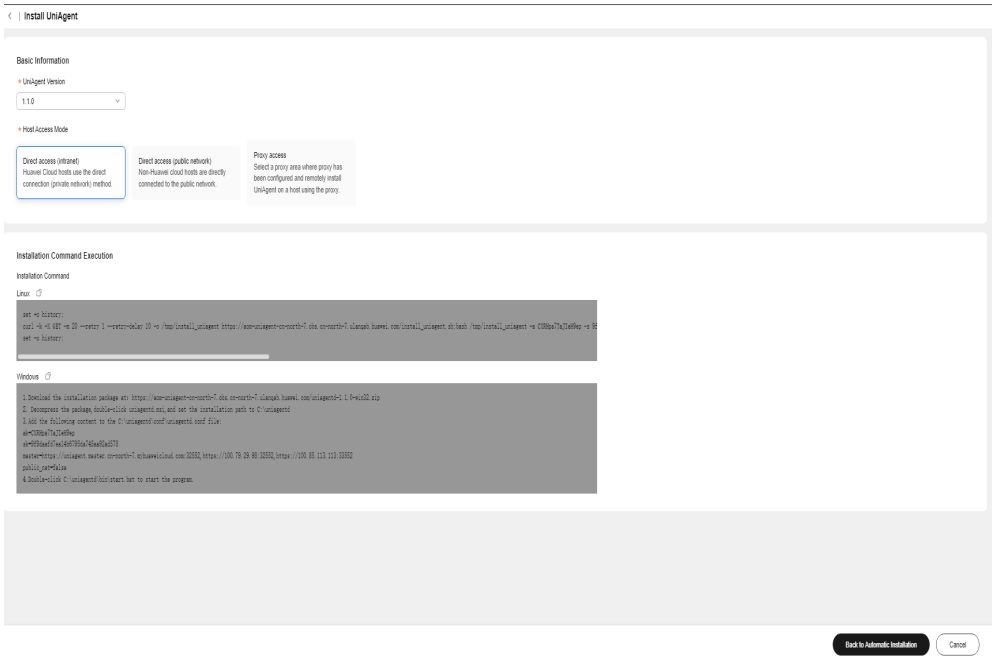
Step 3 On the UniAgent installation page that is displayed, click **Manual installation**.

Figure 2-2 UniAgent installation page



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

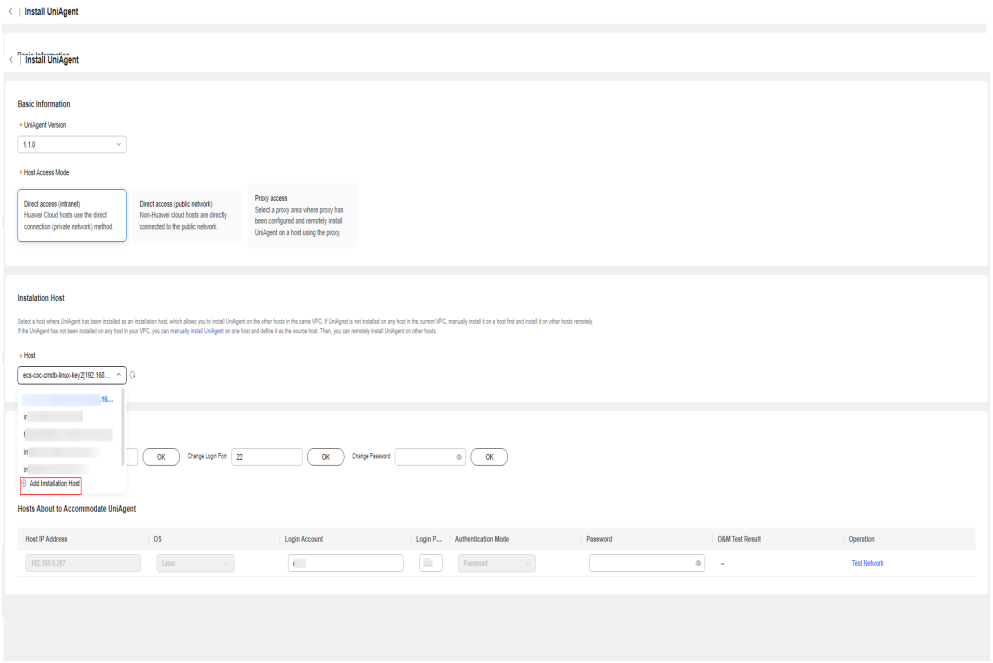
Figure 2-3 Manually installing a UniAgent



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

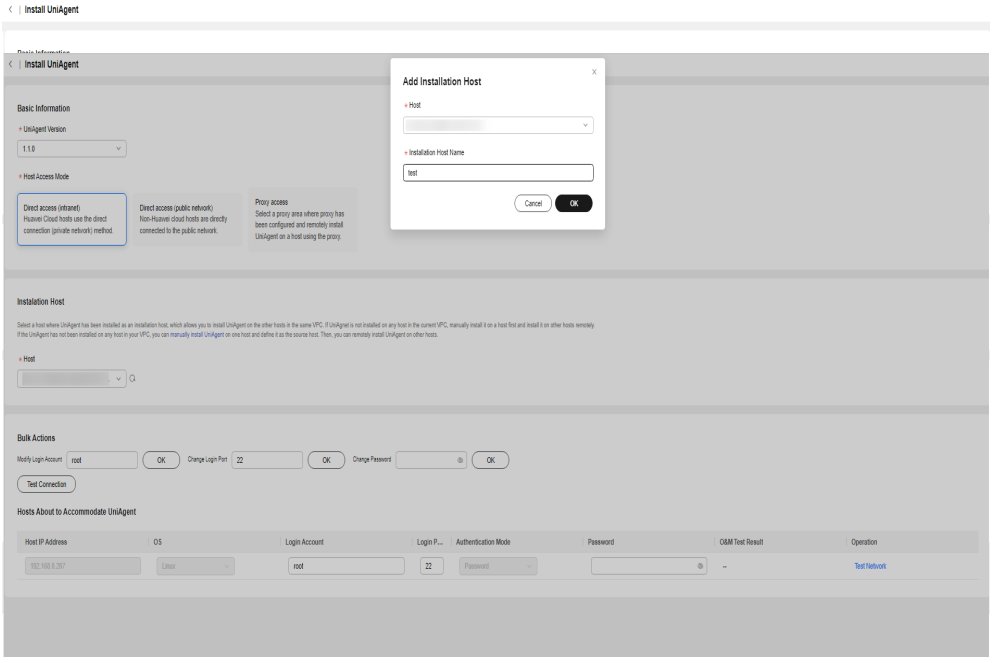
Step 6 Click **Add Installation Host** to set the host where the UniAgent is installed as the installation host.

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

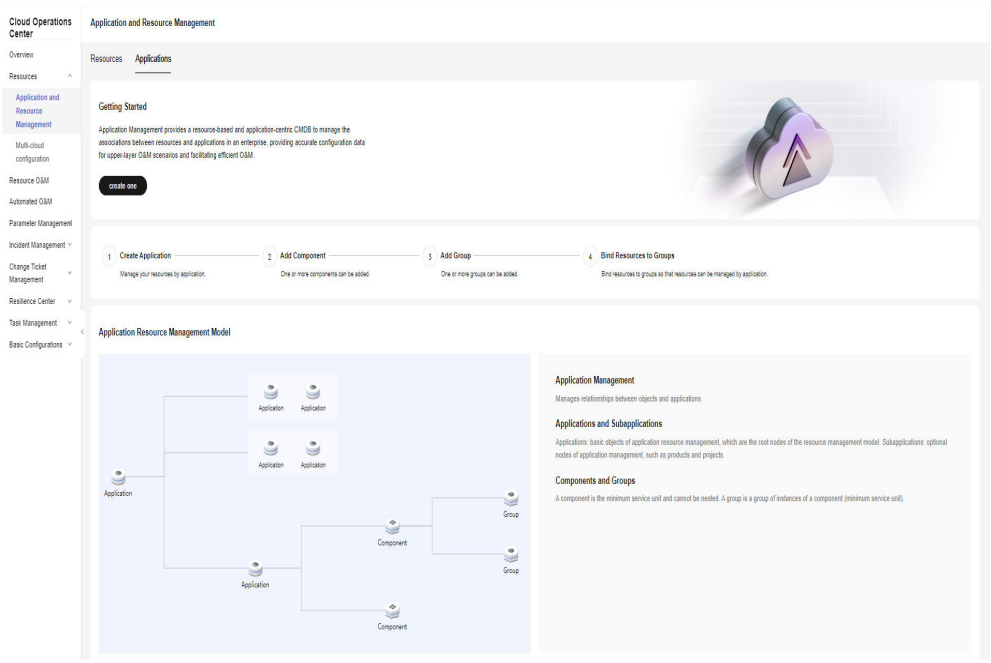
2.2 What Can I Do If Resources Cannot Be Queried on the Resource Management Page?

