Resource Governance Center

User Guide

Issue 02

Date 2025-02-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks 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 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.

Contents

1 Landing Zone Management

1.1 Setting Up a Landing Zone

Background

With RGC:

- You will have the necessary permissions to govern all of the organizational units (OUs) and member accounts in your organization.
- You need to set up a landing zone in RGC and determine which OUs and member accounts to govern in the landing zone. RGC does not extend governance to other existing OUs or member accounts in your organization.
- When existing OUs are governed by RGC, they are called registered OUs.
- After your landing zone is set up, you can still register existing OUs in RGC.

Prerequisites

The current account has enabled Enterprise Center. For details, see **Enabling Enterprise Center**.

Constraints

- When setting up a landing zone, if you choose a region where there is already an active landing zone, you cannot delete the IAM Identity Center account information and then switch to another region to create a new landing zone.
- If you have failed to set up a landing zone and deleted the core OU and accounts, you can set up a new landing zone unless you switch to another account.

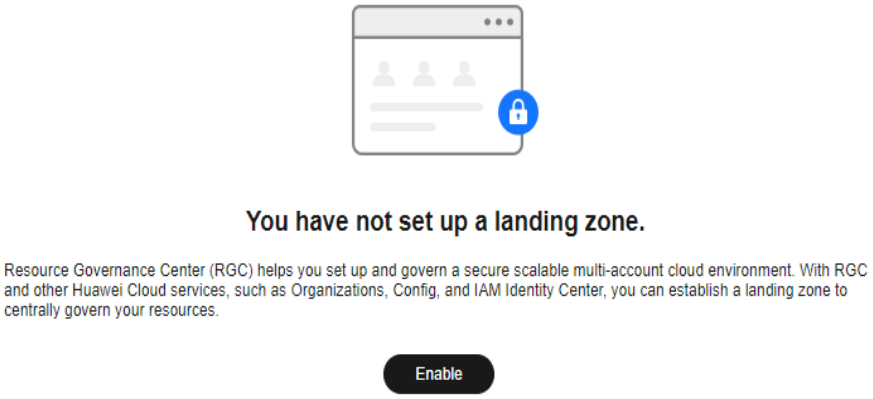
Procedure

Step 1 Log in to Huawei Cloud using an enterprise master account.

Step 2 Click ☰ and choose **Management & Governance** > **Resource Governance Center**.

Step 3 Click **Enable**.

Figure 1-1 Enabling RGC

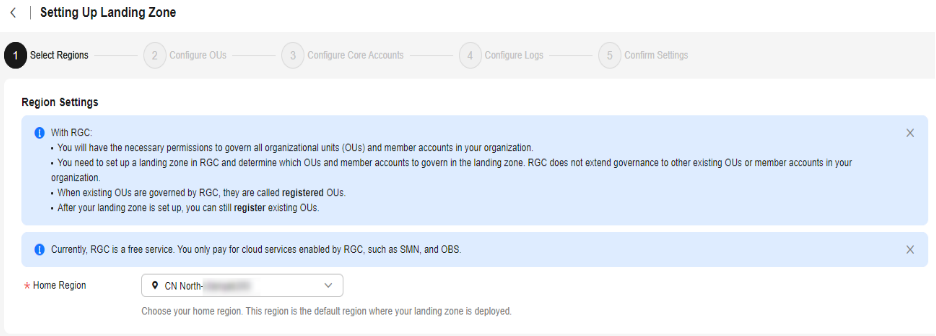


You have not set up a landing zone.

Resource Governance Center (RGC) helps you set up and govern a secure scalable multi-account cloud environment. With RGC and other Huawei Cloud services, such as Organizations, Config, and IAM Identity Center, you can establish a landing zone to centrally govern your resources.

Step 4 Select the home region for RGC. The region will be the default region for your landing zone.

Figure 1-2 Selecting the home region



Region Settings

With RGC:

- You will have the necessary permissions to govern all organizational units (OUs) and member accounts in your organization.
- You need to set up a landing zone in RGC and determine which OUs and member accounts to govern in the landing zone. RGC does not extend governance to other existing OUs or member accounts in your organization.
- When existing OUs are governed by RGC, they are called **registered** OUs.
- After your landing zone is set up, you can still **register** existing OUs.

Currently, RGC is a free service. You only pay for cloud services enabled by RGC, such as SMN, and OBS.

* Home Region: CN North-[redacted]

Choose your home region. This region is the default region where your landing zone is deployed.

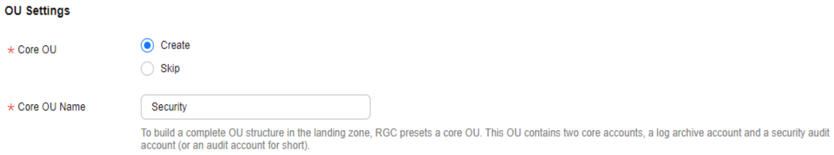
Step 5 Click **Next**.

Step 6 Under **OU Settings**, configure the core OU. You have two options for **Core OU**:

- **Create**: A core OU will be preset in RGC to build a complete OU structure in the landing zone. This OU contains two core accounts: a log archive account and a security audit account (also called an "audit account").

  The OU name must be unique. The default name of the core OU is **Security**. Once your landing zone is set up, the name of the core OU cannot be changed.
- **Skip**: No core OU will be created in RGC.

Figure 1-3 Configuring the core OU



OU Settings

* Core OU: ● Create ○ Skip

* Core OU Name: Security

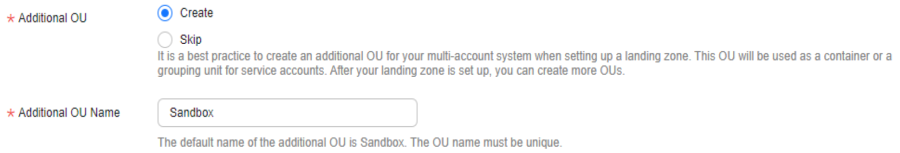
To build a complete OU structure in the landing zone, RGC presets a core OU. This OU contains two core accounts, a log archive account and a security audit account (or an audit account for short).

Step 7 Determine whether to create additional OUs.

To help set up a multi-account system, you are advised to create additional OUs when setting up a landing zone. Each OU functions as a container or grouping unit for service accounts. After your landing zone is set up, you can create more OUs. You have two options for **Additional OU**:

- **Create**: You will need to create an additional OU when you are setting up a landing zone. The OU name must be unique. The default name of the additional OU is **Sandbox**.
- **Skip**: There will be no other OUs except the preset core OU in your landing zone. You can create more OUs after your landing zone is set up.

Figure 1-4 Creating an additional OU



* Additional OU ● Create ○ Skip

It is a best practice to create an additional OU for your multi-account system when setting up a landing zone. This OU will be used as a container or a grouping unit for service accounts. After your landing zone is set up, you can create more OUs.

* Additional OU Name: Sandbox

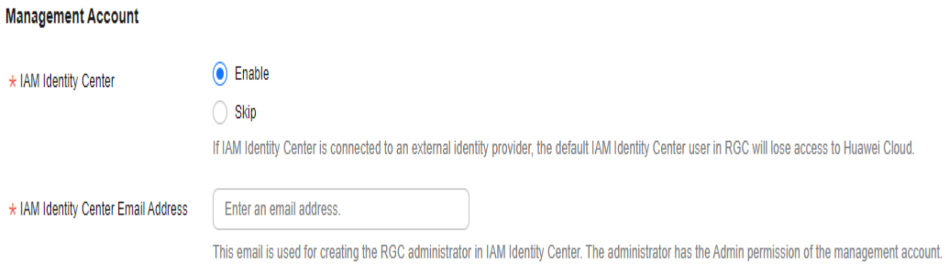
The default name of the additional OU is Sandbox. The OU name must be unique.

Step 8 Click **Next**.

Step 9 On the **Configure Core Accounts** page, configure the management account. You have two options for **IAM Identity Center**:

- **Enable**: You will need to enter the email address associated with the IAM Identity Center account. The email address of the management account must not be used for other IAM Identity Center users. It is used for creating the RGC administrator in IAM Identity Center. The administrator has the Admin permission.
- **Skip**: RGC will not create a user as the RGC administrator, any user groups, or permission sets in IAM Identity Center.

Figure 1-5 Configuring the management account



Management Account

* IAM Identity Center ● Enable ○ Skip

If IAM Identity Center is connected to an external identity provider, the default IAM Identity Center user in RGC will lose access to Huawei Cloud.

* IAM Identity Center Email Address: Enter an email address.

This email is used for creating the RGC administrator in IAM Identity Center. The administrator has the Admin permission of the management account.

Step 10 Configure a log archive account. It is used to store logs of API activities and resource configurations from all accounts.

- Set **Account Type** to **Create new account**.
  - **Email Address**: Enter the email address of the log archive account. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
  - **Account Name**: Specify a unique name for the log archive account. The name cannot be changed once your landing zone is set up. The account

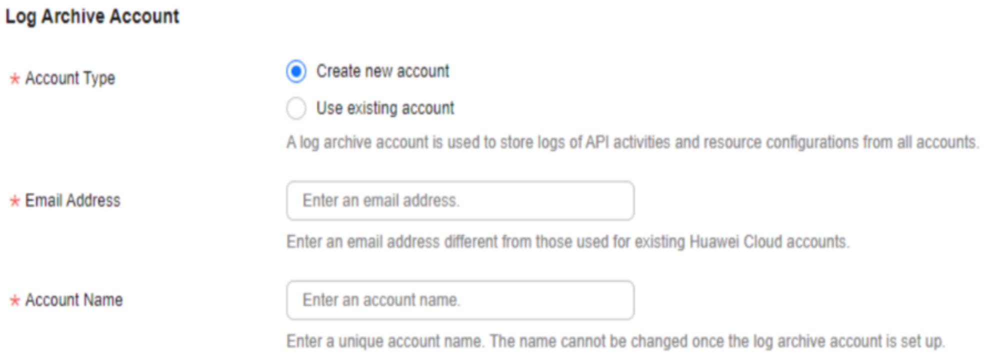
name can only contain digits, letters, underscores (_), and hyphens (-), and it cannot start with a digit. It can have 6 to 32 characters.

- Set **Account Type** to **Use existing account**.

  The existing account you chose must belong to the organization of the management account, and an agency must have been set for the account. For details, see **Setting an Agency**. If there are Config resources in the account, you must delete or modify them before enrolling the account in RGC when you are setting up a landing zone.

  - **Email Address**: Enter the email address of the log archive account. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
  - **Account Name**: Enter the name of the account you have registered with Huawei Cloud.
  - **Account ID**: Enter the ID of the account you have registered with Huawei Cloud. The account ID cannot be the ID of the management account or of a member account in another organization.

Figure 1-6 Configuring a log archive account



Log Archive Account

* Account Type
● Create new account
○ Use existing account
A log archive account is used to store logs of API activities and resource configurations from all accounts.

* Email Address
Enter an email address.
Enter an email address different from those used for existing Huawei Cloud accounts.

* Account Name
Enter an account name.
Enter a unique account name. The name cannot be changed once the log archive account is set up.

Step 11 Configure an audit account. The audit account has permission to access all member accounts in your organization. You are encouraged to strictly control the identity that uses this account.

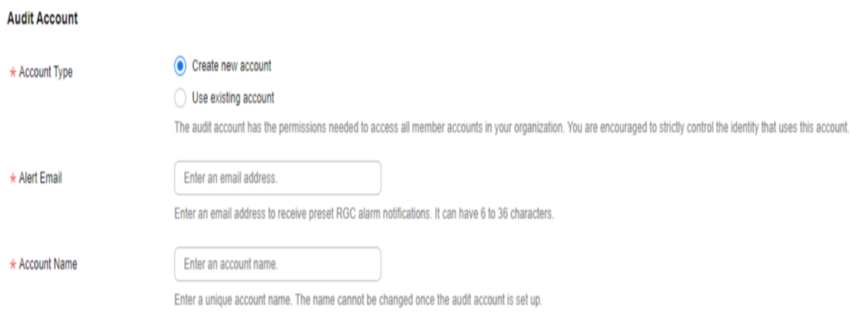
- Set **Account Type** to **Create new account**.
  - **Alert Email**: Enter an email address for the audit account. It is used to receive alerts preset by RGC. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
  - **Account Name**: Specify a unique name for the audit account. The name cannot be changed once your landing zone is set up. The account name can only contain digits, letters, underscores (_), and hyphens (-), and it cannot start with a digit. It can have 6 to 32 characters.
- Set **Account Type** to **Use existing account**.

  The existing account you chose must belong to the organization of the management account, and an agency must have been set for the account. For details, see **Setting an Agency**. If there are Config resources in the account, you must delete or modify them before enrolling the account in RGC when you are setting up a landing zone.

  - **Alert Email**: Enter an email address for the audit account. It is used to receive alerts preset by RGC. It can have a maximum of 64 characters.

- **Account Name**: Enter the name of the account you have registered with Huawei Cloud.
- **Account ID**: Enter the ID of the account you have registered with Huawei Cloud. The account ID cannot be the ID of the management account or of a member account in another organization.

Figure 1-7 Configuring an audit account



Audit Account

* Account Type ● Create new account ○ Use existing account

The audit account has the permissions needed to access all member accounts in your organization. You are encouraged to strictly control the identity that uses this account.

* Alert Email: Enter an email address.

Enter an email address to receive preset RGC alarm notifications. It can have 6 to 36 characters.

* Account Name: Enter an account name.

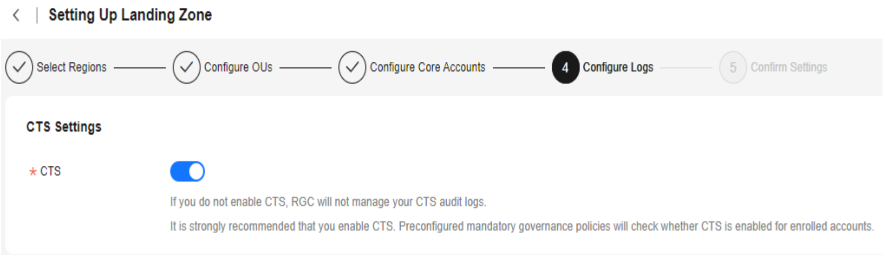
Enter a unique account name. The name cannot be changed once the audit account is set up.

Step 12 Click **Next**.

Step 13 Determine whether to enable CTS.

If you do not enable CTS, RGC will not manage your CTS audit logs. It is strongly recommended that you enable CTS. Preconfigured mandatory governance policies will check whether CTS is enabled for enrolled accounts.

Figure 1-8 Enabling CTS



Setting Up Landing Zone

✓ Select Regions — ✓ Configure OUs — ✓ Configure Core Accounts — 4 Configure Logs — 5 Confirm Settings

CTS Settings

* CTS: ●

If you do not enable CTS, RGC will not manage your CTS audit logs.

It is strongly recommended that you enable CTS. Preconfigured mandatory governance policies will check whether CTS is enabled for enrolled accounts.

Step 14 Configure an OBS bucket for storing logs. You can create a new OBS bucket or use an existing one. If you chose to create a log archive account, you will also need to create an OBS bucket. Log data is encrypted with SSE-OBS, and the keys are created and managed by OBS.

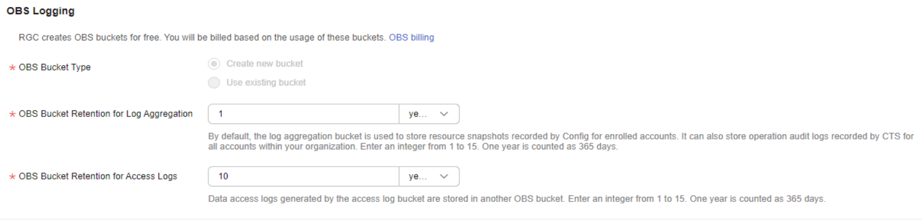
- **Create new bucket**: If you choose this option, you need to configure a retention period for logs in the OBS bucket. Logs are automatically stored in the two default OBS buckets, and you cannot rename them.
  - **OBS Bucket Retention for Log Aggregation**: The default period is one year, but you can change this to up to 15 years.

    This bucket is used to store operation audit logs recorded by CTS for all accounts in an organization and resource snapshots recorded by Config for managed accounts. It is stored in the bucket named **rgcservice-managed-audit-logs-{*Management account ID*}**. **{Management account ID}** represents the actual ID of the management account.
  - **OBS Bucket Retention for Access Logs**: The default period is 10 years, but you can change this to up to 15 years.

The logs for accessing the log aggregation bucket are stored in the bucket **rgcservice-managed-access-logs-{*management account ID*}**.

- **Use existing bucket**: If you choose this option, you need to enter the name of the OBS bucket created by the log archive account. If you use another bucket name, landing zone setup will fail. To ensure data security, you are advised to use a private OBS bucket.

Figure 1-9 Configuring the OBS bucket retention for logging



OBS Logging

RGC creates OBS buckets for free. You will be billed based on the usage of these buckets. OBS billing

* OBS Bucket Type: ● Create new bucket ○ Use existing bucket

* OBS Bucket Retention for Log Aggregation: 1 ye...

By default, the log aggregation bucket is used to store resource snapshots recorded by Config for enrolled accounts. It can also store operation audit logs recorded by CTS for all accounts within your organization. Enter an integer from 1 to 15. One year is counted as 365 days.

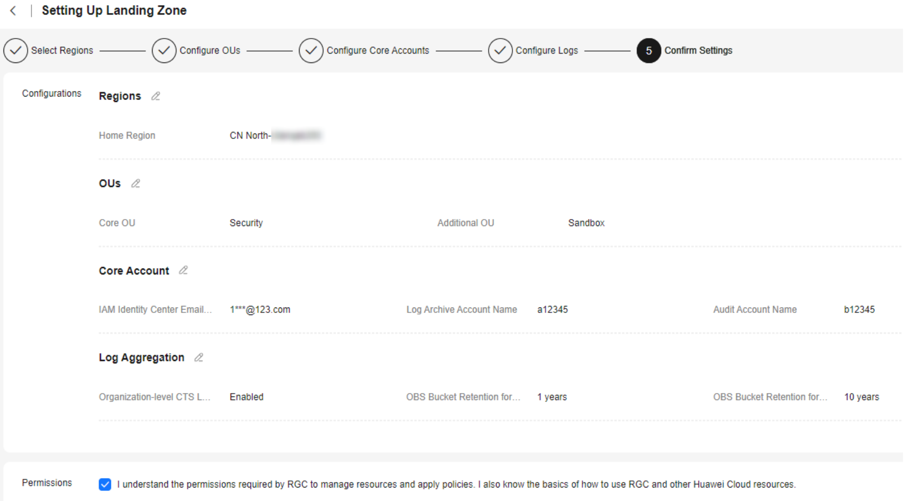
* OBS Bucket Retention for Access Logs: 10 ye...

Data access logs generated by the access log bucket are stored in another OBS bucket. Enter an integer from 1 to 15. One year is counted as 365 days.

Step 15 Review and confirm the landing zone settings, and then select the checkbox **I understand the permissions required by RGC to manage resources and apply policies. I also know the basics of how to use RGC and other Huawei Cloud resources.**

You can log in to the IAM console, choose **Identity Policies** in the navigation pane. On the displayed page, search for **RGCServiceAgencyPolicy** to view the permissions used by RGC to manage resources and enforce policies.

Figure 1-10 Confirming the landing zone settings



Setting Up Landing Zone

✓ Select Regions — ✓ Configure OUs — ✓ Configure Core Accounts — ✓ Configure Logs — 5 Confirm Settings

Configurations

Regions

Home Region: CN North-[redacted]

OUs

Core OU: Security | Additional OU: Sandbox

Core Account

IAM Identity Center Email...: 1***@123.com | Log Archive Account Name: a12345 | Audit Account Name: b12345

Log Aggregation

Organization-level CTS L...: Enabled | OBS Bucket Retention for...: 1 years | OBS Bucket Retention for...: 10 years

Permissions ☑ I understand the permissions required by RGC to manage resources and apply policies. I also know the basics of how to use RGC and other Huawei Cloud resources.

Step 16 Click **Set Up Landing Zone**.

NOTICE

The email address you configured for audit account alerts will receive a subscription confirmation email from the regions governed in RGC. If you want your audit account to receive such emails, click the confirmation link in each email from each region.

----End

Important Notes

- If you want to manage existing OUs and member accounts, see **2.1 Overview of Organization Management**.
- After your landing zone is set up, all preventive governance policies will be attached to the OU that the core account belongs to.
- After your landing zone is set up, the bucket policies **AllowCtsAccessBucket** and **AllowConfigAccessBucket** will be configured for the OBS bucket that stores logs. For details about the bucket policies, go to the OBS console.
- After your landing zone is set up, the object read permission will be configured for the OBS bucket that stores logs so that the core account has permission to view logs in the bucket.

1.2 Viewing Your Landing Zone

After a landing zone is set up, on the **Dashboard** page, you can view details of OUs and accounts, enabled governance policies, non-compliant resources, registered OUs, and enrolled accounts in your landing zone.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 On the **Dashboard** page, get an overview of your landing zone.

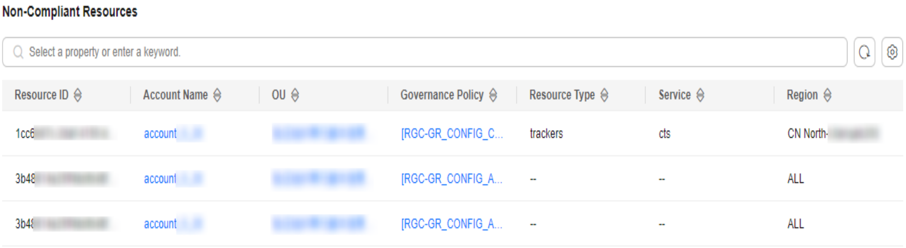
Step 3 Under **OUs and Accounts**, click the number to get an overview of the OUs and accounts.

Step 4 Under **Enabled Governance Policies**, click the number to get an overview of governance policies.

Step 5 Under **Non-Compliant Resources**, click an account name to view the details about non-compliant resources.

You can use the management account to handle the non-compliant resources.

Figure 1-11 Non-compliant resources



Non-Compliant Resources

Resource ID	Account Name	OU	Governance Policy	Resource Type	Service	Region
1cc6[redacted]	account[redacted]	[redacted]	[RGC-GR_CONFIG_C...	trackers	cts	CN North-[redacted]
3b48[redacted]	account[redacted]	[redacted]	[RGC-GR_CONFIG_A...	--	--	ALL
3b48[redacted]	account[redacted]	[redacted]	[RGC-GR_CONFIG_A...	--	--	ALL

Step 6 Under **Registered OUs**, click an OU name to view OU details.

Step 7 Under **Enrolled Accounts**, click an account name to view account details.

----End

1.3 Decommissioning a Landing Zone

The process of cleaning up all of the resources allocated in a landing zone is referred to as decommissioning a landing zone.

If you no longer need a landing zone, you can decommission it. Once it is decommissioned, all resources in the landing zone will be cleaned up.

NOTICE

Decommissioning a landing zone is different from manually deleting all the resources in the landing zone. Manual deletion will not allow you to set up a new landing zone.

Decommissioning does not change your data, including your existing organization data, in the following ways:

- RGC does not remove your data. It only removes parts of the landing zone that it created.
- Some resources remain, such as OBS buckets, RFS templates you created, and agencies. These resources need to be deleted manually before you set up another landing zone.
- All organizational units (OUs) and accounts of a given organization are deleted or moved.
- Resources created in IAM Identity Center during the setup of the landing zone will not be deleted.

⚠ CAUTION

- Exercise caution when decommissioning a landing zone. Once decommissioned, the functions of the current landing zone become unavailable. However, you can re-create that landing zone.
- If you intend to decommission the current landing zone and set up a new one, it is strongly recommended that you **submit a service ticket** to evaluate the consequences before performing decommissioning.

When you request the decommissioning of your landing zone, RGC:

- Disables all governance policies enabled in the landing zone.
- Disables preventive governance policies by removing service control policies (SCPs).
- Deletes all resource stack sets created for the landing zone.
- Deletes records of each account factory account.
- Deletes internal records that identify the home region.

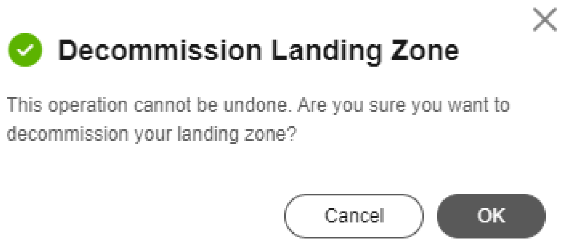
Procedure

Step 1 Log in to Huawei Cloud as the RGC administrator, and navigate to the RGC console.

Step 2 Access the **Landing Zone Settings** page, and click the **Decommissioning** tab.

Step 3 Click **Decommission**. The decommissioning process cannot be undone. Confirm your intent to decommission your landing zone before starting.

Figure 1-12 Decommissioning a landing zone



Decommission Landing Zone

This operation cannot be undone. Are you sure you want to decommission your landing zone?

Step 4 Click **OK**.

----End

Follow-Up Operations

After a landing zone is decommissioned, you need to manually delete the following resources before setting up a new landing zone:

- The core OU. If you want to create a new landing zone and use a core OU with the same name as the original landing zone, you need to manually delete the original core OU. For details, see **Deleting an OU**.
- IAM Identity Center configurations. If the original landing zone uses IAM Identity Center and you want to use another home region for the new landing zone, you need to reset the original IAM Identity Center. For details, see **IAM Identity Center Resetting**.
- The OBS bucket for storing logs. For details about how to delete an OBS bucket, see **Deleting a Bucket**.
- The RGCLoggingResources stack set in RFS. For details about how to delete a stack set, see **Deleting a Stack Set**.
- Templates you created in RFS.
- IAM agencies, including RGCAgencyForStack, RGCBlueprintExecutionAgency, RGCBlueprintStackSetAdminAgency, RGCIAMTokenAccess, and RGCAdminAgency. For details about how to delete agencies, see **Deleting or Modifying Agencies**.

1.4 Updating a Landing Zone

The administrator is responsible for repairing and updating the landing zone at any time. To ensure compliance with the governance rules, the administrator needs to identify and repair drift in a timely manner. Updating a landing zone can help repair certain types of drift.

By updating a landing zone, you can:

- Update the core OU and accounts, including
  - Changing the management account
  - Changing the email address for the audit account
- Update log configurations, including
  - Enabling or disabling CTS
  - Changing the log retention policy

When you update your landing zone, you will automatically receive the latest RGC functions, which you can reach by clicking the **Versions** tab on the **Landing Zone Settings** page.

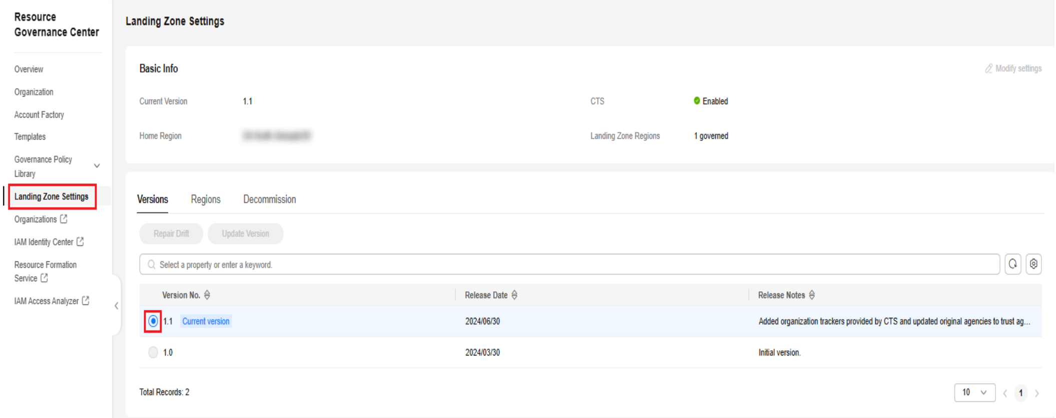
Procedure

Step 1 Log in to Huawei Cloud as the RGC administrator, and navigate to the RGC console.

Step 2 Access the **Landing Zone Settings** page, and click the **Versions** tab.

Step 3 Select the source version you want to update.

Figure 1-13 Selecting a source version



Landing Zone Settings

Basic Info

Current Version 1.1

CTS ● Enabled

Home Region [redacted]

Landing Zone Regions 1 governed

	Version No.	Release Date	Release Notes
●	1.1 Current version	2024/06/30	Added organization trackers provided by CTS and updated original agencies to trust ag...
○	1.0	2024/03/30	Initial version.

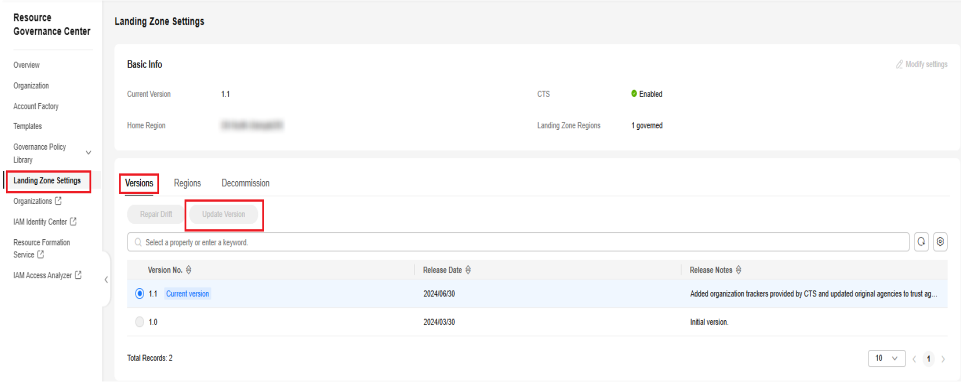
Total Records: 2

NOTE

You can update the current version or upgrade it to a later version.

Step 4 Click **Update Version**.

Figure 1-14 Updating a landing zone



Landing Zone Settings

Basic Info

Current Version	1.1	CTS	Enabled
Home Region	[redacted]	Landing Zone Regions	1 governed

Version No.	Release Date	Release Notes
● 1.1 Current version	2024/06/30	Added organization trackers provided by CTS and updated original agencies to trust ag...
○ 1.0	2024/03/30	Initial version.

Total Records: 2

10 < 1 >

NOTICE

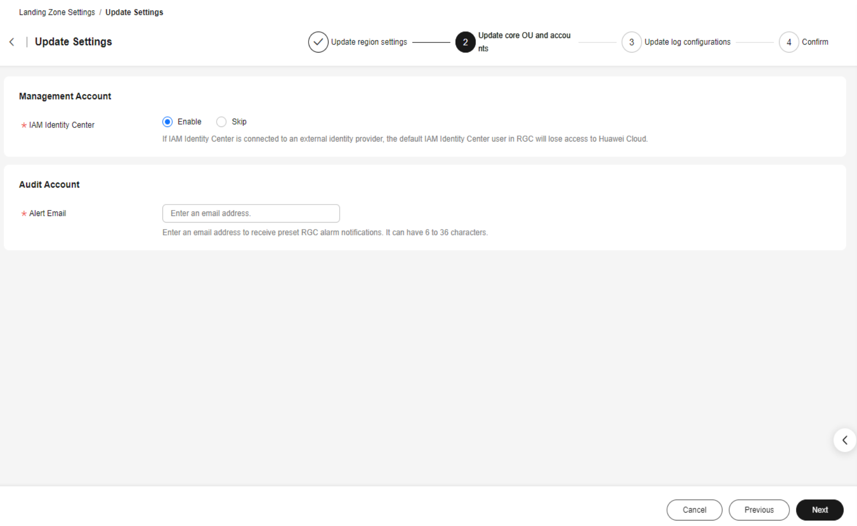
After completing a landing zone update, you cannot undo the update or downgrade to a previous version.

Step 5 Update the core OU and accounts.

- Updating the management account
  - **Enable**: RGC will create an IAM Identity Center user as the administrator. If IAM Identity Center is connected to an external identity provider, the default IAM Identity Center user in RGC will lose access to the cloud.
  - **Skip**: RGC will not create a user as the RGC administrator, any user groups, or permission sets in IAM Identity Center.
- Updating the alert email

  Enter an email address for the audit account. It is used to receive alerts preset by RGC. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.

Figure 1-15 Updating the core OU and accounts


Landing Zone Settings / Update Settings
Update Settings
Update region settings
2 Update core OU and accou nts
3 Update log configurations
4 Confirm
Cancel
Previous
Next

Management Account

* IAM Identity Center ● Enable ○ Skip

If IAM Identity Center is connected to an external identity provider, the default IAM Identity Center user in RGC will lose access to Huawei Cloud.

Audit Account

* Alert Email Enter an email address.

Enter an email address to receive preset RGC alarm notifications. It can have 6 to 36 characters.

Step 6 Click **Next**.

Step 7 Update log configurations.

- Enabling or disabling CTS

  If you do not enable CTS, RGC will not manage your CTS audit logs. It is strongly recommended that you enable CTS. Preconfigured mandatory governance policies will check whether CTS is enabled for enrolled accounts.

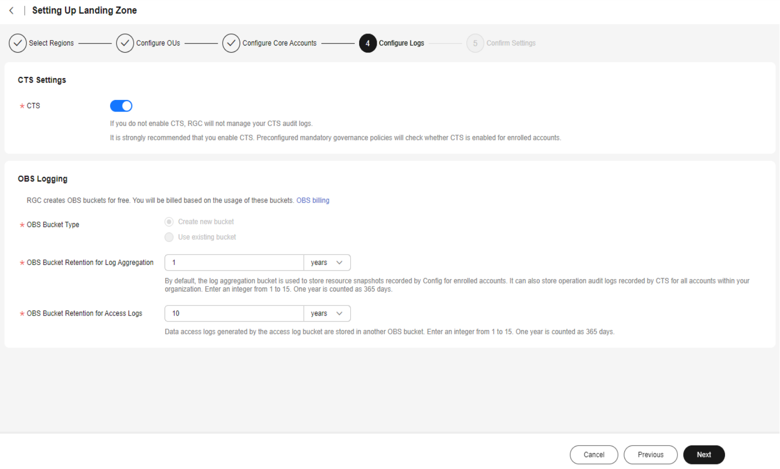
- Updating OBS log configurations
  - **Create new bucket**: If you choose this option, you need to configure a retention period for logs in the OBS bucket. Logs are automatically stored in the two default OBS buckets, and you cannot rename them.
    - **OBS Bucket Retention for Log Aggregation**: The default period is one year, but you can change this to up to 15 years.

      This bucket is used to store operation audit logs recorded by CTS for all accounts in an organization and resource snapshots recorded by Config for managed accounts. It is stored in the bucket named **rgcservice-managed-audit-logs-{*Management account ID*}**. **{Management account ID}** represents the actual ID of the management account.

    - **OBS Bucket Retention for Access Logs**: The default period is 10 years, but you can change this to up to 15 years.

      The logs for accessing the log aggregation bucket are stored in the bucket **rgcservice-managed-access-logs-{*management account ID*}**.
  - **Use existing bucket**: If you choose this option, you need to enter the name of the OBS bucket created by the log archive account. If you use another bucket name, landing zone setup will fail. To ensure data security, you are advised to use a private OBS bucket.

Figure 1-16 Updating log configurations



CTS Settings

* CTS: ● (enabled)

If you do not enable CTS, RGC will not manage your CTS audit logs.

It is strongly recommended that you enable CTS. Preconfigured mandatory governance policies will check whether CTS is enabled for enrolled accounts.

OBS Logging

RGC creates OBS buckets for free. You will be billed based on the usage of these buckets. OBS billing

* OBS Bucket Type: ● Create new bucket ○ Use existing bucket

* OBS Bucket Retention for Log Aggregation: 1 years

By default, the log aggregation bucket is used to store resource snapshots recorded by Config for enrolled accounts. It can also store operation audit logs recorded by CTS for all accounts within your organization. Enter an integer from 1 to 15. One year is counted as 365 days.

* OBS Bucket Retention for Access Logs: 10 years

Data access logs generated by the access log bucket are stored in another OBS bucket. Enter an integer from 1 to 15. One year is counted as 365 days.

Step 8 Click **Next**.

Step 9 Review and confirm the updated settings, and click **OK**. RGC will start updating the landing zone.

After the update is complete, a success message will be displayed.

If the update fails, the landing zone will not be downgraded to a previous version and may enter an undefined state. In this case, **submit a service ticket**.

----End

Related Operations

If you need to update accounts individually, refer to **4.4 Updating an Account**.

2 Organization Management

2.1 Overview of Organization Management

What Is Organizations?

Huawei Cloud Organizations is an account management service for consolidating multiple Huawei Cloud accounts into a single organization so you can manage them all in one place. An organization is composed of one management account, multiple member accounts, one root organizational unit (OU), and other OUs. The root OU and other OUs are organized in a hierarchical, tree-like structure. You can group your accounts into the root OU or any of the other OUs. For details about Organizations, see **What Is Organization?**.

After you set up a landing zone using a management account, the managed organizational structure, OUs, and accounts are displayed on the organization management page.

Basic Concepts

- **Organization**

  An entity that you create to manage multiple accounts. Each organization is composed of **a management account**, **member accounts**, **a root OU**, and various **other OUs**. An organization has exactly one management account along with several member accounts. You can organize the accounts in a hierarchical, tree-like structure with the root OU at the top and nested OUs under it. Each member account can be directly under the root OU or placed under one of the other OUs. The organization management page displays the organization structure.

- **Root OU**

  The root OU is located at the top of the organizational tree, and the branches representing other OUs and accounts reach down. The root OU is displayed on the top of the organization.

- **Core OU**

  When you are setting up a landing zone, a preset core OU (default name: Security) is automatically displayed in the organizational structure. This OU contains two core accounts: a log archive account and a security audit account (also called an "audit account").

- **OUs**

  A container or grouping unit for member accounts. It can be understood as a department, a subsidiary, a project family, or the like, of your enterprise. An OU can also contain other OUs. Each OU can have exactly one parent OU, but a parent OU can have multiple child OUs or nested member accounts.

- **Management account**

  The account used to set up a landing zone. You can use the management account to register OUs and enroll accounts and also manage both in the landing zone.

- **Member accounts**

  An account directly in the root OU or placed in one of the other OUs.

- **Registered OUs**

  If you create OUs in RGC, they will be registered automatically. If you create OUs in Organizations, you need to manually register them so that they can be governed in the landing zone.

- **Enrolled accounts**

  If you create accounts in RGC, they will be automatically enrolled. If you create accounts in Organizations, you need to manually enroll them so that they can be governed in the landing zone.

2.2 Creating an OU

An OU is a container or a grouping unit for member accounts in your organization. You can use an OU to group accounts and manage them as a whole. It can be understood as a department, a subsidiary, a project family, or the like, of your enterprise. You can create various OUs under a parent OU. Each OU can have only one parent OU, but a parent OU can have many other OUs or member accounts.

You can create OUs in the root OU of your organization. OUs can be nested up to five levels deep.

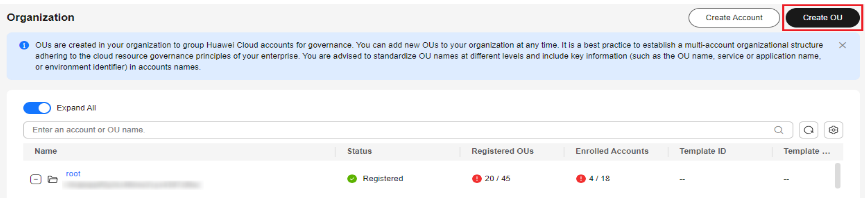
The OUs you created in a landing zone will be automatically registered in RGC.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, and click **Create OU**.

Figure 2-1 Creating an OU

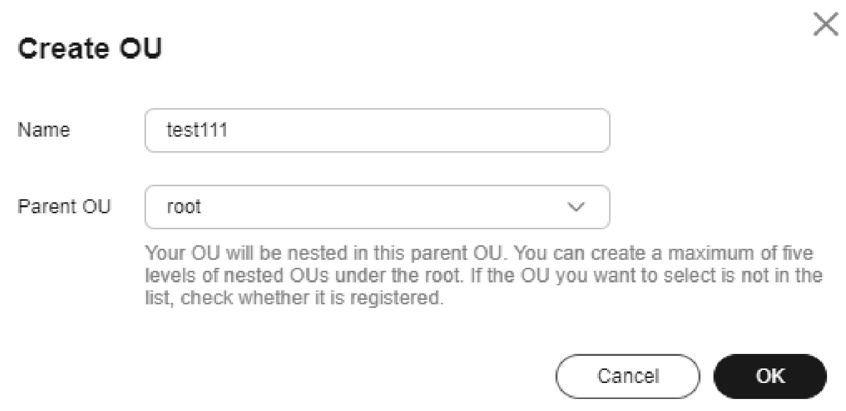


OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...
root [redacted]	Registered	20 / 45	4 / 18	--	--

Step 3 Enter the OU name and select its parent OU.

Figure 2-2 Configuring OU details



Create OU

Name: test111

Parent OU: root

Your OU will be nested in this parent OU. You can create a maximum of five levels of nested OUs under the root. If the OU you want to select is not in the list, check whether it is registered.

Step 4 Click **OK**.

----End

2.3 Registering an OU

If you create an OU via Organizations before setting up a landing zone via RGC, you need to manually register the OU so that it will be governed in the landing zone.

Constraints

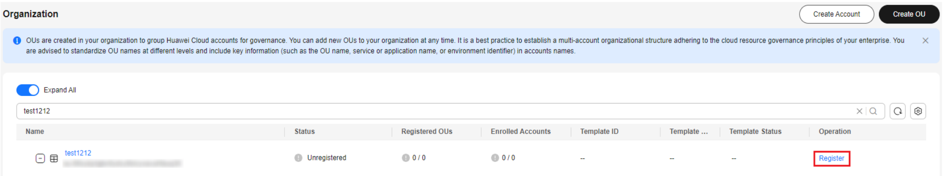
- When an OU is being registered or re-registered, accounts in the OU cannot be unmanaged, enrolled, or updated.
- The core OU cannot be registered or re-registered.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the OU to be registered, and click **Register** in the **Operation** column.

Figure 2-3 Registering an OU



Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

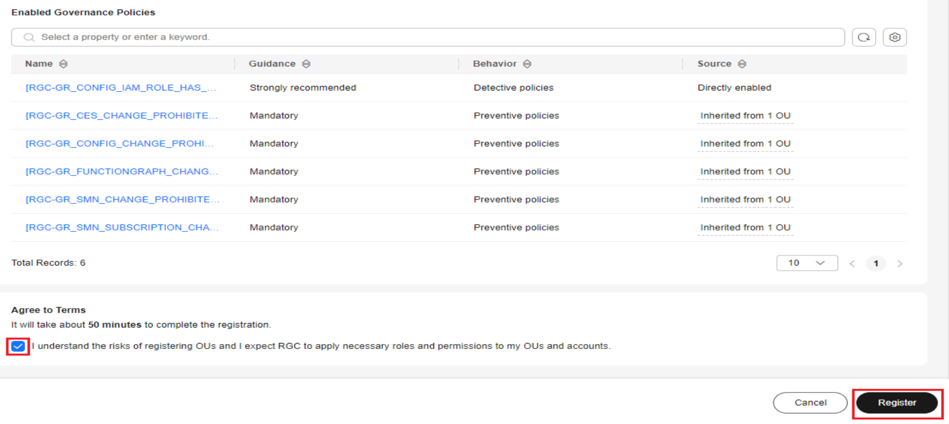
Expand All

test1212

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
test1212 [redacted]	Unregistered	0 / 0	0 / 0	--	--	--	Register

Step 3 Confirm governance policies attached to the OU and member accounts, and select the checkbox **I understand the risks of re-registering OUs and I expect RGC to apply necessary roles and permissions to my OUs and accounts**.

Figure 2-4 Confirming OU details



Enabled Governance Policies

Select a property or enter a keyword.

Name	Guidance	Behavior	Source
[RGC-GR_CONFIG_IAM_ROLE_HAS_...	Strongly recommended	Detective policies	Directly enabled
[RGC-GR_CES_CHANGE_PROHIBITE...	Mandatory	Preventive policies	Inherited from 1 OU
[RGC-GR_CONFIG_CHANGE_PROHI...	Mandatory	Preventive policies	Inherited from 1 OU
[RGC-GR_FUNCTIONGRAPH_CHANG...	Mandatory	Preventive policies	Inherited from 1 OU
[RGC-GR_SMN_CHANGE_PROHIBITE...	Mandatory	Preventive policies	Inherited from 1 OU
[RGC-GR_SMN_SUBSCRIPTION_CHA...	Mandatory	Preventive policies	Inherited from 1 OU

Total Records: 6

Agree to Terms

It will take about **50 minutes** to complete the registration.

☑ I understand the risks of registering OUs and I expect RGC to apply necessary roles and permissions to my OUs and accounts.

Step 4 Click **Register**. It takes a while to register an OU. You can view the OU registration status in the organizational structure. After being registered, the OU can be governed in the landing zone.

----End

2.4 Re-registering an OU

If you need to update multiple accounts in an OU or update the OU, you can re-register the OU.

Constraints

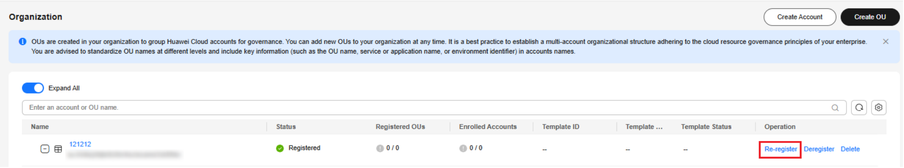
- Any OU that contains accounts that failed to be created or unmanaged cannot be re-registered.
- The core OU cannot be registered or re-registered.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the OU to be re-registered, and click **Re-register** in the **Operation** column.

Figure 2-5 Re-registering an OU



Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

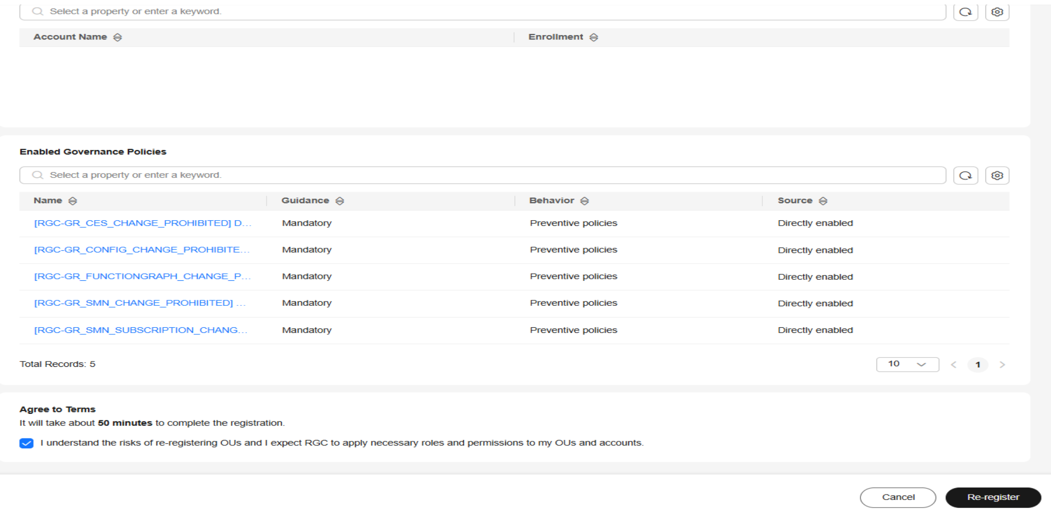
Expand All

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
121212 [redacted]	Registered	0 / 0	0 / 0	--	--	--	Re-register Deregister Delete

Step 3 Confirm governance policies attached to the OU and member accounts, and select the checkbox **I understand the risks of re-registering OUs and I expect RGC to apply necessary roles and permissions to my OUs and accounts**.

Figure 2-6 Confirming OU details



Select a property or enter a keyword.

Account Name	Enrollment

Enabled Governance Policies

Select a property or enter a keyword.

Name	Guidance	Behavior	Source
[RGC-GR_CES_CHANGE_PROHIBITED] D...	Mandatory	Preventive policies	Directly enabled
[RGC-GR_CONFIG_CHANGE_PROHIBITE...	Mandatory	Preventive policies	Directly enabled
[RGC-GR_FUNCTIONGRAPH_CHANGE_P...	Mandatory	Preventive policies	Directly enabled
[RGC-GR_SMN_CHANGE_PROHIBITED] ...	Mandatory	Preventive policies	Directly enabled
[RGC-GR_SMN_SUBSCRIPTION_CHANG...	Mandatory	Preventive policies	Directly enabled

Total Records: 5

Agree to Terms

It will take about **50 minutes** to complete the registration.

☑ I understand the risks of re-registering OUs and I expect RGC to apply necessary roles and permissions to my OUs and accounts.

Step 4 Click **Re-register**. It takes a while to re-register an OU. You can view the OU registration status in the organizational structure. After being re-registered, the OU can be governed in the landing zone.

----End

2.5 Deregistering an OU

If you no longer want a registered OU to be governed in your landing zone or you do not want to re-register an OU that failed to be registered, you can deregister the OU.

Constraints

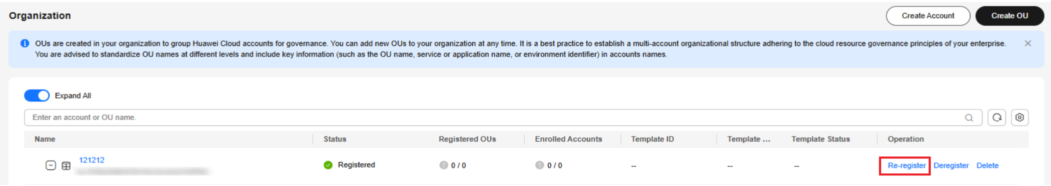
- The core OU or root OU cannot be deregistered.
- Before deregistering an OU, deregister its registered child OUs and unmanage its enrolled accounts, if there are any.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the OU you want to deregister, and click **Deregister** in the **Operation** column.

Figure 2-7 Deregistering an OU



Organization

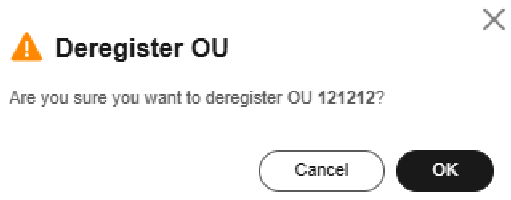
OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
121212 [redacted]	Registered	0 / 0	0 / 0	--	--	--	Re-register Deregister Delete

Step 3 Review and confirm the details of the OU to be deregistered, and click **OK**.

Figure 2-8 Confirming OU details



Deregister OU

Are you sure you want to deregister OU 121212?

----End

2.6 Deleting an OU

If you no longer need an OU, you can delete it on the RGC console. Once deleted, the OU is also deleted from the Organizations console.

Constraints

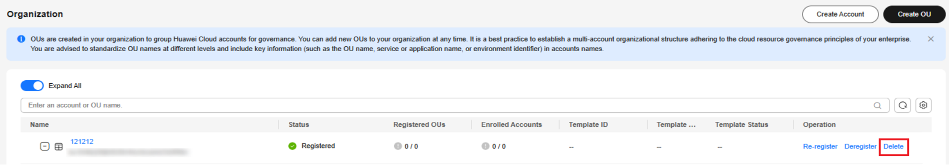
- Unregistered OUs and the core and root OUs cannot be deleted.
- You must first deregister any registered child OUs and unmanage enrolled accounts in an OU, and then you can delete that OU.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the OU you want to delete, and click **Delete** in the **Operation** column.

Figure 2-9 Deleting an OU



Organization

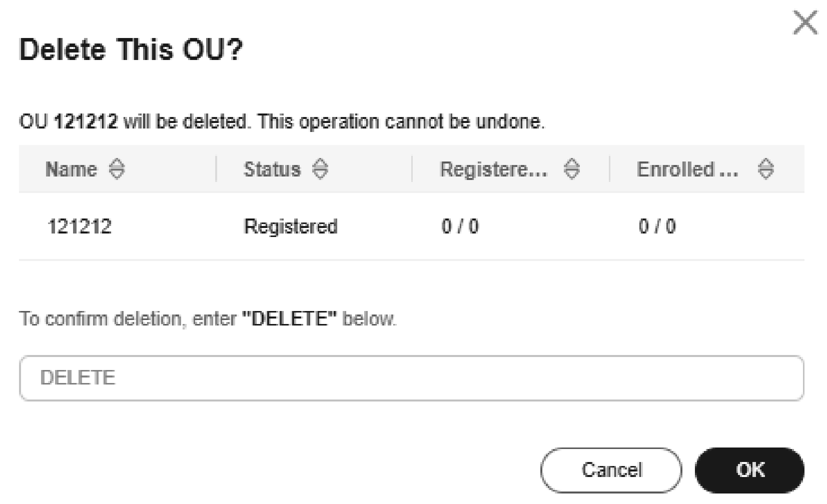
OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
121212 [redacted]	Registered	0 / 0	0 / 0	--	--	--	Re-register Deregister Delete

Step 3 Review and confirm the OU details, and then enter "DELETE".

Figure 2-10 Confirming OU details



Delete This OU?

OU 121212 will be deleted. This operation cannot be undone.

Name	Status	Registere...	Enrolled ...
121212	Registered	0 / 0	0 / 0

To confirm deletion, enter "DELETE" below.

DELETE

Step 4 Click **OK**.

----End

2.7 Viewing Organization Details

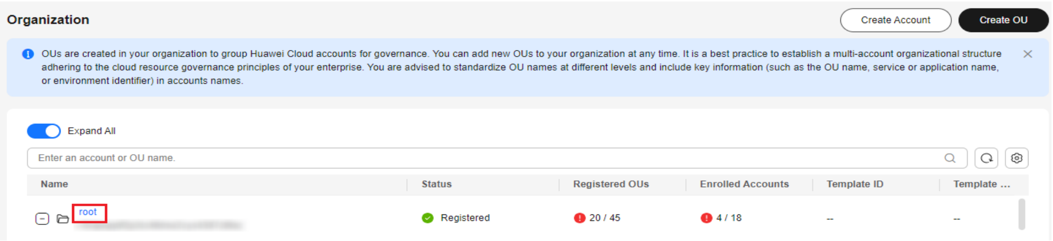
After a landing zone is set up, you can view OU details, non-compliant resources, enabled governance policies, and directly nested OUs and accounts.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, and click the name of an OU you want to view.

Figure 2-11 Locating an OU



Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

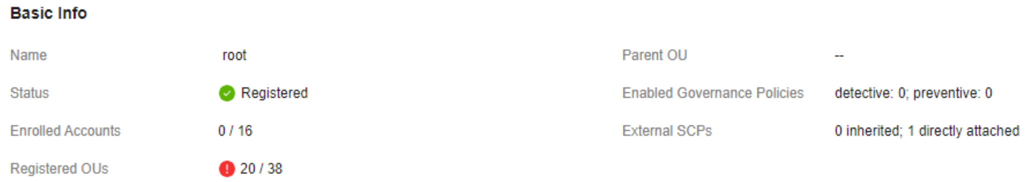
Expand All

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...
root [redacted]	Registered	20 / 45	4 / 18	--	--

Step 3 On the displayed page, view the OU status, parent OU, number of enrolled accounts, number of enabled governance policies, number of registered OUs, and external SCPs.

Figure 2-12 Viewing OU details

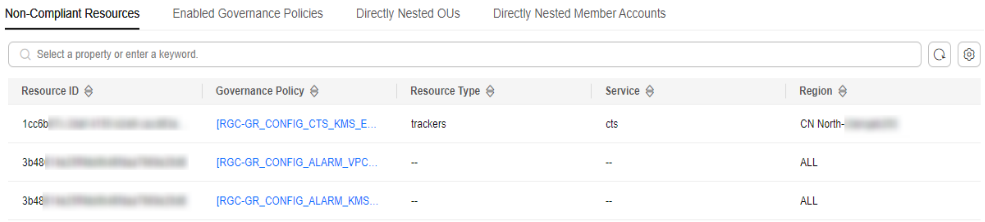


Basic Info

Name	root	Parent OU	--
Status	✓ Registered	Enabled Governance Policies	detective: 0; preventive: 0
Enrolled Accounts	0 / 16	External SCPs	0 inherited; 1 directly attached
Registered OUs	! 20 / 38		

Step 4 Click the **Non-Compliant Resources** tab. The non-compliant resources of the OU are displayed, including the resource ID, resource type, service type, and region.

Figure 2-13 Viewing non-compliant resources

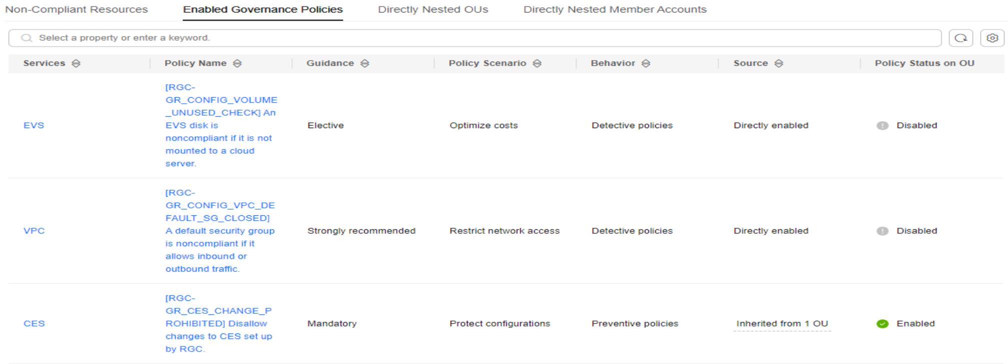

Non-Compliant Resources
Enabled Governance Policies
Directly Nested OUs
Directly Nested Member Accounts
Select a property or enter a keyword.

Resource ID	Governance Policy	Resource Type	Service	Region
1cc6b[redacted]	[RGC-GR_CONFIG_CTS_KMS_E...	trackers	cts	CN North-[redacted]
3b48[redacted]	[RGC-GR_CONFIG_ALARM_VPC...	--	--	ALL
3b48[redacted]	[RGC-GR_CONFIG_ALARM_KMS...	--	--	ALL

Step 5 Click the **Enabled Governance Policies** tab. The governance policies enabled for the OU are displayed.

For details about governance policies, see **5.4 Viewing Governance Policy Details**.

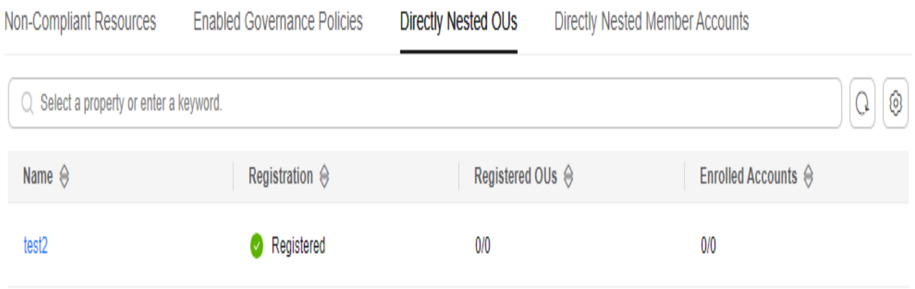
Figure 2-14 Viewing enabled governance policies


Non-Compliant Resources
Enabled Governance Policies
Directly Nested OUs
Directly Nested Member Accounts
Select a property or enter a keyword.

Services	Policy Name	Guidance	Policy Scenario	Behavior	Source	Policy Status on OU
EVS	[RGC-GR_CONFIG_VOLUME_UNUSED_CHECK] An EVS disk is noncompliant if it is not mounted to a cloud server.	Elective	Optimize costs	Detective policies	Directly enabled	Disabled
VPC	[RGC-GR_CONFIG_VPC_DEFAULT_SG_CLOSED] A default security group is noncompliant if it allows inbound or outbound traffic.	Strongly recommended	Restrict network access	Detective policies	Directly enabled	Disabled
CES	[RGC-GR_CES_CHANGE_PROHIBITED] Disallow changes to CES set up by RGC.	Mandatory	Protect configurations	Preventive policies	Inherited from 1 OU	✓ Enabled

Step 6 Click the **Directly Nested OUs** tab. The details of OUs directly nested under the OU are displayed, including the registration status, registered OUs, and enrolled accounts.

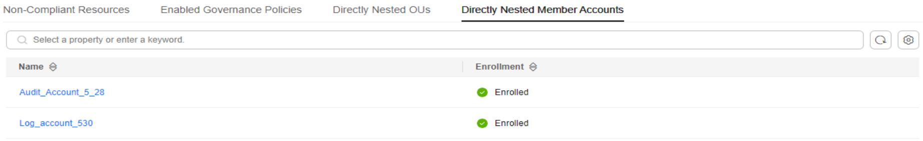
Figure 2-15 Viewing directly nested OUs


Non-Compliant Resources
Enabled Governance Policies
Directly Nested OUs
Directly Nested Member Accounts
Select a property or enter a keyword.

Name	Registration	Registered OUs	Enrolled Accounts
test2	✓ Registered	0/0	0/0

Step 7 Click the **Directly Nested Member Accounts** tab. The details of member accounts directly nested under the OU are displayed, including the account names and enrollment status.

Figure 2-16 Viewing directly nested member accounts


Non-Compliant Resources
Enabled Governance Policies
Directly Nested OUs
Directly Nested Member Accounts
Select a property or enter a keyword.

Name	Enrollment
Audit_Account_5_28	✓ Enrolled
Log_account_530	✓ Enrolled

----End

3 Template Management

3.1 Overview of a Template

Introduction

A template is an HCL-formatted text file that describes your cloud resources. Its format can be .tf, .tf.json, or .zip. In the template, you can define a large scale of instances of different services and specifications. By authoring a template, you can design applications and plan multiple resources to be automatically deployed or destructed together. This makes service organization and management much easier. What's better, each template can be reused in multiple contexts for higher efficiency.

RGC Account Factory allows you to quickly create accounts using a template. The management account can author a template with account baseline configurations in RGC or RFS. In the account factory, you can use the management account to create member accounts under a specified OU, and baseline configurations will be automatically applied to your accounts based on best practices.

For more information about templates, see **Resource Formation Service User Guide**.

Constraints

For details about the constraints on template specifications and quotas, see **Constraints**.

Preset Templates

RGC comes with preset templates for the following scenarios:

- **Network planning**
  - DNS: This template is used to configure DNS endpoints and rules and to associate with VPCs.
  - ER: This template is used to create enterprise routers and attach existing VPCs to them.

- VPC: This template is used to directly create VPCs and subnets.

3.2 Uploading a Template

RGC allows you to use a template file that you upload or you can use a preset template. The following describes how to upload a template file to RGC.

Constraints

- Only .zip files are supported. The maximum .zip file size is 50 KB, but the decompressed file can be up to 1 MB.
- The template content must be within the constraints described in **Template Constraints**.

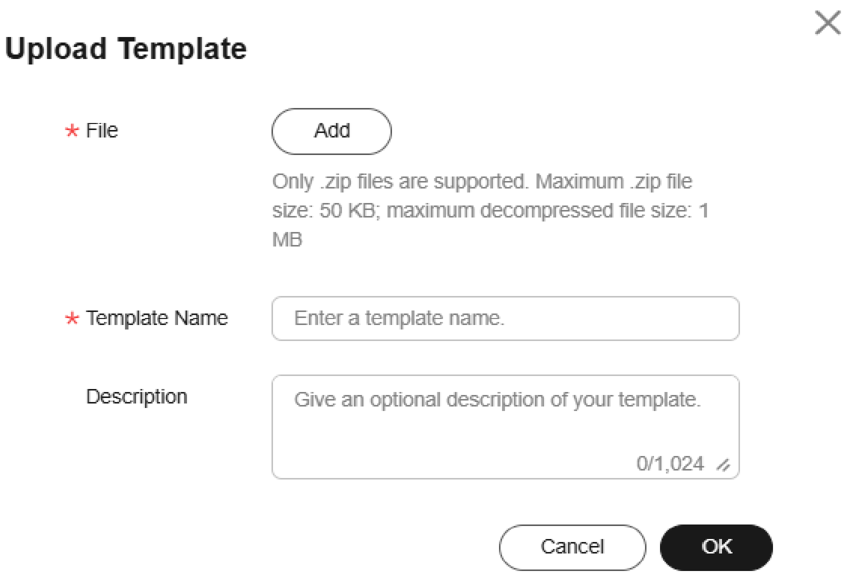
Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Templates** page, and click **Upload Template** in the upper right corner.

Step 3 Click **Add**.

Figure 3-1 Adding a template file



Only .zip files are supported. Maximum .zip file size: 50 KB; maximum decompressed file size: 1 MB

Enter a template name.

Give an optional description of your template.

Step 4 Enter a unique template name.

Step 5 Click **OK**. You can see the template you uploaded in the template list.

----End

3.3 Using a Preset Template

In addition to using a custom template, you can also use a preset template in RGC to quickly create accounts. For details about preset templates provided by RGC, see **Preset Templates**.

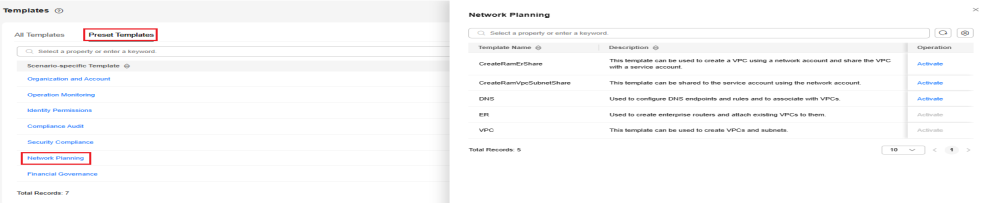
Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Templates** page, and go to the **Preset Templates** page.

Step 3 Click the name of the template you want to use.

Figure 3-2 Clicking a template name


Templates
All Templates
Preset Templates
Select a property or enter a keyword.
Network Planning
Select a property or enter a keyword.
10
1

Scenario-specific Template
Organization and Account
Operation Monitoring
Identity Permissions
Compliance Audit
Security Compliance
Network Planning
Financial Governance

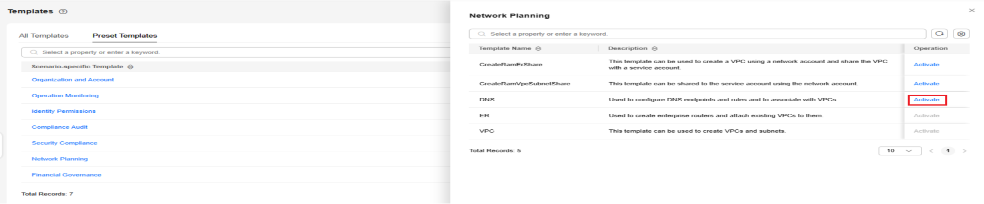
Total Records: 7

Template Name	Description	Operation
CreateRamErShare	This template can be used to create a VPC using a network account and share the VPC with a service account.	Activate
CreateRamVpcSubnetShare	This template can be shared to the service account using the network account.	Activate
DNS	Used to configure DNS endpoints and rules and to associate with VPCs.	Activate
ER	Used to create enterprise routers and attach existing VPCs to them.	Activate
VPC	This template can be used to create VPCs and subnets.	Activate

Total Records: 5

Step 4 Locate the template and click **Activate** in the **Operation** column.

Figure 3-3 Activating a template


Templates
All Templates
Preset Templates
Select a property or enter a keyword.
Network Planning
Select a property or enter a keyword.
10
1

Scenario-specific Template
Organization and Account
Operation Monitoring
Identity Permissions
Compliance Audit
Security Compliance
Network Planning
Financial Governance

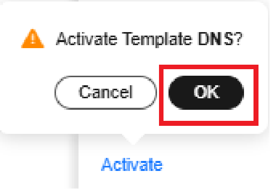
Total Records: 7

Template Name	Description	Operation
CreateRamErShare	This template can be used to create a VPC using a network account and share the VPC with a service account.	Activate
CreateRamVpcSubnetShare	This template can be shared to the service account using the network account.	Activate
DNS	Used to configure DNS endpoints and rules and to associate with VPCs.	Activate
ER	Used to create enterprise routers and attach existing VPCs to them.	Activate
VPC	This template can be used to create VPCs and subnets.	Activate

Total Records: 5

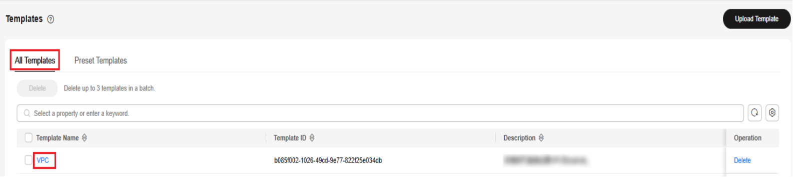
Step 5 Confirm the template information and click **OK**.

Figure 3-4 Confirming the template


Activate Template DNS?

Step 6 Switch back to the **Templates** page. The activated template is displayed in the template list.

Figure 3-5 Template activated


Templates
Upload Template
All Templates
Preset Templates
Delete
Delete up to 3 templates in a batch.
Select a property or enter a keyword.

Template Name	Template ID	Description	Operation
VPC	b085f002-1026-49cd-9e77-822f25e034db	[redacted]	Delete

----End

3.4 Viewing, Modifying, or Deleting a Template

After a template is created, you can view its details and modify its content on the RGC console. Alternatively, you can go to the RFS console and choose **Templates** > **Private Templates** to view and modify the template.

If you have created the maximum number of templates but want to create more, or if you no longer need some templates, you can delete unnecessary templates on the RGC console. Once deleted, the templates are also deleted from the RFS console.

If you have deleted a preset template but still need to use it, you can activate the template by referring to **3.3 Using a Preset Template**.

Constraints

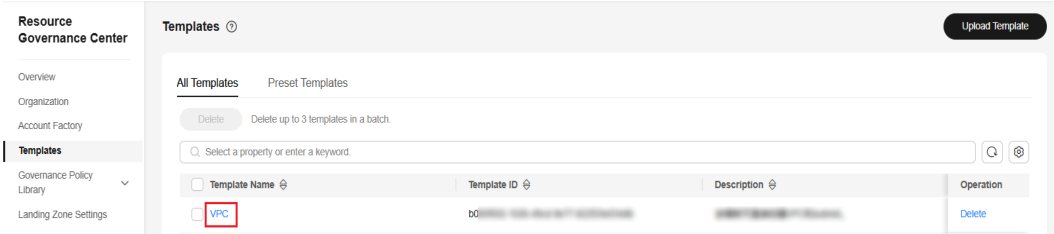
- The new template content must be within the constraints described in **Template Constraints**.
- Deleting a template only deletes the template itself, and the resources created using the template are not deleted.

Viewing or Modifying a Template

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Templates** page, and click the name of the template you want to view or modify.

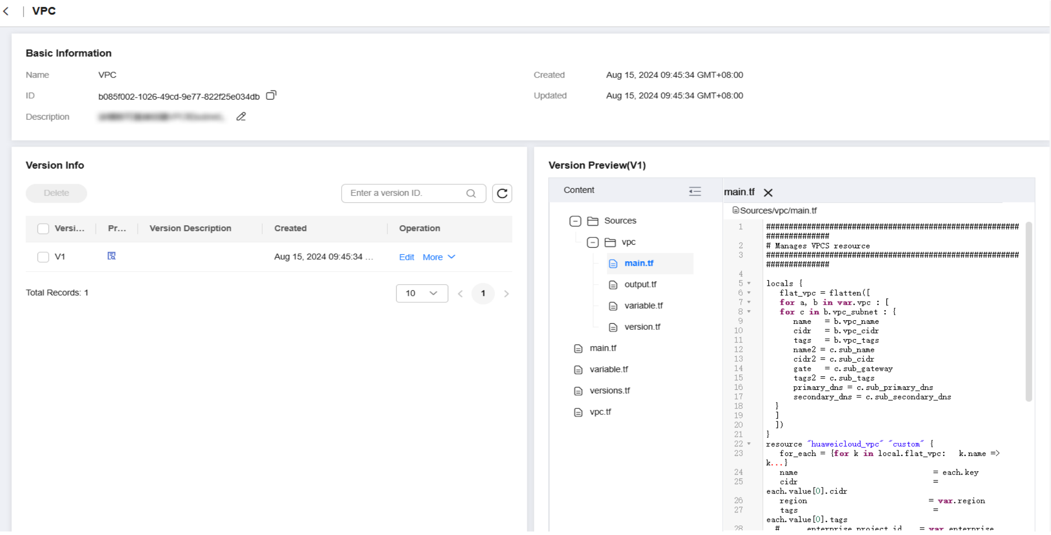
Figure 3-6 Clicking a template name


Resource Governance Center
Overview
Organization
Account Factory
Templates
Governance Policy Library
Landing Zone Settings
Templates
Upload Template
All Templates
Preset Templates
Delete
Delete up to 3 templates in a batch.
Select a property or enter a keyword.

Template Name	Template ID	Description	Operation
VPC	b0[redacted]	[redacted]	Delete

Step 3 Go to the template details page. You can view the template details.

Figure 3-7 Viewing template details



< | VPC

Basic Information

Name VPC

ID b085f002-1026-49cd-9e77-822f25e034db

Description [redacted]

Created Aug 15, 2024 09:45:34 GMT+08:00

Updated Aug 15, 2024 09:45:34 GMT+08:00

Version Info

□ Versi...	Pr...	Version Description	Created	Operation
□ V1			Aug 15, 2024 09:45:34 ...	Edit More

Total Records: 1

Version Preview(V1)

Content: Sources / vpc / main.tf, output.tf, variable.tf, version.tf; main.tf, variable.tf, versions.tf, vpc.tf

main.tf

Sources/vpc/main.tf

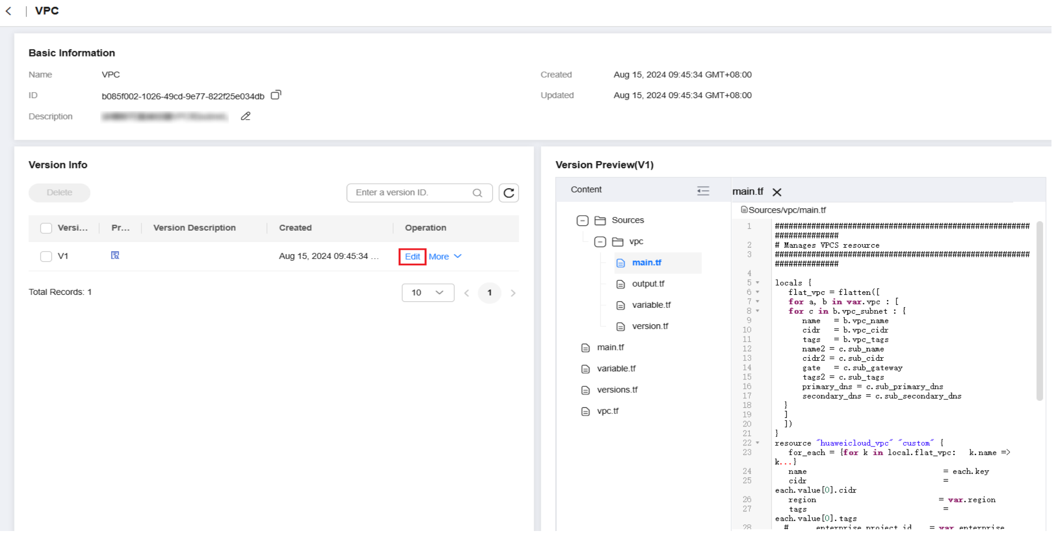
```
##############################################################
##############
# Manages VPCS resource
##############################################################
##############

locals {
   flat_vpc = flatten([
   for a, b in var.vpc : [
   for c in b.vpc_subnet : {
      name   = b.vpc_name
      cidr   = b.vpc_cidr
      tags   = b.vpc_tags
      name2 = c.sub_name
      cidr2 = c.sub_cidr
      gate   = c.sub_gateway
      tags2 = c.sub_tags
      primary_dns = c.sub_primary_dns
      secondary_dns = c.sub_secondary_dns
   }
   ]
   ])
}
resource "huaweicloud_vpc" "custom" {
   for_each = {for k in local.flat_vpc:   k.name =>
k...}
   name                              = each.key
   cidr                              =
each.value[0].cidr
   region                            = var.region
   tags                              =
each.value[0].tags
  #      enterprise_project_id    = var.enterprise
```

Step 4 In the **Template Version** area, locate the template you want to modify, and click **Edit** in the **Operation** column.

For details about the template syntax, see **Templates**.

Figure 3-8 Modifying a template



< | VPC

Basic Information

Name VPC

ID b085f002-1026-49cd-9e77-822f25e034db

Description [redacted]

Created Aug 15, 2024 09:45:34 GMT+08:00

Updated Aug 15, 2024 09:45:34 GMT+08:00

Version Info

□ Versi...	Pr...	Version Description	Created	Operation
□ V1			Aug 15, 2024 09:45:34 ...	Edit More

Total Records: 1

Version Preview(V1)

Content: Sources / vpc / main.tf, output.tf, variable.tf, version.tf; main.tf, variable.tf, versions.tf, vpc.tf

main.tf

Sources/vpc/main.tf

```
##############################################################
##############
# Manages VPCS resource
##############################################################
##############

locals {
   flat_vpc = flatten([
   for a, b in var.vpc : [
   for c in b.vpc_subnet : {
      name   = b.vpc_name
      cidr   = b.vpc_cidr
      tags   = b.vpc_tags
      name2 = c.sub_name
      cidr2 = c.sub_cidr
      gate   = c.sub_gateway
      tags2 = c.sub_tags
      primary_dns = c.sub_primary_dns
      secondary_dns = c.sub_secondary_dns
   }
   ]
   ])
}
resource "huaweicloud_vpc" "custom" {
   for_each = {for k in local.flat_vpc:   k.name =>
k...}
   name                              = each.key
   cidr                              =
each.value[0].cidr
   region                            = var.region
   tags                              =
each.value[0].tags
  #      enterprise_project_id    = var.enterprise
```

Step 5 Modify the template, and then click **Save** in the upper right corner.

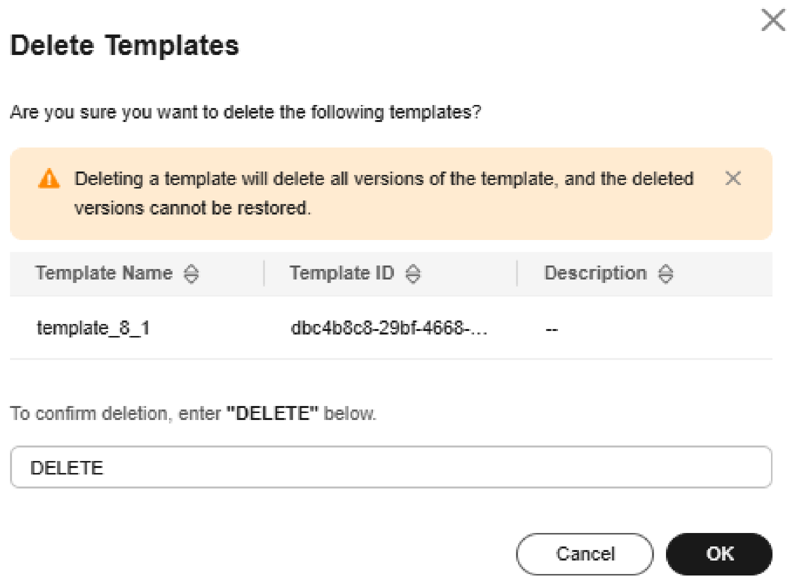
----End

Deleting a Template

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Templates** page, locate the template you want to delete, and click **Delete** in the **Operation** column.

Figure 3-9 Deleting a template



Delete Templates

Are you sure you want to delete the following templates?

Deleting a template will delete all versions of the template, and the deleted versions cannot be restored.

Template Name	Template ID	Description
template_8_1	dbc4b8c8-29bf-4668-...	--

To confirm deletion, enter **"DELETE"** below.

DELETE

Step 3 Review and confirm the template details, and then enter "DELETE".

Step 4 Click **OK**.

----End

4 Account Management

4.1 Creating an Account

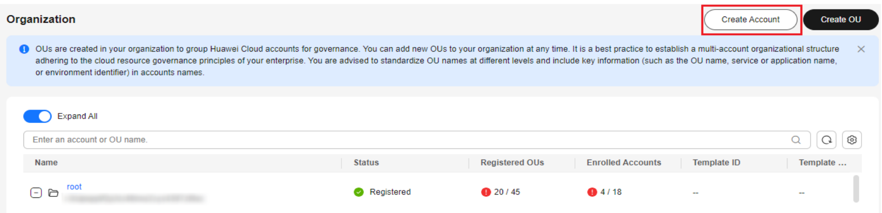
You can create an account in RGC. The account then will be automatically enrolled in RGC.

Procedure

Step 1 Log in to Huawei Cloud as the RGC administrator, and navigate to the RGC console.

Step 2 Access the **Organization** page, and click **Create Account**.

Figure 4-1 Creating an account



OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...
root [redacted]	Registered	20 / 45	4 / 18	--	--

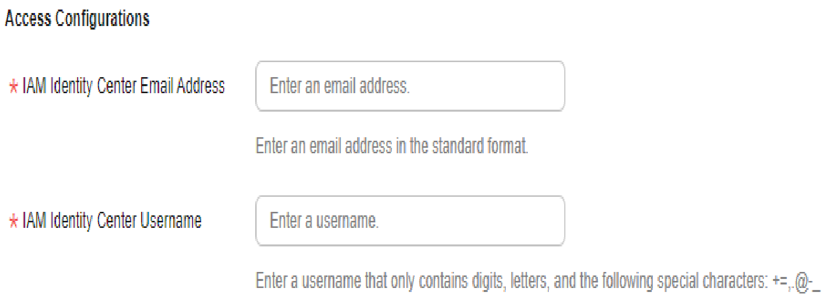
Step 3 Configure account details, including the email address account name. Ensure that they are not currently used for any existing accounts.

The email address cannot be used for password retrieval or other purposes.

Step 4 Configure IAM Identity Center details, including the email address and username.

After an account is created, an IAM Identity Center user is automatically created in RGC. You can use an IAM Identity Center username and password to log in to the management console through the user portal URL, and use the email address to retrieve the password. For details, see **Logging In as an IAM Identity Center User and Accessing Resources**.

Figure 4-2 Configuring IAM Identity Center details


Access Configurations

* IAM Identity Center Email Address: Enter an email address.

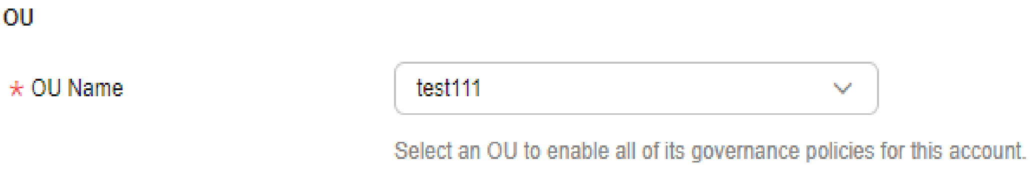
Enter an email address in the standard format.

* IAM Identity Center Username: Enter a username.

Enter a username that only contains digits, letters, and the following special characters: +=,.@-_

Step 5 Select a registered OU where your account will be added, and enable all governance policies configured for the OU for the account.

Figure 4-3 Selecting a registered OU


OU

* OU Name: test111

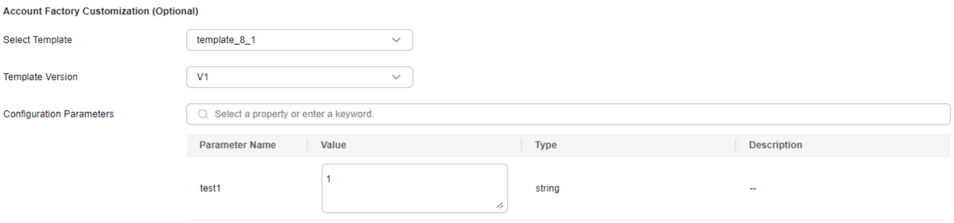
Select an OU to enable all of its governance policies for this account.

Step 6 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

For more information about RFS templates, see **Templates**.

- **Select Template**: Select a template you created in RFS.
- **Template Version**: Select the version for the template.
- **Configuration Parameters**: Modify parameter settings in the template based on service requirements.

Figure 4-4 Configuring a template


Account Factory Customization (Optional)

Select Template: template_8_1

Template Version: V1

Configuration Parameters: Select a property or enter a keyword.

Parameter Name	Value	Type	Description
test1	1	string	--

Step 7 Click **Create Account**. The created account will be displayed in the account list.

----End

4.2 Enrolling an Account

If you created an account via Organizations or invited an account to your organization before setting up a landing zone via RGC, the account will not be automatically enrolled in the landing zone, and you need to manually enroll the account so that it will be governed in the landing zone.

Constraints

- If an account has enabled Config and has a resource recorder, exercise caution when enrolling the account because the recorder configurations will be overwritten after enrollment.
- If you want to transfer an account from one landing zone to another one by performing an account enrollment, unmanage the account from the original landing zone and then enroll it in the new landing zone. If you have enrolled the account in the new landing zone, manually delete the resources, such as agencies and policies, of the account from the original landing zone, or an error will occur.
- Before enrolling an invited account, make sure you have met the requirements in **Prerequisites**. Otherwise, the account enrollment may fail.

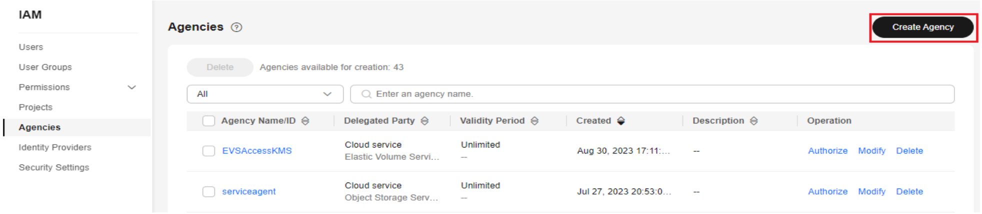
Prerequisites

Perform the following steps only when you want to enroll accounts you invited into your organization. When enrolling accounts you created in the organization, skip the steps.

Step 1 Log in to Huawei Cloud using the account you want to enroll, and navigate to the IAM console.

Step 2 In the navigation pane, choose **Agencies** and click **Create Agency** in the upper right corner.

Figure 4-5 Creating an agency

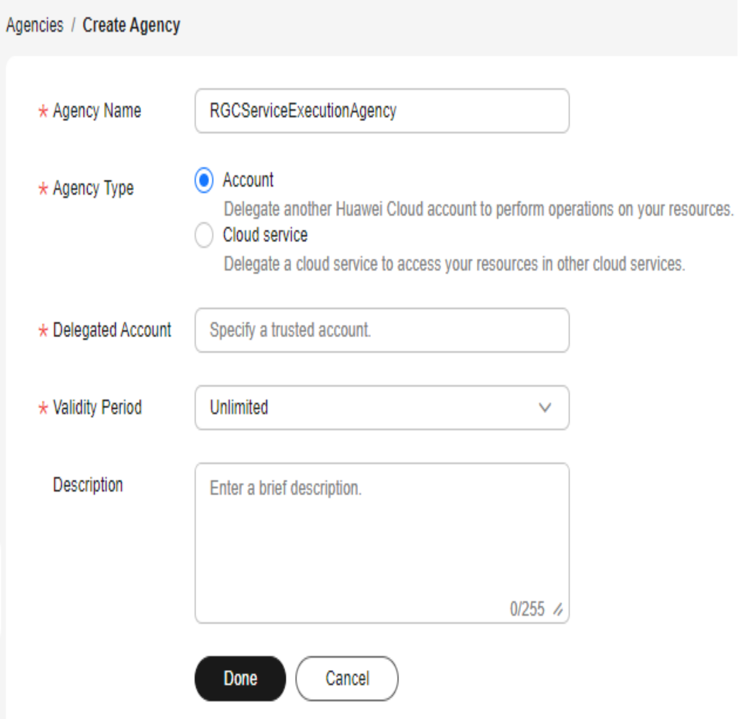


Agencies available for creation: 43

□	Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
□	EVSAccessKMS	Cloud service Elastic Volume Servi...	Unlimited --	Aug 30, 2023 17:11:...	--	Authorize Modify Delete
□	serviceagent	Cloud service Object Storage Serv...	Unlimited --	Jul 27, 2023 20:53:0...	--	Authorize Modify Delete

Step 3 Set the agency name to **RGCServiceExecutionAgency**.

Figure 4-6 Specifying an agency name



Agencies / Create Agency

* Agency Name: RGCServiceExecutionAgency

* Agency Type:
● Account
Delegate another Huawei Cloud account to perform operations on your resources.
○ Cloud service
Delegate a cloud service to access your resources in other cloud services.

* Delegated Account: Specify a trusted account.

* Validity Period: Unlimited

Description: Enter a brief description. 0/255

Step 4 Set **Agency Type** to **Account** and **Delegated Account** to the RGC management account name.

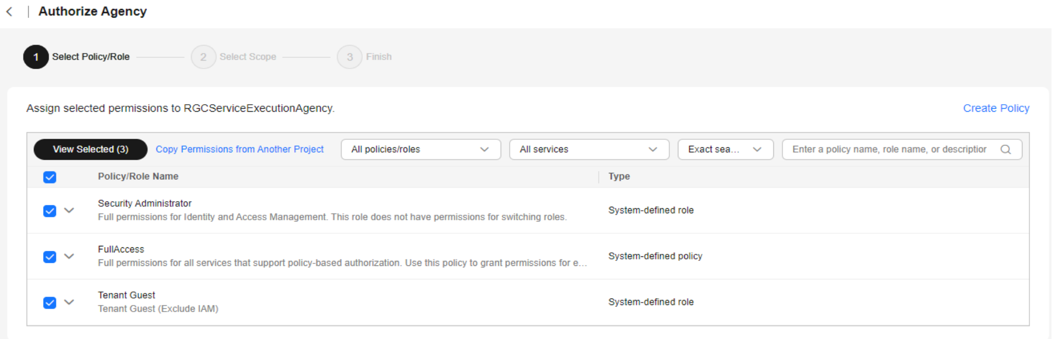
Step 5 Configure a validity period and enter a description for the agency.

Step 6 Click **OK**.

Step 7 In the displayed dialog box, click **Authorize**.

Step 8 Select **Security Administrator**, **FullAccess**, and **Tenant Guest**.

Figure 4-7 Permissions to be granted to the agency



Authorize Agency

1 Select Policy/Role — 2 Select Scope — 3 Finish

Assign selected permissions to RGCServiceExecutionAgency.

Create Policy
View Selected (3)
Copy Permissions from Another Project
All policies/roles
All services
Exact sea...
Enter a policy name, role name, or descriptior

☑	Policy/Role Name	Type
☑	Security Administrator Full permissions for Identity and Access Management. This role does not have permissions for switching roles.	System-defined role
☑	FullAccess Full permissions for all services that support policy-based authorization. Use this policy to grant permissions for e...	System-defined policy
☑	Tenant Guest Tenant Guest (Exclude IAM)	System-defined role

Step 9 Click **Next** to set the authentication scope.

Step 10 Click **OK**. The agency is created. You can then follow the instructions in **Procedure** to enroll the account.

NOTE

Once the **RGCServiceExecutionAgency** agency is created, it cannot be deleted, or RGC services will become unavailable.

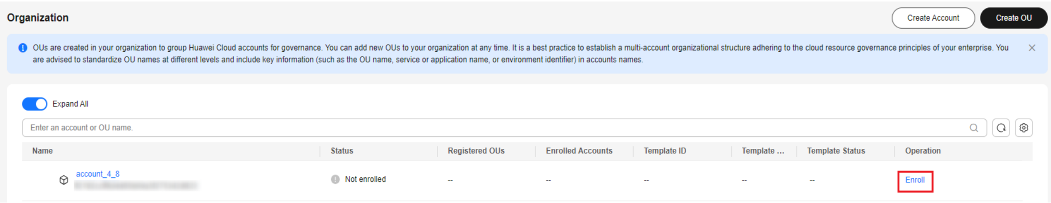
----End

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the account you want to enroll, and click **Enroll** in the **Operation** column.

Figure 4-8 Enrolling an account



Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

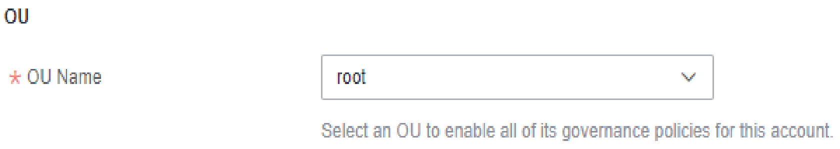
Expand All

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
account_4_8 [redacted]	Not enrolled	--	--	--	--	--	Enroll

Step 3 Select a registered OU where your account will be added, and enable all governance policies configured for the OU for the account.

Figure 4-9 Selecting a registered OU



OU

* OU Name: root

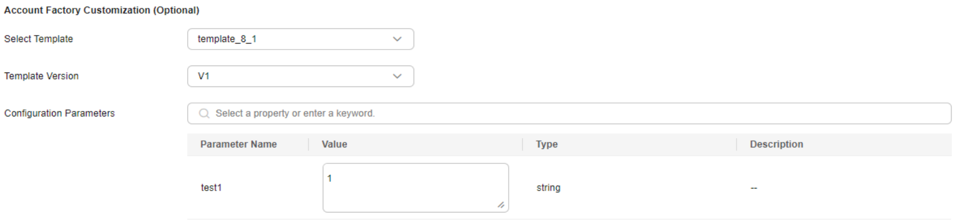
Select an OU to enable all of its governance policies for this account.

Step 4 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

For more information about RFS templates, see **Templates**.

- **Select Template**: Select a template you created in RFS.
- **Template Version**: Select the version for the template.
- **Configuration Parameters**: Modify parameter settings in the template based on service requirements.

Figure 4-10 Configuring a template



Account Factory Customization (Optional)

Select Template: template_8_1

Template Version: V1

Configuration Parameters: Select a property or enter a keyword.

Parameter Name	Value	Type	Description
test1	1	string	--

Step 5 Click **Enroll Account**. You can view the enrollment status in the organizational structure. Once enrolled, the account will be governed in the landing zone.

----End

4.3 Viewing Account Details

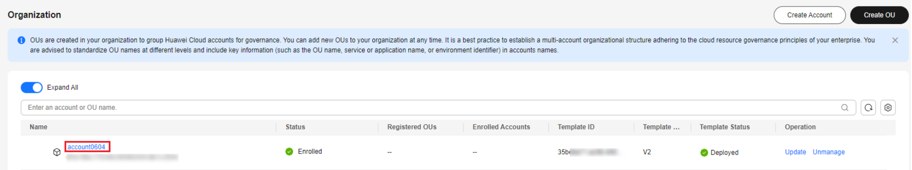
After setting up a landing zone in RGC, you can view the account details, including its enrollment status, non-compliant resources, template details, regions, and external Config rules.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, and click the name of the account you want to view.

Figure 4-11 Viewing account details



Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Expand All

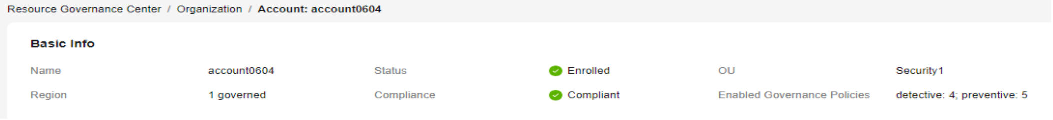
Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
account0604 [redacted]	Enrolled	--	--	35b[redacted]	V2	Deployed	Update Unmanage

Step 3 On the displayed page, view the account status, OU, number of governed regions, compliance status, and number of enabled governance policies.

