

资源治理中心

API 参考

文档版本 01
发布日期 2023-12-22



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 使用前必读.....	1
1.1 概述.....	1
1.2 调用说明.....	1
1.3 终端节点.....	1
1.4 约束与限制.....	1
1.5 基本概念.....	1
2 API 概览.....	3
3 如何调用 API.....	5
3.1 构造请求.....	5
3.2 认证鉴权.....	7
3.3 返回结果.....	8
4 API.....	11
4.1 Landing Zone 管理.....	11
4.1.1 查询主区域.....	11
4.1.2 设置 Landing Zone 前检查.....	12
4.1.3 设置 Landing Zone.....	13
4.1.4 查询 Landing Zone 设置状态.....	17
4.1.5 查询 Landing Zone 可更新状态.....	19
4.1.6 查询 Landing Zone 的配置.....	21
4.1.7 查询当前客户的 Identity Center 用户信息.....	25
4.2 Landing Zone 治理.....	27
4.2.1 列出控制策略.....	27
4.2.2 列出不合规信息.....	30
4.2.3 查询控制策略详细信息.....	32
4.2.4 开启控制策略.....	36
4.2.5 关闭控制策略.....	37
4.2.6 查询控制策略操作状态.....	38
4.2.7 列出开启的控制策略.....	40
4.2.8 列出注册 OU 下开启的控制策略.....	43
4.2.9 列出纳管账号下开启的控制策略.....	47
4.2.10 查询纳管账号的合规状态.....	50
4.2.11 查询注册 OU 的合规状态.....	52

4.2.12 查询注册 OU 开启的控制策略.....	53
4.2.13 查询纳管账号的 Config 规则合规性信息.....	56
4.2.14 列出漂移信息.....	57
5 权限和授权项.....	60
5.1 权限和授权项说明.....	60
5.2 策略授权参考.....	60
6 附录.....	68
6.1 状态码.....	68
6.2 错误码.....	70
6.3 获取账号、IAM 用户、项目、用户组、区域、委托的名称和 ID.....	82
A 修订记录.....	85

1 使用前必读

1.1 概述

欢迎使用资源治理中心（Resource Governance Center，简称RGC）。RGC是照规范性最佳实践提供一种简单的方案发设置和管理多账户环境，用户可以通过RGC服务创建一个Landing Zone，包含一个管理账号和多个成员账号，同时对这些账号进行各种自动化的护栏配置，帮助客户方便快速安全上云。

您可以使用本文档提供API对RGC进行相关操作，如创建、删除、更新、查询等。支持的全部操作请参见[2 API概览](#)。

在调用RGC的API之前，请确保已经充分了解RGC相关概念，详细信息请参见[资源治理中心产品介绍](#)。

1.2 调用说明

RGC提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见[3 如何调用API](#)。

1.3 终端节点

终端节点即调用API的请求地址，不同服务不同区域的终端节点不同，您可以从[地区和终端节点](#)中查询服务的终端节点。

1.4 约束与限制

- RGC服务的使用约束和功能规格限制请参考[约束与限制](#)。
- 更详细的限制请参见具体API的说明。

1.5 基本概念

- 账号
用户注册华为云时的账号，账号对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。由于账号是付费主体，为了确保账号

安全，建议您不要直接使用账号进行日常工作，而是创建用户并使用他们进行日常工作。

- 用户

由账号在IAM中创建的用户，是云服务的使用人员，具有身份凭证（密码和访问密钥）。

在[我的凭证](#)下，您可以查看账号ID和IAM用户ID。通常在调用API的鉴权过程中，您需要用到账号、用户和密码等信息。

- 区域（Region）

从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

详情请参见[区域和可用区](#)。

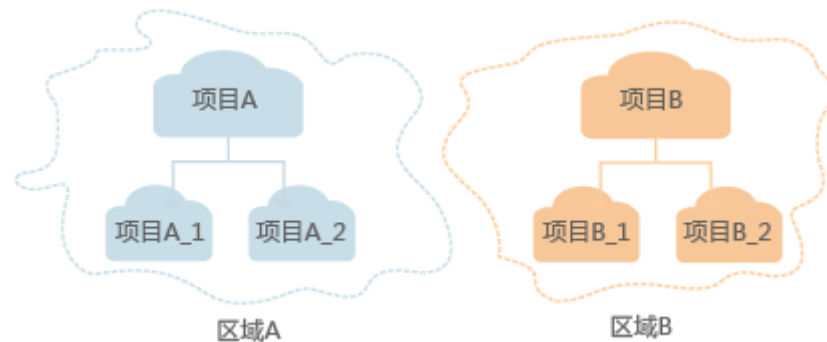
- 可用区（AZ，Availability Zone）

一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

- 项目

区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中的资源，使得资源的权限控制更加精确。

图 1-1 项目隔离模型



同样在[我的凭证](#)下，您可以查看项目ID。

- 企业项目

企业项目是项目的升级版，针对企业不同项目间的资源进行分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。

关于企业项目ID的获取及企业项目特性的详细信息，请参见《[企业管理用户指南](#)》。

2 API 概览

类型	子类型	说明
Landing Zone 管理	查询主区域	查询Landing Zone的主区域。
	设置Landing Zone前的检查	在设置Landing Zone之前，检查当前区域是否可以设置Landing Zone。
	设置Landing Zone	在当前区域创建或者更新Landing Zone。
	获取Landing Zone设置状态	查询Landing Zone的设置状态。
	获取Landing Zone可更新状态	查询Landing Zone当前是否需要升级更新。
	获取Landing Zone的配置	查询当前客户的Landing Zone的所有配置。
	查询当前客户的Identity Center用户信息	查询当前客户的Identity Center用户信息。
Landing Zone 治理	列出控制策略	列出RGC服务里所有的预置控制策略。
	列出不合规信息	列出组织里所有不合规的资源信息。
	查询控制策略详细信息	查询单个预置的控制策略详细信息。
	开启控制策略	给组织下的某个单元开启某个控制策略。
	关闭控制策略	关闭组织下的某个单元的某个控制策略。
	查询控制策略操作状态	根据操作ID查询返回指定ID的操作状态。
	列出开启的控制策略	列出组织里开启的所有控制策略信息。

类型	子类型	说明
	列出纳管账号下开启的控制策略	列出组织里某个纳管账号开启的所有控制策略信息。
	列出注册OU下开启的控制策略	列出组织里某个注册OU开启的所有控制策略信息。
	查询纳管账号的合规状态	查询组织里某个纳管账号的资源合规状态。
	查询注册OU的合规状态	查询注册OU的合规状态。
	查询注册OU开启的控制策略	查询组织里某个注册OU下开启的某个控制策略的详细信息。
	查询纳管账号的Config规则合规性信息	查询纳管账号的Config规则合规性信息。

3 如何调用 API

3.1 构造请求

本节介绍REST API请求的组成，并以调用RGC服务的[获取Landing Zone设置状态](#)接口说明如何调用API。

您还可以通过这个视频教程了解如何构造请求调用API：<https://bbs.huaweicloud.com/videos/102987>。

请求 URI

请求URI由如下部分组成。

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

表 3-1 请求 URL

参数	说明
URI-scheme	传输请求的协议，当前所有API均采用HTTPS协议。
Endpoint	指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从 地区和终端节点 中获取。例如RGC服务在“华北-北京四”区域的Endpoint为“rgc-open.cn-north-4.myhuaweicloud.com”。
resource-path	资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取Landing zone设置状态”API的resource-path为“/v1/landing-zone/status”。
query-string	查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取Landing Zone在“华北-北京四”区域的设置状态，则需使用“华北-北京四”区域的Endpoint（rgc-open.cn-north-4.myhuaweicloud.com），并在[获取](#)

Landing Zone设置状态的URI部分找到resource-path (/v1/landing-zone/status) , 拼接起来如下所示。

```
https://rgc-open.cn-north-4.myhuaweicloud.com/v1/landing-zone/status
```

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**: 请求服务器返回指定资源。
- **PUT**: 请求服务器更新指定资源。
- **POST**: 请求服务器新增资源或执行特殊操作。
- **DELETE**: 请求服务器删除指定资源，如删除对象等。
- **HEAD**: 请求服务器资源头部。
- **PATCH**: 请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在**获取Landing Zone设置状态**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
GET https://rgc-open.cn-north-4.myhuaweicloud.com/v1/landing-zone/status
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

表 3-2

消息头名称	描述	是否必选
Content-Type	消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。	是
X-Auth-Token	用户Token，可选，当使用Token方式认证时，必须填充该字段。	否
Host	表明主机地址。例如： rgc-open.cn-north-4.myhuaweicloud.com	是
X-Sdk-Date	请求发起端的日期和时间	是

📖 说明

API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。AK/SK认证的详细说明请参见[AK/SK认证](#)。

对于[获取Landing Zone设置状态](#)接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
GET https://rgc-open.cn-north-4.myhuaweicloud.com/v1/landing-zone/status
Connection:keep-alive
Content-Type:application/json; charset=UTF-8
Host:console.huawei.com
Projectname:cn-north-4
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

发起请求

您可以使用[curl](#)、[Postman](#)或直接编写代码等方式发送请求调用API。

3.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。

Token 认证

📖 说明

Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

使用Token前请确保Token离过期有足够的时间，防止调用API的过程中Token过期导致调用API失败。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

AK/SK 认证

📖 说明

AK/SK签名认证方式仅支持消息体大小12M以内，12M以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。

- SK(Secret Access Key): 与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见[API签名指南](#)。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

3.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从2xx（成功）到4xx或5xx（错误）的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见[6.1 状态码](#)。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

详细的公共响应消息头字段请参见[表1](#)。

表 3-3 公共响应消息头

消息头名称	描述
Content-Type	资源内容的类型。 类型：String 默认值：无
Connection	指明与服务器的连接是长连接还是短连接。 类型：String 有效值：keep-alive close。 默认值：无。
Date	RGC服务响应的时间。 类型：String 默认值：无
X-Request-Id	由RGC创建来唯一确定本次请求的值，可以通过该值来定位问题。 类型：String 默认值：无

响应消息体

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于查询Landing Zone设置状态接口，返回如下消息体。

```
{
  "deployed_version": "3.5",
  "landing_zone_status": "succeeded",
  "percentage_complete": 100,
  "percentage_details": [
    {
      "percentage_name": "create Organization and enable IAM Identity Center",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create permission sets",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create user groups",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create agencies",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create service-linked-agencies",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create organization unit",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create account of LOGGING type",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create account of SECURITY type",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create user",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create user assignments for SECURITY type account",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create user assignments for LOGGING type account",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create user assignments for primary type account",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create group assignments for SECURITY type account",
      "percentage_status": "succeeded"
    },
    {
      "percentage_name": "create group assignments for LOGGING type account",
      "percentage_status": "succeeded"
    },
    {

