# Resource Governance Center

# Service Overview

**Issue** 03

**Date** 2025-08-05

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

# Contents



# 1 What Is Resource Governance Center?

Resource Governance Center (RGC) offers an easy way to set up and govern a secure, scalable multi-account cloud environment. With RGC, you can:

- Automatically build a basic landing zone to manage your organization and quickly migrate services to the cloud.
- Configure governance policies for your basic landing zone to quickly and conveniently meet cloud governance requirements.
- Use an existing **Infrastructure as Code (IaC)** template to quickly create and configure accounts in the account factory. This ensures consistent account and resource configurations and rapid deployment and launch of new applications.
- Enable governance checks to see if your existing multi-account environment adheres to Landing Zone best practices, even if you have not set up a landing zone through RGC.

## Billing

RGC is a free service, but you may be billed for services, such as Simple Message Notification (SMN) and Object Storage Service (OBS), based on your usage. For details, see **SMN Billing** and **OBS Billing**.

# 2 Application Scenarios

RGC helps you quickly set up and govern a multi-account cloud environment. It can be used in the following scenarios:

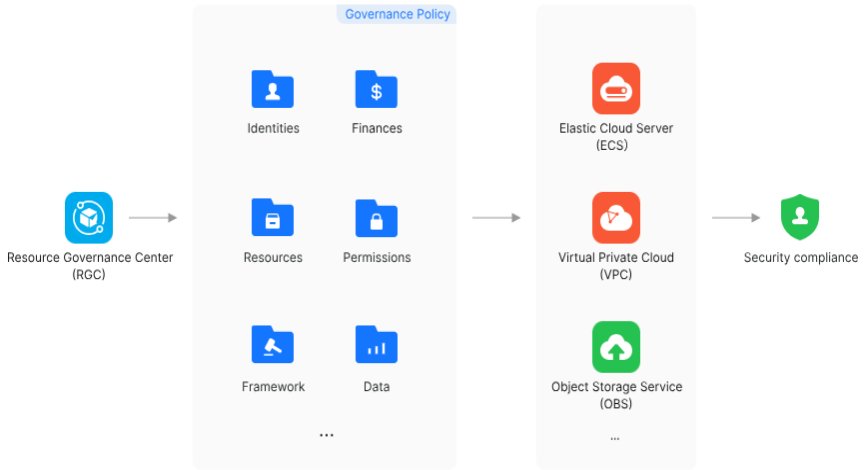
## Automatically Deploying a Landing Zone

A secure, scalable multi-account environment is a prerequisite for secure and convenient cloud migration of enterprise services. RGC automatically deploys a landing zone on Huawei Cloud to accelerate cloud adoption.

## Preventing and Detecting Non-Compliant Operations in an Organization

Governance compliance is critical to cloud migration. Each enterprise imposes governance compliance regulations on their own members. To help you meet these compliance requirements, RGC provides scenario-specific policy packages for you to flexibly select and quickly deploy.

**Figure 2-1** Preventing and detecting non-compliant operations in an organization




## Quickly Deploying and Launching New Applications

Generally, an enterprise has a wide range of service modules and applications. Once a landing zone is set up, you can start migrating applications to the cloud.

To help you do this faster, RGC offers you predefined account configurations that make it easier to create and configure new accounts, so you can launch your applications faster.

# 3 Functions

Before using RGC, you are advised to learn basic concepts about account factory and governance policies so you have a better understanding of the functions provided by RGC.

## Automated Environment Deployment

You can use RGC to automatically set up a multi-account landing zone following best practices. In your landing zone, you will have one management account and two core accounts (an audit account and a log archive account). Also you are provided with organization-wide single sign-on (SSO) access as well as centralized logging and auditing capabilities.

## Account Factory

In the account factory, you can create member accounts under a specified organizational unit (OU), and baseline configurations will be automatically applied to your accounts based on best practices.

## Governance Policies

You can flexibly select scenario-specific compliance packages and enable preventive and detective governance policies to meet enterprise compliance requirements.

## Customized Account Provisioning

RGC provides a framework for flexible account customization. When you create a member account or select an existing member account, you can use a custom IaC template to create custom account configurations.

## Dashboard

You can monitor governance policies, organization-level resource compliance, and organizational structure in real time, as well as monitor the compliance status of your landing zone.

## Landing Zone Governance Check

You can enable Landing Zone governance checks to see if your multi-account cloud environment adheres to the best practices for Landing Zone. The check results serve as a reference for you to optimize costs and improve security and operational efficiency.

# 4 Notes and Constraints

## Constraints

- For details about constraints on Organizations, see **Notes and Constraints**.
- Each organization administrator account can only enable RGC in one home region.

## Supported Regions

You can use RGC to set up landing zones in the following regions:

CN-Hong Kong, LA-Mexico City2, LA-Santiago, LA-Sao Paulo1, AP-Bangkok, AF-Johannesburg, AP-Singapore, AP-Jakarta, AP-Manila, ME-Riyadh, and TR-Istanbul

# 5 Basic Concepts

## IaC

Infrastructure as Code (IaC) is the ability to provision and manage your computing infrastructure using code instead of manual processes.

## Landing Zone

Landing Zone is short for basic multi-account environment that is initially deployed by RGC and complies with the best practice.

## Account

An account functions as a resource container and resource isolation boundary. An account in RGC refers to a Huawei Cloud account.

## Management Account

A management account is the account you used to enable the Organizations service.

You can use the management account to create and manage your multi-account cloud architecture, as well as to manage organization-wide policies.

## Member Account

A member account is the account you created or invited to join your organization via the Organizations service.

Member accounts are used to deploy and manage services or application resources.

## Organization

An organization is an entity you create to manage multiple accounts. Each organization is composed of one management account, multiple member accounts, a root OU, and 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.

## Root OU

After you enable Organizations and create an organization, Organizations automatically generates the root OU. The root OU is located at the top of the organizational tree, and the branches representing other OUs and accounts reach down.

## OU

An organizational unit (OU) is 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.

## Multi-Account Environment

A multi-account environment is a cloud architecture for organizations or enterprises. It consists of one management account and multiple member accounts.

## Best Practices

Best practices are the proven architectures, processes, or methods that produce the best results. In RGC, best practices refer to the cloud service configurations that ensure a secure, scalable multi-account environment.

## Basic Environment

A basic environment is a multi-account cloud environment that is initially deployed by RGC, following best practices. In this environment, there are one management account and two member accounts (an audit account and a log archive account). This environment is preconfigured with organization-wide SSO access as well as centralized logging and auditing capabilities.

## Account Enrollment

Account enrollment means RGC enrolls accounts that are not created in RGC. When an account is enrolled in RGC, RGC applies the best practices to that account.

## Templates

A template is an HCL-formatted text file that describes your cloud resources. Its format can be .tf, .tf.json, or .zip.

## Governance Policies

Governance policies refer to rules predefined for continuous governance of multi-account environments on the cloud.

## Service Control Policies

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The organization management account can use SCPs to limit which permissions can be assigned to member accounts to ensure that they stay within your organization's access control guidelines. SCPs can be attached to an organization, OUs, and member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU.