Resource Governance Center

API Reference

Issue	01
Date	2025-02-20

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Before You Start

Welcome to *Resource Governance Center API Reference*. Resource Governance Center (RGC) offers an easy way to set up and govern a secure and scalable multi-account environment. You can use RGC to create a landing zone that contains one management account and multiple member accounts, and configure auto guardrails for these accounts. This helps you quickly and securely migrate services to the cloud.

This document describes how to use application programming interfaces (APIs) to perform operations on RGC, such as creating, deleting, modifying, and querying. For details about all supported operations, see **2 API Overview**.

If you plan to access RGC through an API, ensure that you are familiar with RGC concepts. For details, see **Resource Governance Center Service Overview**.

Endpoints

An endpoint is the request address for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

Concepts

- Account

  An account is created upon successful registration with Huawei Cloud. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity, which should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

  An IAM user is created by an account to use cloud services. Each IAM user has their own identity credentials (password or access keys).

  The account name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service

(EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

For details, see **Region and AZ**.

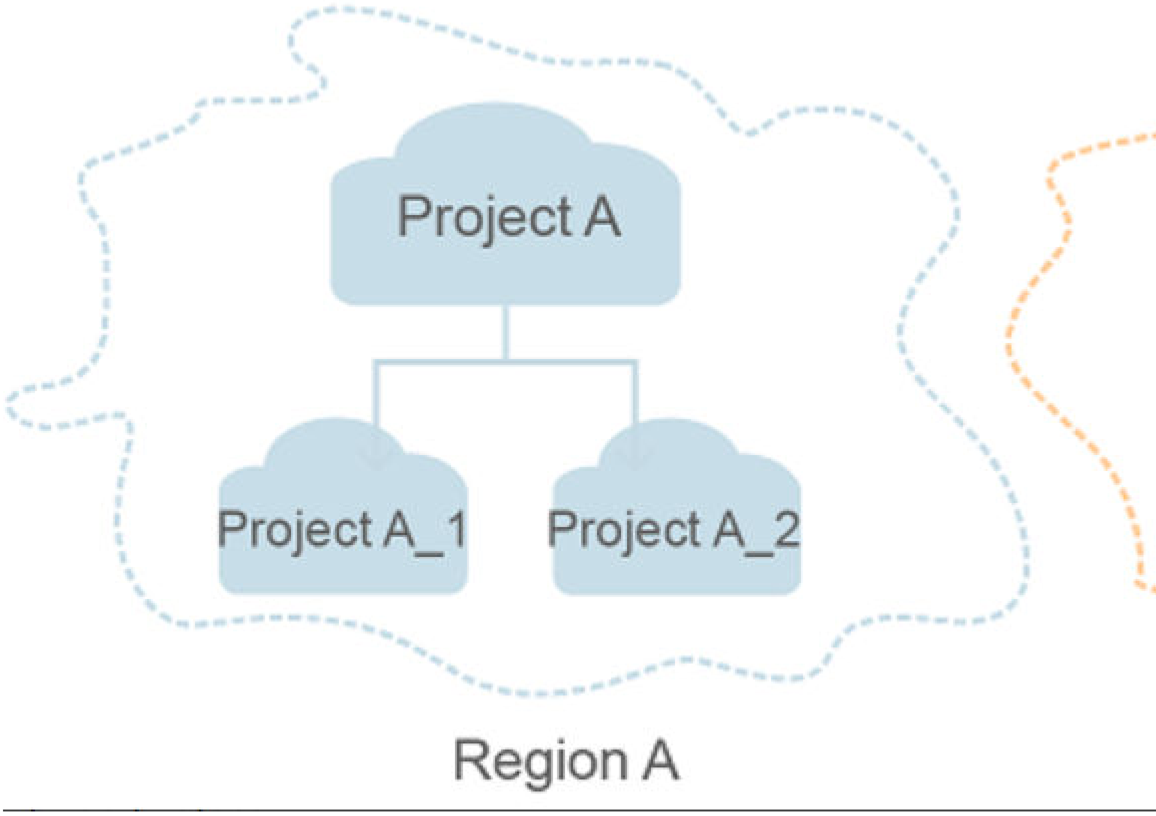
- AZ

  An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected by optical fibers for high-availability networking.

- Project

  A project corresponds to a region. Default projects are defined to group and physically isolate resources (including compute, storage, and network resources) across regions. Users can be granted permissions in a default project to access all resources under their accounts in the region associated with the project. If you need more refined access control, create subprojects under a default project and create resources in subprojects. Then you can assign users the permissions required to access only the resources in the project.

Figure 1-1 Project isolating model



- Enterprise project

  Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

For details about enterprise projects and about how to obtain enterprise project IDs, see **Enterprise Management User Guide**.

2 API Overview

Type	Subtype	Description
Organization Management	Registering an OU	Registers an OU in an organization with RGC.
	Querying registration information	Queries the registration or deregistration information in RGC.
	Querying an enrolled account	Queries an organization account that is enrolled in RGC.
	Creating an account	Creates an account in a registered OU of an organization.
Landing Zone Governance	Enabling a governance policy	Enables a governance policy for an OU in an organization.
	Disabling a governance policy	Disables a governance policy from an OU in an organization.
	Querying the status of a governance policy	Queries the status of an operation by operation ID.
	Listing governance policies enabled for a registered OU	Lists all governance policies enabled for a registered OU in an organization.
	Listing enabled governance policies	Lists governance policies enabled for an organization.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request and uses the RGC API for **querying the governance policy status** as an example to demonstrate how to call an API.

Request URI

A request URI is in the following format:

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

Table 3-1 Parameter description

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints** .
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the resource-path of the API for **querying the governance policy status** is **/v1/governance/operation-control-status/{operation_control_status_id}**, where operation_control_status_id represents the operation ID for enabling or disabling a governance policy.
query-string	An optional query parameter. Ensure that a question mark (?) is included before each query parameter that is in the format of *Parameter name*=*Parameter value*. For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to query the status of a governance policy enabled in the **CN North-Beijing4** region, obtain the endpoint (rgc.cn-north-4.myhuaweicloud.com) for this region and the resource-path (/v1/governance/operation-control-status/{operation_control_status_id}) in the URI of the API used to **query the governance policy status**. Then, construct the URI as follows:

```
https://rgc.cn-north-4.myhuaweicloud.com/v1/governance/operation-control-status/
{operation_control_status_id}
```

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: requests the server to return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API for **querying the governance policy status**, the request method is **GET**. The request is as follows:

```
GET https://rgc.cn-north-4.myhuaweicloud.com/v1/governance/operation-control-status/
{operation_control_status_id}
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request headers are as follows:

Table 3-2

Header	Description	Mandatory
Content-Type	Request body type or format. Its default value is **application/json**. Other values of this field will be provided for specific APIs.	Yes
Authorization	Signature information in the request. For details about AK/SK authentication, see **AK/SK-based Authentication**.	Yes
Host	Host address, for example, rgc.cn-north-4.myhuaweicloud.com.	Yes
X-Sdk-Date	Date and time when the request was sent, for example, **20221107T020014Z**.	Yes

NOTE

APIs support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request. For more information, see **AK/SK-based Authentication**.

For example, the request for the API in **4.2.3 Querying the Operating Status of a Governance Policy** is as follows:

```
GET https://rgc.cn-north-4.myhuaweicloud.com/v1/governance/operation-control-status/c0jquihv-x3ve-1lb9-
qmix-dankod8dg86z
Content-Type: application/json; charset=UTF-8
X-Sdk-Date: 20240527T021902Z
Host: rgc.cn-north-4.myhuaweicloud.com
Authorization: SDK-HMAC-SHA256 Access=xxxxxxxxxxxxxxxxxxx, SignedHeaders=content-type;host;x-sdk-
date, Signature=xxxxxxxxxxxxxxxxxxxx
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

Initiating a Request

You can send the request to call an API through **curl**, **Postman**, or coding.

3.2 Authentication

AK/SK authentication is used for calling APIs. Specifically, requests are encrypted using the access key ID (AK) and secret access key (SK) to provide higher security.

