

Resource Governance Center

Getting Started

Issue 01
Date 2024-01-30



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.

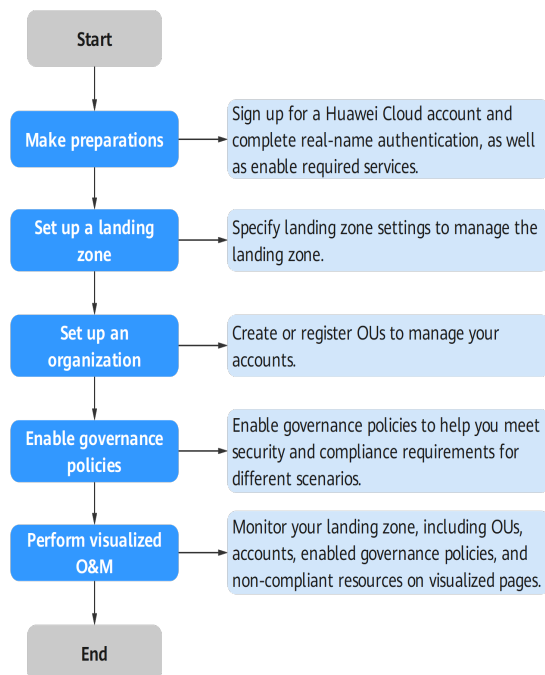
Contents

1 Flowchart.....	1
2 Preparations.....	2
3 Setting Up and Enabling a Landing Zone.....	3
4 Using Governance Policies to Manage Your Landing Zone.....	9
5 Change History.....	12

1 Flowchart

Figure 1-1 shows the flowchart for using RGC.

Figure 1-1 Flowchart for using RGC



2 Preparations

Before using RGC, you need to prepare as described in the following sections:

- [Signing Up for a HUAWEI ID and Completing Real-name Authentication](#)
- [Enabling Enterprise Center](#)

Signing Up for a HUAWEI ID and Completing Real-name Authentication

If you already have a HUAWEI ID, you can skip this part. If you do not have a HUAWEI ID, perform the following operations:

1. Visit <https://www.huaweicloud.com/intl/en-us/> and click **Sign Up**.
2. Complete your sign-up as prompted. For details, see . .

After the registration is successful, the system redirects you to your personal information page.

3. Complete real-name authentication by referring to [Enterprise Real-Name Authentication](#).

NOTE

RGC is a free service, but you will still be billed for any billable services, such as SMN and OBS.

Enabling Enterprise Center

Before enabling RGC, you need to enable Enterprise Center and become the management account of your organization. Do as follows:

Step 1 Go to the Enterprise Center console.

Step 2 Click **Enable for Free**. The **Enable Enterprise Center** page is displayed.

Step 3 Select **I have read and agree to the HUAWEI CLOUD Enterprise Management Service Agreement** and click **Enable for Free**. Your account will become an enterprise master account. For details, see [Enabling Enterprise Center](#).

----End

3 Setting Up and Enabling a Landing Zone

Background

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 in RGC.

Prerequisites

The current account has enable Enterprise Center. For details, see [Enabling Enterprise Center](#).

Setting Up a Landing Zone

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

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

Step 3 Click **Enable**.

Figure 3-1 Enabling RGC

You have not set up a landing zone.



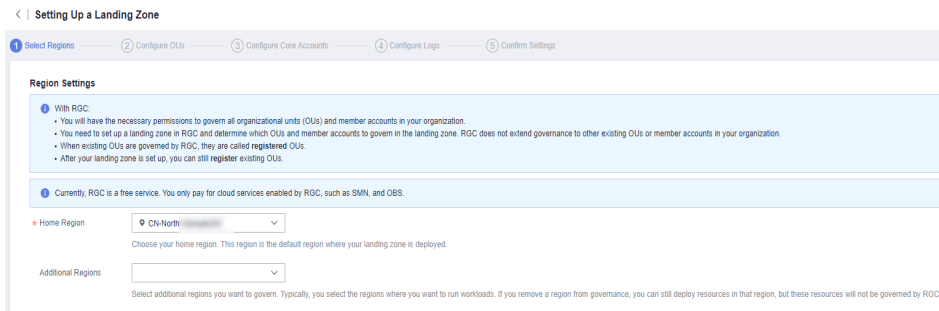
Resource Governance Center

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.