```

```
    "percentage_name": "create group assignments for primary type account",
    "percentage_status": "succeeded"
  },
  {
    "percentage_name": "create resources and controls for LOGGING type account",
    "percentage_status": "succeeded"
  },
  {
    "percentage_name": "create resources and controls for SECURITY type account",
    "percentage_status": "succeeded"
  },
  {
    "percentage_name": "create resources and controls for primary type account",
    "percentage_status": "succeeded"
  }
],
"landing_zone_action_type": "CREATE",
"message": [],
"regions": [
  {
    "region": "cn-north-4",
    "region_configuration_status": "ENABLED"
  },
  {
    "region": "br-cto-beta",
    "region_configuration_status": "DISABLED"
  },
  {
    "region": "cn-southwest-252",
    "region_configuration_status": "DISABLED"
  },
  {
    "region": "cn-north-208",
    "region_configuration_status": "DISABLED"
  }
]
}
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

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

其中，error_code表示错误码，error_msg表示错误描述信息。

4 API

4.1 Landing Zone 管理

4.1.1 查询主区域

功能介绍

查询Landing Zone的主区域。

URI

GET /v1/landing-zone/home-region

请求参数

无

响应参数

状态码： 200

表 4-1 响应 Body 参数

参数	参数类型	描述
home_region	String	区域名称。

请求示例

查询Landing Zone的主区域。

```
GET https://{hostname}/v1/landing-zone/home-region
```


响应示例

状态码： 200

请求成功。

```
{  
  "homeRegion" : "string"  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.2 设置 Landing Zone 前检查

功能介绍

在设置Landing Zone之前，检查当前区域是否可以设置Landing Zone。

URI

POST /v1/landing-zone/pre-launch-check

请求参数

无

响应参数

无

请求示例

在设置Landing Zone之前，检查当前区域是否可以设置Landing Zone。

```
POST https://{hostname}/v1/landing-zone/pre-launch-check
```

响应示例

无

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.3 设置 Landing Zone

功能介绍

在当前区域创建或者更新Landing Zone。

URI

POST /v1/landing-zone/setup

请求参数

表 4-2 请求 Body 参数

参数	是否必选	参数类型	描述
identity_store_email	是	String	管理员纳管账号创建Identity Center用户所用邮箱。 最小长度：3 最大长度：64
home_region	是	String	主区域。 最小长度：1 最大长度：64
setup_landing_zone_action_type	是	String	设置Landing Zone的类型。包括CREATE、REPAIR以及UPDATE。 最小长度：1 最大长度：256
region_configuration_list	是	Array of regionConfigurationList objects	当前纳管账号纳管的区域。 数组长度：1 - 30
organization_structure	是	Array of OrganizationStructureBaseLine objects	基础环境的纳管账号体系。 数组长度：1 - 2

参数	是否必选	参数类型	描述
deny_ungoverned_regions	否	Boolean	是否允许区域拒绝，默认 false。 缺省值： false
cloud_trail_type	否	Boolean	是否允许设置组织汇聚。 缺省值： true
kms_key_id	否	String	加密字段。
logging_configuration	是	logging_configuration object	日志桶设置信息。

表 4-3 regionConfigurationList

参数	是否必选	参数类型	描述
region	是	String	区域名字。 最小长度： 1 最大长度： 36
region_configuration_status	是	String	纳管账号类型 LOGGING, SECURITY。 枚举值： <ul style="list-style-type: none"> • ENABLED • DISABLED

表 4-4 OrganizationStructureBaseline

参数	是否必选	参数类型	描述
organizational_unit_name	是	String	注册OU名称。 最小长度： 1 最大长度： 64
organizational_unit_type	是	String	可设置的注册OU类型。包括核心注册OU和自定义注册OU。 枚举值： <ul style="list-style-type: none"> • CORE • CUSTOM
accounts	否	Array of AccountBaseline objects	纳管账号基本信息。 数组长度： 0 - 100

表 4-5 AccountBaseline

参数	是否必选	参数类型	描述
account_name	是	String	纳管账号名称。 最小长度：6 最大长度：30
account_id	否	String	纳管账号的唯一标识符（ID）。 最小长度：0 最大长度：64
phone	否	String	手机号码。 最小长度：1 最大长度：32
account_email	否	String	纳管账号邮箱。 最小长度：0 最大长度：64
account_type	是	String	纳管账号类型。类型包括 LOGGING，SECURITY和 CUSTOM。 枚举值： <ul style="list-style-type: none"> • LOGGING • SECURITY • CUSTOM

表 4-6 logging_configuration

参数	是否必选	参数类型	描述
logging_bucket	是	LoggingBucketBaseline object	日志基础设置。
access_logging_bucket	是	AccessLoggingBucketBaseline object	访问日志基础设置。

表 4-7 LoggingBucketBaseline

参数	是否必选	参数类型	描述
retention_days	是	Integer	桶保留天数。 最小值：1 最大值：5475

表 4-8 AccessLoggingBucketBaseline

参数	是否必选	参数类型	描述
retention_days	是	Integer	桶保留天数。 最小值：1 最大值：5475

响应参数

无

请求示例

在当前区域创建或者更新Landing Zone。

POST https://{hostname}/v1/landing-zone/setup

```
{
  "identity_store_email" : "string",
  "home_region" : "string",
  "setup_landing_zone_action_type" : "string",
  "region_configuration_list" : [ {
    "region" : "string",
    "region_configuration_status" : "ENABLED"
  } ],
  "organization_structure" : [ {
    "organizational_unit_name" : "string",
    "organizational_unit_type" : "CORE",
    "accounts" : [ {
      "account_name" : "string",
      "account_id" : "string",
      "phone" : "18700000000",
      "account_email" : "string",
      "account_type" : "LOGGING"
    } ]
  } ],
  "deny_ungoverned_regions" : false,
  "cloud_trail_type" : true,
  "kms_key_id" : "",
  "logging_configuration" : {
    "logging_bucket" : {
      "retention_days" : 5475
    },
    "access_logging_bucket" : {
      "retention_days" : 5475
    }
  }
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.4 查询 Landing Zone 设置状态

功能介绍

查询Landing Zone的设置状态。

URI

GET /v1/landing-zone/status

请求参数

无

响应参数

状态码： 200

表 4-9 响应 Body 参数

参数	参数类型	描述
deployed_version	String	部署的Landing Zone版本。 最小长度： 1 最大长度： 64
landing_zone_status	String	Landing Zone的设置状态，包括进行中，已完成。 最小长度： 1 最大长度： 64
percentage_complete	Integer	Landing Zone的完成进度。 最小值： 1 最大值： 100
percentage_details	Array of PercentageDetail objects	Landing Zone设置的详细进度信息。

参数	参数类型	描述
landing_zone_action_type	String	Landing Zone当前需要执行的动作。 最小长度：1 最大长度：64
message	Array of LandingZoneErrorMessage objects	Landing Zone错误消息。
regions	Array of regionConfigurationList objects	纳管的区域信息。 数组长度：1 - 100

表 4-10 PercentageDetail

参数	参数类型	描述
percentage_name	String	进度名称。 最小长度：1 最大长度：128
percentage_status	String	进度状态。 最小长度：1 最大长度：64

表 4-11 LandingZoneErrorMessage

参数	参数类型	描述
level	String	Landing Zone的错误级别。
message	String	Landing Zone详细的错误信息。

表 4-12 regionConfigurationList

参数	参数类型	描述
region	String	区域名字。 最小长度：1 最大长度：36

参数	参数类型	描述
region_configuration_status	String	纳管账号类型LOGGING,SECURITY。 枚举值： <ul style="list-style-type: none">• ENABLED• DISABLED

请求示例

查询Landing Zone的设置状态。

GET https://{hostname}/v1/landing-zone/status

响应示例

状态码： 200

请求成功。

```
{
  "deployed_version": "string",
  "landing_zone_status": "string",
  "percentage_complete": 100,
  "percentage_details": [ {
    "percentage_name": "string",
    "percentage_status": "string"
  } ],
  "landing_zone_action_type": "string",
  "message": [ {
    "level": "string",
    "message": "string"
  } ],
  "regions": [ {
    "region": "string",
    "region_configuration_status": "ENABLED"
  } ]
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.5 查询 Landing Zone 可更新状态

功能介绍

查询Landing Zone当前是否需要升级更新。

URI

GET /v1/landing-zone/available-updates

请求参数

无

响应参数

状态码： 200

表 4-13 响应 Body 参数

参数	参数类型	描述
baseline_update_available	Boolean	Landing Zone基础配置是否可用。
control_update_available	Boolean	当前账号下是否有新的控制策略。
landing_zone_update_available	Boolean	Landing Zone是否可更新。
service_landing_zone_version	String	Landing Zone当前最新的版本号。 最小长度： 1 最大长度： 128
user_landing_zone_version	String	用户当前的Landing Zone版本。 最小长度： 1 最大长度： 128

请求示例

查询Landing Zone当前是否需要升级更新。

```
GET https://{hostname}/v1/landing-zone/available-updates
```

响应示例

状态码： 200

请求成功。

```
{  
  "baseline_update_available": true,  
  "control_update_available": true,  
  "landing_zone_update_available": true,  
  "service_landing_zone_version": "string",  
  "user_landing_zone_version": "string"  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.6 查询 Landing Zone 的配置

功能介绍

查询当前客户的Landing Zone的所有配置。

URI

GET /v1/landing-zone/configuration

请求参数

无

响应参数

状态码： 200

表 4-14 响应 Body 参数

参数	参数类型	描述
common_configuration	CommonConfiguration object	Landing Zone配置信息。
logging_configuration	LoggingConfiguration object	Landing Zone日志配置。
organization_structure	Array of OrganizationStructureBaseLineResponse objects	纳管账号体系基础设置。
regions	Array of regionConfigurationList objects	纳管的区域信息。

表 4-15 CommonConfiguration

参数	参数类型	描述
home_region	String	主区域名。 最小长度：1 最大长度：64
cloud_trail_type	Boolean	CTS配置状态。

表 4-16 LoggingConfiguration

参数	参数类型	描述
access_logging_bucket	AccessLoggingBucketBaseline object	访问日志基础设置。
logging_bucket	LoggingBucketBaseline object	日志基础设置。

表 4-17 AccessLoggingBucketBaseline

参数	参数类型	描述
retention_days	Integer	桶保留天数。 最小值：1 最大值：5475

表 4-18 LoggingBucketBaseline

参数	参数类型	描述
retention_days	Integer	桶保留天数。 最小值：1 最大值：5475

表 4-19 OrganizationStructureBaseLineRsp

参数	参数类型	描述
organizational_unit_name	String	注册OU名称。 最小长度：1 最大长度：64
organizational_unit_type	String	可设置的注册OU类型。包括核心注册OU和自定义注册OU。 枚举值： <ul style="list-style-type: none"> • CORE • CUSTOM
accounts	Array of AccountBaselineRsp objects	纳管账号基本信息。 数组长度：0 - 100

表 4-20 AccountBaselineRsp

参数	参数类型	描述
account_name	String	纳管账号名称。 最小长度：6 最大长度：30
account_id	String	纳管账号的唯一标识符（ID）。 最小长度：0 最大长度：36
account_email	String	纳管账号邮箱。 最小长度：0 最大长度：64
account_type	String	纳管账号类型。类型包括LOGGING，SECURITY和CUSTOM。 枚举值： <ul style="list-style-type: none"> • LOGGING • SECURITY • CUSTOM

表 4-21 regionConfigurationList

参数	参数类型	描述
region	String	区域名字。 最小长度：1 最大长度：36
region_configuration_status	String	纳管账号类型LOGGING,SECURITY。 枚举值： <ul style="list-style-type: none"> ENABLED DISABLED

请求示例

查询当前客户的Landing Zone的所有配置。

```
GET https://{hostname}/v1/landing-zone/configuration
```

响应示例

状态码： 200

请求成功。

```
{
  "common_configuration": {
    "home_region": "string",
    "cloud_trail_type": true
  },
  "logging_configuration": {
    "access_logging_bucket": {
      "retention_days": 5475
    },
    "logging_bucket": {
      "retention_days": 5475
    }
  },
  "organization_structure": [ {
    "organizational_unit_name": "string",
    "organizational_unit_type": "CORE",
    "accounts": [ {
      "account_name": "string",
      "account_type": "LOGGING"
    } ]
  } ],
  "regions": [ {
    "region": "string",
    "region_configuration_status": "ENABLED"
  } ]
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.1.7 查询当前客户的 Identity Center 用户信息

功能介绍

查询当前客户的Identity Center用户信息。

URI

GET /v1/landing-zone/identity-center

请求参数

无

响应参数

状态码： 200

表 4-22 响应 Body 参数

参数	参数类型	描述
identity_store_id	String	Identity Center目录ID。 最小长度： 1 最大长度： 64
user_portal_url	String	Identity Center登录URL。 最小长度： 1 最大长度： 64
permission_sets	Array of PermissionSet objects	IAM身份中心的权限集相关信息。
groups	Array of IdentityCenterGroup objects	Identity Center的用户组信息。

表 4-23 PermissionSet

参数	参数类型	描述
permission_set_id	String	权限集ID。 最小长度： 1 最大长度： 64

参数	参数类型	描述
permission_set_name	String	权限集名称。 最小长度：1 最大长度：64
description	String	权限集描述。 最小长度：1 最大长度：64

表 4-24 IdentityCenterGroup

参数	参数类型	描述
group_id	String	Identity Center的用户组ID。 最小长度：1 最大长度：64
group_name	String	用户组名称。 最小长度：1 最大长度：64
description	String	Identity Center的用户组描述信息。 最小长度：1 最大长度：64

请求示例

查询当前客户的Identity Center用户信息。

```
GET https://{hostname}/v1/landing-zone/identity-center
```

响应示例

状态码： 200

请求成功。

```
{
  "identity_store_id": "string",
  "user_portal_url": "string",
  "permission_sets": [ {
    "permission_set_id": "string",
    "permission_set_name": "string",
    "description": "string"
  } ],
  "groups": [ {
    "group_id": "string",
    "group_name": "string",
    "description": "string"
  } ]
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2 Landing Zone 治理

4.2.1 列出控制策略

功能介绍

列出RGC服务里所有的预置控制策略。

URI

GET /v1/governance/controls

表 4-25 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页页面的最大值。 最小值：1 最大值：2000 缺省值：200
marker	否	String	页面标记。 最小长度：1 最大长度：64

请求参数

无

响应参数

状态码： 200

表 4-26 响应 Body 参数

参数	参数类型	描述
controls	Array of Control objects	控制策略信息。
page_info	PageInfoDto object	本页返回条目数量。

表 4-27 Control

参数	参数类型	描述
identifier	String	控制策略ID。 最小长度：1 最大长度：128
name	String	控制策略名称。 最小长度：1 最大长度：64
description	String	控制策略描述。 最小长度：1 最大长度：64
guidance	String	控制策略必须性。 最小长度：1 最大长度：64
resource	Array of strings	治理资源。
framework	Array of strings	治理策略来自的框架。
service	String	控制策略所属服务。 最小长度：1 最大长度：64
implementation	String	服务控制策略（SCP），配置规则。 最小长度：1 最大长度：64
behavior	String	控制策略类型。包括主动性控制策略Proactive、检测性控制策略Detective、预防性控制策略Preventive。 最小长度：1 最大长度：64

参数	参数类型	描述
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
severity	String	控制策略严重性。 最小长度：1 最大长度：64
control_objective	String	控制策略目标。 最小长度：1 最大长度：128
version	String	控制策略版本。 最小长度：1 最大长度：128
release_date	String	控制策略发布时间。

表 4-28 PageInfoDto

参数	参数类型	描述
next_marker	String	在标签请求参数中使用以获取输出的下一部分。重复此操作，直到响应元素返回null。如果存在，则表示可用的输出比当前响应中包含的输出多。
current_count	Integer	本页返回条目数量。

请求示例

列出RGC服务里所有的预置控制策略。

GET https://{hostname}/v1/governance/controls

响应示例

状态码：200

请求成功。

```
{
  "controls": [ {
    "identifier": "string",
    "name": "string",
    "description": "控制策略ID。",
    "guidance": "string",
    "resource": [ "string" ],
    "framework": [ "string" ],
    "service": "string",
```

```
"implementation": "string",  
"behavior": "string",  
"owner": "string",  
"severity": "string",  
"control_objective": "string",  
"version": "string",  
"release_date": "2023-11-21T06:54:43.941Z"  
}],  
"page_info": {  
  "next_marker": "string",  
  "description": "本页返回条目数量。",  
  "current_count": 0  
}  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.2 列出不合规信息

功能介绍

列出组织里所有不合规的资源信息。

URI

GET /v1/governance/control-violations

表 4-29 Query 参数

参数	是否必选	参数类型	描述
account_id	否	String	账户ID，用于过滤不合规资源。 最大长度：64
organization_unit_id	否	String	注册OU ID，用于过滤不合规资源。 最大长度：64

请求参数

无

响应参数

状态码： 200

表 4-30 响应 Body 参数

参数	参数类型	描述
control_violations	Array of ControlViolation objects	控制策略合规性。

表 4-31 ControlViolation

参数	参数类型	描述
account_id	String	控制策略纳管账号ID。 最小长度：1 最大长度：64
account_name	String	控制策略纳管账号名称。 最小长度：1 最大长度：64
display_name	String	控制策略显示名称。 最小长度：1 最大长度：512
name	String	控制策略名称。 最小长度：1 最大长度：128
control_id	String	控制策略ID。 最小长度：1 最大长度：128
parent_organization_unit_id	String	父注册OU ID。 最小长度：1 最大长度：64
parent_organization_unit_name	String	父注册OU名称。 最小长度：1 最大长度：64
region	String	区域名称。 最小长度：1 最大长度：64
resource	String	控制策略不合规资源。 最小长度：1 最大长度：64

参数	参数类型	描述
resource_type	String	控制策略不合规资源类型。 最小长度：1 最大长度：64
service	String	云服务名称。 最小长度：1 最大长度：64

请求示例

列出组织里所有不合规的资源信息。

```
GET https://{hostname}/v1/governance/control-violations
```

响应示例

状态码：200

请求成功。

```
{
  "control_violations": [ {
    "account_id": "string",
    "account_name": "string",
    "display_name": "string",
    "name": "string",
    "control_id": "string",
    "parent_organization_unit_id": "string",
    "parent_organization_unit_name": "string",
    "region": "string",
    "resource": "string",
    "resource_type": "string",
    "service": "string"
  } ]
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.3 查询控制策略详细信息

功能介绍

查询单个预置的控制策略详细信息。

URI

GET /v1/governance/controls/{control_id}

表 4-32 路径参数

参数	是否必选	参数类型	描述
control_id	是	String	控制策略ID。 最小长度：1 最大长度：128

请求参数

无

响应参数

状态码： 200

表 4-33 响应 Body 参数

参数	参数类型	描述
identifier	String	控制策略ID。 最小长度：1 最大长度：128
implementation	String	服务控制策略（SCP），配置规则。 最小长度：1 最大长度：64
guidance	String	控制策略必须性。 最小长度：1 最大长度：64
resource	Object	治理资源。
service	String	控制策略所属服务。 最小长度：1 最大长度：64
behavior	String	控制策略类型。包括主动性控制策略Proactive、检测性控制策略Detective、预防性控制策略Preventive。 最小长度：1 最大长度：64

参数	参数类型	描述
control_objective	String	控制策略目标。 最小长度：1 最大长度：128
framework	Array of strings	治理策略来自的框架。
artifacts	Array of Artifact objects	控制策略内容。
aliases	Array of strings	控制策略别名。
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
severity	String	控制策略严重性。 最小长度：1 最大长度：64
version	String	控制策略版本。 最小长度：1 最大长度：128
release_date	String	控制策略发布时间。

表 4-34 Artifact

参数	参数类型	描述
content	Content object	控制策略内容。
type	String	策略类型。

表 4-35 Content

参数	参数类型	描述
en	String	英文策略内容。 最小长度：1 最大长度：20480

参数	参数类型	描述
ch	String	中文策略内容。 最小长度：1 最大长度：20480

请求示例

查询单个预置的控制策略详细信息。

```
GET https://{hostname}/v1/governance/controls/{control_id}
```

响应示例

状态码：200

请求成功。

```
{
  "identifier": "string",
  "implementation": "string",
  "guidance": "string",
  "resource": [ "string" ],
  "service": "string",
  "behavior": "string",
  "control_objective": "string",
  "framework": [ "string" ],
  "artifacts": [ {
    "content": {
      "en": "string",
      "ch": "string"
    },
    "type": "string"
  } ],
  "aliases": [ "string" ],
  "owner": "string",
  "severity": "string",
  "version": "string",
  "release_date": "2023-11-21T06:55:57.419Z"
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.4 开启控制策略