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the request headers for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or using the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Request Signing Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 2*xx* (indicating successes) to 4*xx* or 5*xx* (indicating errors). It indicates the status of a request. For more information, see **6.1 Status Codes**.

Response Header

Similar to a request, a response also has a header, for example, **Content-type**.

Table 3-3 describes common response headers.

Table 3-3 Common response headers

Header	Description
Content-Type	Type of the resource content. Type: string Default value: none
Connection	Whether the connection to the server is a long connection or a short connection. Type: string Valid values: keep-alive | close Default value: none
Date	Date when the RGC service responded to the request. Type: string Default value: none
X-Request-Id	Unique identifier of the request. The value is generated by the RGC service and can be used for troubleshooting. Type: string Default value: none

Response Body

The body of a response is often returned in structured format as specified in the **Content-type** header. The response body transfers content except the response header.

The following is the response body for the API in **4.2.3 Querying the Operating Status of a Governance Policy**.

```
{
 "control_operation": {
  "operation_control_status_id": "c0jquihv-x3ve-1lb9-qmix-dankod8dg86z",
  "operation_type": "ENABLE_CONTROL",
  "status": "SUCCEEDED",
  "message": "",
  "start_time": "2024-04-19T16:26:30.518",
  "end_time": "2024-04-19T16:26:30.618"
 }
}
```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{
    "error_msg": "error msg",
    "error_code": "APIGW.0301",
    "request_id": "string"
}
```

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 APIs

4.1 Managing Organizations

4.1.1 Registering an OU

Function

This API is used to register an OU in an organization with RGC.

URI

POST https://{endpoint}/v1/managed-organization/organizational-units/{organizational_unit_id}/register

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
organizational_unit_id	Yes	String	ID of a registered OU.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-2 Response body parameters

Parameter	Type	Description
organizational_unit_operation_id	String	Operation ID of the asynchronous APIs.

Status code: 403

Table 4-3 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-4 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Registering an OU in an organization with RGC

```
POST https://{endpoint}/v1/managed-organization/organizational-units/{organizational_unit_id}/register
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "organizational_unit_operation_id" : "string"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.1.2 Querying Registration Information

Function

This API is used to query the registration and deregistration information in RGC.

URI

GET https://{endpoint}/v1/managed-organization/{operation_id}

Table 4-5 Path Parameters

Parameter	Mandatory	Type	Description
operation_id	Yes	String	Operation ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-6 Response body parameters

Parameter	Type	Description
operation_id	String	Operation ID.
percentage_complete	Integer	Percentage of completion.
status	String	Status

Copyright © Huawei Technologies Co., Ltd.

Parameter	Type	Description
percentage_details	Array of **OrganizationalPercentageDetail** objects	Details about the progress of creating and managing accounts and registering OUs.
message	String	Error messages displayed when creating and managing accounts and registering OUs.

Table 4-7 OrganizationalPercentageDetail

Parameter	Type	Description
percentage_name	String	Progress name.
percentage_status	String	Progress of creating and managing accounts and registering OUs.

Status code: 403

Table 4-8 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-9 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Querying the registration and deregistration information in RGC

```
GET https://{endpoint}/v1/managed-organization/{operation_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "operation_id" : "string",
  "percentage_complete" : 0,
  "status" : "string",
  "percentage_details" : [ {
    "percentage_name" : "string",
    "percentage_status" : "string"
  } ],
  "message" : "string"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.1.3 Querying a Managed Account

Function

This API is used to query an organization account that is managed by RGC.

URI

GET https://{endpoint}/v1/managed-organization/managed-accounts/{managed_account_id}

Table 4-10 Path Parameters

Parameter	Mandatory	Type	Description
managed_account_id	Yes	String	ID of a managed account.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-11 Response body parameters

Parameter	Type	Description
landing_zone_version	String	Version of the landing zone.
manage_account_id	String	ID of a managed account.
account_id	String	ID of a managed account.
account_name	String	Name of a managed account.
account_type	String	Type of a managed account.
owner	String	Source where a managed account was created. It can be CUSTOM or RGC.
state	String	Status of a managed account.
message	String	Description of the error status.
parent_organizational_unit_id	String	ID of a registered parent OU.
parent_organizational_unit_name	String	Name of a registered parent OU.
identity_store_user_name	String	Name of an IAM Identity Center user.
blueprint_product_id	String	Template ID.
blueprint_product_version	String	Template version.
blueprint_status	String	Template deployment status. It can be failed, completed, or processing.
is_blueprint_has_multi_account_resource	Boolean	Whether the template contains multi-account resources.
regions	Array of **regionManagedList** objects	Region information.

Parameter	Type	Description
created_at	String	When a managed account was created under a registered OU in an organization.
updated_at	String	Last time when a managed account under a registered OU in an organization was updated.

Table 4-12 regionManagedList

Parameter	Type	Description
region	String	Region name.
region_status	String	Region status. It can be available or unavailable.

Status code: 403

Table 4-13 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-14 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Querying an organization account that is managed by RGC

```
GET https://{endpoint}/v1/managed-organization/managed-accounts/{managed_account_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "manage_account_id" : "string",
  "account_id" : "string",
  "account_name" : "string",
  "account_type" : "string",
  "owner" : "string",
  "state" : "string",
  "message" : "string",
  "parent_organizational_unit_id" : "string",
  "parent_organizational_unit_name" : "string",
  "identity_store_user_name" : "string",
  "blueprint_product_id" : "string",
  "blueprint_product_version" : "string",
  "blueprint_status" : "string",
  "is_blueprint_has_multi_account_resource" : "boolean",
  "regions" : [ {
    "region" : "string",
    "region_status" : "string"
  } ],
  "created_at" : "2023-11-15T07:32:12.283Z",
  "updated_at" : "2023-11-15T07:32:12.283Z"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.1.4 Creating an Account

Function

This API is used to create an account in a registered OU of an organization.

URI

POST https://{endpoint}/v1/managed-organization/managed-accounts

Request Parameters

Table 4-15 Request body parameters

Parameter	Mandatory	Type	Description
account_name	Yes	String	Name of a managed account.
account_email	No	String	Email address of a managed account.
phone	No	String	Mobile number.
identity_store_user_name	No	String	Name of an IAM Identity Center user.
identity_store_email	No	String	Email address used for IAM Identity Center.
parent_organizational_unit_id	Yes	String	ID of a registered parent OU.
parent_organizational_unit_name	Yes	String	Name of a registered parent OU.
blueprint	No	**Blueprint** object	Templates.

Table 4-16 Blueprint

Parameter	Mandatory	Type	Description
blueprint_product_id	No	String	Template ID.
blueprint_product_version	No	String	Template version.
variables	No	String	Parameters for template deployment.
is_blueprint_has_multi_account_resource	No	Boolean	Whether the template contains multi-account resources.

Response Parameters

Status code: 201

Table 4-17 Response body parameters

Parameter	Type	Description
operation_id	String	Operation ID for creating and managing accounts and registering OUs.

Status code: 403

Table 4-18 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-19 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an account in a registered OU of an organization

```
POST https://{endpoint}/v1/managed-organization/managed-accounts

{
  "account_name" : "string",
  "account_email" : "string",
  "phone" : "18700000000",
  "identity_store_user_name" : "string",
  "identity_store_email" : "string",
  "parent_organizational_unit_id" : "string",
  "parent_organizational_unit_name" : "string",
  "blueprint" : {
    "blueprint_product_id" : "string",
    "blueprint_product_version" : "string",
    "variables" : "string",
    "is_blueprint_has_multi_account_resource" : "boolean"
  }
}
```

Example Responses

Status code: 201

Successful

```
{
  "operation_id" : "string"
}
```

Status Codes

Status Code	Description
201	Successful
403	No permissions.

Error Codes

See **Error Codes**.

4.2 Governing the Landing Zone

4.2.1 Enabling a Governance Policy

Function

This API is used to enable a governance policy for an OU in an organization.

URI

POST https://{endpoint}/v1/governance/controls/enable

Request Parameters

Table 4-20 Request body parameters

Parameter	Mandatory	Type	Description
identifier	Yes	String	Governance policy ID.
target_identifier	Yes	String	ID of an OU.