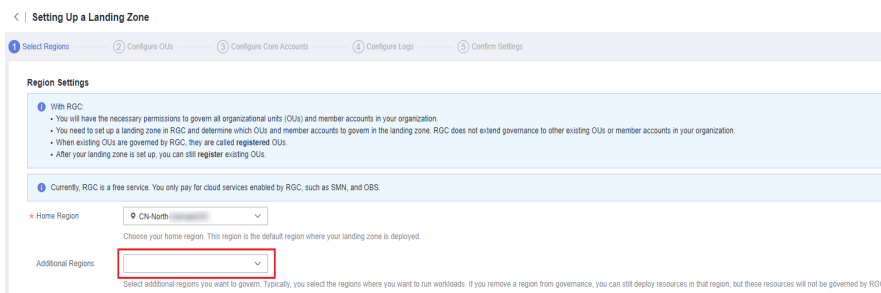
Step 4 Select the home region for RGC. The region will be regarded as the default region to set up your landing zone.

Figure 3-2 Selecting the home region



Step 5 (Optional) Select additional regions to be governed in addition to the home region. After the regions are selected, resources in the regions will also be governed by RGC.

Figure 3-3 Selecting additional regions



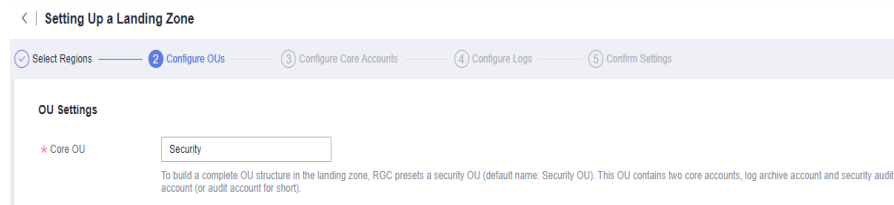
Step 6 Click **Next**.

Step 7 Under **OU Settings**, specify the name for the core OU.

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).

Ensure that the OU name is unique. You are not allowed to change the name once your landing zone is set up.

Figure 3-4 Configuring the core OU

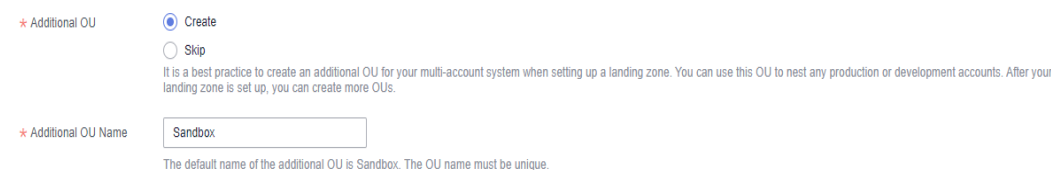


Step 8 Determine whether to create additional OUs.

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.

- **Create:** Create an additional OU while you are setting a landing zone. The OU name must be unique. The default name of the additional OU is **Sandbox**.
- **Skip:** If you choose this option, you will have 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 3-5 Creating an additional OU



Step 9 Click **Next**.

Step 10 On the **Configure Core Accounts** page, configure the management account. Enter the IAM Identity Center email address. 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.

Figure 3-6 Configuring the management account



Step 11 Configure a log archive account. It is used to store logs of API activities and resource configurations from all accounts.

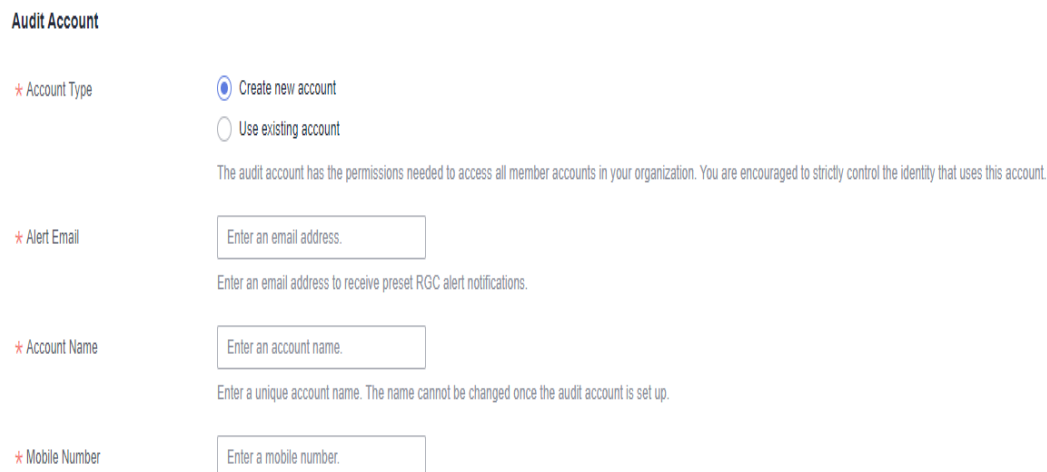
- **Account Type:** You can create an account or use an existing account. The existing account you want to use must belong to the same organization as the management account.

- **Account Name:** Enter the name of the log archive account. Ensure that the name is unique. You are not allowed to change the name once your landing zone is set up. The account name can only contain digits, letters, underscores (_), and hyphens (-), but cannot start with a digit. It can have from 6 to 30 characters.
- **Account ID:** If you choose to use an existing account, enter the ID of the Huawei Cloud account you registered. The account ID cannot be the ID of the management account or of a member account in another organization.

Step 12 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.

- **Account Type:** You can create an account or use an existing account. The existing account must belong to the same organization as the management account.
- **Alert Email:** Enter the email address of the audit account. It is used to receive alarm notifications preset by RGC. The 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 audit account. Ensure that the name is unique. You are not allowed to change the name once your landing zone is set up. The account name can only contain digits, letters, underscores (_), and hyphens (-), but cannot start with a digit. It can have from 6 to 30 characters.
- **Account ID:** If you choose to use an existing account, enter the ID of the Huawei Cloud account you registered. The account ID cannot be the ID of the management account or of a member account in another organization.

Figure 3-7 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 to receive preset RGC alert notifications.

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

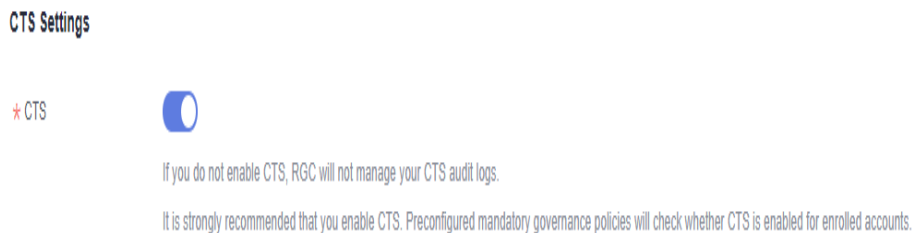
* Mobile Number

Step 13 Click **Next**.

Step 14 and 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 3-8 Enabling CTS



Step 15 Configure the OBS bucket retention for your logs. Logs are automatically stored in the two default OBS buckets, and you are not allowed to rename them.

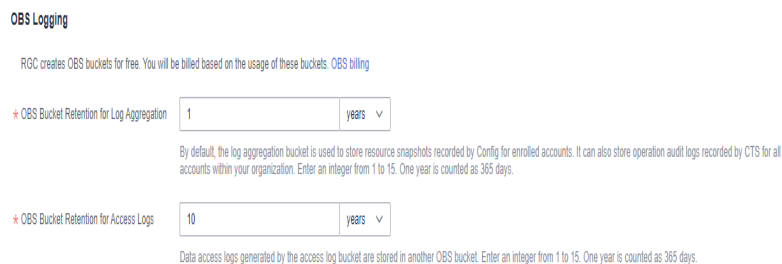
- **OBS Bucket Retention for Log Aggregation:** The default period is one year, but you can change this to up to 15 years.

The configuration snapshots of Config resource recorder and the CTS operation auditing logs are stored in the bucket **rgcservice-managed-audit-logs-*{management account ID}***.

