Resource Governance Center

User Guide

Issue	01
Date	2024-01-30

HUAWEI TECHNOLOGIES CO., LTD.

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

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei 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 Applying for OBT

RGC is in open beta test (OBT). You can apply for OBT and use RGC for free as long as the test lasts.

Procedure

Step 1 Log in to the **management console**.

Step 2 In the upper left corner, click ☰ and choose **Management & Governance** > **Resource Governance Center**.

Step 3 Click **Apply Now** to switch to the page for applying for OBT qualification.

Step 4 Provide various required details, including the enterprise scale, R&D personnel proportion, application scenario, current service phase, and service description.

Step 5 Select the **Agree OBT Trial Service Agreement** to confirm that you have read and agree to the terms and conditions, and click **Apply For OBT**.

----End

The application result will be sent to you via email and SMS within five working days.

 Copyright © Huawei Technologies Co., Ltd.

2 Landing Zone Management

2.1 Viewing Your Landing Zone

After a landing zone is set up, on the **Dashboard** page, you can view information about 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 Get an overview of your landing zone on the **Dashboard** page.

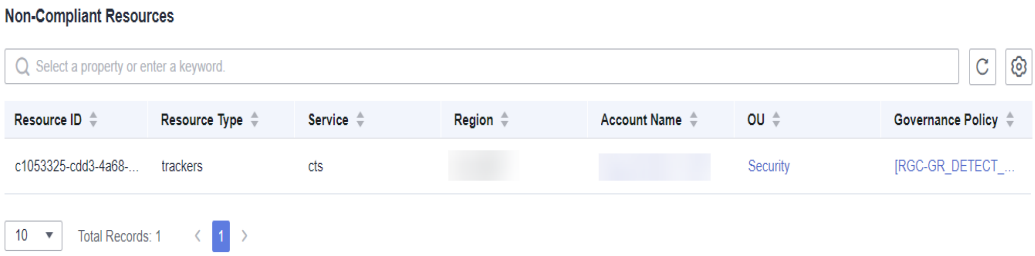
Step 3 Under **OUs and Accounts**, click the number to get an overview of the OUs and accounts.

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 2-1 Non-compliant resources



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

 Copyright © Huawei Technologies Co., Ltd.

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

----End

3 Organization Management

3.1 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 information about Organizations, see **What Is Organizations?**

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 (or an audit account for short).

- **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 register them manually so 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.

3.2 Creating an Account

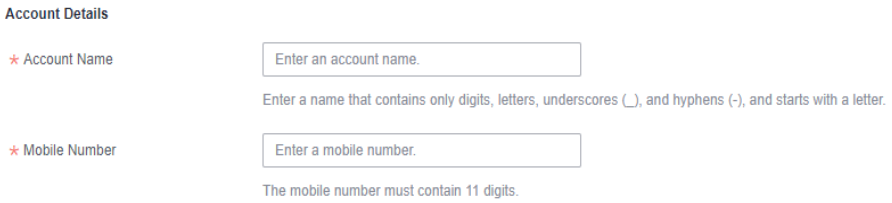
You can create an account in RGC. The account then will be automatically enrolled in RGC.

Procedure

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

Step 2 Click **Create Account**.

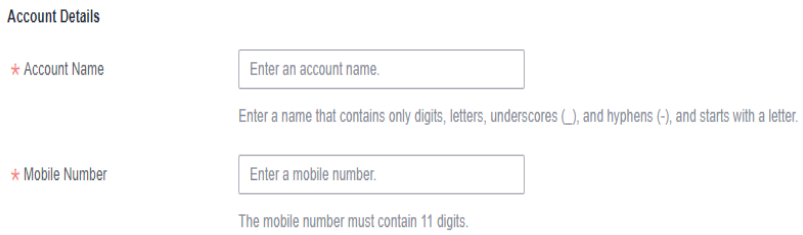
Figure 3-1 Creating an account



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

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

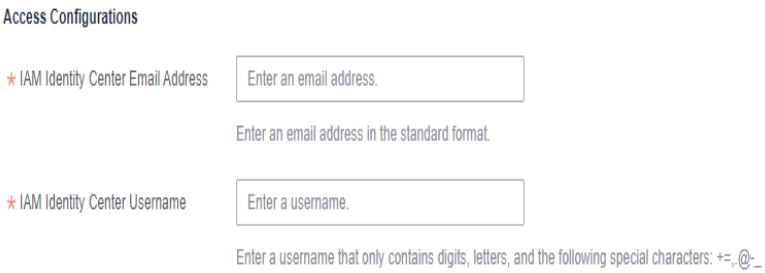
Figure 3-2 Configuring account details



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

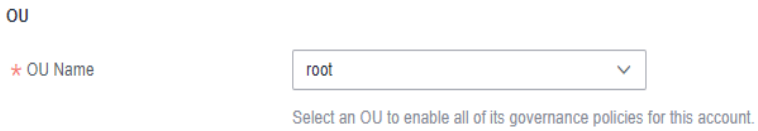
After an account is created, an IAM Identity Center user is automatically created in RGC. You can use an IAM Identity Center username and password to log in to the management console through the user portal URL, and use the email address to retrieve the password. For details, see **Logging In as an IAM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

Figure 3-3 Configuring IAM Identity Center details



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 3-4 Selecting a registered OU



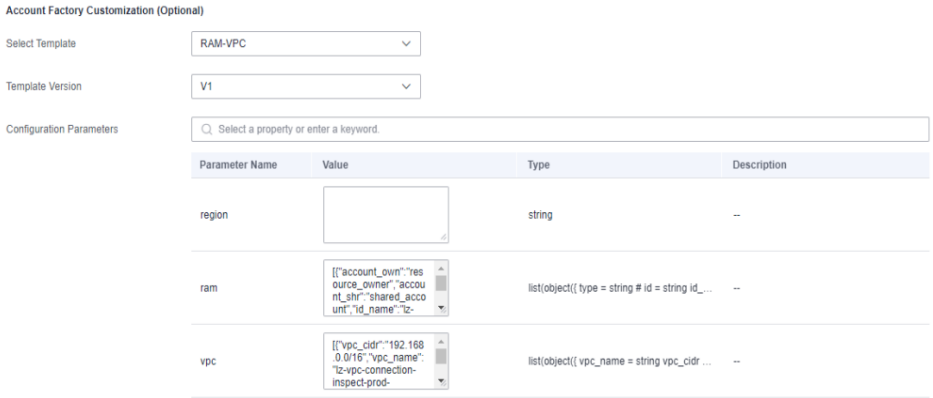
Step 6 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

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

- **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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Configuring a template



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

----End

3.3 Creating an OU

An OU is a container or a logical grouping of 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.

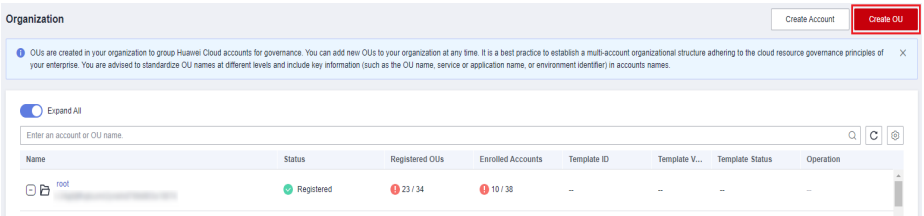
The OUs you created in a landing zone will be automatically registered in RGC.

Procedure

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

Step 2 Click **Create OU**.

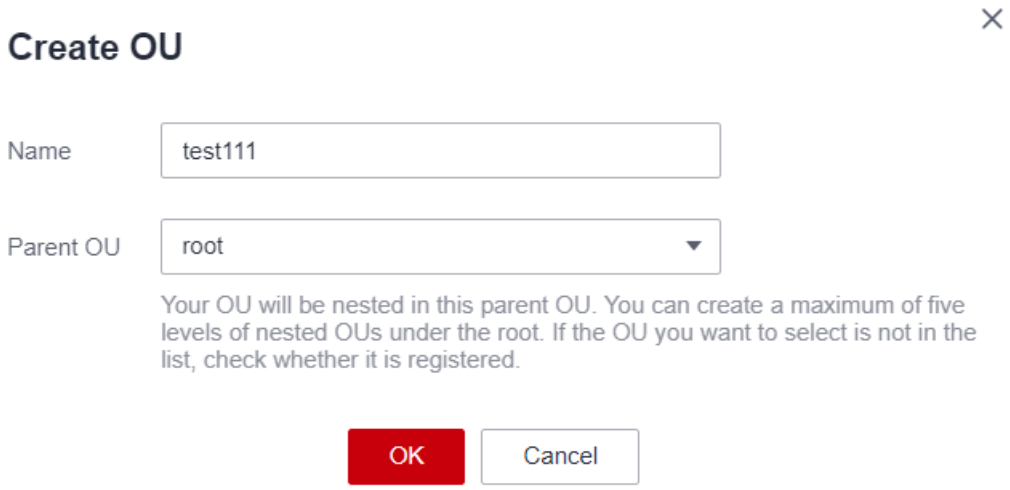
Figure 3-6 Creating an OU



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

Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Configuring OU information



Step 4 Click **OK**.

----End

3.4 Enrolling an Account

Before your landing zone is set up, once you have created an account in Organizations or invited an account to your organization, you still need to manually enroll that account before it can be governed in your landing zone.

Constraints

- If an account has enabled Config and had a resource recorder, exercise caution when enrolling the account because the recorder configurations will be overwritten after enrollment.
- Before enrolling an invited account, make sure you have met the steps in **Prerequisites**. Otherwise, the account enrollment may fail.

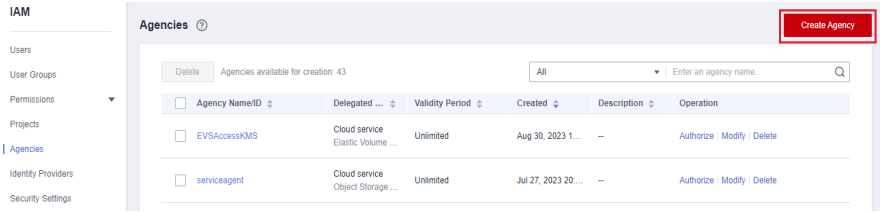
Prerequisites

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.

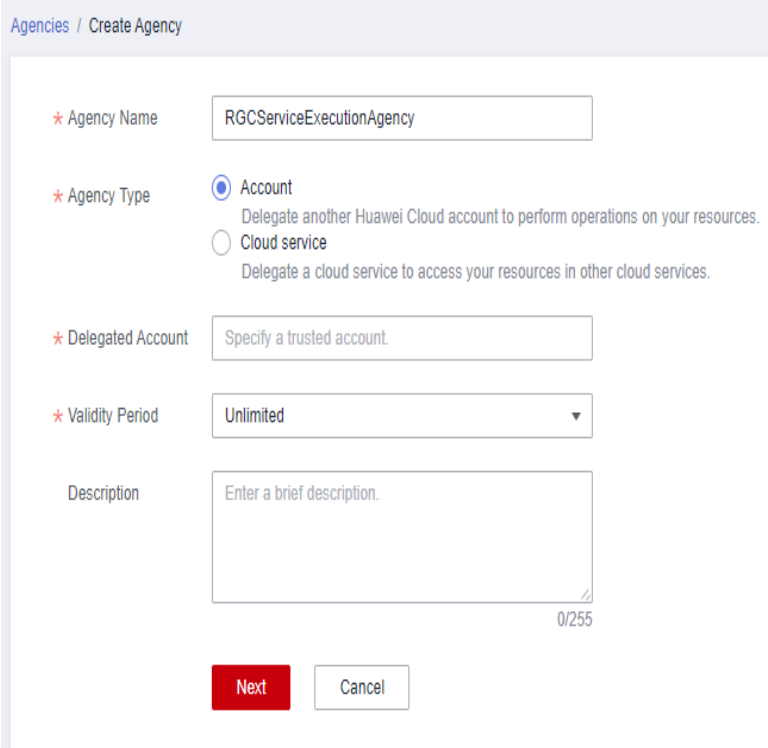
Step 2 In the navigation pane, choose **Agencies** and click **Create Agency** in the upper right corner.