Parameter	Mandatory	Type	Description
parameters	No	Array of **EnableControlParameters** objects	Policy parameters.

Table 4-21 EnableControlParameters

Parameter	Mandatory	Type	Description
key	Yes	String	Name of a policy parameter.
value	Yes	Object	Value of a policy parameter.

Response Parameters

Status code: 201

Table 4-22 Response body parameters

Parameter	Type	Description
control_operate_request_id	String	Operation ID of a governance policy.

Status code: 403

Table 4-23 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-24 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Enabling a governance policy for an OU in an organization

```
POST https://{endpoint}/v1/governance/controls/enable

{
  "identifier" : "string",
  "target_identifier" : "string"
}
```

Example Responses

Status code: 201

Request succeeded.

```
{
  "control_operate_request_id" : "string"
}
```

Status Codes

Status Code	Description
201	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.2.2 Disabling a Governance Policy

Function

This API is used to disable a governance policy from an OU in an organization.

URI

POST https://{endpoint}/v1/governance/controls/disable

Request Parameters

Table 4-25 Request body parameters

Parameter	Mandatory	Type	Description
identifier	Yes	String	Governance policy ID.
target_identifier	Yes	String	ID of an OU.
parameters	No	Array of **EnableControlParameters** objects	Policy parameters.

Table 4-26 EnableControlParameters

Parameter	Mandatory	Type	Description
key	Yes	String	Name of a policy parameter.
value	Yes	Object	Value of a policy parameter.

Response Parameters

Status code: 201

Table 4-27 Response body parameters

Parameter	Type	Description
control_operate_request_id	String	Operation ID of a governance policy.

Status code: 403

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.

Parameter	Type	Description
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-29 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Disabling a governance policy from an OU in an organization

```
POST https://{endpoint}/v1/governance/controls/disable

{
  "identifier" : "string",
  "target_identifier" : "string"
}
```

Example Responses

Status code: 201

Request succeeded.

```
{
  "control_operate_request_id" : "string"
}
```

Status Codes

Status Code	Description
201	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.2.3 Querying the Operating Status of a Governance Policy

Function

This API is used to query the operating status by operation ID.

URI

GET https://{endpoint}/v1/governance/operation-control-status/{operation_control_status_id}

Table 4-30 Path Parameters

Parameter	Mandatory	Type	Description
operation_control_status_id	Yes	String	Request ID for performing operations on a governance policy.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-31 Response body parameters

Parameter	Type	Description
control_operation	**ControlOperation** object	Implementation of a governance policy.

Table 4-32 ControlOperation

Parameter	Type	Description
operation_control_status_id	String	ID of an entity performing operations on a governance policy.
operation_type	String	Type of operations on a governance policy. It can be enabling or disabling operations.
status	String	Implementation status of a governance policy. It can be SUCCEEDED, FAILED, or IN_PROGRESS.

Parameter	Type	Description
message	String	Error messages about the failure to implement a governance policy.
start_time	String	Time when an operation is started.
end_time	String	Time when an operation is ended.

Status code: 403

Table 4-33 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-34 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Querying the operating status by operation ID

```
GET https://{endpoint}/v1/governance/operation-control-status/{operation_control_status_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "control_operation" : {
    "operation_control_status_id" : "string",
    "operation_type" : "string",
    "status" : "string",
    "message" : "string",
    "start_time" : "string",
    "end_time" : "string"
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.2.4 Listing Enabled Governance Policies

Function

This API is used to list all enabled governance policies in an organization.

URI

GET https://{endpoint}/v1/governance/enabled-controls

Table 4-35 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of pages that can be displayed on at once.
marker	No	String	Page marker.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-36 Response body parameters

Parameter	Type	Description
enabled_controls	Array of **EnabledControl** objects	Enabled governance policies.
page_info	**PageInfoDto** object	Number of records displayed on the current page.

Table 4-37 EnabledControl

Parameter	Type	Description
manage_account_id	String	ID of a managed account.
control_identifier	String	Governance policy ID.
name	String	Name of a governance policy.
description	String	Description of a governance policy.
control_objective	String	Pre-defined objective that the governance policy helps you enforce.
behavior	String	Type of a governance policy. A governance policy can be preventive, detective, or proactive.
owner	String	Source where a managed account was created. It can be CUSTOM or RGC.
regional_preference	String	Region options. It can be regional or global.

Table 4-38 PageInfoDto

Parameter	Type	Description
next_marker	String	Used in the marker request parameter to get the next part of the output. Repeat this operation until the response element comes back as null. If present, more output is available than that included in the current response.
current_count	Integer	Number of records displayed on the current page.

Status code: 403

Table 4-39 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-40 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Listing all enabled governance policies in an organization

```
GET https://{endpoint}/v1/governance/enabled-controls
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "enabled_controls" : [ {
    "manage_account_id" : "string",
    "control_identifier" : "string",
    "name" : "string",
    "description" : "string",
    "control_objective" : "string",
    "behavior" : "string",
    "owner" : "string",
    "regional_preference" : "string"
  } ],
  "page_info" : {
    "next_marker" : "string",
    "current_count" : 0
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

4.2.5 Listing Governance Policies Enabled for a Registered OU

Function

This API is used to list all governance policies enabled for a registered OU in an organization.

URI

GET https://{endpoint}/v1/governance/managed-organizational-units/{managed_organizational_unit_id}/controls

Table 4-41 Path Parameters

Parameter	Mandatory	Type	Description
managed_organizational_unit_id	Yes	String	ID of a registered OU.

Table 4-42 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of pages that can be displayed on at once.
marker	No	String	Page marker.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-43 Response body parameters

Parameter	Type	Description
control_summaries	Array of **TargetControl** objects	Summary of governance policies.
page_info	**PageInfoDto** object	Number of records displayed on the current page.

Table 4-44 TargetControl

Parameter	Type	Description
manage_account_id	String	ID of a managed account.
control_identifier	String	Governance policy ID.
state	String	Controls if governance policies are enabled.
version	String	Version of the current governance policy.
name	String	Name of a governance policy.
description	String	Description of a governance policy.
control_objective	String	Pre-defined objective that the governance policy helps you enforce.
behavior	String	Type of a governance policy. A governance policy can be preventive, detective, or proactive.
owner	String	Source where a managed account was created. It can be CUSTOM or RGC.
regional_preference	String	Region options. It can be regional or global.
guidance	String	Necessity of a governance policy.
service	String	Service the governance policy applies to.
implementation	String	Underlying implementation method for the governance policy, such as SCPs and Config rules.

Table 4-45 PageInfoDto

Parameter	Type	Description
next_marker	String	Used in the marker request parameter to get the next part of the output. Repeat this operation until the response element comes back as null. If present, more output is available than that included in the current response.
current_count	Integer	Number of records displayed on the current page.

Status code: 403

Table 4-46 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of the request.
encoded_authorization_message	String	Encrypted error message.
details	Array of **ForbiddenErrorDetail** objects	Error message indicating no permissions for cross-service invoking.

Table 4-47 ForbiddenErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Listing all governance policies enabled for a registered OU in an organization

```
GET https://{endpoint}/v1/governance/managed-organizational-units/{managed_organizational_unit_id}/
controls
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "control_summaries" : [ {
    "manage_account_id" : "string",
    "control_identifier" : "string",
    "state" : "string",
    "version" : "string",
    "name" : "string",
    "description" : "string",
    "control_objective" : "string",
    "behavior" : "string",
    "owner" : "string",
    "regional_preference" : "string",
    "guidance" : "string",
    "service" : "string",
    "implementation" : "string"
  } ],
  "page_info" : {
    "next_marker" : "string",
    "current_count" : 0
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
403	No permissions.

Error Codes

See **Error Codes**.

5 Permissions and Supported Actions

5.1 Introduction

You can use Identity and Access Management (IAM) for fine-grained permissions management of your RGC resources. If your HUAWEI ID does not need individual IAM users, you can skip this section.

With IAM, you can control access to specific Huawei Cloud resources.

If you use IAM users in your account to call an API, the IAM users must be granted the required permissions. The required permissions are determined by the actions supported by the API. Only users with the policies allowing for those actions can call the API successfully.

For example, if an IAM user wants to call an API to query the status of landing zone setup, the user must have been granted permissions that allow the **rgc:landingZoneStatus:get** action.

5.2 Actions Supported by Policy-based Authorization

IAM provides system-defined policies to define common actions supported by cloud services. You can also create custom policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

The organization's management account can use SCPs to ensure your member accounts stay within your organization's access and control guidelines. They can be attached to an organization, OUs, or member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU. The granted permissions can be applied only if they are allowed by the SCPs.

This section describes the elements used by IAM custom policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom policy, see **Creating a Custom Policy**.

- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in a policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.
- The **Condition Key** column includes keys that you can specify in the Condition element of a policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

The following table lists the actions that you can define in custom policies for RGC.

Table 5-1 Actions supported by RGC

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:control:list	Grants permission to list all governance policies.	list	-	-
rgc:controlViolation:list	Grants permission to list non-compliance.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:control:get	Grants permission to get details about a governance policy.	read	-	-
rgc:control:enable	Grants permission to enable a governance policy.	write	-	-
rgc:control:disable	Grants permission to disable a governance policy.	write	-	-
rgc:controlOperate:get	Grants permission to query the status of a governance policy.	read	-	-
rgc:enabledControl:list	Grants permission to list enabled governance policies.	list	-	-
rgc:controlsForOrganizationalUnit:list	Grants permission to list governance policies enabled for a registered OU.	list	-	-
rgc:controlsForAccount:list	Grants permission to list governance policies enabled for an enrolled account.	list	-	-
rgc:complianceStatusForAccount:get	Grants permission to query the resource compliance status of an enrolled account in an organization.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:complianceStatusForOrganizationalUnit:get	Grants permission to query the resource compliance status of all enrolled accounts under a registered OU in an organization.	read	-	-
rgc:controlsForOrganizationalUnit:get	Grants permission to list governance policies enabled for an OU.	read	-	-
rgc:controlsForAccount:get	Grants permission to list governance policies enabled for an account.	read	-	-
rgc:configRuleCompliance:list	Grants permission to query the Config rule compliance for enrolled accounts.	list	-	-
rgc:externalConfigRuleCompliance:list	Grants permission to list the external Config rule compliance for enrolled accounts.	list	-	-
rgc:driftDetail:list	Grants permission to query drift details.	list	-	-
rgc:managedOrganizationalUnit:register	Grants permission to register an OU.	write	-	-
rgc:managedOrganizationalUnit:reRegister	Grants permission to re-register an OU.	write	-	-
rgc:managedOrganizationalUnit:deRegister	Grants permission to deregister an OU.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:operation:get	Grants permission to obtain registration information.	read	-	-
rgc:managedOrganizationalUnit:delete	Grants permission to delete a registered OU.	write	-	-
rgc:managedOrganizationalUnit:get	Grants permission to get details of a registered OU.	read	-	-
rgc:managedOrganizationalUnit:create	Grants permission to create an OU.	write	-	-
rgc:managedOrganizationalUnit:list	Grants permission to list registered OUs for which governance policies are enabled.	list	-	-
rgc:managedAccount:enroll	Grants permission to enroll an account.	write	-	-
rgc:managedAccount:unEnroll	Grants permission to unmanage an account.	write	-	-
rgc:managedAccount:update	Grants permission to update an enrolled account.	write	-	-
rgc:managedAccount:get	Grants permission to get details of an enrolled account.	read	-	-
rgc:managedAccountsForParent:list	Grants permission to list all enrolled accounts in a registered OU.	list	-	-
rgc:managedAccount:create	Grants permission to create an account.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:managedAccount:list	Grants permission to list enrolled accounts for which governance policies are enabled.	list	-	-
rgc:managedCoreAccount:get	Grants permission to get details of an enrolled core account.	read	-	-
rgc:homeRegion:get	Grants permission to identify the home region.	read	-	-
rgc:preLaunch:check	Grants permission to perform pre-checks before landing zone setup.	write	-	-
rgc:landingZone:setup	Grants permission to set up a landing zone.	write	-	-
rgc:landingZone:delete	Grants permission to delete a landing zone.	write	-	-
rgc:landingZoneStatus:get	Grants permission to query the landing zone setup status.	read	-	-
rgc:availableUpdate:get	Grants permission to query the updateable status of a landing zone.	read	-	-
rgc:landingZoneConfiguration:get	Grants permission to query landing zone settings.	read	-	-
rgc:landingZoneIdentityCenter:get	Grants permission to obtain IAM Identity Center user information.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rgc:operation:list	Grants permission to query the status of a registered OU or an enrolled account.	list	-	-
rgc:templateDeployParam:get	Grants permission to obtain template deployment parameters.	read	-	-
rgc:template:create	Grants permission to create a template.	write	-	-
rgc:template:delete	Grants permission to delete a template.	write	-	-
rgc:predefinedTemplate:list	Grants permission to list preset templates.	list	-	-
rgc:managedAccountTemplate:get	Grants permission to get details of a template for enrolled accounts.	read	-	-

Each API of RGC usually supports one or more actions. **Table 5-2** lists the supported actions and dependencies.

Table 5-2 Actions and dependencies supported by RGC APIs

API	Action	Dependencies
POST /v1/managed-organizational/organizational-unit/{organizational_unit_id}/register	rgc:organizationalUnit:register	-
GET /v1/managed-organizational/{operation_id}	rgc:operation:get	-

API	Action	Dependencies
GET /v1/managed-organizational/managed-account/{managed_account_id}	rgc:managedAccount:get	-
POST /v1/managed-organizational/managed-accounts	rgc:account:create	-
POST /v1/governance/control/enable	rgc:control:enable	-
POST /v1/governance/control/disable	rgc:control:disable	-
GET /v1/governance/operated-controls/{control_operate_request_id}	rgc:controlOperate:get	-
GET /v1/governance/enabled-controls	rgc:enabledControls:list	-
GET /v1/governance/managed-organizational-unit/{managed_organizational_unit_id}/controls	rgc:controlsForOrganizationalUnit:list	-

Resources

RGC does not support resource-specific permission control in policies. If you want to allow access to RGC, use the wildcard (*) for the Resource element to apply policies to all resources.

Conditions

RGC does not support service-specific condition keys in policies.

It can only use global condition keys applicable to all services. For details, see **Global Condition Keys**.

6 Appendix

6.1 Status Codes

Table 6-1 Status codes

Status Code	Message	Description
100	Continue	The client continues sending the request. The server has received the initial part of the request and the client should continue sending the remaining part.
101	Switching Protocols	The requester has asked the server to switch protocols and the server is acknowledging that it will do so. The target protocol must be more advanced than the source protocol. For example, the current HTTPS protocol is switched to a later version.
201	Created	The request for creating a resource has been fulfilled.
202	Accepted	The request has been accepted for processing, but the processing has not been completed.
203	Non-Authoritative Information	The server successfully processed the request, but is returning information that may be from another source.
204	NoContent	The server has successfully processed the request, but does not return any content. The status code is returned in response to an HTTP OPTIONS request.
205	Reset Content	The server has fulfilled the request, but the requester is required to reset the content.

Status Code	Message	Description
206	Partial Content	The server has successfully processed a part of the GET request.
300	Multiple Choices	There are multiple options for the location of the requested resource. The response contains a list of resource characteristics and addresses from which the user or user agent (such as a browser) can choose the most appropriate one.
301	Moved Permanently	The requested resource has been assigned a new permanent URI, and the new URI is contained in the response.
302	Found	The requested resource resides temporarily under a different URI.
303	See Other	The response to the request can be found under a different URI. It should be retrieved using a GET or POST method.
304	Not Modified	The requested resource has not been modified. When the server returns this status code, it does not return any resources.
305	Use Proxy	The requested resource must be accessed through a proxy.
306	Unused	This HTTP status code is no longer used.
400	BadRequest	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
402	Payment Required	This status code is reserved for future use.
403	Forbidden	The server understood the request, but is refusing to fulfill it. The client should not repeat the request without modifications.
404	NotFound	The requested resource could not be found. The client should not repeat the request without modifications.
405	MethodNotAllowed	The method specified in the request is not supported for the requested resource. The client should not repeat the request without modifications.

Status Code	Message	Description
406	Not Acceptable	The server could not fulfil the request according to the content characteristics of the request.
407	Proxy Authentication Required	This status code is similar to 401, but the client must first authenticate itself with the proxy.
408	Request Time-out	The server times out when waiting for the request. The client may repeat the request without modifications at any later time.
409	Conflict	The request could not be processed due to a conflict. The resource that the client attempts to create already exits, or the request fails to be processed because of the update of the conflict request.
410	Gone	The requested resource is no longer available. The requested resource has been deleted permanently.
411	Length Required	The server refuses to process the request without a defined Content-Length.
412	Precondition Failed	The server does not meet one of the preconditions that the requester puts on the request.
413	Request Entity Too Large	The request is larger than the server is willing or able to process. The server may close the connection to prevent the client from continuing the request. If the server cannot process the request temporarily, the response will contain a Retry-After header field.
414	Request-URI Too Large	The URI provided was too long for the server to process.
415	Unsupported Media Type	The server is unable to process the media format in the request.
416	Requested range not satisfiable	The requested range is invalid.
417	Expectation Failed	The server fails to meet the requirements of the Expect request header field.
422	UnprocessableEntity	The request is well-formed but unable to be processed due to semantic errors.

Status Code	Message	Description
429	TooManyRequests	The client sends excessive requests to the server within a given time (exceeding the limit on the access frequency of the client), or the server receives excessive requests within a given time (beyond its processing capability). In this case, the client should repeat requests after the time specified in the Retry-After header of the response expires.
500	InternalServerError	The server is able to receive the request but unable to understand the request.
501	Not Implemented	The server does not support the function required to fulfill the request.
502	Bad Gateway	The server was acting as a gateway or proxy and received an invalid response from the upstream server.
503	ServiceUnavailable	The requested service is invalid. The client should not repeat the request without modifications.
504	ServerTimeout	The request cannot be fulfilled within a given time. This status code is returned to the client only when the **Timeout** parameter is specified in the request.
505	HTTP Version not supported	The server does not support the HTTP protocol version used in the request.

6.2 Error Codes

If an error code starting with **APIGW** is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

Table 6-2 Error codes

Status Code	Error Code	Error Message	Description	Solution
400	RGC.400	Bad Request: {0}.	Internal error. Try again later.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
400/404	RGC.404	Not Found: {0}.	Not found.	Contact technical support.
400	RGC.1000	An error occurred when invoking the dependent service {0}, error is {1}	An error occurred when invoking an antecedent service.	Contact technical support.
400	RGC.1001	bad request for query icc instance.	Failed to check whether IAM Identity Center is enabled.	Try again later.
400	RGC.1002	bad request for register region.	Failed to register a region.	Try again later.
400	RGC.1003	bad request for start identity center.	Failed to enable the IAM Identity Center.	Try again later.
400	RGC.1004	bad request for get registered regions.	Failed to obtain a list of the regions with IAM Identity Center enabled.	Try again later.
400	RGC.1005	the queried region is different from the registered region.	The selected home region is different from the region registered with IAM Identity Center.	Select another region as the home region.
400	RGC.1006	create instance fail.	Failed to create an IAM Identity Center instance.	Try again later.
400	RGC.1007	create instance status is not enable.	The IAM Identity Center instance is unavailable.	Try again later.
400	RGC.1008	create permission set fail.	Failed to create permissions.	Try again later.
400	RGC.1009	create user fail.	Failed to create a user.	Try again later.
400	RGC.1010	bad request for get identity center service status.	Failed to obtain the IAM Identity Center status.	Try again later.
400	RGC.1011	bad request for create permission set.	Failed to create a permission set in the IAM Identity Center instance.	Try again later.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1012	bad request for attach managed policy to permission set.	Failed to attach a system-defined policy to a permission set.	Try again later.
400	RGC.1013	bad request for create account assignment.	Failed to assign permissions to the account.	Try again later.
400	RGC.1014	bad request for describe account assignment creation status.	Failed to obtain the creation status of account assignment.	Try again later.
400	RGC.1015	bad request for create group membership.	Failed to add users to a user group.	Try again later.
400	RGC.1016	bad request for create group.	Failed to create a user group.	Try again later.
400	RGC.1017	bad request for create user.	Failed to create an IAM Identity Center user.	Try again later.
400	RGC.1018	bad request for get projects.	Failed to query the project information.	Try again later.
403	RGC.1019	does not have {0} permissions.	No permissions.	Check your permissions.
400	RGC.1021	bad request for create agency.	Failed to create an agency.	Try again later.
400/403	RGC.1022	fail request for assume with service principal.	Failed to switch the agency.	Try again later.
400	RGC.1024	bad request for create service linked agency.	Failed to create the service-linked agency.	Try again later.
403	RGC.1028	Not a management account.	The current account is not the management account.	Check whether the account is the management account.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1029	The organizational unit has been created, but status is create-ou-failed, Details: {0}.	The OU has been created but is in the create-ou-failed state.	Contact technical support.
400	RGC.1032	bad request for enable trust service.	Failed to enable a trusted service.	Try again later.
400	RGC.1033	organizations service not provision.	The Organizations service is not enabled.	Enable the Organizations service.
400	RGC.1034	bad request for authorization header pattern.	Invalid **token** request header.	Ensure that **authorization** request header is valid.
404	RGC.1035	not found for http header:{0}.	HTTP request header not found.	Check whether the HTTP request header exists.
400	RGC.1036	bad request for request proof.	Invalid **proof** request header.	Ensure that **proof** request header is valid.
400	RGC.1037	bad request for impersonate.	Failed to obtain the credential.	Contact technical support.
400	RGC.1038	bad request for listRoles.	Failed to query the permission list.	Contact technical support.
400	RGC.1039	create base line group fail.	Failed to create a baseline user group.	Contact technical support.
400	RGC.1040	retrieve user fail.	Failed to retrieve user information.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1041	describe user fail.	Failed to query user details.	Contact technical support.
400	RGC.1042	show compliance details fail.	Failed to query compliance information.	Contact technical support.
400	RGC.1043	list aggregate compliance fail.	Failed to query the list of compliance rules for resource aggregators.	Contact technical support.