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

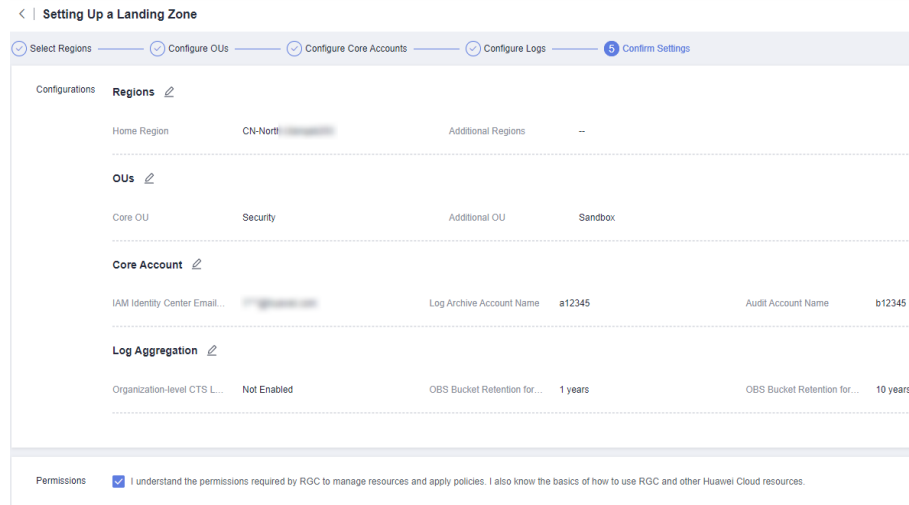
The logs for accessing the log aggregation bucket are stored in the bucket **rgcservice-managed-access-logs-*{management account ID}***.

Figure 3-9 Configuring the OBS bucket retention for logging



Step 16 Review and confirm the landing zone settings, and then select **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.**

Figure 3-10 Confirming the landing zone settings



Step 17 Click **Set Up Landing Zone**.

----End

Follow-up Operations

Deploy and manage existing OUs and member accounts. For details, see [Organization Management](#).

4 Using Governance Policies to Manage Your Landing Zone

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.

You need to register the OUs created in an organization before applying governance policies to them.

Preventive governance policies apply to all member accounts in the OUs, regardless of their enrollment status. Detective governance policies apply only to enrolled accounts.

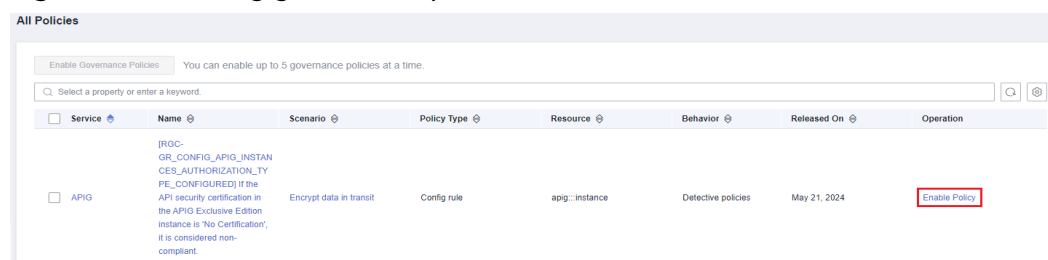
Constraints

- 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

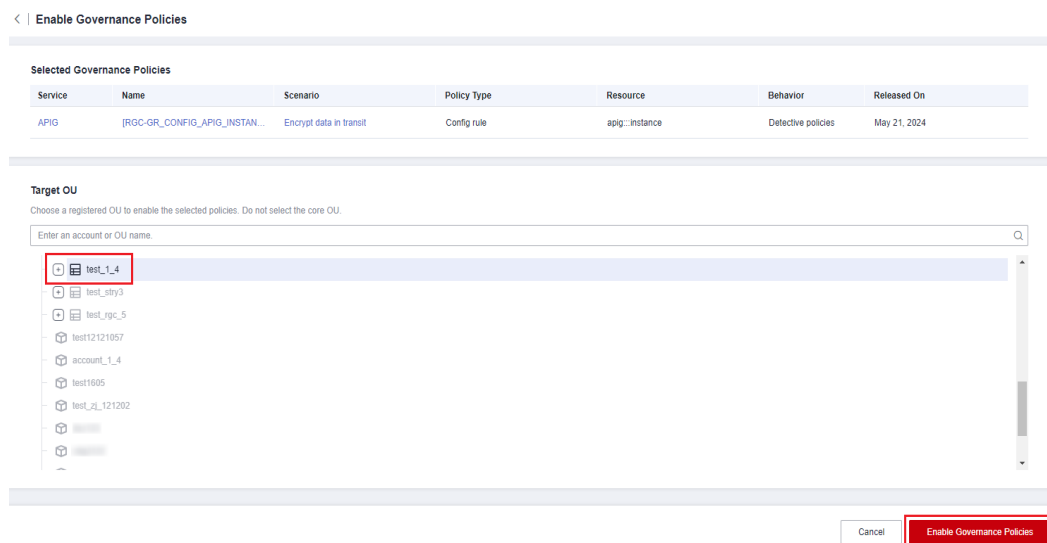
- Step 1** Log in to Huawei Cloud using the management account, and navigate to the RGC console.
- Step 2** Choose **Governance Policy Library > All Policies**. In the policy list, locate the governance policy you want to enable.
- Step 3** Click **Enable Policy** in the **Operation** column.