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 anymore.

Figure 2-6 Description of application management layers



3 FAQs About Resource O&M

3.1 Patch Management FAQs

3.1.1 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.

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

Installation rule baselines provide 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 provide 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.

3.1.3 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.

3.1.4 Why Can't I Select a Node?

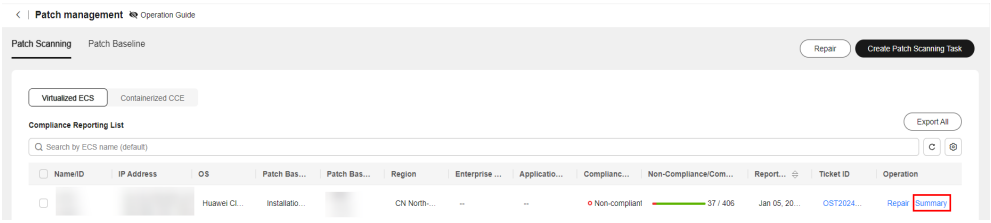
Check whether the node is in the normal state: the resource status is **Running** and the UniAgent status is **Running**.

For details about how to install the UniAgent, see **Performing Operations on a UniAgent**.

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

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

3.1.6 What Can I Do If the lsb_release not found Error Occurs During Patch Operations?

1. Check whether the **lsb_release** command package exists on the ECS instance. If not, install the command package.

2. If the ECS instance contains the **lsb_release** command package, check whether the UniAgent version is later than 1.1.0. If yes, downgrade the UniAgent version to a version earlier than 1.1.0 and try again.

3.2 Automation FAQs

3.2.1 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 the message channel, see **O&M Engineer Management Usage**.

3.2.2 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.

3.2.3 Why Cannot I Select an Instance?

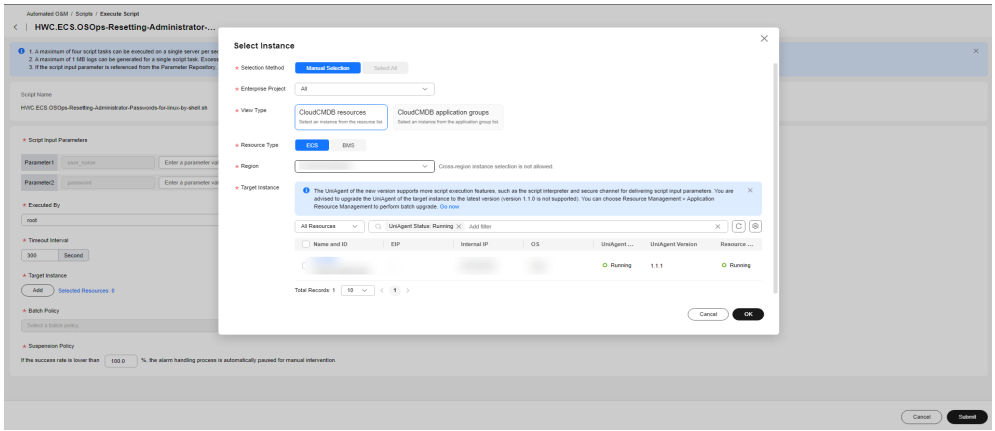
A UniAgent must be installed for instances to perform automatic O&M.

For details about how to install the UniAgent, see **Performing Operations on a UniAgent**.

3.2.4 How Do I Reset the Password Without Restarting a DB Instance?

COC provides common scripts for resetting the password of an administrator or a non-administrator account. This script does not restart the instance. You can run the corresponding common script to reset the password of the instance (currently, only ECS and BMS instances are supported).

Figure 3-2 Executing the common script for resetting passwords



CAUTION

When running a common script in the COC, you need to select an instance. The prerequisites for selecting an instance are as follows:

Your resource instance information has been synchronized to COC. For details, see **Synchronizing Resources**.

The UniAgent has been installed for your instance and is running properly.

To install the UniAgent on an instance, you need to provide the administrator account and password of the instance. If UniAgent is not installed on your resource instance and you forget the password, you cannot install UniAgent and the common script for resetting the password cannot be executed.

3.3 Batch Operation FAQs

3.3.1 What Should I Do If an Error Is Reported When I Switch Images for ECS Resources in Batches?

1. The error message **"code":"Ecs.0021","message":"Failed to check Cinder quotas because the number of Gigabytes exceeded the upper limit** or **CreateRootVolumeTask-fail: call evs api - create volume fail : {"error_msg":"volume gigabytes exceeded volume gigabytes quota!","common_error_code":"CMM.3141","error_code":"EVS.1042"}** is displayed during service ticket execution.

   If the EVS disk quota is insufficient, apply for a higher EVS disk quota. For details, see **Increasing EVS Resource Quotas**.

3.4 FAQs About Parameter Management

3.4.1 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.

3.4.2 Cannot Cross-Region Operations Be Performed on Selected Parameters in the Parameter Repository and Selected Host Instances?

According to the safe production rule, the selected parameters in the parameter repository and host instances cannot be operated across regions. The selected instances and parameter repository must be in the same region.

Figure 3-3 Parameter repository

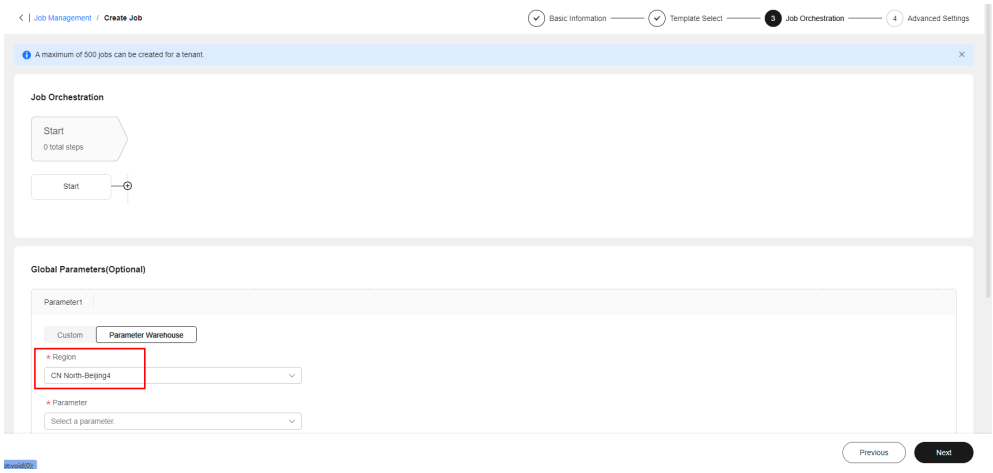
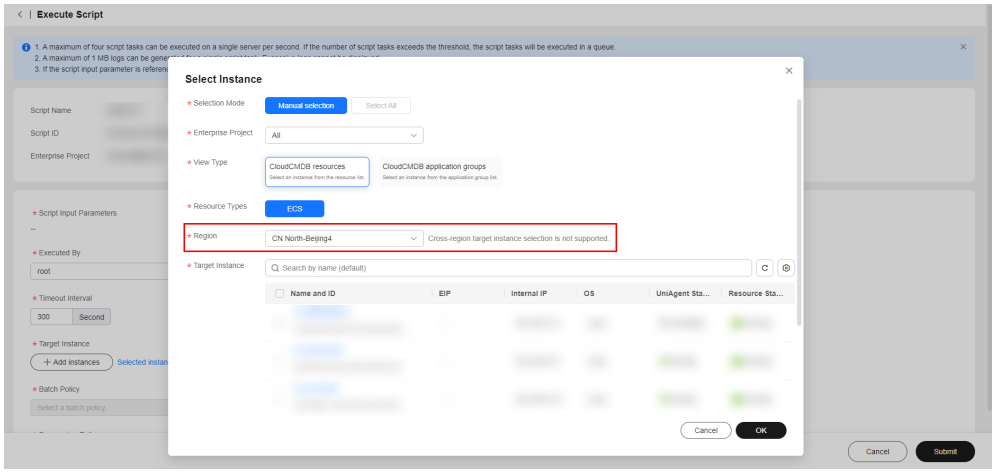