400	RGC.1044	list aggregator fail.	Failed to query the list of resource aggregators.	Contact technical support.
400	RGC.1045	bad request for list groups.	Failed to request for a list of user groups.	Contact technical support.
400	RGC.1046	The user already exists, but the user name is different.	The IAM Identity Center username is different from the one you configured.	Check whether the username is correct and ensure that it is the same as the configured one.
500	RGC.1049	failure reason of creating account is {0}, you can check detail at Organizations view.	Failed to create the account. You can view details on the **Organization** page.	Contact technical support.
400	RGC.1050	Bad Request:{0} not found.	Request error. Related resources are not found.	Check whether the resources are available.
400	RGC.1052	The parent is not managed by RGC.	The parent OU is not registered.	Check whether the parent OU has been registered.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1053	The organization unit child resource is not empty.	The current OU is not empty.	Check whether there are child OUs or member accounts nested under the current OU.
400	RGC.1054	Account {0} requires at least one agency.	At least one agency must be created for the account.	Check the current account.
400	RGC.1055	Maybe exist a policy: {0} not created by RGC, you should delete it if the policy exist.	This policy is not created by RGC and should be deleted.	Check the policy details.
400	RGC.1056	bad request for query iam assume agency.	Failed to switch to the member account identity.	Contact technical support.
400	RGC.1057	The organization unit is not found.	OU not found.	Check whether the OU has been registered.
400	RGC.1058	The requested control policy does not exist.	Governance policy not found.	Check whether the governance policy exists.
400	RGC.1059	The relationship between the control and the specified target does not exist.	The requested governance policy is not enabled for the OU.	Only enabled governance policies can be disabled.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1060	The Root and core organizational units cannot implement additional control strategies.	Governance policies cannot be enabled for or disabled from the root and core OUs.	Do not enable or disable governance policies for the root and core OUs.
400	RGC.1062	Not allowed to perform operations on an OU that is not successfully registered.	Governance policies cannot be enabled or disabled for unregistered OUs.	Ensure that the OUs for which you want to enable or disable governance policies have been registered.
400	RGC.1063	Not allowed to perform operations on an OU. The top-level ou is not successfully registered, ouId is {0}.	Operation not allowed for the organization. The top OU is not registered successfully.	Check the OU.
400	RGC.1065	The landing zone environment {0} operation is in progress. This function is not supported.	The landing zone is being set up. This function is not supported.	Try again later.
400	RGC.1067	The landing zone environment is not set.	The landing zone has not been set up.	Set up the landing zone.
400	RGC.1068	The selected region is invalid.	The selected home region is invalid.	Check whether the home region is available.
400	RGC.1069	The bucket policy is empty.	The bucket policy is empty.	Contact technical support.
400	RGC.1070	bad request for obs.	Failed to request for the OBS service.	Try again later.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1071	Failed to call obs, error message: {0}.	Failed to invoke OBS.	Contact technical support.
400	RGC.1072	Get a unexpected status code.	Failed to request for the Organizations service.	Contact technical support.
400	RGC.1073	Org list accounts occur error.	Failed to query the list of accounts in an OU.	Try again later.
400	RGC.1074	Failed to call the API for deleting a stackSetInstance.	Failed to invoke RFS to delete stackSet instances.	Check whether RFS is running properly and whether stackSet instances are normal.
400	RGC.1075	The baseLine control cannot be operated.	The baseline governance policy cannot be enabled or disabled.	Do not enable or disable the baseline governance policy.
400	RGC.1076	The control state is {0}, can not do current organization unit operation.	Operation not allowed. The governance policy is abnormal.	Ensure that the governance policy is in the correct state, and then try again later.
400	RGC.1078	Manage account should not be our set up account.	The management account cannot be used as a core account.	Ensure that the management account is not used as a core account.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1079	Manage account or core account can not change organization unit.	The management account or core accounts cannot change their OUs.	Contact technical support.
400	RGC.1080	The core and root organization unit can not be delete or deregister.	The root and core OUs cannot be deleted or deregistered.	Do not delete or deregister the root and core OUs.
400	RGC.1081	The parent organization unit type could not be core.	The parent OU cannot be the core OU.	Do not use the core OU as a parent OU.
400	RGC.1083	Create account failed. Reason: The ou type is incorrect.	Failed to create the account because the OU type is incorrect.	Check the OU type.
400	RGC.1084	Create account failed. The action is not supported.	Failed to create the account because the account status is not supported.	Check whether the account is being managed.
400	RGC.1085	The account already exists or is not managed by the RGC.	The account already exists or is not managed by RGC.	Check whether the account is managed by RGC.
400	RGC.1086	fixed parameters cannot be changed.	Fixed parameters cannot be modified.	Do not modify fixed parameters.
400	RGC.1087	The landing zone environment has been set, any parameter cannot be changed.	Parameters cannot be changed after the landing zone is set up.	Do not modify the parameters once the landing zone is set up.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1088	organizationUnitId and accountId can not exist together.	The OU ID and account ID cannot be used as search criteria at the same time.	Use either the OU ID or the account ID for query.
400/404	RGC.1089	The account is not found.	Account not found.	Check whether the account exists.
400	RGC.1090	create assignment failed, failure reason is {0}.	Failed to assign permissions to the IAM Identity Center user.	Contact technical support.
400	RGC.1091	The resource {0} create or deploy failed, you can check detail at RFS view.	Failed to create or deploy resources. Go to the RFS console for details.	Go to RFS for details.
400	RGC.1092	[RFS]The RFS returns a failure message to deploy stackSet instances.	Failed to invoke RFS to deploy stackSet instances.	Ensure that RFS is working properly or stackSet instances are normal, and then try again.
400	RGC.1093	[RFS]The RFS returns a failure message to create stackSet instances.	Failed to invoke RFS to create stackSet instances.	Ensure that RFS is working properly or stackSet instances are normal, and then try again.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1094	[RFS]The RFS returns a failure message to create stackSet.	Failed to invoke RFS to create stackSet.	Ensure that RFS is working properly or stackSet is normal, and then try again.
400	RGC.1095	Information of IAM Identity Center user {0} cannot be found.	The IAM Identity Center user information cannot be found.	Contact technical support.
400	RGC.1096	The IAM Identity Center user already exists, but the email addresses are different.	The IAM Identity Center user already exists, but its email address is different from the previously configured address.	Ensure that the email address is the same as the one you configured.
500	RGC.1097	Failed to build the account assignment information.	User information not found.	Contact technical support.
400	RGC.1098	The account type is not custom, can not be un-enroll.	The account is not a custom account and cannot be unmanaged.	Check whether the account is a custom account.
400	RGC.1099	The pap returned error.	Failed to invoke PAP APIs.	Try again later.
400	RGC.1100	The account already exists and is managed by the RGC.	The account is already managed by RGC.	Check whether the account is correct.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1102	The account already exists, but the parentOrganizationUnitId is different.	The account already exists, but the parent OU ID is different from the one you configured.	Ensure that the parent OU of the account is the same as the one you configured.
400	RGC.1104	The create account task is timeout.	Account creation timed out.	Try again later.
400	RGC.1105	bad request for list entrity. The entrity is empty.	Failed to query the parent OU for the account.	Check whether the account information is correct.
400	RGC.1106	Org list create account status occur error.	An error occurred when querying the status of the created account.	Ensure that the organization account is being created or the Organizations service is working properly, and then try again.
400	RGC.1107	The administrator user does not exist.	The IAM Identity Center administrator was not found.	Check whether the account information is correct.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1108	The control detail is not found.	Failed to query the governance policy details. The governance policy was not found.	Check whether the governance policy ID is correct.
400	RGC.1109	Failed to get the policy of the {0} OBS bucket of {1} account, error message: {2}.	Failed to obtain the policy of the OBS bucket.	Contact technical support.
400	RGC.1110	Please accept the open beta of resource governance center service.	The account did not apply for RGC OBT.	Apply for RGC OBT.
404	RGC.1111	not found for http header.	The HTTP request header was not found.	Try again later.
400	RGC.1112	bad request for invalid user profile.	Failed to obtain the user configuration file.	Try again later.
400	RGC.1113	get token fail.	Failed to obtain the token.	Contact technical support.
400	RGC.1114	The idc user {0} is not created for account {1}, maybe you need to use a unused Idc name.	IAM Identity Center username in use.	Change the IAM Identity Center username and try again.
400	RGC.1115	phone number is required in domestic.	Mobile number required.	Check whether the mobile number specified for the core OU is valid.
400	RGC.1116	get a not normal response when get token.	An error occurred when obtaining the token.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
500	RGC.1117	can't find policy: {0}	Failed to query the policy. The policy was not found.	Check whether the policy name is correct.
400	RGC.1118	Account {0} have no trust agency RGCServiceExecution-Agency, maybe you need to try update account or landingzone.	Your account does not have a trust agency RGCServiceExecution-Agency. Update your account or landing zone.	Change the account and try again.
500/400	RGC.1119	Rfs list templates occur error.	Failed to query the RFS template.	Contact technical support.
400	RGC.1120	[RFS]The RFS returns a failure message to list stackSet {0}.	Failed to query the RFS stack set.	Contact technical support.
409	RGC.1200	concurrent modification.	A conflict occurs during the landing zone setup.	Try again later.
400	RGC.1201	The core and root organization unit can not be register.	The root OU and core OU cannot be registered.	Check whether the registered OU is available and check the OU type.
400	RGC.1202	The account already exists, but the account type is not custom.	The current account is not a custom account.	Check the account type.
400	RGC.1203	The account status is {0}, can not do current account operation.	This operation is not allowed for the current account.	Check the account status.
400	RGC.1204	The organization unit status is {0}, can not do current account operation.	This operation is not allowed for accounts in the current OU.	Check the OU status.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1205	The organization unit status is {0}, can not do current organization unit operation.	This operation is not allowed for the current OU.	Check the OU status.
409	RGC.1206	The organization unit conflict, the organization unit is registered.	The OU is already registered.	Call the API for re-registering the OU.
400	RGC.1207	The parent organization unit type could not be core or root.	The parent OU cannot be the root OU.	Check the type of the parent OU.
400	RGC.1208	The parent organizational unit status is {0}, can not do current organizational unit operation.	Operation not allowed. The parent OU is abnormal.	Check the status of the parent OU.
404	RGC.1209	No landing zone has been created for this account.	No landing zone is set up for the current account.	Check whether a landing zone has been set up for the current account.
400	RGC.1210	The landing zone environment status is not successful.	Operation not allowed. The landing zone failed to be set up.	Check whether a landing zone is set up for the current account.
400	RGC.1211	The organization unit name has existed in Organization,please input unique and unused organization unit name.	Duplicate OU name. Enter a unique OU name.	Check whether the OU to be registered is correct.
400	RGC.1212	Failed to query role id from pap.	Failed to invoke PAP to query permissions.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1213	Failed to create agency pap.	Failed to invoke PAP to create an agency.	Contact technical support.
400	RGC.1214	Failed to allpy role id pap.	Failed to invoke PAP to grant project permissions to the agency.	Contact technical support.
400	RGC.1217	IAM list projects occur error.	Failed to invoke IAM to list projects.	Contact technical support.
400	RGC.1218	The account status conflict, the account is enrolled.	The current account is already enrolled.	Do not attempt to enroll the account again.
400	RGC.1219	time format or range error.	Incorrect time format.	Contact technical support.
400	RGC.1220	Domain tag not found, domainId is {0}.	Tags attached to the tenant not found.	Check whether the tenant ID is correct.
400	RGC.1221	Domain info not found, domainId is {0}.	Tenants not found.	Check whether the tenant ID is correct.
400	RGC.1222	email is required in global.	Email address required.	Enter an email address.
400	RGC.1223	Failed to create role.	Failed to create a custom policy.	Contact technical support.
400	RGC.1224	startTime should not be later than endTime.	The start time cannot be later than the end time.	Specify the correct time range.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1225	Some accounts under the organization unit are in the Operation state.	There are account-related operations in progress under the OU.	Try again later.
404	RGC.1226	Can't find the ou, ouId is {0}.	OU not found.	Check the OU ID.
404	RGC.1227	Can't find the account, accountId is {0}.	Account not found.	Check the account ID.
400	RGC.1228	The stack set instance delete failed, you can check detail at RFS view.	Failed to delete the stack instance. Go to the RFS console for details.	Contact technical support.
400	RGC.1229	The stack set delete failed, you can check detail at RFS view.	Failed to delete the stack set. Go to the RFS console for details.	Contact technical support.
400	RGC.1230	Should not have custom account.	Custom accounts are not supported.	Check the account type.
400	RGC.1231	Should have one Core Organization Unit.	The core OU is required.	Check the OU type.
400	RGC.1232	Core Organization Unit should has two accounts.	Two accounts required for the core OU.	Check the number of accounts.
400	RGC.1233	Core Organization can only has two accounts,one must be AUDIT type,another one must be LOGGING type.	Each landing zone needs two core accounts (an audit account and a log archive account).	Modify input parameters.
400	RGC.1234	An existed Core Account has been created,the same name should be given.	The names of core accounts must remain the same as before.	Modify input parameters.
400	RGC.1235	The notification email of Audit account should be given.	An email address is required for the audit account.	Modify input parameters.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1236	When exist account scene, account name should be given.	The account already exists, but the account name is missing.	Modify input parameters.
400	RGC.1237	The organization name is empty.	The OU name is required.	Enter a correct OU name.
404	RGC.1238	The parent organization unit not found.	Parent OU not found.	Check whether the parent OU exists.
400	RGC.1239	When exist account scene, account id and name does not match.	The account already exists, but the account ID and the account name do not match.	Modify input parameters.
404	RGC.1240	RGCServiceExecution-Agency cannot be found.	"RGCServiceExecution-Agency" not found.	Contact technical support.
404	RGC.1242	Not found this control, control id is {0}.	Governance policy not found.	Contact technical support.
404	RGC.1243	control not started, control id is {0}.	Governance policy not enabled.	Contact technical support.
400	RGC.1244	Skip the creation of core OU. Only existing accounts can be used.	Skip the creation of the core OU. Only existing accounts can be used.	Modify input parameters.
400	RGC.1245	The operation is not allowed because the SCP is updated or deleted.	Operation not allowed. The SCP has been updated or deleted.	Contact technical support.
409	RGC.1246	The SCP name conflict, please delete the old SCP and try again.	Duplicate SCP name. Delete the existing SCP and try again.	Check the SCP.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.1247	The core account is deleted, the core account is closed, or the core organizational unit is deleted, can not do current operation.	Operation not allowed. The core accounts have been disabled or deleted, or the core OU has been deleted.	Contact technical support.
400	RGC.1248	The control parameter is incorrect.	Incorrect parameters.	Modify input parameters.
403/400/4003	RGC.4003	Error information about authentication failure.	Authentication failed.	Contact technical support.
400	RGC.4004	The organizational unit name must be unique.	Duplicate name. Enter a unique OU name.	Modify input parameters.
400	RGC.4005	The organizational unit of the same type already exist.	The OU of the same type already exists.	Modify input parameters.
400	RGC.4006	The account name must be unique.	Duplicate name. Enter a unique account name.	Modify input parameters.
400	RGC.4007	The landing zone has been set successfully and cannot be set again.	Operation not allowed. The landing zone has already been set up.	Modify input parameters.
400	RGC.4008	The account email is not required.	Email address not required.	Modify input parameters.
400	RGC.4009	The account phone number is not required.	Mobile number not required.	Modify input parameters.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.4012	Bad Request:account id and ou id are both empty.	Request error. Both the account ID and OU ID are empty.	Modify input parameters.