Figure 4-1 Enabling governance policies



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

Figure 4-2 Selecting an OU



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

----End

Viewing How a Governance Policy Is Applied

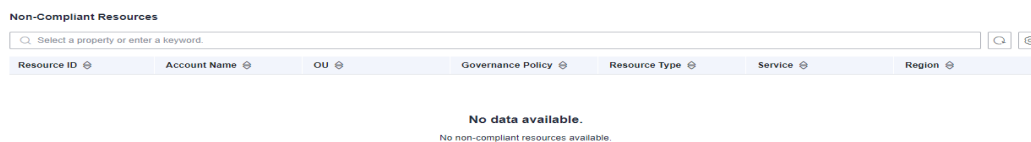
Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

Step 2 On the **Dashboard** page, view information about **OUs and Accounts, Enabled Governance Policies, Non-Compliant Resources, Registered OUs, and Enrolled Accounts** in your landing zone.

Step 3 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 4-3 Non-compliant resources



----End

Disabling a Governance Policy

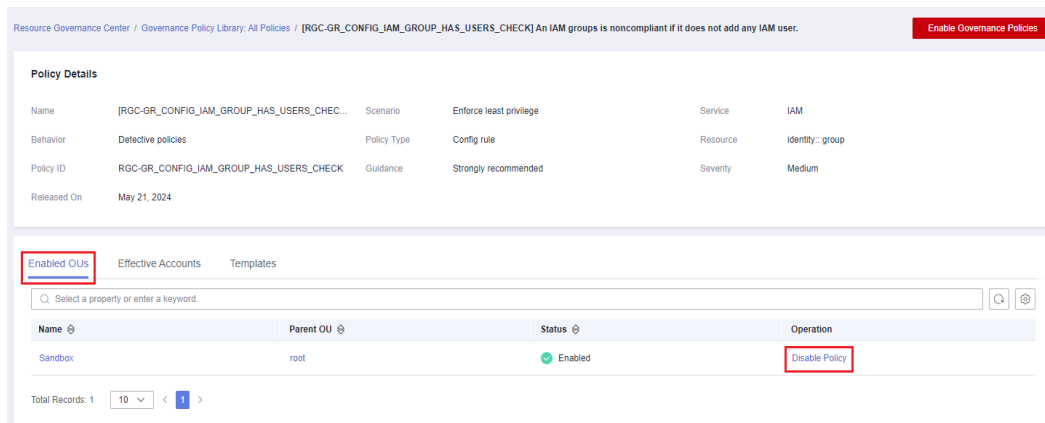
Step 1 Log in to Huawei Cloud using the management account, and navigate to the RGC console.

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 from which you want to disable this policy.

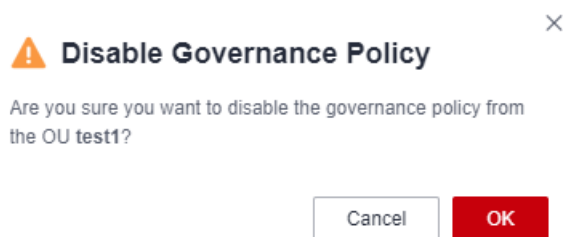
Figure 4-4 Disabling a governance policy



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

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

Figure 4-5 Disabling a governance policy



-----End

5 Change History

Released On	Change History
2023-12-22	This issue is the first official release.