Figure 3-4 Selecting host instances



3.5 Resource O&M Permissions and Supported Actions

This section describes fine-grained permissions management for your COC resources. If your Huawei Cloud account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups and assign policies or roles to these groups. The users then inherit permissions from the groups The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

You can grant users permissions by using You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions that match users' job responsibilities. Policies are a fine-grained authorization strategy that defines permissions required to perform certain operations on specific cloud resources under certain conditions. This type of authorization is API-based and is ideal for least privilege access.

For details about the COC system policies, see **COC Permission Management**.

NOTE

If you want to allow or deny the access to an API, use policy-based authorization.

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions can call the API successfully. For example, if an IAM user wants to call an API to query ECSs, the user must be granted the permissions allowing for action **ecs:servers:list**.

Actions

COC provides system-defined policies that can be used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control. Actions supported by policies are specific to APIs. Common concepts related to policies include:

- Permissions: allow or deny operations on specified resources under specific conditions.
- APIs: REST APIs that can be called by a user who has been granted specific permissions.
- Actions: specific operations that are allowed or denied.
- Related actions: actions which a specific action depends on. When allowing an action for a user, you also need to allow any existing action dependencies for that user.
- IAM or enterprise projects: the authorization scope of a custom policy. A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions supported by both IAM and enterprise projects can take effect for user groups of both IAM and Enterprise Management. Policies that contain actions only supported by IAM projects can only take effect for IAM user groups.

  For details about the differences between IAM and enterprise projects, see **Differences Between IAM and Enterprise Management**.
- Authorization by instance or tag: application scope of custom policies. For APIs that support both authorization by instance and authorization by tag, custom policies take effect for both authorized instances and instances with tags defined in the policies. For APIs that only support authorization by tag, custom policies take effect only for instances with specified tags.

  Currently, this function is unavailable in the **CN North-Ulanqab1** region.

  NOTE

  In the table for supported actions, the check mark (√) indicates that an action can take effect for the corresponding type of projects, and the cross symbol (x) indicates that an action cannot take effect.

COC supports the following actions that can be defined in custom policies:

Table 3-2 Custom policy actions supported by resource O&M

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
Resource Synchronization	coc:instance:listResources	Grants permission to query the resource list.	-	√	x	x	x

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
	coc:application:listResources	Grants permission to query the application resource list.	-	√	x	x	x
	coc:instance:syncResources	Grants permission to synchronize the resource list.		√	x	x	x
Scheduled O&M	coc:schedule:list	Grants permission to query the scheduled task list.	-	√	x	x	x
	coc:schedule:enable	Grants permission to enable scheduled tasks.	-	√	x	x	x
	coc:schedule:update	Grants permission to update scheduled tasks.	-	√	√	x	x
	coc:schedule:disable	Grants permission to disable the scheduled task list.	-	√	x	x	x
	coc:schedule:approve	Grants permission to review the scheduled task list.	-	√	x	x	x

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
	coc:schedule:create	Grants permission to create a scheduled task list.	-	√	√	x	x
	coc:schedule:delete	Grants permission to delete scheduled tasks.	-	√	x	x	x
	coc:schedule:count	Grants permission to query the number of scheduled tasks.	-	√	x	x	x
	coc:schedule:get	Grants permission to query the scheduled task records.	-	√	x	x	x
	coc:schedule:getHistories	Grants permission to query the execution history of a scheduled task.	-	√	x	x	x
In-Depth Diagnosis	coc:application:GetDiagnosisTaskDetails	Grants permission to query application resource diagnosis tasks.	aom:uniagentAgent:install; aom:uniagentAgent:uninstall;	√	x	x	x
	coc:application:CreateDiagnosisTask	Grants permission to create application diagnosis tasks.		√	x	x	x