If there are non-compliant resources, **Non-compliant** will be displayed.

Figure 4-12 Viewing account details



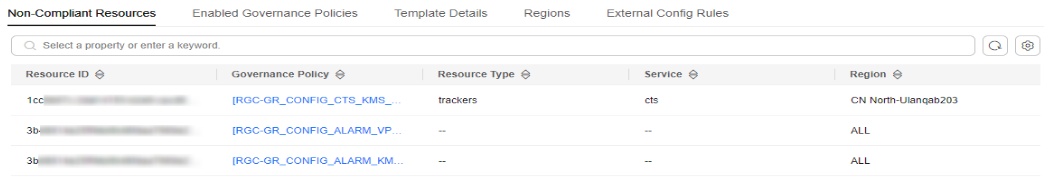
Resource Governance Center / Organization / Account: account0604

Basic Info

Name	account0604	Status	Enrolled	OU	Security1
Region	1 governed	Compliance	Compliant	Enabled Governance Policies	detective: 4; preventive: 5

Step 4 Click the **Non-Compliant Resources** tab. The non-compliant resources of the account are displayed, including the resource ID, resource type, governance policy, and region for each resource.

Figure 4-13 Viewing non-compliant resources



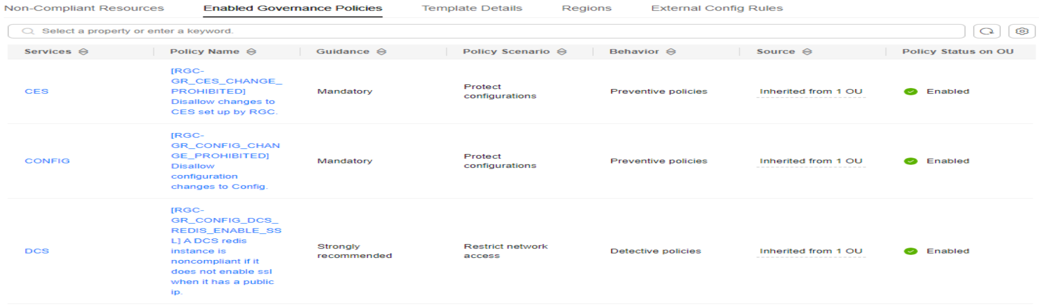
Select a property or enter a keyword.

Resource ID	Governance Policy	Resource Type	Service	Region
1cc[redacted]	[RGC-GR_CONFIG_CTS_KMS_...	trackers	cts	CN North-Ulanqab203
3b[redacted]	[RGC-GR_CONFIG_ALARM_VP...	--	--	ALL
3b[redacted]	[RGC-GR_CONFIG_ALARM_KM...	--	--	ALL

Step 5 Click the **Enabled Governance Policies** tab. The governance policies enabled for the account are displayed.

For details about governance policies, see **5.4 Viewing Governance Policy Details**.

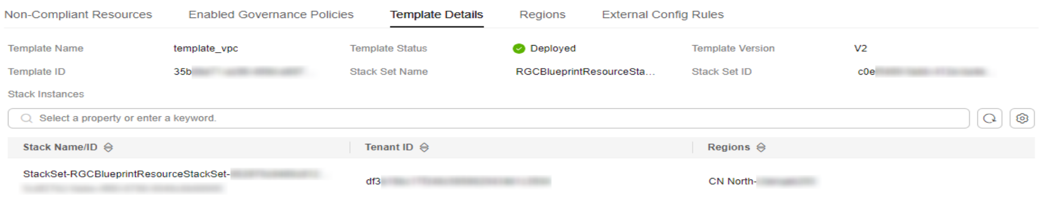
Figure 4-14 Viewing enabled governance policies



Services	Policy Name	Guidance	Policy Scenario	Behavior	Source	Policy Status on OU
CES	[RGC-GR_CES_CHANGE_PROHIBITED] Disallow changes to CES set up by RGC.	Mandatory	Protect configurations	Preventive policies	Inherited from 1 OU	Enabled
CONFIG	[RGC-GR_CONFIG_CHANGE_PROHIBITED] Disallow configuration changes to Config.	Mandatory	Protect configurations	Preventive policies	Inherited from 1 OU	Enabled
DCS	[RGC-GR_CONFIG_DCS_REDIS_ENABLE_SSL] A DCS redis instance is noncompliant if it does not enable ssl when it has a public ip.	Strongly recommended	Restrict network access	Detective policies	Inherited from 1 OU	Enabled

Step 6 Click the **Template Details** tab. The details of the RFS templates used by the account are displayed. If the account does not use any templates, no information will be displayed.

Figure 4-15 Viewing template details

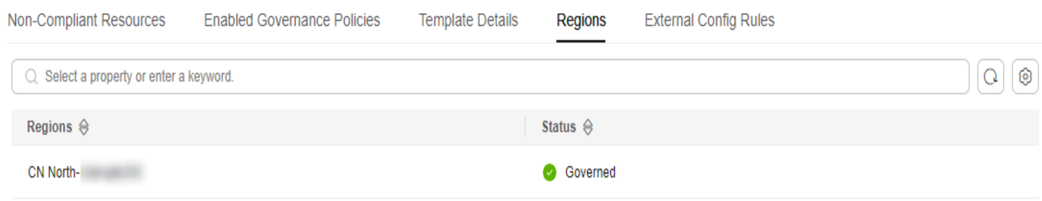


Template Name template_vpc
Template Status Deployed
Template Version V2
Template ID 35b[redacted]
Stack Set Name RGCBlueprintResourceSta...
Stack Set ID c0e[redacted]
Stack Instances

Stack Name/ID	Tenant ID	Regions
StackSet-RGCBlueprintResourceStackSet-[redacted]	df3[redacted]	CN North-[redacted]

Step 7 Click the **Regions** tab. The details about the regions governed are displayed. In those regions, the accounts and their resources are all governed by the landing zone. Resources in other regions are not governed.

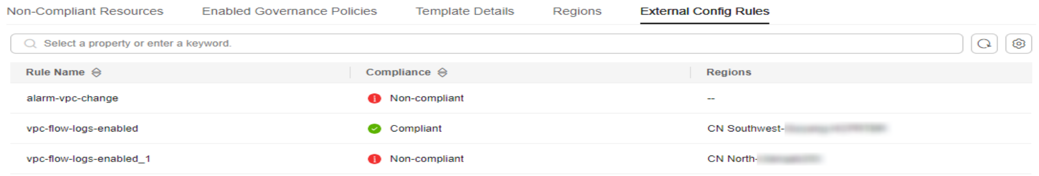
Figure 4-16 Viewing governed regions



Regions	Status
CN North-[redacted]	Governed

Step 8 Click the **External Config Rules** tab. Config rules other than those enabled for the current landing zone are displayed, as well as the regions where the rules apply.

Figure 4-17 Viewing external Config rules



Rule Name	Compliance	Regions
alarm-vpc-change	Non-compliant	--
vpc-flow-logs-enabled	Compliant	CN Southwest-[redacted]
vpc-flow-logs-enabled_1	Non-compliant	CN North-[redacted]

----End

4.4 Updating an Account

If you want to change the OU, templates, and template versions of an account, you can update the account.

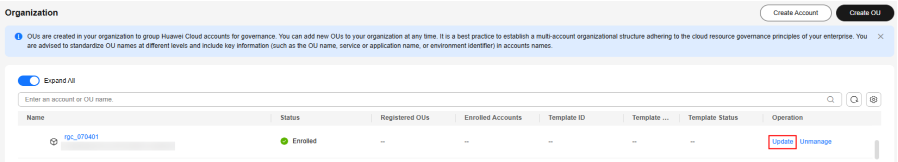
If you change the OU of an account, the governance policies of the new OU may be different from those of the original OU. Ensure that the governance policies of the new OU meet your account requirements before performing this operation.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the account you want to update, and click **Update** in the **Operation** column.

Figure 4-18 Updating an account



Organization

Create Account | Create OU

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

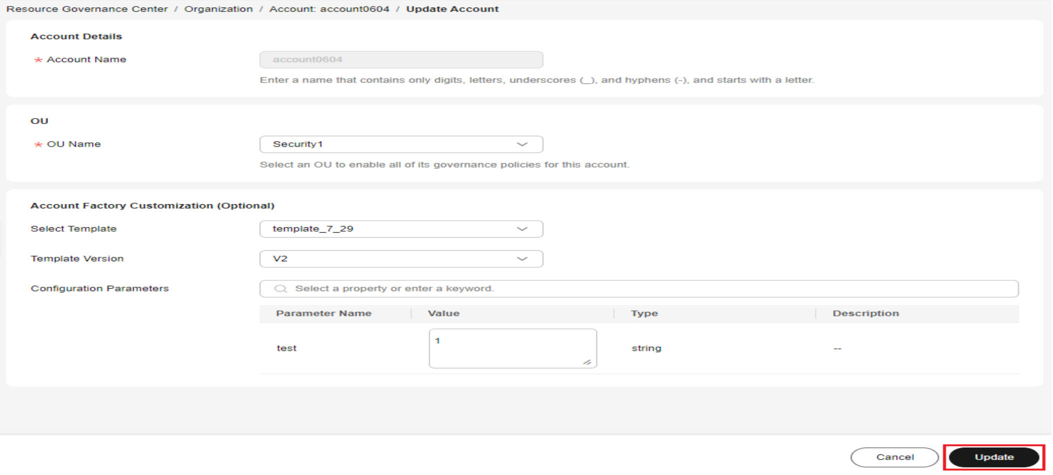
Expand All

Enter an account or OU name.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
rgc_070401	Enrolled	--	--	--	--	--	Update Unmanage

Step 3 Select a new OU, new templates, and template versions for the account.

Figure 4-19 Changing an account



Resource Governance Center / Organization / Account: account0604 / Update Account

Account Details

* Account Name: account0604

Enter a name that contains only digits, letters, underscores (_), and hyphens (-), and starts with a letter.

OU

* OU Name: Security1

Select an OU to enable all of its governance policies for this account.

Account Factory Customization (Optional)

Select Template: template_7_29

Template Version: V2

Configuration Parameters: Select a property or enter a keyword.

Parameter Name	Value	Type	Description
test	1	string	--

Cancel | Update

Step 4 Click **Update** in the lower right corner. After the account is updated, you can click its name to view its details.

----End

4.5 Unmanaging an Account

If you no longer want an enrolled account to be governed in your landing zone or you do not want to enroll again an OU that failed to be enrolled, you can unmanage the account.

Constraints

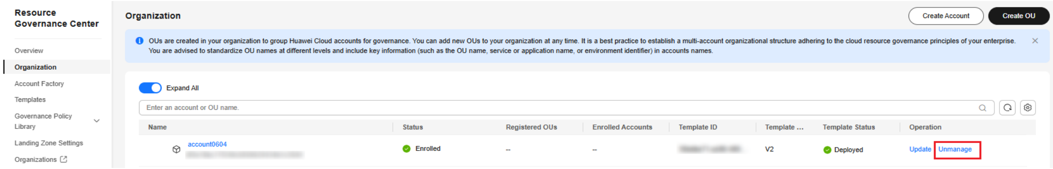
- Accounts to be unmanaged must be in RGC.
- Only those accounts that have been enrolled, failed to be enrolled, or failed to be unmanaged can be unmanaged.
- No operations are allowed for the OU of the account to be unmanaged.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Organization** page, locate the account you want to unmanage, and click **Unmanage** in the **Operation** column.

Figure 4-20 Unmanaging an account



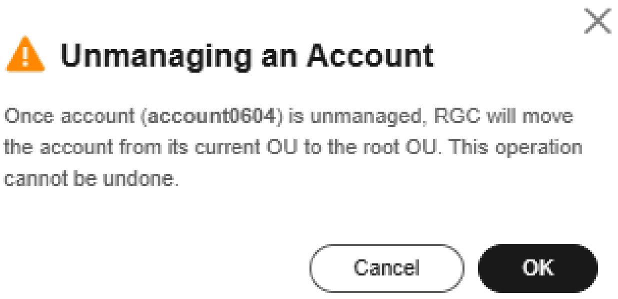
Organization

OUs are created in your organization to group Huawei Cloud accounts for governance. You can add new OUs to your organization at any time. It is a best practice to establish a multi-account organizational structure adhering to the cloud resource governance principles of your enterprise. You are advised to standardize OU names at different levels and include key information (such as the OU name, service or application name, or environment identifier) in accounts names.

Name	Status	Registered OUs	Enrolled Accounts	Template ID	Template ...	Template Status	Operation
account0604 [redacted]	Enrolled	--	--	[redacted]	V2	Deployed	Update Unmanage

Step 3 Review and confirm the details of the account to be unmanaged, and click **OK**.

Figure 4-21 Confirming account details



Unmanaging an Account

Once account (account0604) is unmanaged, RGC will move the account from its current OU to the root OU. This operation cannot be undone.

Step 4 View the account under the root OU. It status changes to **Unmanaged**.

----End

4.6 Using Account Factory to Create Accounts

The management account can create a template with baseline configurations for member accounts. In the account factory, you can use the management account to create member accounts under a specified OU, and baseline configurations will be automatically applied to your accounts based on best practices. The management account can use templates in RGC but cannot create templates on the RGC console. You can create templates on the RFS console if needed.

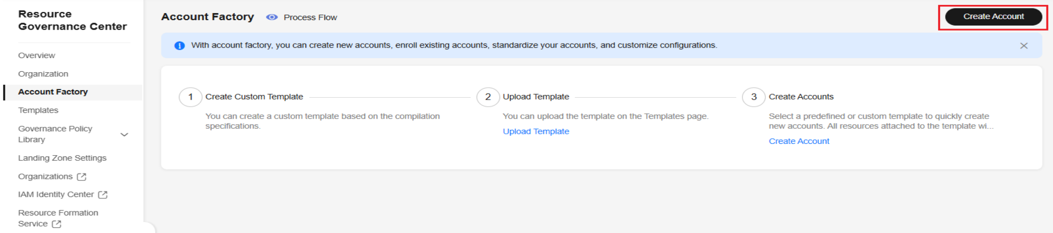
You can select a preconfigured or custom template to quickly create new accounts. All resource configurations defined in the template can be automatically applied to the new accounts.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Access the **Account Factory** page, and click **Create Account** in the upper right corner.

Figure 4-22 Creating an account



Resource Governance Center

Overview
Organization
Account Factory
Templates
Governance Policy Library
Landing Zone Settings
Organizations
IAM Identity Center
Resource Formation Service

Account Factory · Process Flow · Create Account

With account factory, you can create new accounts, enroll existing accounts, standardize your accounts, and customize configurations.

1 Create Custom Template
You can create a custom template based on the compilation specifications.

2 Upload Template
You can upload the template on the Templates page.
Upload Template

3 Create Accounts
Select a predefined or custom template to quickly create new accounts. All resources attached to the template wi...
Create Account

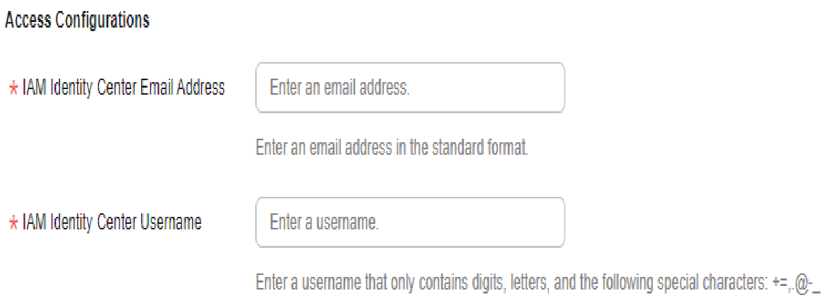
Step 3 Configure account details, including the email address account name. Ensure that they are not currently used for any existing accounts.

The email address cannot be used for password retrieval or other purposes.

Step 4 Configure IAM Identity Center details, including the email address and username.

After an account is created, an IAM Identity Center user is automatically created in RGC. You can use an IAM Identity Center username and password to log in to the management console through the user portal URL, and use the email address to retrieve the password. For details, see **Logging In as an IAM Identity Center User and Accessing Resources**.

Figure 4-23 Configuring IAM Identity Center details



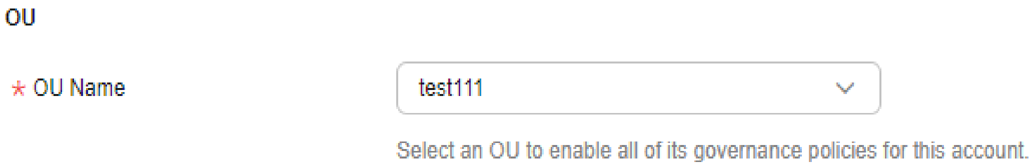
Access Configurations

* IAM Identity Center Email Address: Enter an email address.
Enter an email address in the standard format.

* IAM Identity Center Username: Enter a username.
Enter a username that only contains digits, letters, and the following special characters: +=,.@-_

Step 5 Select a registered OU where your account will be added, and enable all governance policies configured for the OU for the account.

Figure 4-24 Selecting a registered OU



OU

* OU Name: test111

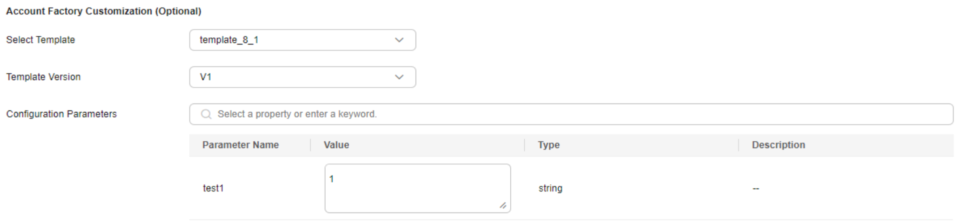
Select an OU to enable all of its governance policies for this account.

Step 6 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

For more information about RFS templates, see **Templates**.

- **Select Template**: Select a template you created in RFS.
- **Template Version**: Select the version for the template.
- **Configuration Parameters**: Modify parameter settings in the template based on service requirements.

Figure 4-25 Configuring a template



Account Factory Customization (Optional)

Select Template: template_8_1

Template Version: V1

Configuration Parameters: Select a property or enter a keyword.

Parameter Name	Value	Type	Description
test1	1	string	--

Step 7 Click **Create Account**. The created account will be displayed in the account list.

----End

5 Governance Policy Management

5.1 Overview of Governance Policies

Governance policies provide ongoing governance for your landing zone environment. They enable you to quickly detect risks in the landing zone from the management account. In this way, you can eliminate the risks and maintain the landing zone in a timely manner to ensure compliance across the landing zone.

Behavior

- Preventive: Preventive governance policies explicitly deny certain actions from being taken. They are implemented by SCPs. When a preventative governance policy is applied to a specified OU, all member accounts directly nested under this OU will inherit this policy.
- Detective: Detective governance policies identify non-compliant resource configurations and inform you of such resources. They are implemented by Config rules. You can view those non-compliant resources on the RGC console. When a detective governance policy is applied to a specified OU, all member accounts directly nested under this OU will inherit this policy.
- Proactive: Proactive governance policies check the resource configurations described in the IaC template before they are deployed. These policies are implemented by using ResourceFormation hooks. If any non-compliant configurations are found, the next operation using the template will be blocked.

Guidance

- Mandatory: Governance policies are always enforced in the core OU and core accounts after you enable RGC and set up a landing zone. These policies cannot be disabled.
- Strongly recommended: Governance policies are designed to enforce Huawei Cloud best practices for your multi-account environment. After setting up a landing zone, you are strongly recommended to enable these policies.
- Elective: Governance policies are designed for cloud governance. You can enable these policies as needed.

Scenarios

- Establish logging and monitoring
- Enforce the least privilege
- Limit network access
- Encrypt data at rest
- Protect data integrity
- Protect configurations
- Optimize costs
- Encrypt data in transit
- Improve availability
- Manage vulnerabilities
- Use strong authentication
- Improving resiliency
- Manage secrets
- Prepare for disaster recovery
- Prepare for incident response
- Balance loads

5.2 Governance Policy Guidance

5.2.1 Mandatory Governance Policies

Mandatory governance policies are owned by RGC. These policies are applied by default to every OU on your landing zone, and they cannot be disabled.

RGC-GR_AUDIT_BUCKET_DELETION_PROHIBITED

Name: The deletion of logging buckets is prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents deletion of OBS buckets created in the log archive account.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_DELETION_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:DeleteBucket"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED

Name: Any changes to encryption for logging buckets are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents changes to encryption for OBS buckets created in RGC.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutEncryptionConfiguration"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED

Name: Any lifecycle configuration changes to logging buckets are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents lifecycle configuration changes for the OBS buckets created in RGC.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutLifecycleConfiguration"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED

Name: Any changes to logging configurations for logging buckets are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents configuration changes for OBS buckets created in RGC.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutBucketLogging"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED

Name: Any changes to bucket policies for logging buckets are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents policy changes for OBS buckets created in RGC.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutBucketPolicy",
            "obs:bucket:DeleteBucketPolicy"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_CES_CHANGE_PROHIBITED

Name: Any changes to Cloud Eye configured in RGC are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents configuration changes to Cloud Eye that RGC has configured for monitoring the environment.

```
{
    "Version": "5.0",
    "Statement": [{
            "Sid": "CES_CHANGE_PROHIBITED",
            "Effect": "Deny",
            "Action": [
                "ces:alarms:put*",
                "ces:alarms:delete*",
                "ces:alarms:addResources"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotMatch": {
                    "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
                },
                "StringMatch": {
                    "g:ResourceTag/rgcservice-managed": "RGC-ConfigComplianceChangeEventRule"
                }
            }
        },
        {
            "Sid": "CES_TAG_CHANGE_PROHIBITED",
            "Effect": "Deny",
            "Action": [
                "ces:tags:create"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotMatch": {
                    "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
                },
                "ForAnyValue:StringMatch": {
                    "g:TagKeys": "rgcservice-managed"
                }
            }
        }
    ]
}
```

RGC-GR_CONFIG_CHANGE_PROHIBITED

Name: Any changes to the Config recorder are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents configuration changes to Config.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "CONFIG_CHANGE_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "rms:trackerConfig:delete",
            "rms:trackerConfig:put"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_FUNCTIONGRAPH_CHANGE_PROHIBITED

Name: Any changes to FunctionGraph functions configured in RGC are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents changes to FunctionGraph set by RGC.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "FUNCTIONGRAPH_CHANGE_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "functiongraph:function:createFunction",
            "functiongraph:function:deleteFunction",
            "functiongraph:function:updateFunctionCode",
            "functiongraph:function:updateMaxInstanceConfig",
            "functiongraph:function:createVersion",
            "functiongraph:function:createEvent",
            "functiongraph:function:deleteEvent",
            "functiongraph:function:updateEvent",
            "functiongraph:function:updateReservedInstanceCount",
            "functiongraph:function:updateFunctionConfig"
        ],
        "Resource": [
            "functiongraph:*:*:function:rgcservice-managed/RGC-NotificationForwarder"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_SMN_CHANGE_PROHIBITED

Name: Any changes to SMN notifications configured in RGC are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents changes to simple message notification (SMN) configured in RGC.

```
{
    "Version": "5.0",
    "Statement": [{
            "Sid": "SMN_CHANGE_PROHIBITED",
            "Effect": "Deny",
            "Action": [
                "smn:topic:update*",
                "smn:topic:delete*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotMatch": {
                    "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
                },
                "ForAnyValue:StringMatch": {
                    "g:ResourceTag/rgcservice-managed": [
                        "RGC-SecurityNotifications",
                        "RGC-AllConfigNotifications",
                        "RGC-AggregateSecurityNotifications"
                    ]
                }
            }
        },
        {
            "Sid": "SMN_TAG_CHANGE_PROHIBITED",
            "Effect": "Deny",
            "Action": [
                "smn:tag:create",
                "smn:tag:delete"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotMatch": {
                    "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
                },
                "ForAnyValue:StringMatch": {
                    "g:TagKeys": "rgcservice-managed"
                }
            }
        }
    ]
}
```

RGC-GR_SMN_SUBSCRIPTION_CHANGE_PROHIBITED

Name: Any changes to SMN subscriptions in RGC are prohibited.