功能介绍

给组织下的某个单元开启某个控制策略。

URI

POST /v1/governance/controls/enable

请求参数

表 4-36 请求 Body 参数

参数	是否必选	参数类型	描述
identifier	是	String	控制策略ID。 最小长度：1 最大长度：128
target_identifier	是	String	组织单元的ID信息。 最小长度：1 最大长度：2048

响应参数

状态码： 201

表 4-37 响应 Body 参数

参数	参数类型	描述
control_operation_request_id	String	控制策略的操作ID。 最小长度：1 最大长度：64

请求示例

给组织下的某个单元开启某个控制策略。

```
POST https://{hostname}/v1/governance/controls/enable
{
  "identifier": "string",
  "target_identifier": "string"
}
```

响应示例

状态码： 201

请求成功。

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

状态码

状态码	描述
201	请求成功。

错误码

请参见[错误码](#)。

4.2.5 关闭控制策略

功能介绍

关闭组织下的某个单元的某个控制策略。

URI

POST /v1/governance/controls/disable

请求参数

表 4-38 请求 Body 参数

参数	是否必选	参数类型	描述
identifier	是	String	控制策略ID。 最小长度： 1 最大长度： 128
target_identifier	是	String	组织单元的ID信息。 最小长度： 1 最大长度： 2048

响应参数

状态码： 201

表 4-39 响应 Body 参数

参数	参数类型	描述
control_operate_request_id	String	控制策略的操作ID。 最小长度：1 最大长度：64

请求示例

关闭组织下的某个单元的某个控制策略。

```
POST https://{hostname}/v1/governance/controls/disable
{
  "identifier": "string",
  "target_identifier": "string"
}
```

响应示例

状态码：201

请求成功。

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

状态码

状态码	描述
201	请求成功。

错误码

请参见[错误码](#)。

4.2.6 查询控制策略操作状态

功能介绍

根据操作ID查询返回指定ID的操作状态。

URI

GET /v1/governance/operation-control-status/{operation_control_status_id}

表 4-40 路径参数

参数	是否必选	参数类型	描述
operation_control_status_id	是	String	操作控制策略的请求ID。 最小长度：1 最大长度：36

请求参数

无

响应参数

状态码：200

表 4-41 响应 Body 参数

参数	参数类型	描述
control_operation	ControlOperation object	控制策略实施的情况。

表 4-42 ControlOperation

参数	参数类型	描述
operation_control_status_id	String	本次操作控制策略的ID。 最小长度：1 最大长度：64
operation_type	String	操作类型，启用控制策略或禁用控制策略。 最小长度：1 最大长度：64
status	String	控制策略实施的状态 SUCCEEDED FAILED IN_PROGRESS。 最小长度：1 最大长度：64
message	String	控制策略实施失败的错误信息。 最小长度：1 最大长度：2048
start_time	String	操作开始的时间。
end_time	String	操作结束的时间。

请求示例

根据操作ID查询返回指定ID的操作状态。

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

响应示例

状态码： 200

请求成功。

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

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.7 列出开启的控制策略

功能介绍

列出组织里开启的所有控制策略信息。

URI

GET /v1/governance/enabled-controls

表 4-43 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页页面的最大值。 最小值： 1 最大值： 2000 缺省值： 200

参数	是否必选	参数类型	描述
marker	否	String	页面标记。 最小长度：1 最大长度：64

请求参数

无

响应参数

状态码：200

表 4-44 响应 Body 参数

参数	参数类型	描述
enabled_controls	Array of EnabledControl objects	开启控制策略信息。
page_info	PageInfoDto object	本页返回条目数量。

表 4-45 EnabledControl

参数	参数类型	描述
manage_account_id	String	管理纳管账号ID。 最小长度：1 最大长度：64
control_identifier	String	控制策略标识。 最小长度：1 最大长度：128
name	String	控制策略名称。 最小长度：1 最大长度：64
description	String	控制策略描述。 最小长度：1 最大长度：64

参数	参数类型	描述
control_objective	String	控制策略目标。 最小长度：1 最大长度：128
behavior	String	控制策略类型。包括主动性控制策略Proactive、检测性控制策略Detective、预防性控制策略Preventive。 最小长度：1 最大长度：64
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
regional_preference	String	区域选项，取值有两种分别是：区域的regional和全局的global。 最小长度：1 最大长度：128

表 4-46 PageInfoDto

参数	参数类型	描述
next_marker	String	在标签请求参数中使用以获取输出的下一部分。重复此操作，直到响应元素返回null。如果存在，则表示可用的输出比当前响应中包含的输出多。
current_count	Integer	本页返回条目数量。

请求示例

列出组织里开启的所有控制策略信息。

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

响应示例

状态码： 200

请求成功。

```
{
  "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",  
  "description" : "本页返回条目的数量。",  
  "current_count" : 0  
}  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.8 列出注册 OU 下开启的控制策略

功能介绍

列出组织里某个注册OU开启的所有控制策略信息。

URI

GET /v1/governance/managed-organization-units/
{managed_organization_unit_id}/controls

表 4-47 路径参数

参数	是否必选	参数类型	描述
managed_organiza- tion_unit _id	是	String	注册OU ID。 最大长度：64

表 4-48 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页页面的最大值。 最小值：1 最大值：2000 缺省值：200

参数	是否必选	参数类型	描述
marker	否	String	页面标记。 最小长度：1 最大长度：64

请求参数

无

响应参数

状态码：200

表 4-49 响应 Body 参数

参数	参数类型	描述
control_summaries	Array of TargetControl objects	治理策略概要。
state	String	控制策略启用状态。 最小长度：1 最大长度：64
page_info	PageInfoDto object	本页返回条目数量。

表 4-50 TargetControl

参数	参数类型	描述
manage_account_id	String	管理纳管账号ID。 最小长度：1 最大长度：64
control_identifier	String	控制策略标识。 最小长度：1 最大长度：128
state	String	控制策略启用状态。 最小长度：1 最大长度：64

参数	参数类型	描述
version	String	控制策略当前版本号。 最小长度：1 最大长度：64
name	String	控制策略名称。 最小长度：1 最大长度：64
description	String	控制策略描述信息。 最小长度：1 最大长度：64
control_objective	String	控制策略目标。 最小长度：1 最大长度：128
behavior	String	控制策略类型。包括主动性控制策略Proactive、检测性控制策略Detective、预防性控制策略Preventive。 最小长度：1 最大长度：64
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
regional_preference	String	区域选项，取值有两种分别是：区域的regional和全局的global。 最小长度：1 最大长度：128
guidance	String	控制策略必须性。 最小长度：1 最大长度：64
service	String	控制策略所属服务。 最小长度：1 最大长度：64
implementation	String	服务控制策略（SCP），配置规则。 最小长度：1 最大长度：64

表 4-51 PageInfoDto

参数	参数类型	描述
next_marker	String	在标签请求参数中使用以获取输出的下一部分。重复此操作，直到响应元素返回null。如果存在，则表示可用的输出比当前响应中包含的输出多。
current_count	Integer	本页返回条目数量。

请求示例

列出组织里某个注册OU开启的所有控制策略信息。

```
GET https://{hostname}/v1/governance/managed-organization-units/{managed_organization_unit_id}/controls
```

响应示例

状态码： 200

请求成功。

```
{
  "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"
  } ],
  "state": "string",
  "page_info": {
    "next_marker": "string",
    "description": "本页返回条目数量。",
    "current_count": 0
  }
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.9 列出纳管账号下开启的控制策略

功能介绍

列出组织里某个纳管账号开启的所有控制策略信息。

URI

GET /v1/governance/managed-accounts/{managed_account_id}/controls

表 4-52 路径参数

参数	是否必选	参数类型	描述
managed_account_id	是	String	纳管账号ID。 最大长度：64

表 4-53 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页页面的最大值。 最小值：1 最大值：2000 缺省值：200
marker	否	String	页面标记。 最小长度：1 最大长度：64

请求参数

无

响应参数

状态码：200

表 4-54 响应 Body 参数

参数	参数类型	描述
control_summaries	Array of TargetControl objects	治理策略概要。

参数	参数类型	描述
state	String	控制策略启用状态。 最小长度：1 最大长度：64
page_info	PageInfoDto object	本页返回条目数量。

表 4-55 TargetControl

参数	参数类型	描述
manage_accoun t_id	String	管理纳管账号ID。 最小长度：1 最大长度：64
control_identif ier	String	控制策略标识。 最小长度：1 最大长度：128
state	String	控制策略启用状态。 最小长度：1 最大长度：64
version	String	控制策略当前版本号。 最小长度：1 最大长度：64
name	String	控制策略名称。 最小长度：1 最大长度：64
description	String	控制策略描述信息。 最小长度：1 最大长度：64
control_object ive	String	控制策略目标。 最小长度：1 最大长度：128
behavior	String	控制策略类型。包括主动性控制策略Proactive、 检测性控制策略Detective、预防性控制策略 Preventive。 最小长度：1 最大长度：64

参数	参数类型	描述
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
regional_preference	String	区域选项，取值有两种分别是：区域的regional和全局的global。 最小长度：1 最大长度：128
guidance	String	控制策略必须性。 最小长度：1 最大长度：64
service	String	控制策略所属服务。 最小长度：1 最大长度：64
implementation	String	服务控制策略（SCP），配置规则。 最小长度：1 最大长度：64

表 4-56 PageInfoDto

参数	参数类型	描述
next_marker	String	在标签请求参数中使用以获取输出的下一部分。重复此操作，直到响应元素返回null。如果存在，则表示可用的输出比当前响应中包含的输出多。
current_count	Integer	本页返回条目数量。

请求示例

列出组织里某个纳管账号开启的所有控制策略信息。

GET https://{hostname}/v1/governance/managed-accounts/{managed_account_id}/controls

响应示例

状态码：200

请求成功。

```
{
  "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"  
}],  
"state": "string",  
"page_info": {  
  "next_marker": "string",  
  "description": "本页返回条目数量。",  
  "current_count": 0  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.10 查询纳管账号的合规状态

功能介绍

查询组织里某个纳管账号的资源合规状态。

URI

GET /v1/governance/managed-accounts/{managed_account_id}/compliance-status

表 4-57 路径参数

参数	是否必选	参数类型	描述
managed_account_id	是	String	纳管账号ID。 最大长度：64

表 4-58 Query 参数

参数	是否必选	参数类型	描述
control_id	否	String	启用的控制策略信息。 最小长度：1 最大长度：128

请求参数

无

响应参数

状态码：200

表 4-59 响应 Body 参数

参数	参数类型	描述
compliance_status	String	合规状态。 最小长度：1 最大长度：128

请求示例

查询组织里某个纳管账号的资源合规状态。