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
	coc:job:action	Grants permission to operate service tickets.		√	x	x	x
Script/Job Management	coc:document:create	Grants permission to create documents.	aom:uniagentAgent:install; aom:uniagentAgent:list; aom:uniagentInstallHost:list; aom:uniagentProxyRegion:get; iam:agencies:list;	√	x	x	x
	coc:document:listRunbookAtomics	Grants permission to view the atomic capability list of a job.		√	x	x	x
	coc:document:getRunbookAtomicDetails	Grants permission to query details about an atomic capability of a job.		√	x	x	x
	coc:document:list	Grants permission to query the document list.		√	x	x	x
	coc:document:delete	Grants permission to delete documents.		√	x	x	x
	coc:document:update	Grants permission to modify documents.		√	x	x	x
	coc:document:get	Grants permission to view documents.		√	x	x	x

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
	coc:document:analyzeRisk	Grants permission to analyze document risks.		√	x	x	x
	coc:instance:executeDocument	Grants permission to execute documents on an ECS.		√	x	x	x
Batch management of cloud phone servers and cloud phones	coc:instance:autoBatchInstances	Grants permission to enable automatic instance batching.	ecs:serverKeypairs:list;(IAM V3) ecs:servers:get; ecs:cloudServers:list; ecs:cloudServers:rebuild; ecs:cloudServers:changeOS; ecs:cloudServers:showServer; ecs:cloudServers:stop; ecs:cloudServers:reboot; ecs:cloudServers:start; ims:images:get; ims:images:list; bss:order:view; billing:contract:viewDiscount;	√	x	x	x
	coc:instance:executeDocument	Grants permission to execute documents on an ECS.		√	x	x	x
	coc:instance:startRDSInstance	Grants permission to enable RDS DB instances.		√	√	x	x
	coc:instance:stopRDSInstance	Grants permission to stop an RDS DB instance.		√	√	x	x
	coc:instance:restartRDSInstance	Grants permission to reboot an RDS DB instance.		√	√	x	x
	coc:instance:start	Grants permission to start ECSs.		√	√	x	x

Functions	Action	Description	Dependency	IAM Project	Enterprise Project	Authorization by Instance	Authorization by Tag
	coc:instance:reboot	Grants permission to restart ECSs.		√	√	x	x
	coc:instance:stop	Grants permission to disable ECSs.		√	√	x	x
	coc:instance:reinstallOS	Grants permission to reinstall ECS OSs.		√	√	x	x
	coc:instance:changeOS	Grants permission to change the OS of an ECS.		√	√	x	x

4 FAQs About Fault Management

4.1 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 **Fault Management** > **Incidents** and click **Create** to create an incident ticket. For details, see **Creating an Incident**.

Converting an Alarm to an Incident

Choose **Fault Management** > **Incidents** to create an incident ticket. For details, see section "Converting an Alarm to an Incident".

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 personnel. For details, see **O&M Engineer Management Overview**.

Step 3 Set shift scheduling and add agents to the shift scheduling. For details, see **Overview**.

Step 4 Integrate with the monitoring system to automatically report alarms. For details, see **Monitoring System Integration Management**.

Step 5 Configure transition rules and generate incidents based on the rules. For details, see **Forwarding rules**.

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

----End

4.2 How Can I Receive an Incident Ticket Notification?

Step 1 Log in to **COC**.

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

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

----End

4.3 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 war room request for an incident that has been accepted. For details, see **Starting a War Room**.

For details about how to use a war room, see **WarRoom**.

5 FAQs About Change Ticket Management

5.1 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, VMs are unavailable, unplanned changes for urgent service requirements, or changes cannot be evaluated and reviewed in time through regular procedures.

Differences in Review

Review is supported for both regular and urgent changes.

5.2 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.

6 Resilience Center FAQs

6.1 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.

6.2 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.

6.3 What Is a Failure Mode?

A failure 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.

6.4 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.

6.5 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.

6.6 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.