Figure 3-8 Creating an agency



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

Figure 3-9 Specifying an agency name



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

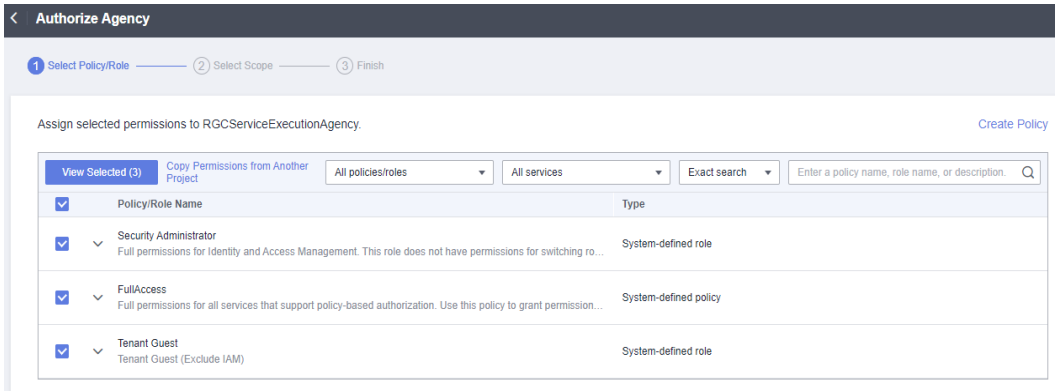
Step 5 Configure a validity period and enter a description for the agency.

Step 6 Click **Next**. The authentication page is displayed.

Step 7 Select **Security Administrator**, **FullAccess**, and **Tenant Guest**.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-10 Permissions to be granted to the agency



Step 8 Click **Next** to set the authentication scope.

Step 9 Click **OK**. The agency is created. You can then follow the instructions in **Procedure** to enroll the account.

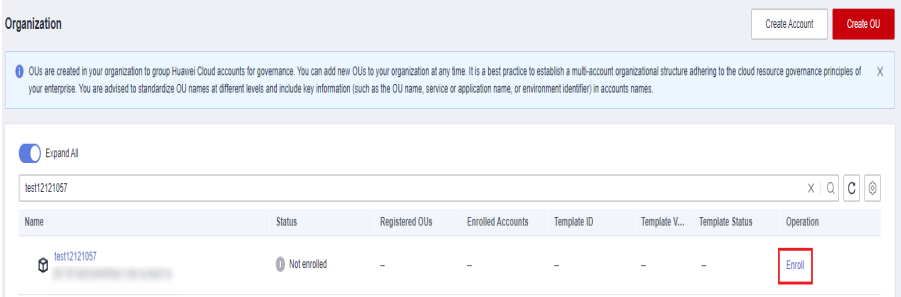
----End

Procedure

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

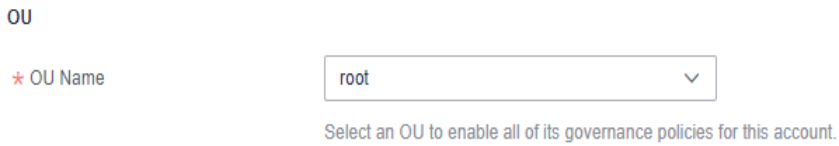
Step 2 Locate the account you want to enroll and click **Enroll** in the **Operation** column.

Figure 3-11 Enrolling an account



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 3-12 Selecting a registered OU



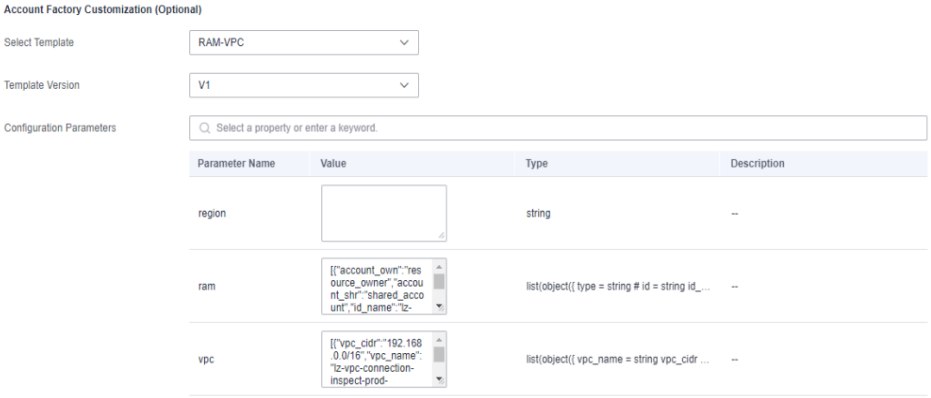
Step 4 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

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

Copyright © Huawei Technologies Co., Ltd.

- **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 3-13 Configuring a template



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

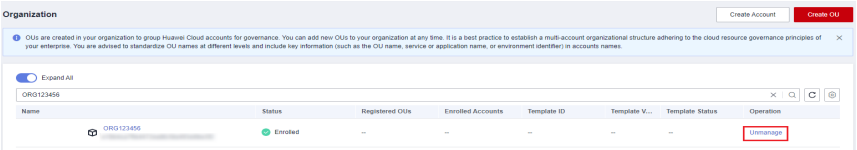
Unmanaging an Account

If you no longer want an account to be managed, you can unmanage it from the RGC console.

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

Step 2 Locate the account you want to unmanage and click **Unmanage** in the **Operation** column.