```
GET https://{hostname}/v1/governance/managed-accounts/{managed_account_id}/compliance-status
```

响应示例

状态码：200

请求成功。

```
{  
  "compliance_status": "string"  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.11 查询注册 OU 的合规状态

功能介绍

查询组织里某个注册OU下所有纳管账号的资源合规状态。

URI

GET /v1/governance/managed-organization-units/
{managed_organization_unit_id}/compliance-status

表 4-60 路径参数

参数	是否必选	参数类型	描述
managed_organiza- tion_unit _id	是	String	注册OU ID。 最大长度：64

表 4-61 Query 参数

参数	是否必选	参数类型	描述
control_id	否	String	启用的控制策略信息。 最小长度：1 最大长度：128

请求参数

无

响应参数

状态码：200

表 4-62 响应 Body 参数

参数	参数类型	描述
compliance_st atus	String	合规状态。 最小长度：1 最大长度：128

请求示例

查询组织里某个注册OU下所有纳管账号的资源合规状态。

GET https://{hostname}/v1/governance/managed-organization-units/{managed_organization_unit_id}/compliance-status

响应示例

状态码： 200

请求成功。

```
{  
  "compliance_status": "string"  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.12 查询注册 OU 开启的控制策略

功能介绍

查询组织里某个注册OU下开启的某个控制策略的详细信息。

URI

GET /v1/governance/managed-organization-units/
{managed_organization_unit_id}/controls/{control_id}

表 4-63 路径参数

参数	是否必选	参数类型	描述
managed_organization_unit_id	是	String	注册OU ID。 最大长度： 64
control_id	是	String	控制策略ID。 最小长度： 1 最大长度： 128

请求参数

无

响应参数

状态码： 200

表 4-64 响应 Body 参数

参数	参数类型	描述
control	EnabledControl object	开启控制策略信息。
regions	Array of strings	开启的区域。
state	String	是否允许启用控制策略。
state_message	String	状态说明。
version	String	控制策略当前版本。 最小长度： 1 最大长度： 64

表 4-65 EnabledControl

参数	参数类型	描述
manage_account_id	String	管理纳管账号ID。 最小长度： 1 最大长度： 64
control_identifier	String	控制策略标识。 最小长度： 1 最大长度： 128
name	String	控制策略名称。 最小长度： 1 最大长度： 64
description	String	控制策略描述。 最小长度： 1 最大长度： 64
control_objective	String	控制策略目标。 最小长度： 1 最大长度： 128

参数	参数类型	描述
behavior	String	控制策略类型。包括主动性控制策略Proactive、检测性控制策略Detective、预防性控制策略Preventive。 最小长度：1 最大长度：64
owner	String	纳管账号的创建来源，包括CUSTOM和RGC。 最小长度：1 最大长度：128
regional_preference	String	区域选项，取值有两种分别是：区域的regional和全局的global。 最小长度：1 最大长度：128

请求示例

查询组织里某个注册OU下开启的某个控制策略的详细信息。

```
GET https://{hostname}/v1/governance/managed-organization-units/{managed_organization_unit_id}/controls/{control_id}
```

响应示例

状态码：200

请求成功。

```
{
  "control": {
    "manage_account_id": "string",
    "control_identifier": "string",
    "name": "string",
    "description": "string",
    "control_objective": "string",
    "behavior": "string",
    "owner": "string",
    "regional_preference": "string"
  },
  "regions": [ "string" ],
  "state": "string",
  "state_message": "string",
  "version": "string"
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.13 查询纳管账号的 Config 规则合规性信息

功能介绍

查询纳管账号的Config规则合规性信息

URI

GET /v1/governance/managed-accounts/{managed_account_id}/config-rule-compliances

表 4-66 路径参数

参数	是否必选	参数类型	描述
managed_account_id	是	String	纳管账号ID。 最大长度：64

请求参数

无

响应参数

状态码：200

表 4-67 响应 Body 参数

参数	参数类型	描述
account_id	String	纳管账号ID
config_rule_compliances	Array of ConfigRuleCompliance objects	Config规则合规性信息

表 4-68 ConfigRuleCompliance

参数	参数类型	描述
rule_name	String	合规规则。
status	String	合规状态。
region	String	区域信息。

参数	参数类型	描述
control_id	String	控制策略ID。 最小长度：1 最大长度：128

请求示例

查询组织里某个纳管账号的Config规则合规性信息

GET https://{hostname}/v1/governance/managed-accounts/{managed_account_id}/config-rule-compliances

响应示例

状态码：200

请求成功。

```
{  
  "account_id": "string",  
  "config_rule_compliances": [{  
    "rule_name": "string",  
    "status": "string",  
    "region": "string",  
    "control_id": "string"  
  }]  
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

4.2.14 列出漂移信息

功能介绍

列出Landing Zone的所有漂移详细信息。

URI

GET /v1/governance/drift-details

请求参数

无

响应参数

状态码： 200

表 4-69 响应 Body 参数

参数	参数类型	描述
drift_details	Array of DriftDetail objects	漂移详细信息。

表 4-70 DriftDetail

参数	参数类型	描述
manage_account_id	String	管理纳管账号ID。 最小长度： 1 最大长度： 64
drift_type	String	漂移类型。 最小长度： 1 最大长度： 64
drift_target_id	String	漂移发生的纳管账号ID或注册OU ID。 最小长度： 1 最大长度： 64
drift_target_type	String	漂移目标类型，类型有accountId和policyId。 最小长度： 1 最大长度： 64
drift_message	String	漂移信息。 最小长度： 1 最大长度： 512
parent_organization_unit_id	String	父注册OU ID。 最小长度： 1 最大长度： 64

请求示例

列出Landing Zone的所有漂移详细信息。

```
GET https://{hostname}/v1/governance/drift-details
```

响应示例

状态码： 200

请求成功。

```
{
  "drift_details": [{
    "manage_account_id": "string",
    "drift_type": "string",
    "drift_target_id": "string",
    "drift_target_type": "string",
    "drift_message": "string",
    "parent_organization_unit_id": "string"
  }]
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见[错误码](#)。

5 权限和授权项

5.1 权限和授权项说明

如果您需要对您所拥有的RGC进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），如果华为账号所具备的权限功能已经能满足您的要求，您可以跳过本章节，不影响您使用RGC服务的其他功能。

通过IAM，您可以通过授权控制主体（IAM用户、用户组、IAM委托）对华为云资源的访问范围。

账号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。

例如，用户要查询Landing Zone设置状态，那么这个IAM用户被授予的策略中必须包含允许“rgc:landingZoneStatus:get”的授权项，该接口才能调用成功。

5.2 策略授权参考

云服务在IAM预置了常用授权项，称为系统策略。如果IAM系统策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建IAM自定义策略来进行精细的访问控制，IAM自定义策略是对系统策略的扩展和补充。

除IAM服务外，[Organizations](#)服务中的[服务控制策略](#)（Service Control Policies，以下简称SCP）也可以使用这些授权项元素设置访问控制策略。

SCP是一种基于组织的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。服务策略可以关联到组织、组织单元和成员账号。当服务策略关联到组织或组织单元时，该组织或组织单元下所有账号受到该策略影响。IAM策略授予权限的有效性受SCP限制，只有在SCP允许范围内的权限才能生效。

本章节介绍IAM服务策略授权场景中自定义策略和组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑IAM自定义策略，请参考[创建自定义策略](#)。
- 如何使用这些元素编辑SCP自定义策略，请参考[创建SCP](#)。

操作 (Action)

操作 (Action) 即为策略中支持的操作项。

- “访问级别”列描述如何对操作进行分类 (list、read和write等)。此分类可帮助您了解在策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
 - 资源类型支持通配符号*表示所有。如果此列没有值 (-)，则必须在策略语句的Resource元素中指定所有资源类型 (“*”)。
 - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
 - 资源类型列中必需资源在表中用星号 (*) 标识，表示使用此操作必须指定该资源类型。
- “条件键”列包括了可以在策略语句的Condition元素中支持指定的键值。
 - 如果该操作项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
 - 如果该操作项资源类型列没有值 (-)，则表示条件键对整个操作项生效。
 - 如果此列没有值 (-)，表示此操作不支持指定条件键。

您可以在自定义策略语句的Action元素中指定以下RGC的相关操作。

表 5-1 RGC 支持的操作项

操作项	描述	访问级别	资源类型 (*为必须)	条件键
rgc:homeRegion:get	授予获取主区域的权限。	read	-	-
rgc:preLaunch:check	授予登录前检查的权限。	write	-	-
rgc:landingZone:setup	授予设置着陆区的权限。	write	-	-
rgc:landingZoneStatus:get	授予获取设置着陆区当前状态的权限。	read	-	-
rgc:availableUpdates:get	授予获取着陆区可更新信息的权限。	read	-	-
rgc:landingZoneConfiguration:get	授予获取着陆区配置信息的权限。	read	-	-
rgc:landingZoneIdentityCenter:get	授予获取着陆区相关用户中心信息的权限。	read	-	-
rgc:organizationalUnit:register	授予注册组织单元的权限。	write	-	-
rgc:organizationalUnit:reRegister	授予重新注册组织单元的权限。	write	-	-

操作项	描述	访问级别	资源类型 (*为必须)	条件键
rgc:organizationalUnit:deRegister	授予去注册组织单元的权限。	write	-	-
rgc:operation:get	授予获取注册组织单元或者重新注册组织单元或者取消注册单元当前状态的权限。	read	-	-
rgc:managedOrganizationalUnits:delete	授予删除组织单元的权限。	write	-	-
rgc:managedOrganizationalUnits:get	授予获取纳管组织单元的权限。	read	-	-
rgc:organizationalUnit:create	授予创建组织单元的权限。	write	-	-
rgc:managedOrganizationalUnits:list	授予列出所有纳管组织单元的权限。	list	-	-
rgc:account:enroll	授予纳管账号的权限。	write	-	-
rgc:account:unEnroll	授予去纳管账号的权限。	write	-	-
rgc:managedAccount:update	授予更新账号的权限。	write	-	-
rgc:managedAccount:get	授予获取纳管账号的权限。	read	-	-
rgc:managedAccountsForParent:list	授予列出某个组织单元下所有账号的权限。	list	-	-
rgc:account:create	授予创建账号的权限。	write	-	-
rgc:managedAccounts:list	授予列出所有纳管账号的权限。	list	-	-
rgc:managedCoreAccount:get	授予获取核心账号的权限。	read	-	-
rgc:controls:list	授予列出控制策略的权限。	list	-	-
rgc:controlViolations:list	授予列出不合规控制策略的权限。	list	-	-

操作项	描述	访问级别	资源类型 (*为必须)	条件键
rgc:control:get	授予获取控制策略的权限。	read	-	-
rgc:control:enable	授予开启控制策略的权限。	write	-	-
rgc:control:disable	授予关闭控制策略的权限。	write	-	-
rgc:controlOperate:get	授予获取开启或者关闭控制策略当前状态的权限。	read	-	-
rgc:enabledControls:list	授予列出组织开启的控制策略的权限。	list	-	-
rgc:controlsForOrganizationUnit:list	授予列出某个组织单元开启的控制策略的权限。	list	-	-
rgc:controlsForAccount:list	授予列出某个账号开启的控制策略的权限。	list	-	-
rgc:complianceStatusForAccount:get	授予获取某个账号合规状态的权限。	read	-	-
rgc:complianceStatusForOrganizationUnit:get	授予获取某个组织单元下所有纳管账号的资源合规状态的权限。	read	-	-
rgc:controlsForOrganizationUnit:get	授予获取某个组织单元下某个控制策略的权限。	read	-	-
rgc:configRuleCompliance:list	授予列出某个账号下所有配置规则合规信息的权限。	list	-	-

RGC的API通常对应着一个或多个操作项。[表2](#)API与操作项的关系展示了API与操作项的关系，以及该API需要依赖的操作项。

表 5-2 API 与操作项的关系

API	对应的操作项	依赖的操作项
GET /v1/landing-zone/home-region	rgc:homeRegion:get	-

API	对应的操作项	依赖的操作项
POST /v1/landing-zone/pre-launch-check	rgc:preLaunch:check	-
POST /v1/landing-zone/setup	rgc:landingZone:setup	-
GET /v1/landing-zone/status	rgc:landingZoneStatus:get	-
GET /v1/landing-zone/available-updates	rgc:availableUpdates:get	-
GET /v1/landing-zone/configuration	rgc:landingZoneConfiguration:get	-
GET /v1/landing-zone/identity-center	rgc:landingZoneIdentityCenter:get	-
POST /v1/managed-organization/organization-unit/{organization_unit_id}/register	rgc:organizationalUnit:register	-
POST /v1/managed-organization/organization-unit/{organization_unit_id}/re-register	rgc:organizationalUnit:reRegister	-
POST /v1/managed-organization/managed-organization-unit/{managed_organization_unit_id}/de-register	rgc:organizationalUnit:deRegister	-
GET /v1/managed-organization/{operation_id}	rgc:operation:get	-
DELETE /v1/managed-organization/managed-organization-unit/{managed_organization_unit_id}	rgc:managedOrganizationalUnits:delete	-
GET /v1/managed-organization/managed-organization-unit/{managed_organization_unit_id}	rgc:managedOrganizationalUnits:get	-
POST /v1/managed-organization/managed-organization-units	rgc:organizationalUnit:create	-

API	对应的操作项	依赖的操作项
GET /v1/managed-organization/managed-organization-units	rgc:managedOrganizationalUnits:list	-
POST /v1/managed-organization/account/{account_id}/enroll	rgc:account:enroll	-
POST /v1/managed-organization/managed-account/{managed_account_id}/un-enroll	rgc:account:unEnroll	-
POST /v1/managed-organization/managed-account/{managed_account_id}/update	rgc:managedAccount:update	-
GET /v1/managed-organization/managed-account/{managed_account_id}	rgc:managedAccount:get	-
GET /v1/managed-organization/managed-organization-unit/{managed_organization_unit_id}/managed-accounts	rgc:managedAccountsForParent:list	-
POST /v1/managed-organization/managed-accounts	rgc:account:create	-
GET /v1/managed-organization/managed-accounts	rgc:managedAccounts:list	-
GET /v1/managed-organization/managed-organization-unit/{managed_organization_unit_id}/managed-accounts	rgc:managedCoreAccount:get	-
GET /v1/governance/controls	rgc:controls:list	-
GET /v1/governance/control-violations	rgc:controlViolations:list	-
GET /v1/governance/controls/{control_id}	rgc:control:get	-

API	对应的操作项	依赖的操作项
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-organization-unit/{managed_organization_unit_id}/controls	rgc:controlsForOrganizationUnit:list	-
GET /v1/governance/managed-account/{managed_account_id}/controls	rgc:controlsForAccount:list	-
GET /v1/governance/managed-account/{managed_account_id}/compliance-status	rgc:complianceStatusForAccount:get	-
GET /v1/governance/managed-organization-unit/{managed_organization_unit_id}/compliance-status	rgc:complianceStatusForOrganizationUnit:get	-
GET /v1/governance/managed-organization-unit/{managed_organization_unit_id}/controls/{control_id}	rgc:controlsForOrganizationUnit:get	-
GET /v1/governance/account/{account_id}/config-rule-compliances	rgc:configRuleCompliance:list	-
GET /v1/governance/drift-details	rgc:driftDetails:list	-

资源类型 (Resource)

RGC服务不支持在策略中的资源中指定资源进行权限控制。如需允许访问RGC服务，请在策略的Resource元素中使用通配符号*，表示策略将应用到所有资源。

条件 (Condition)

RGC服务不支持在策略中的条件键中配置服务级的条件键。

RGC可以使用适用于所有服务的全局条件键，请参考[全局条件键](#)。

6 附录

6.1 状态码

表 6-1 状态码

状态码	编码	错误码说明
100	Continue	继续请求。 这个临时响应用来通知客户端，它的部分请求已经被服务器接收，且仍未被拒绝。
101	Switching Protocols	切换协议。只能切换到更高级的协议。 例如，切换到HTTP的新版本协议。
201	Created	创建类的请求完全成功。
202	Accepted	已经接受请求，但未处理完成。
203	Non-Authoritative Information	非授权信息，请求成功。
204	NoContent	请求完全成功，同时HTTP响应不包含响应体。 在响应OPTIONS方法的HTTP请求时返回此状态码。
205	Reset Content	重置内容，服务器处理成功。
206	Partial Content	服务器成功处理了部分GET请求。
300	Multiple Choices	多种选择。请求的资源可包括多个位置，相应可返回一个资源特征与地址的列表用于用户终端（例如：浏览器）选择。
301	Moved Permanently	永久移动，请求的资源已被永久的移动到新的URI，返回信息会包括新的URI。
302	Found	资源被临时移动。

状态码	编码	错误码说明
303	See Other	查看其它地址。 使用GET和POST请求查看。
304	Not Modified	所请求的资源未修改，服务器返回此状态码时，不会返回任何资源。
305	Use Proxy	所请求的资源必须通过代理访问。
306	Unused	已经被废弃的HTTP状态码。
400	BadRequest	非法请求。 建议直接修改该请求，不要重试该请求。
401	Unauthorized	在客户端提供认证信息后，返回该状态码，表明服务端指出客户端所提供的认证信息不正确或非法。
402	Payment Required	保留请求。
403	Forbidden	请求被拒绝访问。 返回该状态码，表明请求能够到达服务端，且服务端能够理解用户请求，但是拒绝做更多的事情，因为该请求被设置为拒绝访问，建议直接修改该请求，不要重试该请求。
404	NotFound	所请求的资源不存在。 建议直接修改该请求，不要重试该请求。
405	MethodNotAllowed	请求中带有该资源不支持的方法。 建议直接修改该请求，不要重试该请求。
406	Not Acceptable	服务器无法根据客户端请求的内容特性完成请求。
407	Proxy Authentication Required	请求要求代理的身份认证，与401类似，但请求者应当使用代理进行授权。
408	Request Time-out	服务器等候请求时发生超时。 客户端可以随时再次提交该请求而无需进行任何更改。
409	Conflict	服务器在完成请求时发生冲突。 返回该状态码，表明客户端尝试创建的资源已经存在，或者由于冲突请求的更新操作不能被完成。
410	Gone	客户端请求的资源已经不存在。 返回该状态码，表明请求的资源已被永久删除。
411	Length Required	服务器无法处理客户端发送的不带Content-Length的请求信息。
412	Precondition Failed	未满足前提条件，服务器未满足请求者在请求中设置的其中一个前提条件。

状态码	编码	错误码说明
413	Request Entity Too Large	由于请求的实体过大，服务器无法处理，因此拒绝请求。为防止客户端的连续请求，服务器可能会关闭连接。如果只是服务器暂时无法处理，则会包含一个Retry-After的响应信息。
414	Request-URI Too Large	请求的URI过长（URI通常为网址），服务器无法处理。
415	Unsupported Media Type	服务器无法处理请求附带的媒体格式。
416	Requested range not satisfiable	客户端请求的范围无效。
417	Expectation Failed	服务器无法满足Expect的请求头信息。
422	Unprocessable Entity	请求格式正确，但是由于含有语义错误，无法响应。
429	TooManyRequests	表明请求超出了客户端访问频率的限制或者服务端接收到多于它能处理的请求。建议客户端读取相应的Retry-After首部，然后等待该首部指出的时间后再重试。
500	InternalServerError	表明服务端能被请求访问到，但是不能理解用户的请求。
501	Not Implemented	服务器不支持请求的功能，无法完成请求。
502	Bad Gateway	充当网关或代理的服务器，从远端服务器接收到了一个无效的请求。
503	ServiceUnavailable	被请求的服务无效。 建议直接修改该请求，不要重试该请求。
504	ServerTimeout	请求在给定的时间内无法完成。客户端仅在为请求指定超时（Timeout）参数时会得到该响应。
505	HTTP Version not supported	服务器不支持请求的HTTP协议的版本，无法完成处理。