400	RGC.4013	Bad Request:neither account id or ou id is empty.	Request error. Neither the account ID nor the OU ID is empty.	Modify input parameters.
400	RGC.4014	Bad Request:operation cannot be found.	Request error. Operation not found.	Contact technical support.
400	RGC.4015	The home region must be the same as the current region.	The home region must be the current region.	Modify input parameters.
400	RGC.4016	Failed to get project ID for account: {0} and region: {1}. Generate the project ID and try again.	Failed to obtain the project ID. Generate a project ID and try again.	Generate a project ID and try again.
400	RGC.4017	The blueprint param of account cannot be empty.	The template parameters cannot be empty.	Modify input parameters.
400	RGC.4018	The account name cannot be the same as the administrator account name.	The account name must be different from the administrator's account name.	Modify input parameters.
400	RGC.4019	The {0} account already exists in the RGC.	The account already exists in RGC.	Modify input parameters.
400	RGC.4021	create agency token error.	Incorrect token for creating an agency.	Contact technical support.
400	RGC.4022	The mode of creating a new account or using an existing account cannot be changed.	The method (either creating a new account or using an existing account) cannot be changed.	Modify input parameters.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.4031	The current operation cannot be performed because {0} operation has succeeded.	Operation not allowed. Related operations have been performed.	Modify input parameters.
400	RGC.4032	The policy {0} is not created by RGC, maybe you should consider to delete it.	Governance policy not created by RGC. You can choose to delete it.	Delete the governance policy and try again.
400	RGC.4033	The current operation cannot be performed because {0} operation has failed.	Operation not allowed. The previous operation failed.	Modify input parameters.
400	RGC.4034	The {0} organization unit name is required.	Enter an OU name.	Modify input parameters.
400	RGC.4035	The {0} organization unit name is not required.	OU name not required.	Modify input parameters.
400	RGC.4036	OBS bucket retention info is required.	OBS bucket retention information required.	Modify input parameters.
400	RGC.4037	OBS bucket retention info is not required.	OBS bucket retention information not required.	Modify input parameters.
400	RGC.4038	IAM Identity Center information is required, such as identity_store_user_name or identity_store_email.	IAM Identity Center information required, such as **identity_store_user_name** or **Identity_store_email**.	Modify input parameters.
400	RGC.4039	IAM Identity Center information is not required, such as identity_store_user_name and identity_store_email.	IAM Identity Center information not required, such as **identity_store_user_name** and **Identity_store_email**.	Modify input parameters.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.4040	The bucket does not exist in {0}.	Bucket not found.	Modify input parameters.
400	RGC.4041	Failed to verify the {0} OBS bucket, failure message: {1}.	Failed to check if the bucket exists.	Contact technical support.
400	RGC.4042	The operation is not allowed because the account is frozen.	Operation not allowed. The account has been frozen.	Contact technical support.
400	RGC.4043	The operation is not allowed because the account is restricted.	Operation not allowed. The account has been restricted.	Contact technical support.
400	RGC.4045	Not support to change the blueprint product of account.	Modifying template parameters not allowed.	Modify input parameters.
400	RGC.4046	The state of account does not support to take the operation of updating account.	Account update not allowed for accounts in the current state.	Check the account status.
400	RGC.4047	The {0} account has requested close account operation, can not do current operation.	Operation not allowed. The account has been requested to be closed.	Check the account status.
400	RGC.4048	The {0} operation does not require additional OU parameter.	Additional OU parameters not required.	Modify input parameters.
400	RGC.4049	The {0} parameter cannot be changed by the REPAIR operation.	Parameter cannot be modified by conducting repair.	Modify input parameters.
400	RGC.4050	The {0} parameter cannot be changed because the related steps have been performed.	Parameter cannot be modified. Related operations have been performed.	Modify input parameters.

Status Code	Error Code	Error Message	Description	Solution
400	RGC.4051	The {0} parameter cannot add enabled region because the related steps have been performed.	Another region cannot be added. Related operations have been performed.	Modify input parameters.
400	RGC.4053	The {0} account already exists in the RGC and cannot be used as a repair account. Please change the account.	The account already exists in RGC. It cannot be used for repairing. Change the account.	Modify input parameters.
400	RGC.4054	The primary account cannot update. Please change the account.	Administrator account cannot be updated. Change the account.	Modify input parameters.
400	RGC.5003	The {0} account is in the {1} state and the operation cannot be performed.	Operation not allowed for accounts in the current state.	Check the account status.
400	RGC.5004	The {0} organizational unit is in the {1} state and the operation cannot be performed.	Operation not allowed for OUs in the current state.	Check the OU status.
400	RGC.5006	The {0} config rule is in the {1} state and cannot be deleted.	Config rule in the current state cannot be deleted.	Contact technical support.
400	RGC.5009	Failed to process the {0} account. The failure message: {1}.	Failed to process the account.	Contact technical support.
400	RGC.5010	Failed to process the {0} organizational unit. The failure message: {1}.	Failed to process the OU.	Contact technical support.
400	RGC.5013	Failed to set the policy for the {0} OBS bucket of {1} account, error message: {2}.	Failed to configure the OBS bucket policy.	Contact technical support.
400	RGC.5014	Some accounts under the organizational unit are create-failed or un-enroll-failed.	Failed to create or unmanage some accounts under the OU.	Contact technical support.

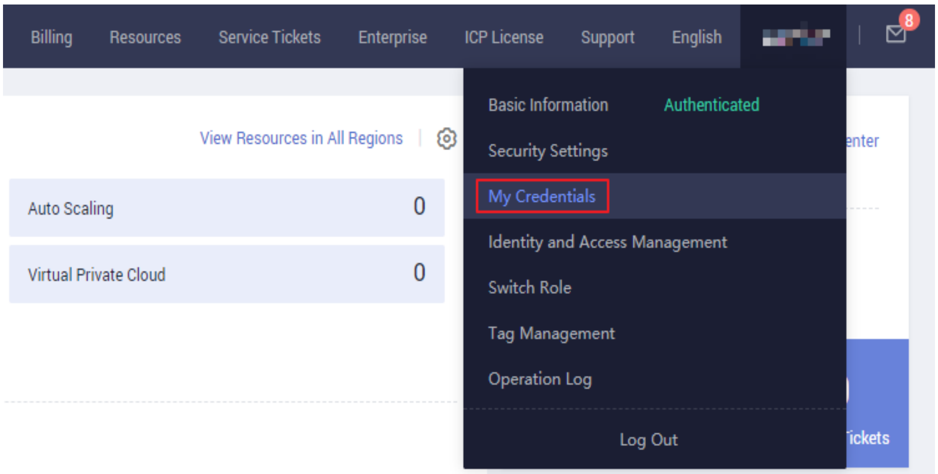
Status Code	Error Code	Error Message	Description	Solution
400	RGC.5015	{0} have no control content, please check database.	Governance policy not found.	Contact technical support.
400	RGC.5016	control {0} is not existed, please check database.	Governance policy not found.	Contact technical support.
400	RGC.5017	Failed to set ACLs for the {0} OBS bucket of {1} account, error message: {2}.	Failed to set ACLs for the OBS bucket.	Contact technical support.
400	RGC.5018	create agency credential error.	Failed to create agency credentials.	Contact technical support.
500	RGC.5021	attach policy: {0} to agency: {1} fail.	Failed to attach the policy to the agency.	Contact technical support.
500	RGC.5023	get PredefinedTemplates error, errorMessage: {0}.	Failed to obtain the preset template.	Contact technical support.
400	RGC.6001	[RFS]List stack instances error, you can check detail at RFS view.	[RFS] An error occurred when listing stack instances. Go to the RFS console for details.	Contact technical support.
400	RGC.6002	Failed to obtain template deploy params from RFS.	Failed to obtain template deployment parameters from RFS.	Contact technical support.
400	RGC.6003	Failed to delete template: {0}.	Failed to delete the template.	Contact technical support.
400	RGC.6004	[RFS]The stack delete failed, you can check detail at RFS view.	[RFS] Failed to delete the stack. Go to the RFS console for details.	Contact technical support.

6.3 Obtaining Information About Account, IAM User, Group, Project, Region, and Agency

Obtaining Account, IAM User, and Project Information

- **Using the console**
  a. On the Huawei Cloud homepage, click **Console** in the upper right corner.
  b. Hover over the username in the upper right corner and choose **My Credentials**.

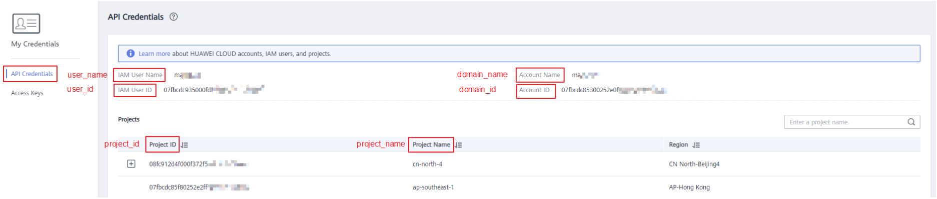
Figure 6-1 My Credentials



  c. View the account name, account ID, username, user ID, project name, and project ID on the **API Credentials** page.

  The project ID varies depending on the region where the service is located.

Figure 6-2 Viewing the account, user, and project information



API Credentials

Learn more about HUAWEI CLOUD accounts, IAM users, and projects.

IAM User Name ma[redacted]
IAM User ID 07fbcdc935000fdf[redacted]
Account Name ma[redacted]
Account ID 07fbcdc85300252e0f[redacted]

Projects

Enter a project name.

Project ID	Project Name	Region
08fc912d4f000f372f5[redacted]	cn-north-4	CN North-Beijing4
07fbcdc85f80252e2ff[redacted]	ap-southeast-1	AP-Hong Kong

- **Calling an API**
  – For details about how to obtain a user ID, see **Listing IAM Users**.
  – For details about how to obtain a project ID, see **Querying Project Information**.

Obtaining User Group Information

Step 1 Log in to the IAM console, and choose **User Groups** from the navigation pane.

Step 2 Expand the details page of a user group and view the group name and ID.

----End

Obtaining Region Information

Step 1 Log in to the IAM console, and choose **Projects** from the navigation pane.

Step 2 The value in the **Project Name** column is the ID of the region which the project belongs to.

----End

Obtaining Agency Information

Step 1 Log in to the IAM console, and choose **Agencies** from the navigation pane.

Step 2 Hover over the target agency. The name and ID of this agency are displayed.

----End