Figure 3-14 Unmanaging an account



Step 3 Click **OK**. Exercise caution when unmanaging an account because this operation cannot be undone.

You can view the management status in the organizational structure. After being unmanaged, the account is moved from its parent OU to the root OU.

----End

3.5 Registering an OU

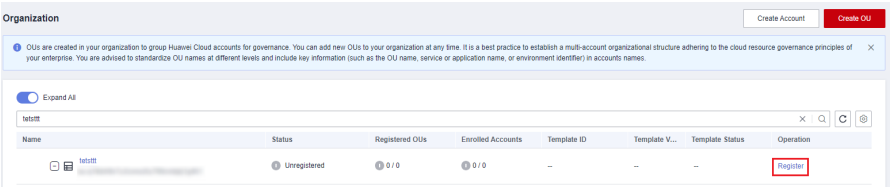
If you create an OU in Organizations before your landing zone is set up, you need to manually register the OU so that it can be governed in your landing zone.

Procedure

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

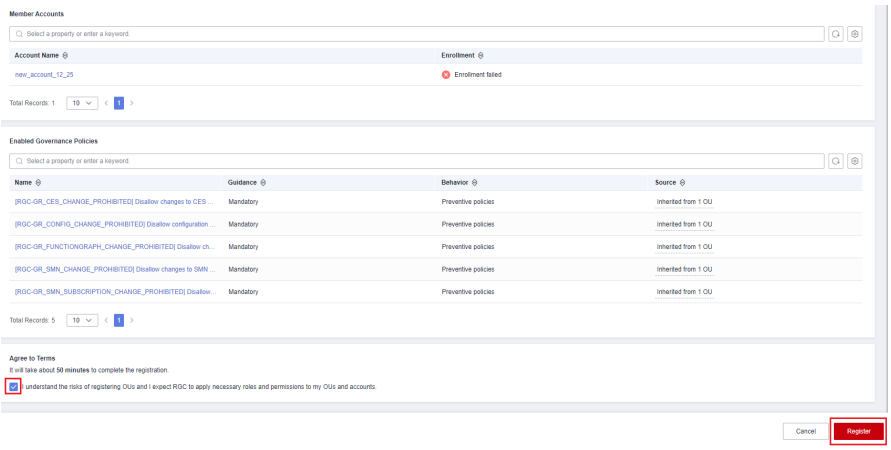
Step 2 Locate the OU to be registered and click **Register** in the **Operation** column.

Figure 3-15 Registering an OU



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

Figure 3-16 Confirming OU information



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

3.6 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.

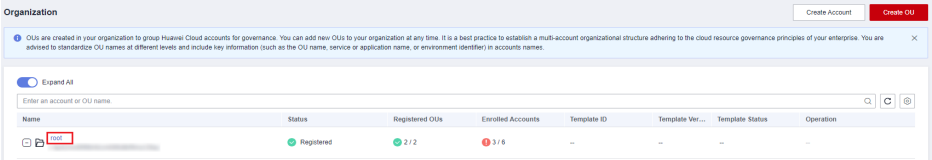
Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 Click the name of an OU you want to view.

Figure 3-17 Locating an OU

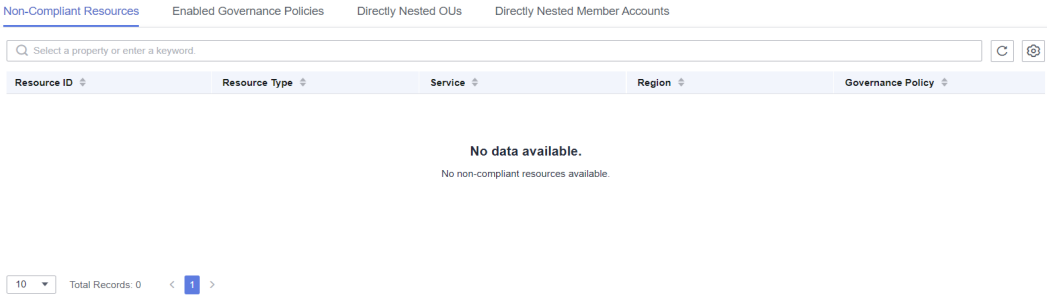


Step 3 On the displayed page, view the OU status, parent OU, number of enrolled accounts, number of enabled governance policies, number of registered OUs, and external SCPs.

Figure 3-18 Viewing OU details

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

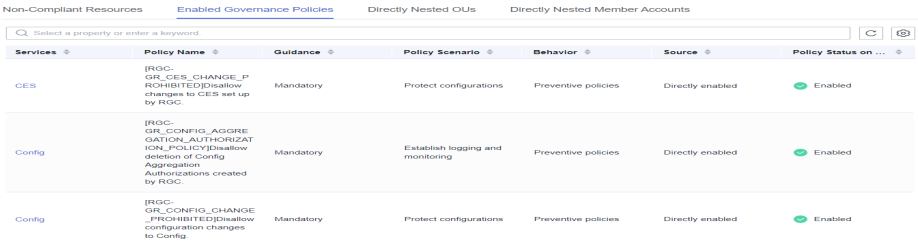
Figure 3-19 Viewing non-compliant resources



Step 5 Click the **Enabled Governance Policies** tab to view governance policies enabled for the current OU.

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

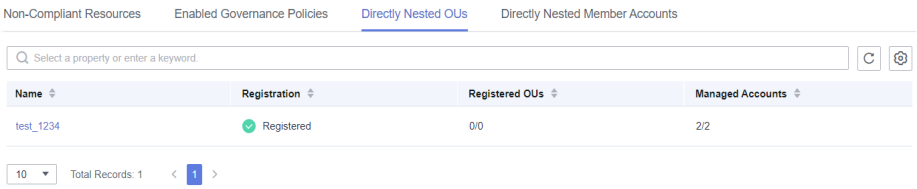
Figure 3-20 Viewing enabled governance policies



Copyright © Huawei Technologies Co., Ltd.