6.2 错误码

当您调用API时，如果遇到“APIGW”开头的错误码，请参见[API网关错误码](#)进行处理。

表 6-2 错误码

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.400	Bad Request: {0}.	云服务内部错误，请重试。	请联系技术支持。
400	rgcservice.1001	bad request for query icc instance.	查询是否开通IAM身份中心实例失败。	请稍后重试。
400	rgcservice.1002	bad request for register region.	注册区域失败。	请稍后重试。
400	rgcservice.1003	bad request for start identity center.	启动IAM身份中心失败。	请稍后重试。
400	rgcservice.1004	bad request for get registered regions.	查询IAM身份中心实例已开通的区域列表失败。	请稍后重试。
400	rgcservice.1005	the queried region is different from the registered region.	所选主区域和已注册的IAM身份中心的区域不一致。	请重新选择主区域。
400	rgcservice.1006	create instance fail.	创建IAM身份中心实例失败。	请稍后重试。
400	rgcservice.1007	create instance status is not enable.	IAM身份中心实例状态不可用。	请稍后重试。
400	rgcservice.1008	create permission set fail.	创建权限失败。	请稍后重试。
400	rgcservice.1009	create user fail.	创建用户失败。	请稍后重试。
400	rgcservice.1010	bad request for get identity center service status.	获取IAM身份中心状态失败。	请稍后重试。
400	rgcservice.1011	bad request for create permission set.	在IIC实例中创建权限集失败。	请稍后重试。
400	rgcservice.1012	bad request for attach managed policy to permission set.	将系统管理策略附加到权限集失败。	请稍后重试。
400	rgcservice.1013	bad request for create account assignment.	给账号分配权限失败。	请稍后重试。
400	rgcservice.1014	bad request for describe account assignment creation status.	获取账号分配创建状态失败。	请稍后重试。
400	rgcservice.1015	bad request for create group membership.	用户组绑定用户失败。	请稍后重试。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1016	bad request for create group.	创建用户组失败。	请稍后重试。
400	rgcservice.1017	bad request for create user.	创建IIC用户失败。	请稍后重试。
400	rgcservice.1018	bad request for get projects.	查询项目信息失败。	请稍后重试。
403	rgcservice.1019	does not have {0} permissions.	当前账号没有权限。	请检查账号权限。
400	rgcservice.1021	bad request for create agency.	创建委托失败。	请稍后重试。
400/403	rgcservice.1022	fail request for assume with service principal.	委托切换失败。	请稍后重试。
400	rgcservice.1024	bad request for create service linked agency.	创建服务关联委托失败。	请稍后重试。
403	rgcservice.1028	Not a management account.	当前账号不是管理账号。	请检查账号是否管理账号。
400	rgcservice.1032	bad request for enable trust service.	启用可信服务失败。	请稍后重试。
400	rgcservice.1033	organizations service not provision.	组织服务未开通。	请开通组织服务。
400	rgcservice.1034	bad request for authorization header pattern.	Token请求头非法。	请检查 authorization请求头是否合法传入。
403	rgcservice.1035	not found for http header:{0}.	无法找到HTTP请求头。	请检查 HTTP请求头是否存在。
400	rgcservice.1036	bad request for request proof.	proof请求头非法。	请检查 proof请求头是否合法传入。
400	rgcservice.1037	bad request for impersonate.	获取凭据失败。	请联系技术支持。
400	rgcservice.1038	bad request for listRoles.	查询权限列表失败。	请联系技术支持。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1039	create base line group fail.	创建基线用户组失败。	请联系技术支持。
400	rgcservice.1040	retrieve user fail.	检索用户失败。	请联系技术支持。
400	rgcservice.1041	describe user fail.	查询用户详情失败。	请联系技术支持。
400	rgcservice.1042	show compliance details fail.	查询合规性信息失败。	请联系技术支持。
400	rgcservice.1043	list aggregate compliance fail.	查询资源聚合器合规规则列表失败。	请联系技术支持。
400	rgcservice.1044	list aggregator fail.	查询资源聚合器列表失败。	请联系技术支持。
400	rgcservice.1045	bad request for list groups.	请求用户组列表失败。	请联系技术支持。
400	rgcservice.1046	The user already exists, but the user name is different.	IAM身份中心用户已存在，但用户名与预留用户名不同。	请检查用户名是否正确，填写保持一致。
500	rgcservice.1049	create account failed, failure reason {0}.	创建账号失败。	请稍后重试。
400	rgcservice.1050	Bad Request:{0} not found.	请求错误，未找到相关资源。	请确认资源是否存在。
400	rgcservice.1052	The parent is not managed by RGC.	父级组织单元未注册。	请检查父级组织单元是否已注册。
400	rgcservice.1053	The organization unit child resource is not empty.	当前组织单元的子资源不为空。	请检查是否存在子组织单元或成员账号
400	rgcservice.1054	The account is not managed by RGC.	当前账号未纳管。	请检查当前账号。
400	rgcservice.1055	The organization unit is not managed by RGC.	当前组织单元未注册。	请检查当前组织单元。
400	rgcservice.1056	bad request for query iam assume agency.	切换到成员账号身份失败。	请联系技术支持。
400	rgcservice.1057	The organization unit is not found.	组织单元不存在。	请检查组织单元是否已注册成功。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1058	The requested control policy does not exist.	控制策略不存在。	请检查操作的控制策略是否存在。
400	rgcservice.1059	The relationship between the control and the specified target does not exist.	组织单元未启用请求的控制策略。	不允许关闭未开启的控制策略。
400	rgcservice.1060	The Root and core organizational units cannot implement additional control strategies.	root和基础组织单元不允许开启或禁用控制策略。	根组织单元和基础组织单元不允许进行控制策略开启与关闭操作。
400	rgcservice.1062	Not allowed to perform operations on an OU that is not successfully registered.	未注册的组织单元不能开启或禁用控制策略。	请操作注册成功的组织单元。
400	rgcservice.1065	The {0} operation is not complete.	操作尚未完成，请稍后重试。	请稍后重试。
400	rgcservice.1067	The landing zone environment is not set.	Landing Zone环境未设置。	请设置Landing Zone环境。
400	rgcservice.1068	The selected region is invalid.	所选主区域无效。	请检查主区域可用性状态。
400	rgcservice.1069	The bucket policy is empty.	桶策略为空。	请联系技术支持。
400	rgcservice.1070	bad request for obs.	请求云服务OBS失败。	请稍后重试。
400	rgcservice.1072	Get a unexpected status code.	请求云服务Organizations失败。	请联系技术支持。
400	rgcservice.1073	Org list accounts occur error.	查询组织单元中账号列表失败。	请稍后重试。
400	rgcservice.1074	Failed to call the API for deleting a stackSetInstance.	调用云服务RFS删除stackSet实例失败。	请检查云服务RFS运行是否正常，stackSet实例资源是否正常。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1075	The baseLine control cannot be operated.	基线控制策略不支持开启与禁用操作。	基线控制策略不允许进行控制策略开启与关闭操作。
400	rgcservice.1076	The control state is {0}, can not do current organization unit operation.	控制策略操作状态异常，不允许进行操作。	请确认控制策略与组织单元的关系处于正确的结束态后再进行操作。
500	rgcservice.1077	This account has existed,should not be our account,failed reason {0}.	账号已存在。	请检查当前账号是否已存在。
400	rgcservice.1078	Manage account should not be our set up account.	管理账号不能作为核心账号。	请检查账号，管理账号不能作为核心账号。
500	rgcservice.1079	Move account Organizations report failed.	移动账号失败。	请联系技术支持。
400	rgcservice.1080	The core and root organization unit can not be delete or deregister.	不能删除或取消注册基础组织单元和根组织单元。	不能删除或取消注册基础组织单元和根组织单元。
400	rgcservice.1081	The parent organization unit type could not be core.	父组织单元不能是基础组织单元。	父组织单元不能是基础组织单元。
400	rgcservice.1082	bad request for create iic user.	创建IAM身份中心用户失败。	请稍后重试。
400	rgcservice.1083	Create account failed. Reason: The ou type is incorrect.	创建账号失败，组织单元类型不正确。	请检查组织单元类型。
400	rgcservice.1084	Create account failed. The action is not supported.	创建账号失败，账号状态不支持。	请检查账号当前状态是否为纳管中。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1085	The account already exists or is not managed by the RGC.	账号已经存在或没有被RGC纳管。	请检查账号是否由RGC纳管。
400	rgcservice.1086	fixed parameters cannot be changed.	固定参数不允许被修改。	请不要修改固定参数。
400	rgcservice.1087	The landing zone environment has been set, any parameter cannot be changed.	Landing Zone环境已经设置完成，参数不能被修改。	请不要修改参数。
400	rgcservice.1088	organizationUnitId and accountId can not exist together.	组织单元ID与账号ID不能同时作为查询条件。	仅使用组织单元ID或账号ID进行查询。
404	rgcservice.1089	The account is not found.	账号不存在。	请检查账号是否存在。
400	rgcservice.1090	create assignment failed, failure reason is {0}.	给账号的IIC用户分配权限失败。	请联系技术支持。
	rgcservice.1091	The resource {0} create or deploy failed, you can check detail at RFS view.	资源创建或部署失败，请前往RFS查看详情。	请前往RFS查看详情。
400	rgcservice.1092	[RFS]The RFS returns a failure message to deploy stackSet instances.	调用云服务RFS部署stackSet实例返回失败。	请检查云服务RFS或对应资源stackSet实例是否正常，正常后请再次重试。
400	rgcservice.1093	[RFS]The RFS returns a failure message to create stackSet instances.	调用云服务RFS创建stackSet实例返回失败。	请检查云服务RFS或对应资源stackSet实例是否正常，正常后请再次重试。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1094	[RFS]The RFS returns a failure message to create stackSet.	调用云服务RFS创建stackSet返回失败。	请检查云服务RFS或对应资源stackSet是否正常, 正常后请再次重试。
400	rgcservice.1095	The user already exists, but the user details cannot be queried.	用户已存在, 但无法查询用户详情。	请稍后重试。
400	rgcservice.1096	The user already exists, but the email address of the user is different.	账号已存在, 账号邮箱与用户之前配置的邮箱不同。	请检查账号邮箱, 填写保持一致。
404	rgcservice.1097	No user information is found.	找不到用户信息。	请联系技术支持。
400	rgcservice.1098	The account type is not custom, can not be unenroll.	非自定义账号, 不能取消纳管。	请检查要取消纳管的账号是否正确。
	rgcservice.1099	The pap returned error.	调用云服务PAP接口失败。	请稍后重试。
400	rgcservice.1100	The account already exists and is managed by the RGC.	该账号已被RGC纳管。	请检查纳管的账号是否正确。
400	rgcservice.1102	The account already exists, but the parentOrganizationUnitId is different.	该账号已存在, 但父组织单元ID与预留ID不同。	请检查账号所属父组织单元是否正确, 填写保持一致。
400	rgcservice.1103	The account already exists, but the parentOrganizationUnitName is different.	该账号已存在, 但父组织单元名称与预留名称不同。	请检查账号所属父组织单元是否正确, 填写保持一致。
400	rgcservice.1104	The create account task is timeout.	创建账号超时。	请稍后重试。
400	rgcservice.1105	bad request for list entry. The entry is empty.	查询账号所属父组织单元失败。	请检查账号信息是否正确。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1106	Org list create account status occur error.	查询创建的账号状态异常。	请检查 Organization 账号是否正在创建中或 Organization 服务是否正常，正常后请再次尝试。
400	rgcservice.1107	The administrator user does not exist.	IAM 身份中心管理员用户不存在。	请检查账号信息是否正确。
400	rgcservice.1108	The control detail is not found.	查询控制策略详情失败，控制策略不存在。	请检查控制策略 ID 是否正确。
400	rgcservice.1109	The bucket policy does not exist.	查询桶策略失败，该桶策略不存在。	请稍后重试。
400	rgcservice.1110	Please accept the open beta of resource access service.	账号未开通 RGC 公测。	请申请开通 RGC 公测。
404	rgcservice.1111	not found for http header.	HTTP 请求头不存在。	请稍后重试。
400	rgcservice.1112	bad request for invalid user profile.	获取用户配置文件失败。	请稍后重试。
400	rgcservice.1113	get op svc pki token fail.	获取 pkiToken 失败。	请联系技术支持。
400	rgcservice.1114	The account already exists, but the account phone number is different.	设置 Landing Zone 失败，手机号与之前填写不一致。	请检查账号的电话号码。
400	rgcservice.1115	phone number is required in domestic.	请填写手机号。	请检查基础组织单元下的账号的手机号码是否存在。
400	rgcservice.1116	get a empty pki token.	获取 PKIToken 为空。	请联系技术支持。
500	rgcservice.1117	can't find {0} in v3 or v5 policy.	查询策略失败，策略不存在。	请检查策略名是否正确。