Implementation: SCPs

Behavior: preventive

Function: This policy prevents changes to SMN subscriptions configured in RGC. These subscriptions will trigger notifications for Config rules compliance changes.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "SMN_SUBSCRIPTION_CHANGE_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "smn:topic:subscribe",
            "smn:topic:deleteSubscription"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            },
            "ForAnyValue:StringMatch": {
                "g:ResourceTag/rgcservice-managed": [
                    "RGC-SecurityNotifications",
                    "RGC-AllConfigNotifications",
                    "RGC-AggregateSecurityNotifications"
                ]
            }
        }
    }]
}
```

RGC-GR_CONFIG_CTS_TRACKER_EXISTS

Name: This policy is non-compliant if there are no CTS trackers in an account.

Implementation: Config rules

Behavior: detective

Function: This policy checks whether a CTS tracker is created in an account.

```
terraform {
    required_providers {
        huaweicloud = {
            source = "huaweie.com/provider/huaweicloud"

            version = ">=1.51.0"
        }
    }
}
provider "huaweicloud" {
    endpoints = {}
    insecure = true
}
variable "ConfigName" {
    description = "config name"
    type = string
    default = "cts-tracker-exists"
}
variable "PolicyAssignmentName" {
    description = "policy assignment name"
    type = string
    default = "rgc_cts_tracker_exists"
}
variable "ConfigRuleDescription" {
    description = "config rule description"
    type = string
    default = "This policy is non-compliant if there are no CTS trackers in an account."
}#
To be updated
variable "RegionName" {
    description = "policy region"
    type = string
}
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
    name =
        var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"rms_policy_assignment_check" {
    name =
        var.PolicyAssignmentName
    description =
        var.ConfigRuleDescription
    policy_definition_id =
        try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
    period = "TwentyFour_Hours"
    status = "Enabled"
}
```

RGC-GR_CONFIG_OBS_BUCKET_PUBLIC_READ_POLICY_CHECK

Name: This policy is non-compliant if an OBS bucket allows public read.

Implementation: Config rules

Behavior: detective

Function: This policy checks whether an OBS bucket allows public read.

```
terraform {
    required_providers {
        huaweicloud = {
            source = "huawei.com/provider/huaweicloud"

            version = ">=1.51.0"
        }
    }
}
provider "huaweicloud" {
    endpoints = {}
    insecure = true
}
variable "ConfigName" {
    description = "config name"
    type = string
    default = "obs-bucket-public-read-policy-check"
}
variable "PolicyAssignmentName" {
    description = "policy assignment name"
    type = string
    default = "rgc_obs_bucket_public_read_policy_check"
}
variable "ConfigRuleDescription" {
    description = "config rule description"
    type = string
    default = "This policy is non-compliant if an OBS bucket allows public read."
}
variable "ResourceProvider" {
    description = "resource provider"
    type = string
    default = "obs"
}
variable "ResourceType" {
    description = "resource type"
    type = string
    default = "buckets"
}
variable "RegionName" {
    description = "policy region"
    type = string
}
variable "IsGlobalResource" {
    description = "is global resource"
    type = bool
    default = false
}
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
    name =
        var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
```

```
"rms_policy_assignment_check" {
    name =
        var.IsGlobalResource ? format("%s",
            var.PolicyAssignmentName) : format("%s_%s",
            var.PolicyAssignmentName,
            var.RegionName)
    description =
        var.ConfigRuleDescription
    policy_definition_id =
        try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
    status = "Enabled"

    policy_filter {
        region =
            var.RegionName
        resource_provider =
            var.ResourceProvider
        resource_type =
            var.ResourceType
    }
}
```

RGC-GR_CONFIG_OBS_BUCKET_PUBLIC_WRITE_POLICY_CHECK

Name: This policy is non-compliant if an OBS bucket allows public write.

Implementation: Config rules

Behavior: detective

Function: This function checks whether an OBS bucket allows public write.

```
terraform {
    required_providers {
        huaweicloud = {
            source = "huawei.com/provider/huaweicloud"

            version = ">=1.51.0"
        }
    }
}
provider "huaweicloud" {
    endpoints = {}
    insecure = true
}
variable "ConfigName" {
    description = "config name"
    type = string
    default = "obs-bucket-public-write-policy-check"
}
variable "PolicyAssignmentName" {
    description = "policy assignment name"
    type = string
    default = "rgc_obs_bucket_public_write_policy_check"
}
variable "ConfigRuleDescription" {
    description = "config rule description"
    type = string
        default = "This policy is non-compliant if an OBS bucket allows public write."
}
variable "ResourceProvider" {
    description = "resource provider"
    type = string
    default = "obs"
}
variable "ResourceType" {
    description = "resource type"
    type = string
    default = "buckets"
}
variable "RegionName" {
    description = "policy region"
    type = string
}
variable "IsGlobalResource" {
    description = "is global resource"
    type = bool
    default = false
}
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
    name =
        var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"rms_policy_assignment_check" {
    name =
        var.IsGlobalResource ? format("%s",
            var.PolicyAssignmentName) : format("%s_%s",
            var.PolicyAssignmentName,
            var.RegionName)
    description =
        var.ConfigRuleDescription
    policy_definition_id =
        try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
    status = "Enabled"

    policy_filter {
        region =
            var.RegionName
        resource_provider =
            var.ResourceProvider
        resource_type =
            var.ResourceType
    }
}
```

5.2.2 Strongly Recommended Governance Policies

API Gateway (APIG)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_APIG_INSTANCES_AUTHORIZATION_TYPE_CONFIGURED	Checks whether security authentication is provided for a dedicated API gateway. This policy is non-compliant if security authentication is not provided.	Encrypting data in transit	Medium	apig:::instance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_APIG_INSTANCES_SSL_ENABLED	Checks whether any domain name of a dedicated API gateway is associated with an SSL certificate. This policy is non-compliant if any domain name is not associated with an SSL certificate.	Encrypting data in transit	Medium	apig:::instance

AS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_AS_GROUP_IN_VPC	Checks whether an AS group is in the specified VPC. This policy is non-compliant if an AS group is not in the specified VPC.	Controlling network access	High	as:::group

BMS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_BMS_KEY_PAIR_SECURITY_LOGIN	Checks whether a key pair is used for BMS login. This policy is non-compliant if a key pair is not used.	Using strong authentication	High	bms:::instance

CBR

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CBR_BACKUP_ENCRYPTED_CHECK	Checks whether CBR backup is encrypted. This policy is non-compliant if the backup is not encrypted.	Encrypting data at rest	High	cbr:::checkpoint

Cloud Container Engine (CCE)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CCE_ENDPOINT_PUBLIC_ACCESS	Checks whether a public IP address is bound to a CCE cluster. This policy is non-compliant if a public IP address is bound.	Controlling network access	Medium	cce:::cluster
RGC-GR_CONFIG_CCE_CLUSTER_IN_VPC	Checks whether a CCE cluster is in the specified VPC. This policy is non-compliant if a CCE cluster is not in the specified VPC.	Controlling network access	High	cce:::cluster

CCM

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_PCA_CERTIFICATE_AUTHORITY_EXPIRATION_CHECK	Checks whether a private CA expires within a specified period. This policy is non-compliant if it expires within a specified period.	Encrypting data in transit	Medium	ccm:::private Certificate
RGC-GR_CONFIG_PCA_CERTIFICATE_EXPIRATION_CHECK	Checks whether a private certificate expires within a specified period. This policy is non-compliant if it expires within a specified period.	Encrypting data in transit	Medium	ccm:::private Certificate

Content Delivery Network (CDN)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CDN_ENABLE_HTTPS_CERTIFICATE	Checks whether an HTTPS certificate is configured for CDN. This policy is non-compliant if an HTTPS certificate is not configured.	Encrypting data in transit	Critical	cdn:::domain
RGC-GR_CONFIG_CDN_ORIGIN_PROTOCOL_NO_HTTP	Checks whether CDN uses HTTPS for origin pull. This policy is non-compliant if HTTPS is not used.	Encrypting data in transit	Critical	cdn:::domain

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CDN_SECURITY_POLICY_CHECK	Checks whether a Transport Layer Security (TLS) version earlier than v1.2 is used for CDN. This policy is non-compliant if a TLS version earlier than v1.2 is used.	Encrypting data in transit	High	cdn:::domain
RGC-GR_CONFIG_CDN_USE_MY_CERTIFICATE	Checks whether CDN uses your own certificates. This policy is non-compliant if CDN uses your own certificates.	Encrypting data in transit	High	cdn:::domain

CFW

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CFW_POLICY_NOT_EMPTY	Checks whether a CFW instance has protection policies configured. This policy is non-compliant if no protection policies are configured.	Controlling network access	Medium	cfw:::eipProtection

CodeArts Build

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CLOUDBUILDSERVER_ENCRYPTION_PARAMETER_CHECK	Checks whether encryption is enabled for custom parameters (except for predefined parameters) of a CodeArts project. This policy is non-compliant if encryption is not enabled.	Encrypting data at rest	Medium	codearts:::deployApplication

Cloud Search Service (CSS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSS_CLUSTER_AUTHORITY_ENABLE	Checks whether authentication is enabled for a CSS cluster. This policy is non-compliant if authentication is not enabled.	Using strong authentication	Critical	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_DISK_ENCRYPTION_CHECK	Checks whether disk encryption is enabled for a CSS cluster. This policy is non-compliant if disk encryption is not enabled.	Encrypting data at rest	High	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_KIBANA_NOT_ENABLE_WHITE_LIST	Checks whether all IP addresses are whitelisted for Kibana to access a CSS cluster. This policy is non-compliant if all IP addresses are whitelisted.	Controlling network access	Critical	css:::cluster

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSS_CLUSTER_NO_PUBLIC_ZONE	Checks whether public network access is enabled for a CSS cluster. This policy is non-compliant if public network access is enabled.	Encrypting data at rest	High	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_NOT_ENABLE_WHITE_LIST	Checks whether all IP addresses are whitelisted for a CSS cluster. This policy is non-compliant if all addresses are whitelisted.	Controlling network access	Critical	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_SECURITY_MODE_ENABLE	Checks whether security mode is enabled for a CSS cluster. This policy is non-compliant if security mode is not enabled.	Enforcing the least privilege	High	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_HTTPS_REQUIRED	Checks whether HTTPS access is enabled for a CSS cluster. This policy is non-compliant if HTTPS access is not enabled.	Encrypting data in transit	Medium	css:::cluster

Cloud Trace Service (CTS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CTS_KMS_ENCRYPTED_CHECK	Checks whether a CTS tracker is encrypted using KMS. This policy is non-compliant if the tracker is not encrypted.	Encrypting data at rest	Medium	cts:::tracker
RGC-GR_CONFIG_CTS_SUPPORT_VALIDATE_CHECK	Checks whether trace file verification is enabled for a CTS tracker. This policy is non-compliant if the verification is not enabled.	Protecting data integrity	Medium	cts:::tracker

Distributed Cache Service (DCS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DCS_MEMCACHED_ENABLE_SSL	Checks whether a DCS Memcached instance supports public access but not SSL. This policy is non-compliant if the instance supports public access but not SSL.	Encrypting data in transit	High	dcs:::instance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DCS_MEMCACHED_NO_PUBLIC_IP	Checks whether a public IP address is bound to a DCS Memcached instance. This policy is non-compliant if a public IP address is bound.	Controlling network access	High	dcs:::instance
RGC-GR_CONFIG_DCS_MEMCACHED_PASSWORD_ACCESS	Checks whether a DCS Memcached instance can be accessed without a password. This policy is non-compliant if the instance can be accessed without a password.	Using strong authentication	Medium	dcs:::instance
RGC-GR_CONFIG_DCS_REDIS_ENABLE_SSL	Checks whether a DCS Redis instance supports public access but not SSL. This policy is non-compliant if the instance supports public access but not SSL.	Controlling network access	High	dcs:::instance
RGC-GR_CONFIG_DCS_REDIS_HIGH_TOLERANCE	Checks whether a DCS Redis instance is highly available. This policy is non-compliant if the instance is not highly available.	Improving availability	Low	dcs:::instance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DCS_REDIS_NO_PUBLIC_IP	Checks whether a public IP address is bound to a DCS Redis instance. This policy is non-compliant if a public IP address is bound.	Controlling network access	High	dcs:::instance
RGC-GR_CONFIG_DCS_REDIS_PASSWORD_ACCESS	Checks whether a DCS Redis instance can be accessed without a password. This policy is non-compliant if the instance can be accessed without a password.	Using strong authentication	Medium	dcs:::instance
RGC-GR_CONFIG_DCS_MEMCACHED_IN_VPC	Checks whether a DCS Memcached instance is in the specified VPC. This policy is non-compliant if the instance is not in the specified VPC.	Controlling network access	Medium	dcs:::instance
RGC-GR_CONFIG_DCS_REDIS_IN_VPC	Checks whether a DCS Redis instance is in the specified VPC. This policy is non-compliant if the instance is not in the specified VPC.	Controlling network access	Medium	dcs:::instance

Document Database Service (DDS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DDS_INSTANCE_ENABLE_SSL	Checks whether SSL is enabled for a DDS instance. This policy is non-compliant if SSL is not enabled.	Encrypting data in transit	High	dds:::instance
RGC-GR_CONFIG_DDS_INSTANCE_HAS_EIP	Checks whether a public IP address is bound to a DDS instance. This policy is non-compliant if a public IP address is bound.	Controlling network access	High	dds:::instance
RGC-GR_CONFIG_DDS_INSTANCE_PORT_CHECK	Checks whether a DDS instance has unallowed ports enabled. This policy is non-compliant if the instance has unallowed ports enabled.	Controlling network access	High	dds:::instance

DEW

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSMS_SECRETS_ROTATION_SUCCESS_CHECK	Checks whether a CSMS secret rotation is successful. This policy is non-compliant if the rotation fails.	Enforcing the least privilege	High	csms:::secret

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_KMS_NOT_SCHEDULED_FOR_DELETION	Checks whether a KMS key is scheduled to be deleted. This policy is non-compliant if the key is scheduled to be deleted.	Protecting data integrity	Critical	kms:::key
RGC-GR_CONFIG_KMS_ROTATION_ENABLED	Checks whether key rotation is enabled for a KMS key. This policy is non-compliant if rotation is not enabled.	Encrypting data at rest	Medium	kms:::key

Distributed Message Service (DMS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DMS_KAFKA_NOT_ENABLE_PRIVATE_SSL	Checks whether SSL encryption is enabled for accessing a DMS Kafka instance over a private network. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data in transit	Medium	dms:::kafkaInstance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DMS_KAFKA_NOT_ENABLE_PUBLIC_SSL	Checks whether SSL encryption is enabled for accessing a DMS Kafka instance over a public network. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data in transit	Medium	dms:::kafkaInstance
RGC-GR_CONFIG_DMS_KAFKA_PUBLIC_ACCESS_ENABLED_CHECK	Checks whether a DMS Kafka instance can be accessed over a public network. This policy is non-compliant if the instance can be accessed over a public network.	Controlling network access	High	dms:::kafkaIZnstance
RGC-GR_CONFIG_DMS_RABBITMQ_NOT_ENABLE_SSL	Checks whether SSL encryption is enabled for a DMS RabbitMQ instance. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data at rest	High	dms:::rabbitmqInstance
RGC-GR_CONFIG_DMS_ROCKETMQ_NOT_ENABLE_SSL	Checks whether SSL encryption is enabled for a DMS Reliability instance. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data at rest	High	dms:::rocketmqInstance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DMS_RABBITMQ_PUBLIC_ACCESS_ENABLED_CHECK	Checks whether a DMS RabbitMQ instance can be accessed over a public network. This policy is non-compliant if the instance can be accessed over a public network.	Controlling network access	Medium	dms:::rabbitmqInstance
RGC-GR_CONFIG_DMS_RELIABILITY_PUBLIC_ACCESS_ENABLED_CHECK	Checks whether a DMS RocketMQ instance can be accessed over a public network. This policy is non-compliant if the instance can be accessed over a public network.	Controlling network access	Medium	dms:::rocketmqInstance

Data Replication Service (DRS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DRS_DATA_GUARD_JOB_NOT_PUBLIC	Checks whether DRS supports real-time disaster recovery through a public network. This policy is non-compliant if real-time disaster recovery through a public network is supported.	Controlling network access	High	drs:::job

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DRS_MIGRATION_JOB_NOT_PUBLIC	Checks whether DRS supports real-time migration through a public network. This policy is non-compliant if real-time migration through a public network is supported.	Controlling network access	High	drs:::job
RGC-GR_CONFIG_DRS_SYNCHRONIZATION_JOB_NOT_PUBLIC	Checks whether DRS supports real-time synchronization through a public network. This policy is non-compliant if real-time synchronization through a public network is supported.	Controlling network access	High	drs:::job

Data Warehouse Service (DWS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DWS_ENABLE_KMS	Checks whether KMS encryption is enabled for a DWS cluster. This policy is non-compliant if KMS encryption is not enabled.	Encrypting data at rest	Medium	dws:::cluster

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DWS_ENABLE_SSL	Checks whether SSL connection is enabled for a DWS cluster. This policy is non-compliant if SSL connection is not enabled.	Encrypting data in transit	Medium	dws:::cluster
RGC-GR_CONFIG_DWS_CLUSTERS_NO_PUBLIC_IP	Checks whether a DWS cluster has a public IP address bound. This policy is non-compliant if the cluster has a public IP address bound.	Controlling network access	High	dws:::cluster
RGC-GR_CONFIG_DWS_CLUSTERS_IN_VPC	Checks whether a DWS cluster is in the specified VPC. This policy is non-compliant if the cluster is not in the specified VPC.	Controlling network access	High	dws:::cluster

Elastic Cloud Server (ECS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_INSTANCE_KEY_PAIR_LOGIN	Checks whether an ECS has a key pair configured. This policy is non-compliant if no key pair is configured.	Controlling network access	High	ecs:::instanceV1

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_INSTANCE_NO_PUBLIC_IP	Checks whether a public IP address is bound to an ECS. This policy is non-compliant if a public IP address is bound.	Controlling network access	Medium	compute:::instance
RGC-GR_CONFIG_ECS_MULTIPLE_PUBLIC_IP_CHECK	Checks whether multiple public IP addresses are bound to an ECS. This policy is non-compliant if multiple public IP addresses are bound.	Controlling network access	Low	compute:::instance
RGC-GR_CONFIG_ECS_INSTANCE_AGENCY_ATTACH_IAM_AGENCY	Checks whether an ECS has any IAM agencies. This policy is non-compliant if an ECS has no IAM agencies.	Enforcing the least privilege	Low	ecs:::instanceV1
RGC-GR_CONFIG_ECS_IN_ALLOWED_SECURITY_GROUPS	Checks whether an ECS not attached with specified tags is associated with the specified high-risk security groups. This policy is non-compliant if these ECSs are associated with the specified high-risk security groups.	Controlling network access	High	ecs:::instanceV1

ECS and VPC

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_INSTANCE_IN_VPC	Checks whether an ECS is in the specified VPC. This policy is non-compliant if the ECS is not in the specified VPC.	Controlling network access	Medium	ecs:::instanceV1

Elastic Load Balance (ELB)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ELB_LOADBALANCERS_NO_PUBLIC_IP	Checks whether a public IP address is bound to a load balancer. This policy is non-compliant if a public IP address is bound.	Controlling network access	Medium	elb:::loadBalancer
RGC-GR_CONFIG_ELB_TLS_HTTPS_LISTENERS_ONLY	Checks whether HTTPS is configured for any listener of a load balancer. This policy is non-compliant if HTTPS is not configured for any listener.	Encrypting data in transit	Medium	elb:::listener

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ELB_PREDEFINED_SECURITY_POLICY_HTTPS_CHECK	Checks whether a predefined security policy is configured for the HTTPS listener of a dedicated load balancer. This policy is non-compliant if the predefined security policy is not configured.	Controlling network access	Medium	elb:::loadBalancer
RGC-GR_CONFIG_ELB_HTTP_TO_HTTPS_REDIRECTION_CHECK	Checks whether requests to an HTTP listener can be redirected to an HTTPS listener. This policy is non-compliant if requests cannot be redirected.	Controlling network access	Medium	elb:::listener

EVS and ECS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VOLUMES_ENCRYPTED_CHECK	Checks whether an EVS disk attached to a cloud server is encrypted. This policy is non-compliant if the disk is not encrypted.	Encrypting data at rest	Low	evs:::volume

FunctionGraph

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_FUNCTION_GRAPH_PUBLIC_ACCESS_PROHIBITED	Checks whether functions in FunctionGraph allow public access. This policy is non-compliant if the functions allow public access.	Controlling network access	Critical	fgs:::function

GaussDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_INSTANCE_IN_VPC	Checks whether a GaussDB instance is in the specified VPC. This policy is non-compliant if the instance is not in the specified VPC.	Controlling network access	Medium	gaussdb:::opengaussInstance
RGC-GR_CONFIG_GAUSSDB_INSTANCE_NO_PUBLIC_IP_CHECK	Checks whether a GaussDB instance has any EIPs associated. This policy is non-compliant if the instance has any EIPs associated.	Controlling network access	High	gaussdb:::opengaussInstance
RGC-GR_CONFIG_GAUSSDB_INSTANCE_SSL_ENABLE	Checks whether SSL encryption is enabled for a GaussDB instance. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data in transit	High	gaussdb:::opengaussInstance

GeminiDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_DISK_ENCRYPTION	Checks whether disk encryption is enabled for a GeminiDB instance. This policy is non-compliant if disk encryption is not enabled.	Encrypting data at rest	Medium	gaussdb:::mongoInstance

Identity and Access Management (IAM)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_ROOT_ACCESS_KEY_CHECK	Checks whether there are available access keys for an account. This policy is non-compliant if there are available access keys.	Enforcing the least privilege	Critical	identity:::accessKey
RGC-GR_CONFIG_ROOT_ACCOUNT_MFA_ENABLED	Checks whether multi-factor authentication (MFA) is enabled for an account. This policy is non-compliant if MFA is not enabled.	Enforcing the least privilege	High	identity:::acl
RGC-GR_CONFIG_IAM_GROUP_HAS_USERS_CHECK	Checks whether IAM users are added to an IAM user group. This policy is non-compliant if the users are not added to a user group.	Enforcing the least privilege	Medium	identity:::group

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_USER_ACCESS_MODE	Checks whether an IAM user can gain access to both the console and APIs. This policy is non-compliant if the user can gain access to both the console and APIs.	Enforcing the least privilege	Medium	identity:::user
RGC-GR_CONFIG_IAM_USER_CONSOLE_AND_API_ACCESS_AT_CREATION	Checks whether access keys are set for an IAM user accessing from the console. This policy is non-compliant if access keys are set.	Managing confidentiality	Medium	identity:::user
RGC-GR_CONFIG_IAM_USER_SINGLE_ACCESS_KEY	Checks whether an IAM user has multiple access keys in the active state. This policy is non-compliant if the user has multiple access keys in the active state.	Managing confidentiality	High	identity:::user
RGC-GR_CONFIG_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Checks whether MFA is enabled for an IAM user accessing from the console. This policy is non-compliant if MFA is not enabled.	Enforcing the least privilege	Medium	identity:::user

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Checks whether an IAM policy grants the admin permission (*:*:*, *:*, or *). This policy is non-compliant if the IAM policy grants the admin permission.	Enforcing the least privilege	High	identity:::protectionPolicy
RGC-GR_CONFIG_IAM_ROLE_HAS_ALL_PERMISSIONS	Checks whether an IAM custom policy grants the allow permission (*:*). This policy is non-compliant if the IAM policy grants the allow permission.	Enforcing the least privilege	Low	identity:::role
RGC-GR_CONFIG_IAM_USER_MFA_ENABLED	Checks whether MFA is enabled for an IAM user. This policy is non-compliant if MFA is not enabled.	Enforcing the least privilege	Medium	identity:::user
RGC-GR_CONFIG_ACCESS_KEYS_ROTATED	Checks whether an IAM user's access key is rotated within the specified number of days. This policy is non-compliant if the key is not rotated within the specified number of days.	Enforcing the least privilege	High	identity:::accessKey

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_PASSWORD_POLICY	Checks whether the password of an IAM user meets the password strength requirements. This policy is non-compliant if the password does not meet the requirements.	Using strong authentication	High	identity:::user
RGC-GR_CONFIG_IAM_USER_LAST_LOGIN_CHECK	Checks whether an IAM user logs in to the system within a specified period. This policy is non-compliant if the user does not log in to the system within the specified period.	Enforcing the least privilege	Low	identity:::user
RGC-GR_CONFIG_IAM_POLICY_IN_USE	Checks whether an IAM policy has been attached to any IAM users, user groups, or agencies. This policy is non-compliant if the IAM policy has not been attached.	Enforcing the least privilege	Low	identity:::protectionPolicy

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_ROLE_IN_USE	Checks whether an IAM permission has been granted to any IAM users, user groups, or agencies. This policy is non-compliant if the permission has not been granted.	Enforcing the least privilege	Low	identity:::role
RGC-GR_CONFIG_IAM_USER_LOGIN_PROTECTION_ENABLED	Checks whether login protection is enabled for an IAM user. This policy is non-compliant if protection is not enabled.	Using strong authentication	Medium	identity:::user
RGC-GR_CONFIG_IAM_USER_GROUP_MEMBERSHIP_CHECK	Checks whether an IAM user is in a specified IAM user group. This policy is non-compliant if the user is not in a specified user group.	Enforcing the least privilege	Medium	identity:::user
RGC-GR_CONFIG_IAM_AGENCIES_MANAGED_POLICY_CHECK	Checks whether an IAM agency has specified IAM policies and permissions. This policy is non-compliant if the agency has no specified IAM policies and permissions.	Enforcing the least privilege	High	identity:::agency

IMS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IMS_IMAGES_ENABLE_ENCRYPTION	Checks whether encryption is enabled for a private image. This policy is non-compliant if encryption is not enabled.	Encrypting data at rest	High	images:::image

MapReduce Service (MRS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MRS_CLUSTER_KERBEROS_ENABLED	Checks whether Kerberos authentication is enabled for an MRS cluster. This policy is non-compliant if authentication is not enabled.	Using strong authentication	Medium	mrs:::cluster
RGC-GR_CONFIG_MRS_CLUSTER_NO_PUBLIC_IP	Checks whether a public IP address is bound to an MRS cluster. This policy is non-compliant if a public IP address is bound.	Controlling network access	Medium	mrs:::cluster
RGC-GR_CONFIG_MRS_CLUSTER_IN_ALLOWED_SECURITY_GROUPS	Checks whether an MRS cluster is in a specified security group. This policy is non-compliant if the cluster is not in the specified security group.	Controlling network access	Medium	mrs:::cluster

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MRS_CLUSTER_IN_VPC	Checks whether an MRS cluster is in the specified VPC. This policy is non-compliant if the cluster is not in the specified VPC.	Controlling network access	Medium	mrs:::cluster

NAT

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_PRIVATE_NAT_GATEWAY_AUTHORIZED_VPC_ONLY	Checks whether a private NAT gateway is in a specified VPC. This policy is non-compliant if the NAT gateway is not in the specified VPC.	Controlling network access	High	nat:::privateGateway

Object Storage Service (OBS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_OBS_BUCKET_POLICY_GRANTEE_CHECK	Checks whether an OBS bucket policy allows a prohibited access action. This policy is non-compliant if the bucket policy allows a prohibited access action.	Enforcing the least privilege	High	obs:::bucket

Relational Database Service (RDS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_RDS_INSTANCE_NO_PUBLIC_IP	Checks whether a public IP address is bound to an RDS instance. This policy is non-compliant if a public IP address is bound.	Controlling network access	High	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCES_ENABLE_KMS	Checks whether storage encryption is enabled for an RDS instance. This policy is non-compliant if storage encryption is not enabled.	Encrypting data at rest	Low	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_PORT_CHECK	Checks whether an RDS instance has forbidden ports. This policy is non-compliant if the instance has forbidden ports.	Controlling network access	High	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_SSL_ENABLE	Checks whether SSL encryption is enabled for an RDS instance. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data at rest	High	rds:::instance

Scalable File Service Turbo (SFS Turbo)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_SFSTURBO_ENCRYPTED_CHECK	Checks whether SFS Turbo is configured to encrypt files using KMS. This policy is non-compliant if SFS Turbo is not configured to encrypt files using KMS.	Encrypting data at rest	Low	sfsturbo:::dir

TaurusDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_IN_VPC	Checks whether a TaurusDB instance is in a specified VPC. This policy is non-compliant if the instance is not in the specified VPC.	Controlling network access	High	gaussdb:::mysqlInstance
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_NO_PUBLIC_IP_CHECK	Checks whether a TaurusDB instance has an EIP associated. This policy is non-compliant if the instance has an EIP associated.	Controlling network access	High	gaussdb:::mysqlInstance
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_SSL_ENABLE	Checks whether SSL encryption is enabled for a TaurusDB instance. This policy is non-compliant if SSL encryption is not enabled.	Encrypting data in transit	High	gaussdb:::mysqlInstance

Virtual Private Cloud (VPC)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VPC_SG_PORTS_CHECK	Checks whether the inbound source IP address of a security group is set to 0.0.0.0/0 and all TCP/UDP ports are enabled. This policy is non-compliant if the inbound source IP address is set to 0.0.0.0/0 and all TCP/UDP ports are enabled.	Controlling network access	High	networking:::secgroup
RGC-GR_CONFIG_VPC_ACL_UNUSED_CHECK	Checks whether a network ACL is associated with any subnets. This policy is non-compliant if the network ACL is not associated with any subnets.	Protecting configurations	Low	vpc:::networkAcl
RGC-GR_CONFIG_VPC_DEFAULT_SG_CLOSED	Checks whether the default security group of a VPC allows inbound or outbound traffic. This policy is non-compliant if the default security group allows inbound or outbound traffic.	Controlling network access	High	networking:::secgroup

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VPC_SG_RESTRICTED_SSH	Checks whether the inbound source IP address of a security group is set to 0.0.0.0/0 and TCP port 22 is enabled. This policy is non-compliant if the inbound source IP address is set to 0.0.0.0/0 and TCP port 22 is enabled.	Controlling network access	High	networking:::secgroup

Web Application Firewall (WAF)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_WAF_INSTANCE_POLICY_NOT_EMPTY	Checks whether a WAF domain name has protection policies configured. This policy is non-compliant if the domain name has no protection policies configured.	Controlling network access	Medium	waf:::cloudInstance

5.2.3 Elective Governance Policies

*

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_REGULAR_MATCHING_OF_NAMES	Checks whether a resource name matches a regular expression pattern. This policy is non-compliant if the resource name does not match.	Protecting configurations	Low	*

APIG

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_APIG_INSTANCES_EXECUTION_LOGGING_ENABLED	Checks whether a dedicated API gateway is configured with access logs. This policy is non-compliant if the gateway is not configured with access logs.	Establishing logging and monitoring	Medium	apig:::instance

Auto Scaling

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_AS_CAPACITY_REBALANCING	Checks whether the scaling policy of **EQUILIBRIUM_DISTRIBUTE** is applied when an AS group scales in or out. This policy is non-compliant if this scaling policy is not applied.	Improving availability	Medium	as:::group
RGC-GR_CONFIG_AS_GROUP_ELB_HEALTHCHECK_REQUIRED	Checks whether ELB health check is enabled for an AS group associated with load balancers. This policy is non-compliant if health check is not enabled.	Improving availability	Low	as:::group
RGC-GR_CONFIG_AS_MULTIPLE_AZ	Checks whether an auto scaling (AS) group is deployed in multiple AZs. This policy is non-compliant if the group is not deployed in multiple AZs.	Improving availability	Medium	as:::group
RGC-GR_CONFIG_AS_GROUP_IPV6_DISABLED	Checks whether an IPv6 shared bandwidth is assigned to an AS group. This policy is non-compliant if an IPv6 shared bandwidth is assigned.	Optimizing costs	Low	as:::group

CBR

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CBR_POLICY_MINIMUM_FREQUENCY_CHECK	Checks whether the execution frequency of a backup policy is within the specified range. This policy is non-compliant if the frequency is lower than the specified range.	Preparing for disaster recovery	Medium	cbr:::policy
RGC-GR_CONFIG_CBR_VAULT_MINIMUM_RETENTION_CHECK	Checks whether a CBR vault has policies attached or has any policies that can be retained within the required number of days. This policy is non-compliant if the vault has no policies attached or has no such policies.	Preparing for disaster recovery	Medium	cbr:::vault

CBR and ECS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_PROTECTED_BY_CBR	Checks whether an ECS has a backup vault attached. This policy is non-compliant if the ECS has no backup vault attached.	Preparing for disaster recovery	Medium	ecs:::instanceV1

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_LAST_BACKUP_CREATED	Checks whether an ECS has a backup created within the specified time period. This policy is non-compliant if the ECS has a backup created beyond the specified time period.	Preparing for disaster recovery	Low	ecs:::instanceV1

CBR and EVS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_EVS_PROTECTED_BY_CBR	Checks whether an EVS disk has a backup vault attached. This policy is non-compliant if the disk has no backup vaults attached.	Preparing for disaster recovery	Medium	evs:::volume
RGC-GR_CONFIG_EVS_LAST_BACKUP_CREATED	Checks whether an EVS disk has a backup created within the specified time period. This policy is non-compliant if the disk has a backup created beyond the specified time period.	Preparing for disaster recovery	Low	evs:::volume

CBR and SFS Turbo

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_SFSTURBO_PROTECTED_BY_CBR	Checks whether an SFS Turbo system has a backup vault attached. This policy is non-compliant if the system has no backup vaults attached.	Preparing for disaster recovery	Medium	sfs:::turbo

CCE

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CCE_CLUSTER_END_OF_MAINTENANCE_VERSION	Checks whether a CCE cluster version is end of maintenance (EOM). This policy is non-compliant if the version is EOM.	Managing vulnerabilities	Medium	cce:::cluster
RGC-GR_CONFIG_CCE_CLUSTER_OLDEST_SUPPORTED_VERSION	Checks whether a CCE cluster is using the oldest supported version. This policy is non-compliant if the cluster is using the oldest supported version.	Managing vulnerabilities	Medium	cce:::cluster
RGC-GR_CONFIG_ALLOWED_CCE_FLAVORS	Checks whether the flavors of a CCE cluster match any of the specified flavors. This policy is non-compliant if the flavors do not match.	Protecting configurations	Low	cce:::cluster

CCM

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_PCA_CERTIFICATE_AUTHORITY_ROOT_DISABLE	Checks whether private root CAs are disabled. This policy is non-compliant if CAs are not disabled.	Managing confidentiality	Medium	scm:::certificate
RGC-GR_CONFIG_PCA_ALGORITHM_CHECK	Checks whether CCM uses a prohibited key algorithm or signature hash algorithm. This policy is non-compliant if CCM uses such algorithms.	Encrypting data in transit	High	ccm:::privateCertificate

Cloud Eye

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALARM_ACTION_ENABLED_CHECK	Checks whether Cloud Eye alarming is enabled. This policy is non-compliant if alarming is not enabled.	Establishing logging and monitoring	Medium	ces:::alarmRule
RGC-GR_CONFIG_ALARM_RESOURCE_CHECK	Checks whether a resource has specified metrics associated for alarming. This policy is non-compliant if the resource has no specified metrics associated.	Establishing logging and monitoring	Low	ces:::alarmRule

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALARM_SETTINGS_CHECK	Checks whether the settings of a specified metric meet the requirements. This policy is non-compliant if the requirements are not met.	Establishing logging and monitoring	Low	ces:::alarmRule

Cloud Eye and DEW

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALARM_KMS_DISABLE_OR_DELETE_KEY	Checks whether alarms are configured to monitor the operation of disabling KMS or scheduling to delete a key. This policy is non-compliant if no alarms are configured.	Establishing logging and monitoring	Critical	ces:::alarmRule

Cloud Eye and OBS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALARM_OBS_BUCKET_POLICY_CHANGE	Checks whether alarms are configured to monitor the changes of OBS bucket policies. This policy is non-compliant if no alarms are configured.	Establishing logging and monitoring	Critical	ces:::alarmRule

Cloud Eye and VPC

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALARM_VPC_CHANGE	Checks whether alarms are configured to monitor VPC changes. This policy is non-compliant if no alarms are configured.	Establishing logging and monitoring	High	ces:::alarmRule

CodeArts Deploy

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CODEARTSDEPLOY_HOST_CLUSTER_RESOURCE_STATUS	Checks whether a host cluster in the CodeArts project is available. This policy is non-compliant if the cluster is unavailable.	Improving availability	Low	codeartsDeploy:::host

Config

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_TRACKER_CONFIG_ENABLED_CHECK	Checks whether the resource recorder is enabled for an account. This policy is non-compliant if the resource recorder is not enabled.	Establishing logging and monitoring	Medium	rms:::resourceRecorder

CSS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSS_CLUSTER_BACKUP_AVAILABLE	Checks whether the snapshot function is enabled for a CSS cluster. This policy is non-compliant if this function is not enabled.	Improving resiliency	Medium	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_MULTIPLE_AZ_CHECK	Checks whether a CSS cluster is deployed in multiple AZs for disaster recovery. This policy is non-compliant if the cluster is not deployed in multiple AZs.	Improving availability	Medium	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_MULTIPLE_INSTANCES_CHECK	Checks whether a CSS cluster has multiple nodes deployed for disaster recovery. This policy is non-compliant if the cluster does not have multiple nodes deployed.	Improving availability	Medium	css:::cluster
RGC-GR_CONFIG_CSS_CLUSTER_IN_VPC	Checks whether a CSS cluster is in the specified VPC. This policy is non-compliant if the cluster is not in the specified VPC.	Controlling network access	Critical	css:::cluster

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSS_CLUSTER_SLOWLOG_ENABLE	Checks whether slow query log is enabled for a CSS cluster. This policy is non-compliant if this function is not enabled.	Establishing logging and monitoring	Medium	css:::cluster

CTS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MULTI_REGION_CTS_TRACKER_EXISTS	Checks whether a CTS tracker has been created and enabled for the specified region list for an account. This policy is non-compliant if no trackers are created and enabled for the specified region list.	Establishing logging and monitoring	High	cts:::tracker
RGC-GR_CONFIG_CTS_OBS_BUCKET_TRACK	Checks whether all CTS trackers in an account track specified OBS buckets. This policy is non-compliant if all trackers do not track specified OBS buckets.	Establishing logging and monitoring	High	cts:::tracker

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CTS_TRACKER_ENABLED_SECURITY	Checks whether there are CTS trackers that comply with security best practices. This policy is non-compliant if no such trackers exist.	Establishing logging and monitoring	High	cts:::tracker

DEW

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSMS_SECRETS_AUTO_ROTATION_ENABLED	Checks whether automatic rotation is enabled for CSMS secrets. This policy is non-compliant if automatic rotation is not enabled.	Managing confidentiality	Medium	csms:::secret
RGC-GR_CONFIG_CSMS_SECRETS_PERIODIC_ROTATION	Checks whether a CSMS secret is rotated within the specified number of days. This policy is non-compliant if the secret is not rotated within the specified number of days.	Managing confidentiality	Medium	csms:::secret

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSMS_SECRETS_USING_CMK	Checks whether a CSMS secret uses the specified KMS keys. This policy is non-compliant if the secret does not use such keys.	Encrypting data at rest	High	csms:::secret

DDS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DDS_INSTANCE_HAMODE	Checks whether a DDS instance matches the specified type. This policy is non-compliant if the instance does not match.	Protecting configurations	Low	dds:::instance
RGC-GR_CONFIG_DDS_INSTANCE_ENGINE_VERSION_CHECK	Checks whether a DDS instance uses the specified version or higher. This policy is non-compliant if the instance uses an unspecified version or earlier.	Managing vulnerabilities	Low	dds:::instance

DWS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DWS_ENABLE_SNAPSHOT	Checks whether automated snapshots are enabled for a DWS cluster. This policy is non-compliant if automated snapshots are not enabled.	Improving resiliency	Medium	dws:::cluster
RGC-GR_CONFIG_DWS_MAINTAIN_WINDOW_CHECK	Checks whether the O&M time window of a DWS cluster is consistent with the specified time window. This policy is non-compliant if the time window is not consistent with the specified one.	Preparing for incident response	Medium	dws:::cluster
RGC-GR_CONFIG_DWS_ENABLE_LOG_DUMP	Checks whether log dump is enabled for a DWS cluster. This policy is non-compliant if log dump is not enabled.	Establishing logging and monitoring	Medium	dws:::cluster

ECS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALLOWED_ECS_FLAVORS	Checks whether an ECS flavor matches the specified one. This policy is non-compliant if the flavor does not match.	Protecting configurations	Low	ecs:::instanceV1

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALLOWED_IMAGES_BY_NAME	Checks whether the name of an ECS image matches one of the specified names. This policy is non-compliant if the image name does not match.	Managing vulnerabilities	High	ecs:::instanceV1
RGC-GR_CONFIG_ECS_ATTACHED_HSS_AGENTS_CHECK	Checks whether an ECS has an HSS agent attached and has protection enabled. This policy is non-compliant if the ECS has no HSS agent attached and has no protection enabled.	Managing vulnerabilities	Medium	ecs:::instanceV1

ECS and IMS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ALLOWED_IMAGES_BY_ID	Checks whether the image ID of an ECS matches one of the specified image IDs. This policy is non-compliant if the image ID does not match.	Managing vulnerabilities	High	ecs:::instanceV1

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_APPROVED_IMS_BY_TAG	Checks whether an ECS uses any of the IMS images with the specified tag. This policy is non-compliant if the ECS does not use such images.	Managing vulnerabilities	Medium	ecs:::instanceV1

EIP

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_EIP_USE_IN_SPECIFIED_DAYS	Checks whether an EIP is bound to any instances in specified number of days. This policy is non-compliant if the EIP is not bound in specified number of days.	Optimizing costs	Medium	vpc:::eipAssociate

ELB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ELB_MULTIPLE_AZ_CHECK	Checks whether the load balancer has registered with instances in multiple AZs. This policy is non-compliant if the load balancer has registered with instances in fewer than two AZs.	Balancing loads	Medium	elb:::loadbalancer
RGC-GR_CONFIG_ELB_MEMBERS_WEIGHT_CHECK	Checks whether the weight of a backend server is 0 and the load balancing algorithm used by its associated backend server group is not SOURCE_IP. This policy is non-compliant if the weight is 0 and the algorithm is not SOURCE_IP.	Improving availability	Low	elb:::member

EVS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_EVS_USE_IN_SPECIFIED_DAYS	Checks whether an EVS disk is bound to any instances in specified number of days. This policy is non-compliant if the disk is not bound in specified number of days.	Optimizing costs	Medium	evs:::volume
RGC-GR_CONFIG_VOLUME_UNUSED_CHECK	Checks whether an EVS disk is attached to a cloud server. This policy is non-compliant if the disk is not attached.	Optimizing costs	High	evs:::volume
RGC-GR_CONFIG_ALLOWED_VOLUME_SPECS	Checks whether the type of an EVS disk is within the allowed type list. This policy is non-compliant if the disk type is not within the list.	Protecting configurations	Low	evs:::volume

FunctionGraph

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_FUNCTION_GRAPH_CONCURRENCY_CHECK	Checks whether the number of concurrent requests of a FunctionGraph function is within the specified range. This policy is non-compliant if the number is not within the specified range.	Improving availability	Medium	fgs:::function
RGC-GR_CONFIG_FUNCTION_GRAPH_INSIDE_VPC	Checks whether a FunctionGraph function is in the specified VPC. This policy is non-compliant if the function is not in the specified VPC.	Controlling network access	Low	fgs:::function
RGC-GR_CONFIG_FUNCTION_GRAPH_SETTINGS_CHECK	Checks whether the runtime, timeout duration, or memory limit of a FunctionGraph function is within the specified range. This policy is non-compliant if they are not within the specified range.	Managing vulnerabilities	Medium	fgs:::function

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_FUNCTION_GRAPH_LOGGING_ENABLED	Checks whether logging is enabled for a FunctionGraph function. This policy is non-compliant if logging is not enabled.	Establishing logging and monitoring	Medium	fgs:::function

GaussDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_AUDITLOG	Checks whether audit logging is enabled for a GaussDB instance. This policy is non-compliant if audit logging is not enabled.	Establishing logging and monitoring	Medium	gaussdb:::opengaussInstance
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_BACKUP	Checks whether backup is enabled for a GaussDB instance. This policy is non-compliant if backup is not enabled.	Improving resiliency	Medium	gaussdb:::opengaussInstance
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_ERRORLOG	Checks whether error log collection is enabled for a GaussDB instance. This policy is non-compliant if error log collection is not enabled.	Establishing logging and monitoring	Low	gaussdb:::opengaussInstance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_SLOWLOG	Checks whether slow-query logging is enabled for a GaussDB instance. This policy is non-compliant if slow-query logging is not enabled.	Establishing logging and monitoring	Low	gaussdb:::opengaussInstance
RGC-GR_CONFIG_GAUSSDB_INSTANCE_MULTIPLE_AZ_CHECK	Checks whether a GaussDB resource is deployed across AZs. This policy is non-compliant if the resource is not deployed across AZs.	Improving availability	Medium	gaussdb:::opengaussInstance

GeminiDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_NOSQL_DEPLOY_IN_SINGLE_AZ	Checks whether GeminiDB is deployed in a single AZ. This policy is non-compliant if GeminiDB is deployed in a single AZ.	Improving availability	Medium	gaussdb:::mongoInstance
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_BACKUP	Checks whether backup is enabled for GeminiDB. This policy is non-compliant if backup is not enabled.	Improving resiliency	Medium	gaussdb:::mongoInstance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_ERROR_LOG	Checks whether error logging is enabled for GeminiDB. This policy is non-compliant if error logging is not enabled.	Establishing logging and monitoring	Low	gaussdb:::mongoInstance
RGC-GR_CONFIG_GAUSSDB_NOSQL_SUPPORT_SLOW_LOG	Checks whether GeminiDB supports slow-query logging. This policy is non-compliant if slow-query logging is not supported.	Establishing logging and monitoring	Low	gaussdb:::mongoInstance

GES

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GES_GRAPHS_LTS_ENABLE	Checks whether LTS is enabled for GES graphs. This policy is non-compliant if LTS is not enabled.	Establishing logging and monitoring	Medium	ges:::graph
RGC-GR_CONFIG_GES_GRAPHS_MULTI_AZ_SUPPORT	Checks whether GES supports cross-AZ HA. This policy is non-compliant if cross-AZ HA is not supported.	Improving availability	Medium	ges:::graph

IAM

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS	Checks whether an IAM policy allows any blocked action on KMS keys. This policy is non-compliant if the IAM policy allows such actions.	Enforcing the least privilege	Medium	● identity:::role ● identity:::protectionPolicy
RGC-GR_CONFIG_IAM_USER_CHECK_NON_ADMIN_GROUP	Checks whether a non-root user is added to the **admin** user group. This policy is non-compliant if such users are added.	Enforcing the least privilege	Low	identity:::user
RGC-GR_CONFIG_IAM_USER_NO_POLICIES_CHECK	Checks whether an IAM user is directly assigned a policy or permission. This policy is non-compliant if the user is directly assigned a policy or permission.	Enforcing the least privilege	Low	identity:::user

MRS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MRS_CLUSTER_MULTIAZ_DEPLOYMENT	Checks whether an MRS cluster is deployed in multiple AZs. This policy is non-compliant if the cluster is not deployed in multiple AZs.	Improving availability	Medium	mrs:::cluster
RGC-GR_CONFIG_MRS_CLUSTER_ENCRYPT_ENABLE	Requires KMS keys be not in a "pending deletion" state.	Protecting data integrity	Medium	mrs:::cluster

RDS

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_BACKUP	Checks whether backup is enabled for an RDS instance. This policy is non-compliant if backup is not enabled.	Improving resiliency	Medium	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_ERRORLOG	Checks whether error log collection is enabled for an RDS instance. This policy is non-compliant if error log collection is not enabled.	Establishing logging and monitoring	Low	rds:::instance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_SLOWLOG	Checks whether slow-query logging is enabled for an RDS instance. This policy is non-compliant if slow-query logging is not enabled.	Establishing logging and monitoring	Low	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_LOGGING_ENABLED	Checks whether logs are collected for an RDS instance. This policy is non-compliant if no logs are collected.	Establishing logging and monitoring	Medium	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_MULTI_AZ_SUPPORT	Checks whether an RDS instance can only be deployed in one AZ. This policy is non-compliant if the instance can only be deployed in one AZ.	Improving availability	Medium	rds:::instance
RGC-GR_CONFIG_ALLOWED_RDS_FLAVORS	Checks whether the flavor of an RDS instance is within the specified range. This policy is non-compliant if the flavor is not within the specified range.	Protecting configurations	Low	rds:::instance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_RDS_INSTANCES_IN_VPC	Checks whether an RDS resource is in the specified VPC. This policy is non-compliant if the resource is not in the specified VPC.	Controlling network access	High	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_AUDITLOG	Checks whether an RDS resource has audit logging enabled or the audit logs can be stored for a specified period of time. This policy is non-compliant if audit logging is not enabled or audit logs cannot be stored for a specified period of time.	Establishing logging and monitoring	Medium	rds:::instance
RGC-GR_CONFIG_RDS_INSTANCE_ENGINE_VERSION_CHECK	Checks whether the version of the database engine for an RDS instance is earlier than the specified version. This policy is non-compliant if the version is earlier than the specified one.	Managing vulnerabilities	Low	rds:::instance

OBS and Access Analyzer

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_OBS_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED	Checks whether an OBS bucket policy allows any blacklisted action to external users. This policy is non-compliant if the bucket policy allows such actions.	Enforcing the least privilege	High	obs:::bucket
RGC-GR_CONFIG_OBS_BUCKET_SSL_REQUESTS_ONLY	Checks whether an OBS bucket policy allows actions without SSL encryption. This policy is non-compliant if the bucket policy allows such actions.	Encrypting data in transit	Medium	obs:::bucket

Organizations

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ACCOUNT_PART_OF_ORGANIZATIONS	Checks whether an account joins an organization. This policy is non-compliant if the account does not join an organization.	Enforcing the least privilege	High	organizations:::accountAssociate

SMN

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_SMN_LTS_ENABLE	Checks whether trace analysis is enabled for an SMN topic. This policy is non-compliant if trace analysis is not enabled.	Establishing logging and monitoring	Medium	smn:::topic

TaurusDB

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_AUDITLOG	Checks whether audit logging is enabled for a TaurusDB instance. This policy is non-compliant if audit logging is not enabled.	Establishing logging and monitoring	Medium	gaussdb:::mysqlInstance
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_BACKUP	Checks whether backup is enabled for a TaurusDB instance. This policy is non-compliant if backup is not enabled.	Improving resiliency	Medium	gaussdb:::mysqlInstance
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_ERRORLOG	Checks whether error logging is enabled for a TaurusDB instance. This policy is non-compliant if error logging is not enabled.	Establishing logging and monitoring	Low	gaussdb:::mysqlInstance

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_SLOWLOG	Checks whether slow-query logging is enabled for a TaurusDB instance. This policy is non-compliant if slow-query logging is not enabled.	Establishing logging and monitoring	Low	gaussdb:::mysqlInstance
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_MULTIPLE_AZ_CHECK	Checks whether a TaurusDB instance is deployed across AZs. This policy is non-compliant if the instance is not deployed across AZs.	Improving availability	Medium	gaussdb:::mysqlInstance

VPC

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_EIP_UNBOUND_CHECK	Checks whether an EIP is bound to any resources. This policy is non-compliant if the EIP is not bound.	Optimizing costs	Medium	vpc:::eipAssociate
RGC-GR_CONFIG_VPC_FLOW_LOGS_ENABLED	Checks whether flow logs are enabled for a VPC. This policy is non-compliant if flow logs are not enabled.	Establishing logging and monitoring	Medium	vpc:::flowLog

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_EIP_BANDWIDTH_LIMIT	Checks whether the bandwidth of an EIP is less than the specified value. This policy is non-compliant if the bandwidth is less than the specified value.	Improving availability	Medium	vpc:::eip

VPN

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VPN_CONNECTIONS_ACTIVE	Checks whether the VPN connection is normal. This policy is non-compliant if the connection is not normal.	Improving availability	Medium	vpnaas:::siteConnectionV2

5.3 Enabling or Disabling Governance Policies

RGC provides multiple types of governance policies. Mandatory governance policies are automatically applied to OUs created in RGC. You can use the management account to enable strongly recommended or elective governance policies as needed.

After you enable governance policies, RGC creates and manages resources in your management account. Do not modify or delete resources created by RGC. Otherwise, the governance policies may become ineffective.

Constraints

- You can only manually enable or disable strongly recommended and elective governance policies.
- Governance policies cannot be attached to the root OU or core OU.

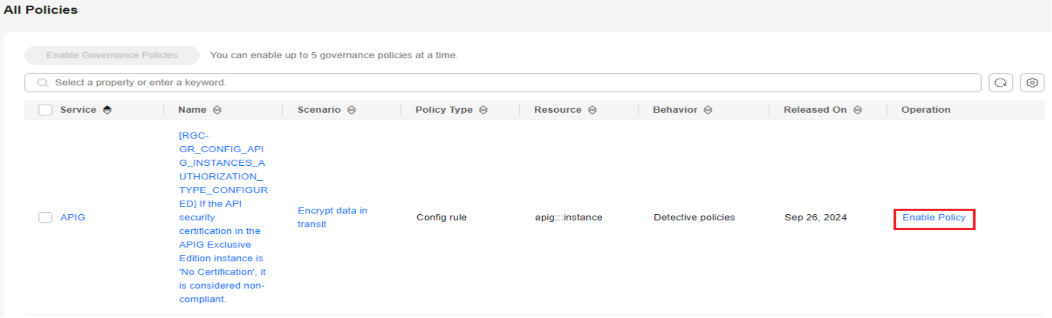
Enabling a Governance Policy

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Choose **Governance Policy Library** > **All Policies**. In the policy list, locate the governance policy you want to enable.

Step 3 Click **Enable Policy** in the **Operation** column.

Figure 5-1 Enabling a governance policy



All Policies

Enable Governance Policies

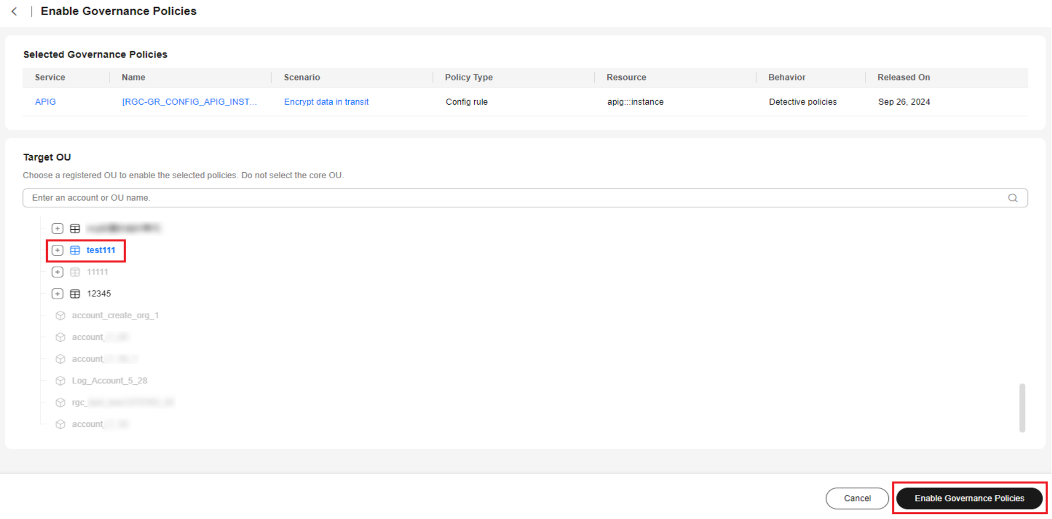
You can enable up to 5 governance policies at a time.

Select a property or enter a keyword.

Service	Name	Scenario	Policy Type	Resource	Behavior	Released On	Operation
□ APIG	[RGC-GR_CONFIG_APIG_INSTANCES_AUTHORIZATION_TYPE_CONFIGURED] If the API security certification in the APIG Exclusive Edition instance is 'No Certification', it is considered non-compliant.	Encrypt data in transit	Config rule	apig:::instance	Detective policies	Sep 26, 2024	Enable Policy

Step 4 Select an OU that you want to enable this policy for.

Figure 5-2 Selecting an OU



Enable Governance Policies

Selected Governance Policies

Service	Name	Scenario	Policy Type	Resource	Behavior	Released On
APIG	[RGC-GR_CONFIG_APIG_INST...	Encrypt data in transit	Config rule	apig:::instance	Detective policies	Sep 26, 2024

Target OU

Choose a registered OU to enable the selected policies. Do not select the core OU.

Step 5 Click **Enable Governance Policies** in the lower right corner. This may take several minutes.

----End

Enabling Governance Policies in Batches

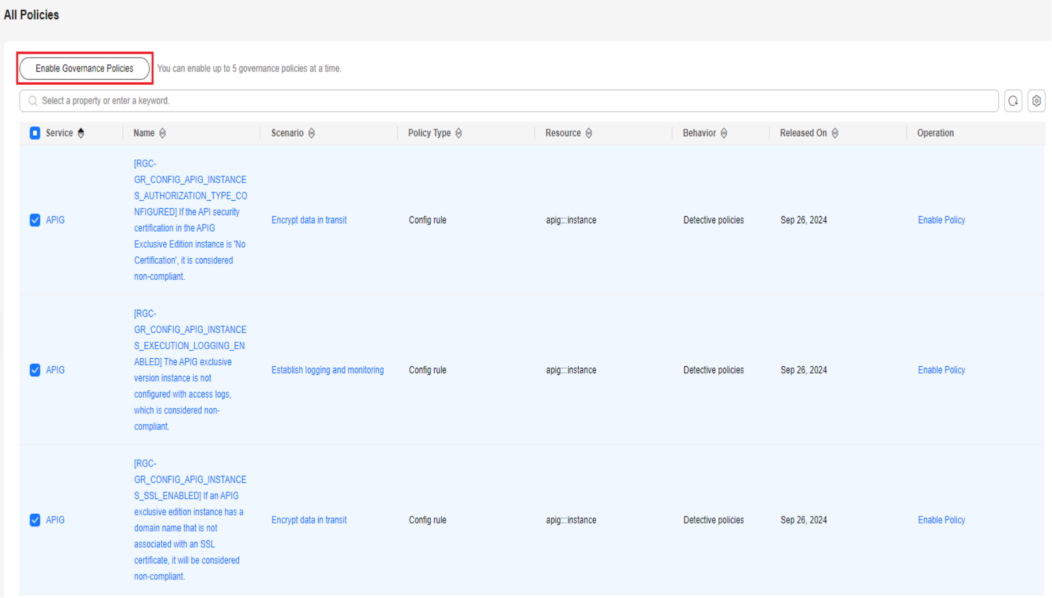
You can enable up to five governance policies in a batch.

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Choose **Governance Policy Library** > **All Policies**. In the policy list, locate the governance policy you want to enable.

Step 3 Click **Enable Governance Policies** above the policy list.

Figure 5-3 Enabling governance policies in batches



All Policies

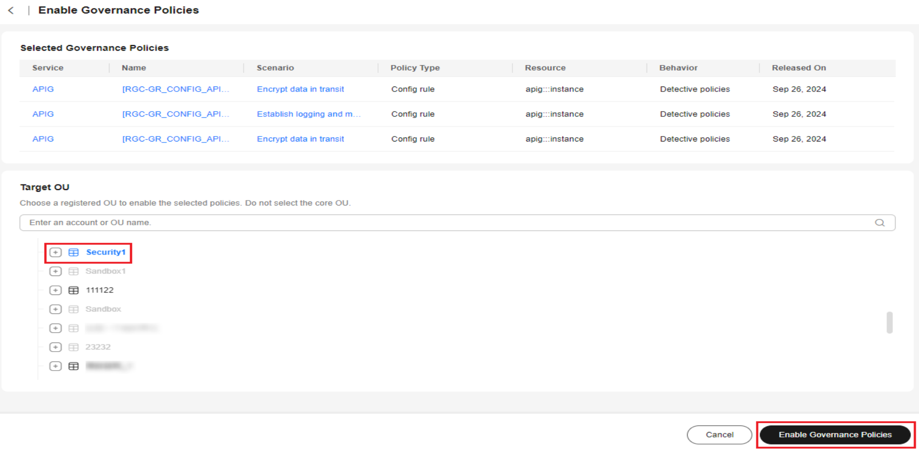
Enable Governance Policies   You can enable up to 5 governance policies at a time.

Select a property or enter a keyword.

☑ Service	Name	Scenario	Policy Type	Resource	Behavior	Released On	Operation
☑ APIG	[RGC-GR_CONFIG_APIG_INSTANCES_AUTHORIZATION_TYPE_CONFIGURED] If the API security certification in the APIG Exclusive Edition instance is 'No Certification', it is considered non-compliant.	Encrypt data in transit	Config rule	apig::instance	Detective policies	Sep 26, 2024	Enable Policy
☑ APIG	[RGC-GR_CONFIG_APIG_INSTANCES_EXECUTION_LOGGING_ENABLED] The APIG exclusive version instance is not configured with access logs, which is considered non-compliant.	Establish logging and monitoring	Config rule	apig::instance	Detective policies	Sep 26, 2024	Enable Policy
☑ APIG	[RGC-GR_CONFIG_APIG_INSTANCES_SSL_ENABLED] If an APIG exclusive edition instance has a domain name that is not associated with an SSL certificate, it will be considered non-compliant.	Encrypt data in transit	Config rule	apig::instance	Detective policies	Sep 26, 2024	Enable Policy

Step 4 Select an OU that you want to enable the selected policies for.

Figure 5-4 Selecting an OU



< | Enable Governance Policies

Selected Governance Policies

Service	Name	Scenario	Policy Type	Resource	Behavior	Released On
APIG	[RGC-GR_CONFIG_API...	Encrypt data in transit	Config rule	apig:::instance	Detective policies	Sep 26, 2024
APIG	[RGC-GR_CONFIG_API...	Establish logging and m...	Config rule	apig:::instance	Detective policies	Sep 26, 2024
APIG	[RGC-GR_CONFIG_API...	Encrypt data in transit	Config rule	apig:::instance	Detective policies	Sep 26, 2024

Target OU

Choose a registered OU to enable the selected policies. Do not select the core OU.

Enter an account or OU name.

- Security1
- Sandbox1
- 111122
- Sandbox
- [redacted]
- 23232
- [redacted]

Cancel   Enable Governance Policies

Step 5 Click **Enable Governance Policies** in the lower right corner. This may take several minutes.

----End

Disabling a Governance Policy

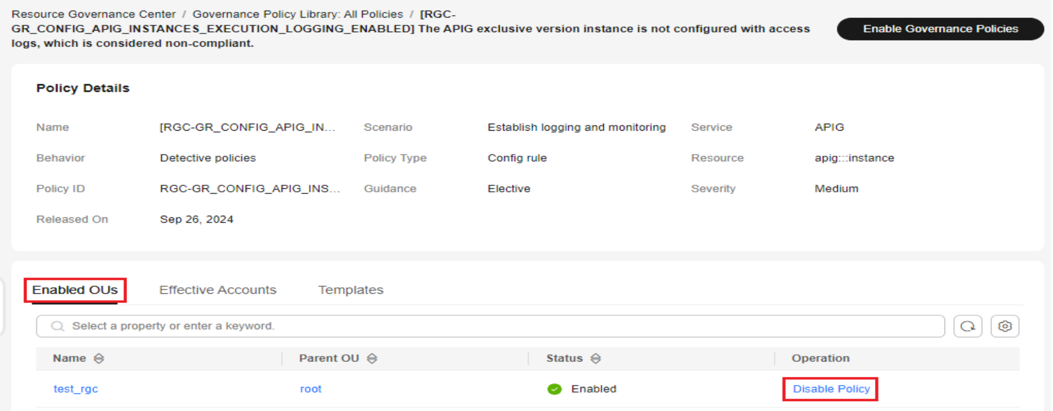
Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Choose **Governance Policy Library** > **All Policies**. In the policy list, locate the governance policy you want to disable.

Step 3 Click the policy name. The policy details are displayed.

Step 4 On the **Enabled OUs** page, choose the OU that you want to disable this policy from.

Figure 5-5 Disabling a governance policy



Resource Governance Center / Governance Policy Library: All Policies / [RGC-GR_CONFIG_APIG_INSTANCES_EXECUTION_LOGGING_ENABLED] The APIG exclusive version instance is not configured with access logs, which is considered non-compliant.

Enable Governance Policies

Policy Details

Name	[RGC-GR_CONFIG_APIG_IN...	Scenario	Establish logging and monitoring	Service	APIG
Behavior	Detective policies	Policy Type	Config rule	Resource	apig:::instance
Policy ID	RGC-GR_CONFIG_APIG_INS...	Guidance	Elective	Severity	Medium
Released On	Sep 26, 2024				

Enabled OUs | Effective Accounts | Templates

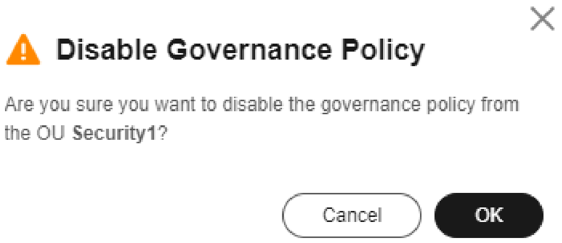
Select a property or enter a keyword.

Name	Parent OU	Status	Operation
test_rgc	root	Enabled	Disable Policy

Step 5 Click **Disable Policy** in the **Operation** column.

Step 6 Click **OK**. This may take several minutes.

Figure 5-6 Disabling a governance policy



Disable Governance Policy

Are you sure you want to disable the governance policy from the OU Security1?

----End

5.4 Viewing Governance Policy Details

You can view details about currently enabled governance policies in the policy categories and policy list.

Procedure

Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 Choose **Governance Policy Library** > **All Policies**. In the policy list, locate the governance policy you want to view.

Step 3 Click the policy name. The policy details are displayed.

Table 5-1 Governance policy parameters

Parameter	Description
Name	The name of the governance policy.

Parameter	Description
Resource	The resource that is governed by the governance policy.
Guidance	The extent to which the governance policy is applied to OUs. The guidance can be mandatory, strongly recommended, or elective.
Scenario	The pre-defined objective that the governance policy helps you enforce.
Behavior	The behavior of the governance policy. A governance policy's behavior can be preventive or detective.
Severity	The relative risk associated with any violation of the governance policy.
Service	The service that the governance policy applies to.
Policy Type	The underlying implementation method for the governance policy, which can be SCPs or Config rules.
Policy ID	A unique identifier of each governance policy.
Released On	The date when the governance policy was enabled.

----End

6 Drift Detection and Repair

About Drift

When you set up a landing zone, all the accounts, OUs, and resources will be compliant with the rules enforced by the governance policies applied. When you and your organization members use the landing zone, you can access the organization and manage SCPs via either RGC or Organizations. Operations performed on the two portals may result in changes to the compliance status of resources governed in the landing zone. If the resources do not comply with the governance policies, the following types of drift will occur:

- SCPs

  The SCPs configured for each OU in RGC are inconsistent with those configured in Organizations, or they are absent from Organizations.

- Organizational structure

  The OUs and accounts governed in RGC are different from those in Organizations.

When any of these inconsistencies arises, the current landing zone becomes non-compliant, which may result in unexpected consequences.

In such cases, RGC allows you to trigger periodic drift detection for accounts, OUs, and SCPs, and receive alerts when drift is detected. If any drift is identified, you can eliminate it by updating the landing zone or repairing the drift.

When the core OU or core accounts are in a drifted state, you are not allowed to create accounts in RGC.

Detecting Drift

RGC detects drift automatically. To detect drift, the RGCServiceExecutionAgency agency requires persistent access to your management account so that RGC can make read-only API calls to Organizations. These API calls will be recorded in CTS traces.

Drift messages are aggregated by Simple Message Notification (SMN). The management account can subscribe to SMN notifications. For details, see **Publishing a JSON Message Using SMN**. This way, you can receive drift notifications and repair drift in a timely manner. In RGC, you can detect the following types of governance drift:

- Organizational structure drift
  - SCPs have been updated.
  - SCPs have been deleted.
  - SCPs have been attached to OUs.
  - SCPs have been attached to accounts.
  - SCPs have been detached from OUs.
  - SCPs have been detached from accounts.
- Account drift
  - Accounts have been moved to another OU.
  - Accounts have been closed.
  - Accounts have been removed from an organization.

NOTE

- If the same type of drift occurs on the same group of resources multiple times, RGC will only send an SMN notification for the first resource that drifts.
- If drift for a resource has been repaired, RGC will only send another SMN notification if drift recurs for that resource.

Examples:

- If you modify an SCP multiple times, you will receive an SMN notification for the first time you modify it.
- If you modify an SCP, then repair drift, then modify it again, and then the drift recurs, you will receive two SMN notifications.

Types of Drift to Repair Right Away

You can ensure your landing zone is compliant by updating settings or repairing drift. Although drift detection is automatic, the steps to repair drift must be done on the RGC console.

Most types of drift can be repaired by administrators. A few types of drift must be repaired immediately, including deletion of an OU required by the RGC landing zone. The following are some examples of how to avoid drift that requires immediate repair:

- Do not delete the core OU. The core OU originally named "Security" during landing zone setup should not be deleted. If you delete it, there will be drift. You will see an error message on the RGC console, instructing you to update or repair your landing zone immediately. You will not be able to perform any other operations in RGC until the update or repair is complete.
- Do not delete core accounts. If you delete a core account from a core OU, for example, deleting the log archive account from the core OU, your landing zone will be in a drifted state. You must update or repair the landing zone before you can continue using the RGC console.

Repairing Drift

If there is drift, you will see an error message on the RGC console, instructing you to update or repair your landing zone immediately. You only need to repair drift by clicking **update the landing zone**, **repair the landing zone**, or **re-register the new OU** as instructed.

If you have performed as instructed but drift persists, you can **submit a service ticket** for technical support.

7 CTS Auditing

Scenarios

RGC supports the recording of RGC operations through CTS. You can query RGC traces and use them for historical operation audits and backtracks.

Prerequisites

CTS has been enabled.

Key RGC Operations Recorded by CTS

Table 7-1 RGC operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Pre-checking for Landing Zone	LandingZone	checkLaunch
Deleting a landing zone	LandingZone	deleteLandingZone
Setting up a landing zone	LandingZone	setupLandingZone
Disabling a governance policy	Control	DisableGovernancePolicy
Enabling a governance policy	Control	EnableGovernancePolicy
Creating an account	Account	createAccount
Enrolling an account	Account	enrollAccount
Unmanaging an account	Account	unEnrollAccount
Updating an enrolled account	Account	updateManagedAccount

Operation	Resource Type	Trace Name
Creating an OU	OrganizationUnit	createManagedOrganizationalUnit
Deleting an OU	OrganizationUnit	deleteManagedOrganizationalUnits
Re-registering an OU	OrganizationUnit	reRegisterOrganizationalUnit
Registering an OU	OrganizationUnit	registerOrganizationalUnit
Deregistering an OU	OrganizationUnit	deregisterOrganizationalUnit
Creating a template.	Template	createTemplate
Deleting a template	Template	deleteTemplate

Querying Audit Logs

For details about how to query audit logs, see **Viewing CTS Traces in the Trace List**.