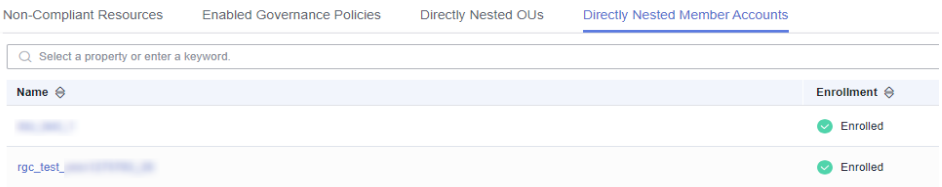
Step 6 Click the **Directly Nested OUs** tab to view the information about OUs directly nested under the current OU, including the registration status, registered OUs, and enrolled accounts.

Figure 3-21 Viewing directly nested OUs



Step 7 Click the **Directly Nested Member Accounts** tab to view the information about member accounts directly nested under the current OU, including the external Config rules, landing zone version, and enrollment status.

Figure 3-22 Viewing directly nested member accounts



----End

Copyright © Huawei Technologies Co., Ltd.

4 Account Factory

4.1 (Optional) Creating a Custom Template

You can use the management account to configure a baseline template for accounts in RFS. In the account factory, you can create member accounts under a specified OU, and baseline configurations will be automatically applied to your accounts based on best practices.

Currently, custom templates are not supported in RGC.

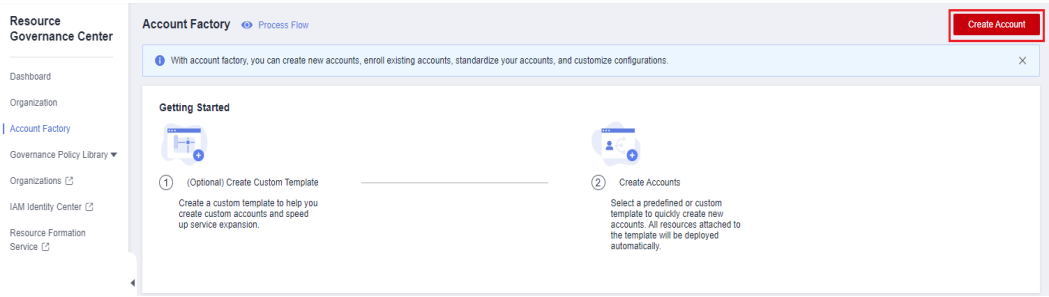
Procedure

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

Step 2 Create a template. For details, see **Compiling a Template to Create an EVS Disk**.

Step 3 Click **Create Account**.

Figure 4-1 Creating an account



If the template and its version can be selected in **Account Factory**, the template was created successfully.

----End

 Copyright © Huawei Technologies Co., Ltd.

4.2 Creating an Account and Deploying a Template

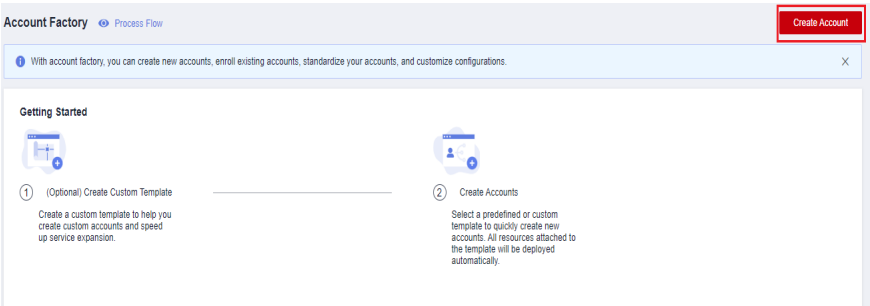
You can select a preconfigured or custom template to quickly create new accounts. All resource configurations defined in the template can be automatically applied to the new accounts.

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.

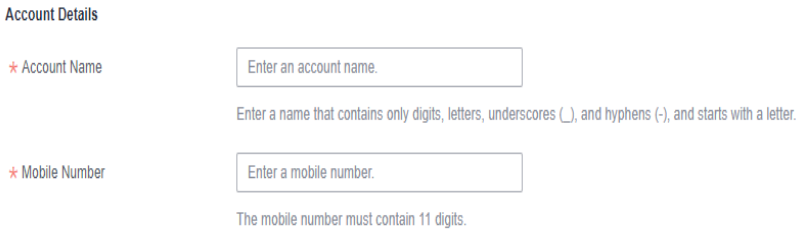
Figure 4-2 Creating an account



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

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

Figure 4-3 Configuring account details

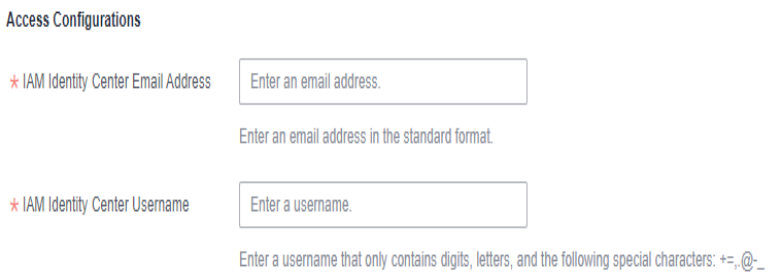


Step 4 Configure IAM Identity Center details, including the email address and username.

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**.