状态码	错误码	错误信息	描述	处理措施
404	rgcservice.1118	The account type is invalid.	查询核心账号详情失败，账号类型不合法。	请检查查询的核心账号类型是否正确。
500/400	rgcservice.1119	Rfs list templates occur error.	查询RFS模版失败。	请联系技术支持。
409	rgcservice.1200	concurrent modification.	设置Landing Zone冲突。	请稍后重试。
400	rgcservice.1201	The core and root organization unit can not be register.	无法注册根和基础组织单元。	请检查注册的组织单元是否已存在并检查类型。
400	rgcservice.1202	The account already exists, but the account type is not custom.	当前的账号非自定义账号。	请检查纳管的账号的类型。
400	rgcservice.1203	The account status is {0}, can not do current account operation.	当前账号无法执行该操作，请检查账号状态。	请检查账号状态。
400	rgcservice.1204	The organization unit status is {0}, can not do current account operation.	组织单元状态异常，无法进行账户操作。	请检查账号所属的组织单元状态。
400	rgcservice.1205	The organization unit status is {0}, can not do current organization unit operation.	组织单元状态异常，无法进行组织单元操作。	请检查组织单元状态。
409	rgcservice.1206	The organization unit conflict, the organization unit is registered.	组织单元已注册成功，不能再次注册。	如果需要再次注册请调用重注册接口。
400	rgcservice.1207	The parent organization unit type could not be core or root.	父组织单元类型不能是根组织单元。	请检查父组织单元类型。
400	rgcservice.1208	The organization unit is managed by other management account.	组织单元由其他管理账号管理。	请检查组织单元ID。

状态码	错误码	错误信息	描述	处理措施
404	rgcservice.1209	No landing zone has been created for this account.	当前账号未开通Landing Zone。	请检查当前账号是否已开通LandingZone。
404	rgcservice.1210	The landing zone environment status is failed.	Landing Zone开通失败，暂不支持该操作。	请检查当前账号是否已成功开通LandingZone。
400	rgcservice.1211	The organization unit name has existed in Organization,please input unique and unused organization unit name.	组织单元名称重复，请输入唯一的组织单元名称。	请检查要注册的组织单元是否正确。
400	rgcservice.1212	Failed to query role id from pap.	调用云服务PAP查询权限失败。	请联系技术支持。
400	rgcservice.1213	Failed to create agency pap.	调用云服务PAP创建委托失败。	请联系技术支持。
400	rgcservice.1214	Failed to allpy role id pap.	调用云服务PAP为委托授予项目的权限失败。	请联系技术支持。
400	rgcservice.1215	The account maybe invited to Organization,you need manually create a full access agency named OrganizationAccountAccessAgency to its manage account.	邀请作为Landing Zone核心账号的子账号，需要创建该账号到管理账号的委托，委托应该包括子账号所有权限，该权限名称为OrganizationAccountAccessAgency。	请为邀请的子账号创建Full Access权限的委托OrganizationAccountAccessAgency，委托给管理账号。
400	rgcservice.1216	bad request for delete service linked agency.	调用云服务PAP删除服务关联委托失败。	请联系技术支持。
400	rgcservice.1217	IAM list projects occur error.	调用云服务IAM列出项目失败。	请联系技术支持。
400	rgcservice.1218	The account status conflict, the account is enrolled.	当前账号已纳管。	当前账号已为纳管状态，无需再次纳管。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1220	Domain tag not found, domainId is {0}.	未查询到租户标签。	请确认租户ID是否正确。
400	rgcservice.1221	Domain info not found, domainId is {0}.	未查询到租户信息。	请确认租户ID是否正确。
	rgcservice.1222	email is required in global.	请填写Email信息。	请输入Email。
400	rgcservice.1223	Failed to create role.	创建自定义策略失败。	请联系技术支持。
400	rgcservice.1224	startTime should not be later than endTime.	请正确填写时间段，开始时间不能晚于结束时间。	请正确填写时间区域。
400	rgcservice.1225	Some accounts under the organization unit are in the Operation state.	组织单元下存在正在操作的账号。	请稍后重试。
403	rgcservice.1226	Can't find the ou, ould is {0}.	组织单元不存在。	请检查组织单元ID。
403	rgcservice.1227	Can't find the account, accountId is {0}.	账号不存在。	请检查账号ID。
400	rgcservice.1230	Should not have custom account.	不支持自定义账号。	请检查账号类型。
400	rgcservice.1231	Should have one Core Organization Unit.	必须包含基础组织单元。	请检查组织单元类型。
400	rgcservice.1232	Core Organization Unit should has two accounts.	基础组织单元必须包含两个账号。	请检查账号个数。
400	rgcservice.1233	Core Organization can only has two accounts,one must be AUDIT type,another one must be LOGGING type.	Landing Zone只有两个核心账号，一个为审计账号，一个为日志账号。	请调整输入参数。
400	rgcservice.1234	An existed Core Account has been created,the same name should be given.	Landing Zone重新设置时，核心账号不能修改名称。	请调整输入参数。

状态码	错误码	错误信息	描述	处理措施
400	rgcservice.1235	Audit account's notification email should be given.	审计账号需要填写通知邮箱。	请调整输入参数。
400	rgcservice.1236	When exist account scene, account name should be given.	账号已存在，但账号名称为空。	请调整输入参数。
400	rgcservice.1237	The organization name is empty.	组织单元名称为空。	请正确填写组织单元名称。
403	rgcservice.1238	The parent organization unit not found.	父组织单元不存在。	请检查是否存在父组织单元。
400	rgcservice.1239	When exist account scene, account id and name does not match.	账号已存在，但账号ID和名称不匹配。	请调整输入参数。

6.3 获取账号、IAM 用户、项目、用户组、区域、委托的名称和 ID

获取账号、IAM 用户、项目的名称和 ID

- 从控制台获取账号名、账号ID、用户名、用户ID、项目名称、项目ID
 - a. 在华为云首页右上角，单击“控制台”。
 - b. 在右上角的用户名中选择“我的凭证”。

图 6-1 进入我的凭证



- c. 在“我的凭证”界面，API凭证页签中，查看账号名、账号ID、用户名、用户ID、项目名称、项目ID。

每个区域的项目ID有所不同，需要根据业务所在的区域获取对应的项目ID。

图 6-2 查看账号名、账号 ID、用户名、用户 ID、项目名称、项目 ID



- 调用API获取用户ID、项目ID
 - 获取用户ID请参考：[管理员查询IAM用户列表](#)。
 - 获取项目ID请参考：[查询指定条件下的项目列表](#)。

获取用户组名称和 ID

步骤1 登录华为云，进入IAM控制台，选择“用户组”页签。

步骤2 单击需要查询的用户组前的下拉框，即可查询用户组名称、用户组ID。

图 6-3 查询用户组名称、用户组 ID



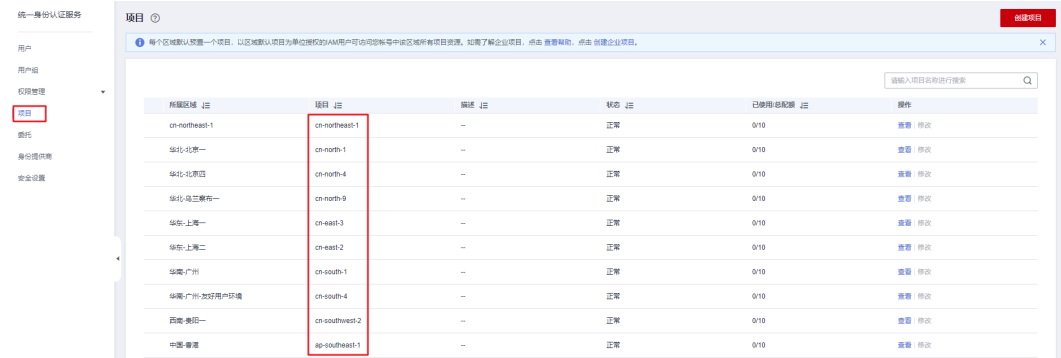
----结束

获取区域 ID

步骤1 登录华为云，进入IAM控制台，选择“项目”页签。

步骤2 “项目”列的内容即为所属区域对应的ID。

图 6-4 查看区域 ID



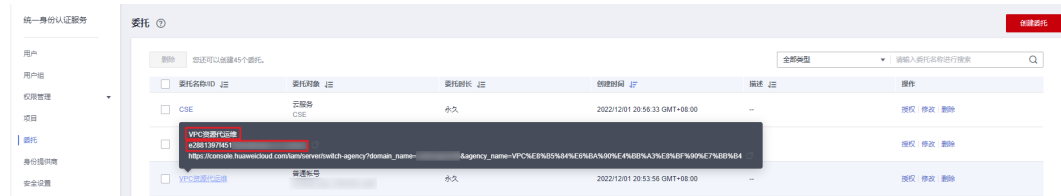
----结束

获取委托名称和 ID

步骤1 登录华为云，进入IAM控制台，选择“委托”页签。

步骤2 鼠标移动到需要查询名称和ID的委托上，黑色框中出现的第一行为委托名称，第二行为委托ID。

图 6-5 查看委托 ID



----结束

A 修订记录

发布日期	修订记录
2023-12-22	第一次正式发布