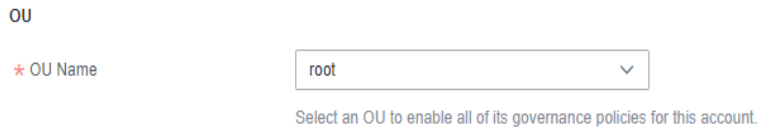
Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Configuring IAM Identity Center details



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 4-5 Selecting a registered OU

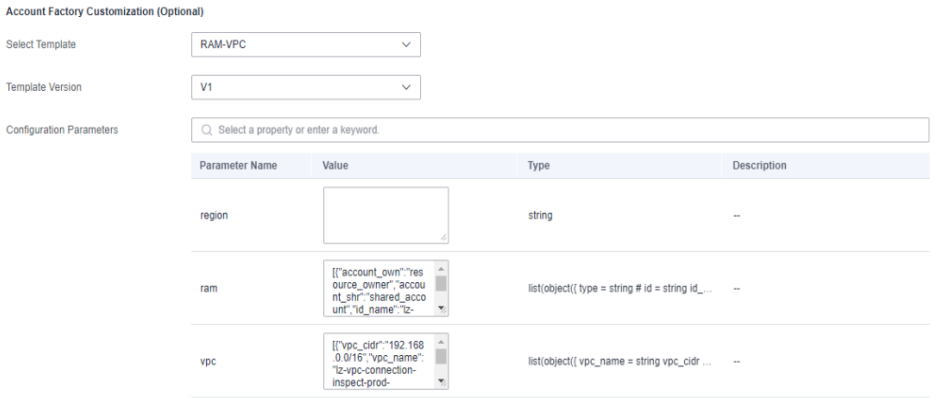


Step 6 (Optional) Configure an RFS template in the account factory. Select an RFS template and its version. If you select an RFS, you can copy and create accounts in batches.

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

- **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 4-6 Configuring a template



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

----End

 Copyright © Huawei Technologies Co., Ltd.

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 directly nested member accounts under this OU will inherit this policy.
- Detective: Detective governance policies identify non-compliant resource configurations and inform you of such resources when they are discovered. They are implemented by Config rules. You can view these resources on the RGC console. When a detective governance policy is applied to a specified OU, all directly nested member accounts under this OU will inherit this policy.

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 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

- Establishing logging and monitoring
- Enforcing the least privilege

 Copyright © Huawei Technologies Co., Ltd.

- Limiting network access
- Encrypting data at rest
- Protecting data integrity
- Protecting configurations
- Optimizing costs

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

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_CT_AUDIT_BUCKET_ENCRYPTION_CHANGES_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:PprincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_CT_AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_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_CT_AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_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_CT_AUDIT_BUCKET_POLICY_CHANGES_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

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

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_CONFIG_ENABLED

Implementation: SCPs

Behavior: preventive

Function: This policy enables Config in all available regions.

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "CONFIG_CHANGE_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "rms:trackerConfig:delete",
            "rms:trackerConfig:put"
        ],
        "Resource": [
            "*"
        ],
```

```
        "Condition": {
            "StringNotMatch": {
                "g:PprincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_FUNCTIONGRAPH_CHANGE_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:PprincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_SMN_CHANGE_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

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"
                ]
            }
```

```
    }
  }]
}
```

5.2.2 Strongly Recommended Governance Policies

Cloud Trace Service (CTS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MULTI_REGION_CTS_TRACKER_EXISTS	This policy checks whether a CTS tracker has been created and enabled for the specified region list for an account. If not, the account is considered non-compliant.	Establishing logging and monitoring	High	cts:::tracker

Identity and Access Management (IAM)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_IAM_ROOT_ACCESS_KEY_CHECK	This policy checks whether there are available access keys for an account. If yes, the account is considered non-compliant.	Enforcing the least privilege	Critical	identity:::accessKey

 Copyright © Huawei Technologies Co., Ltd.

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ROOT_ACCOUNT_MFA_ENABLED	This policy checks whether multi-factor authentication (MFA) is enabled for an account. If not, the account is considered non-compliant.	Enforcing the least privilege	High	identity:::acl
RGC-GR_CONFIG_IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	This policy checks whether an IAM policy grants the admin permission (*:*:*, *:*, or *). If yes, the IAM policy is considered non-compliant.	Enforcing the least privilege	High	identity:::protectionPolicy
RGC-GR_CONFIG_IAM_ROLE_HAS_ALL_PERMISSIONS	This policy checks whether an IAM custom policy grants the allow *:* permission. If yes, the IAM policy is considered non-compliant.	Enforcing the least privilege	Low	identity:::role
RGC-GR_CONFIG_IAM_USER_MFA_ENABLED	This policy checks whether MFA is enabled for an IAM user. If not, the user is considered non-compliant.	Enforcing the least privilege	Medium	identity:::user

Relational Database Service (RDS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_RDS_INSTANCE_NO_PUBLIC_IP	This policy checks whether a public IP address is bound to an RDS instance. If yes, the instance is considered non-compliant.	Controlling network access	High	rds:::instance

Elastic Volume Service (EVS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VOLUME_UNUSED_CHECK	This policy checks whether an EVS disk is attached to a cloud server. If not, the EVS disk is considered non-compliant.	Optimizing costs	High	evs:::volume

 Copyright © Huawei Technologies Co., Ltd.

Virtual Private Cloud (VPC)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VPC_SG_PORTS_CHECK	This policy 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. If yes, the security group is considered non-compliant.	Controlling network access	High	networking::: secgroup
RGC-GR_CONFIG_VPC_DEFAULT_SG_CLOSED	This policy checks whether the default security group of a VPC allows inbound or outbound traffic. If yes, the default security group is considered non-compliant.	Controlling network access	High	networking::: secgroup
RGC-GR_CONFIG_VPC_FLOW_LOGS_ENABLED	This policy checks whether flow logs are enabled for a VPC. If not, the VPC is considered non-compliant.	Establishing logging and monitoring	Medium	vpc:::flowLog

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_VPC_SG_RESTRICTED_SSH	This policy 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. If yes, the security group is considered non-compliant.	Controlling network access	High	networking::: secgroup

Cloud Container Engine (CCE)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CCE_ENDPOINT_PUBLIC_ACCESS	This policy checks whether a public IP address is bound to a CCE cluster. If yes, the CCE cluster is considered non-compliant.	Controlling network access	Medium	cce:::cluster

 Copyright © Huawei Technologies Co., Ltd.

Cloud Search Service (CSS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_CSS_CLUSTER_HTTPS_REQUIRED	This policy checks whether HTTPS access is enabled for a CSS cluster. If not, the cluster is considered non-compliant.	Encrypting data in transit	Medium	css:::cluster

Data Warehouse Service (DWS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_DWS_ENABLE_LOG_DUMP	This policy checks whether log dump is enabled for a DWS cluster. If not, the cluster is considered non-compliant.	Establishing logging and monitoring	Medium	dws:::cluster

Elastic Cloud Server (ECS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_INSTANCE_NO_PUBLIC_IP	This policy checks whether a public IP address is bound to an ECS. If yes, the ECS is considered non-compliant.	Controlling network access	Medium	compute:::instance

 Copyright © Huawei Technologies Co., Ltd.

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ECS_MULTIPLE_PUBLIC_IP_CHECK	This policy checks whether multiple public IP addresses are bound to an ECS. If yes, the ECS is considered non-compliant.	Controlling network access	Low	compute:::instance

Elastic Load Balance (ELB)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_ELB_TLS_HTTPS_LISTENERS_ONLY	This policy checks whether HTTPS is configured for any listener of a load balancer. If not, the load balancer is considered non-compliant.	Encrypting data in transit	Medium	elb:::listener

MapReduce Service (MRS)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_MRS_CLUSTER_NO_PUBLIC_IP	This policy checks whether a public IP address is bound to an MRS cluster. If yes, the cluster is considered non-compliant.	Controlling network access	Medium	mrs:::cluster

API Gateway (APIG)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_API_INSTANCES_EXECUTION_LOGGING_ENABLED	This policy checks whether a dedicated API gateway is configured with access logs. If not, the gateway is considered non-compliant.	Establishing logging and monitoring	Medium	apig:::instance
RGC-GR_CONFIG_API_INSTANCES_AUTHORIZATION_TYPE_CONFIGURED	This policy checks whether security authentication is provided for a dedicated API gateway. If not, the gateway is considered non-compliant.	Encrypting data in transit	Medium	apig:::instance
RGC-GR_CONFIG_API_INSTANCES_SSL_ENABLED	This policy checks whether any domain name of a dedicated API gateway is associated with an SSL certificate. If not, the gateway is considered non-compliant.	Encrypting data in transit	Medium	apig:::instance

 Copyright © Huawei Technologies Co., Ltd.

FunctionGraph

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_FUNCTION_GRAPH_PUBLIC_ACCESS_PROHIBITED	This policy checks whether functions in FunctionGraph allow public access. If yes, the functions are considered non-compliant.	Controlling network access	Critical	fgs:::function

Simple Message Notification (SMN)

Policy Name	Function	Scenario	Severity	Resource
RGC-GR_CONFIG_SMN_LTS_ENABLE	This policy checks whether event analysis is enabled for an SMN topic. If not, the topic is considered non-compliant.	Establishing logging and monitoring	Medium	smn:::topic

5.2.3 Elective Governance Policies

None

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.

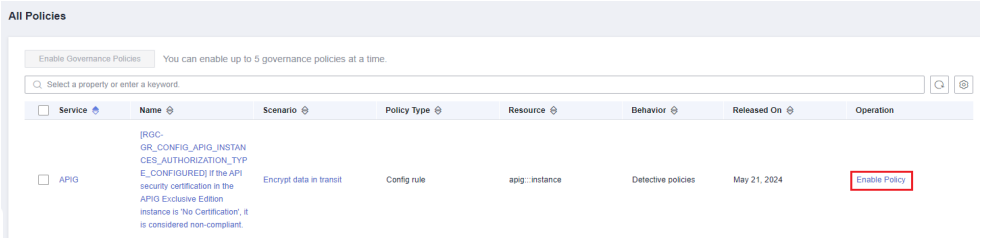
Enabling a Governance Policy

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.

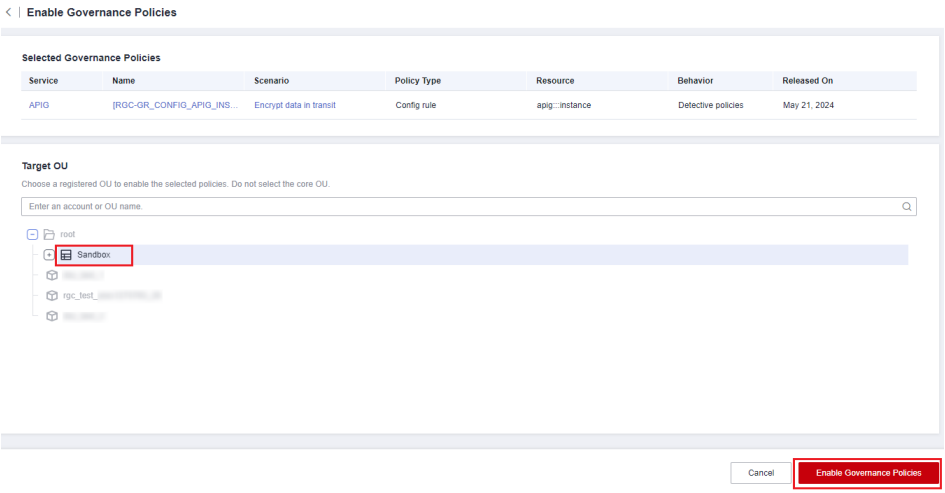
Step 3 Click **Enable Policy** in the **Operation** column.

Figure 5-1 Enabling a governance policy



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

Figure 5-2 Selecting an 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.

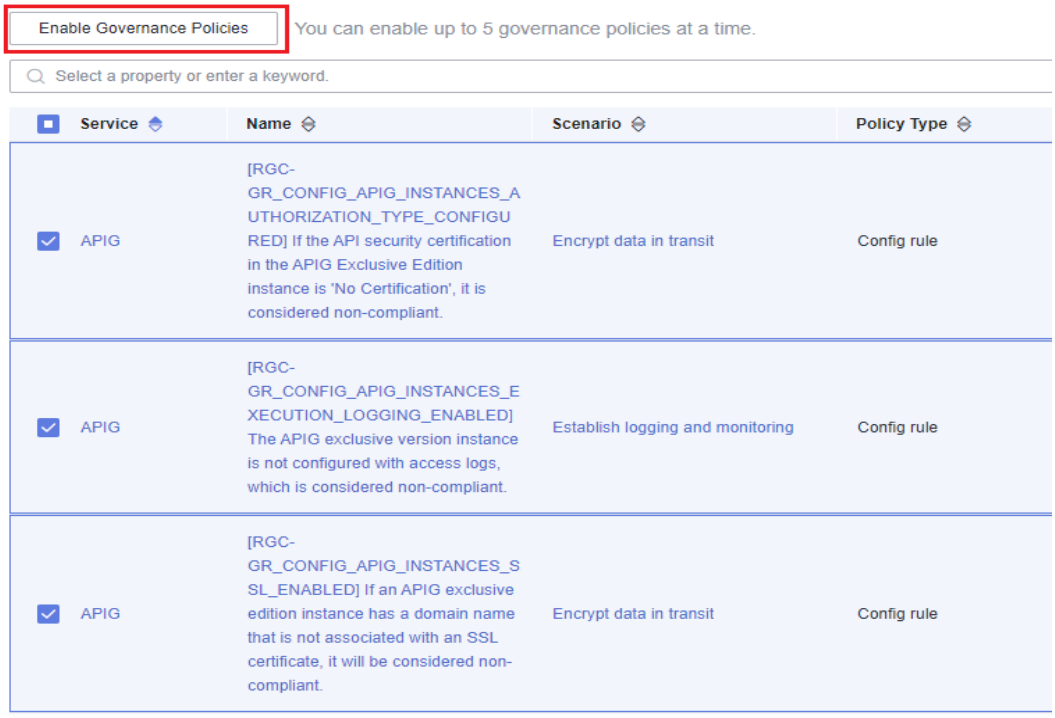
Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

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

Copyright © Huawei Technologies Co., Ltd.

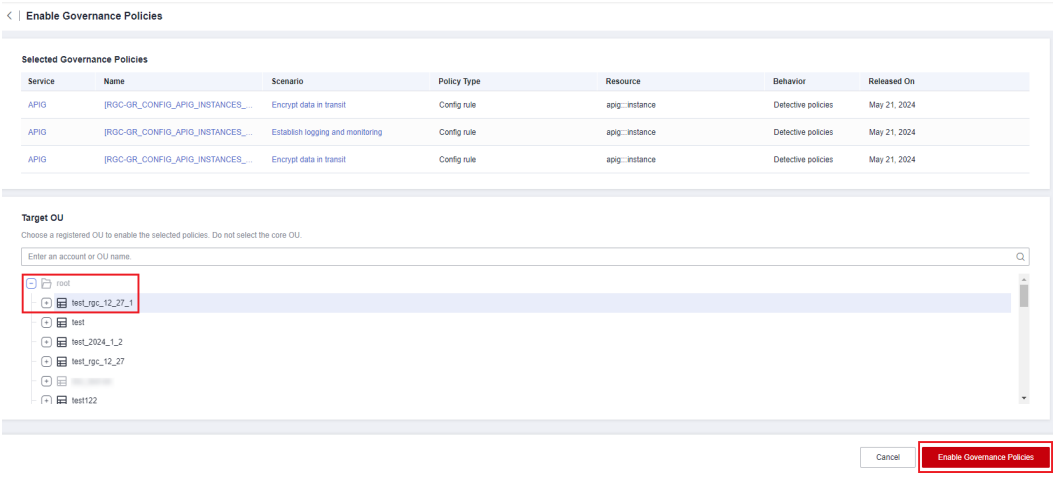
Step 3 Click **Enable Governance Policies** above the policy list.

Figure 5-3 Enabling governance policies in batches



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

Figure 5-4 Selecting an OU



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.

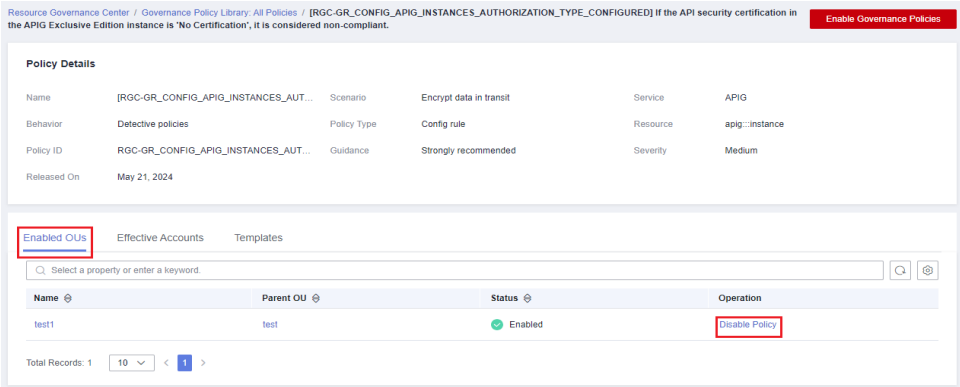
Copyright © Huawei Technologies Co., Ltd.

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 from which you want to disable this policy.

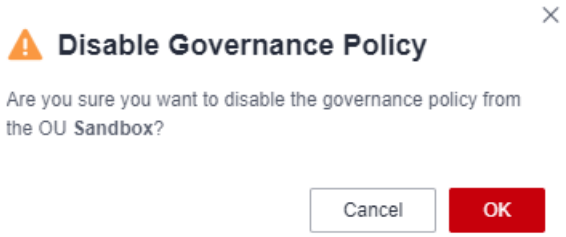
Figure 5-5 Disabling a governance policy



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



----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.
Policy Owner	The cloud service that owns and maintains the governance policy.
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.
Framework	The industry-standard compliance framework that the governance policy helps to enforce.
Severity	The relative risk associated with any violation of the governance policy.
Service	The service to which the governance policy applies.
Implementation	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

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2024-01-30	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.