

统一身份认证

API 参考

文档版本 48
发布日期 2021-11-15



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。

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 参数说明	3
1.5 基本概念	4
2 API 概览	6
3 如何调用 API	15
3.1 构造请求	15
3.2 认证鉴权	17
3.3 返回结果	19
4 快速入门	21
4.1 密钥定期自动化轮换	21
4.2 企业管理华为云上多租户的联邦认证	23
4.3 对 IAM 用户的权限进行安全审计	26
5 API	30
5.1 Token 管理	30
5.1.1 获取 IAM 用户 Token (使用密码)	30
5.1.2 获取 IAM 用户 Token (使用密码+虚拟 MFA)	41
5.1.3 获取委托 Token	54
5.1.4 校验 Token 的有效性	64
5.2 访问密钥管理	70
5.2.1 获取委托的临时访问密钥和 securitytoken	70
5.2.2 获取用户的临时访问密钥和 securitytoken	76
5.2.3 获取联邦用户的临时访问密钥和 securitytoken	81
5.2.4 创建永久访问密钥	87
5.2.5 查询所有永久访问密钥	90
5.2.6 查询指定永久访问密钥	92
5.2.7 修改指定永久访问密钥	95
5.2.8 删除指定永久访问密钥	98
5.3 区域管理	99
5.3.1 查询区域列表	100

5.3.2 查询区域详情.....	103
5.4 项目管理.....	105
5.4.1 查询指定条件下的项目列表.....	106
5.4.2 查询指定 IAM 用户的项目列表.....	109
5.4.3 查询 IAM 用户可以访问的项目列表.....	112
5.4.4 创建项目.....	115
5.4.5 修改项目信息.....	118
5.4.6 查询项目详情.....	121
5.4.7 设置项目状态.....	124
5.4.8 查询项目详情与状态.....	126
5.4.9 查询项目配额.....	128
5.5 账号管理.....	131
5.5.1 查询 IAM 用户可以访问的账号详情.....	131
5.5.2 查询账号密码强度策略.....	133
5.5.3 按条件查询账号密码强度策略.....	135
5.5.4 查询账号配额.....	138
5.6 IAM 用户管理.....	142
5.6.1 管理员查询 IAM 用户列表.....	142
5.6.2 查询 IAM 用户详情（推荐）.....	147
5.6.3 查询 IAM 用户详情.....	150
5.6.4 查询 IAM 用户所属用户组.....	153
5.6.5 管理员查询用户组所包含的 IAM 用户.....	156
5.6.6 管理员创建 IAM 用户（推荐）.....	159
5.6.7 管理员创建 IAM 用户.....	164
5.6.8 修改 IAM 用户密码.....	168
5.6.9 修改 IAM 用户信息（推荐）.....	170
5.6.10 管理员修改 IAM 用户信息（推荐）.....	172
5.6.11 管理员修改 IAM 用户信息.....	178
5.6.12 管理员删除 IAM 用户.....	182
5.7 用户组管理.....	183
5.7.1 查询用户组列表.....	183
5.7.2 查询用户组详情.....	186
5.7.3 创建用户组.....	189
5.7.4 更新用户组.....	191
5.7.5 删除用户组.....	194
5.7.6 查询 IAM 用户是否在用户组中.....	196
5.7.7 添加 IAM 用户到用户组.....	197
5.7.8 移除用户组中的 IAM 用户.....	199
5.8 权限管理.....	200
5.8.1 查询权限列表.....	200
5.8.2 查询权限详情.....	207
5.8.3 查询租户授权信息.....	212

5.8.4 查询全局服务中的用户组权限.....	217
5.8.5 查询项目服务中的用户组权限.....	222
5.8.6 为用户组授予全局服务权限.....	228
5.8.7 为用户组授予项目服务权限.....	229
5.8.8 查询用户组是否拥有全局服务权限.....	231
5.8.9 查询用户组是否拥有项目服务权限.....	233
5.8.10 查询用户组的所有项目权限列表.....	234
5.8.11 查询用户组是否拥有所有项目指定权限.....	239
5.8.12 移除用户组的所有项目服务权限.....	241
5.8.13 移除用户组的全局服务权限.....	243
5.8.14 移除用户组的项目服务权限.....	244
5.8.15 为用户组授予所有项目服务权限.....	246
5.9 自定义策略管理.....	248
5.9.1 查询自定义策略列表.....	248
5.9.2 查询自定义策略详情.....	253
5.9.3 创建云服务自定义策略.....	258
5.9.4 创建委托自定义策略.....	264
5.9.5 修改云服务自定义策略.....	270
5.9.6 修改委托自定义策略.....	276
5.9.7 删除自定义策略.....	283
5.10 委托管理.....	284
5.10.1 查询指定条件下的委托列表.....	284
5.10.2 查询委托详情.....	287
5.10.3 创建委托.....	290
5.10.4 修改委托.....	293
5.10.5 删除委托.....	297
5.10.6 查询全局服务中的委托权限.....	298
5.10.7 查询项目服务中的委托权限.....	303
5.10.8 为委托授予全局服务权限.....	308
5.10.9 为委托授予项目服务权限.....	310
5.10.10 查询委托是否拥有全局服务权限.....	312
5.10.11 查询委托是否拥有项目服务权限.....	313
5.10.12 移除委托的全局服务权限.....	315
5.10.13 移除委托的项目服务权限.....	317
5.10.14 查询委托下的所有项目服务权限列表.....	318
5.10.15 为委托授予所有项目服务权限.....	321
5.10.16 检查委托下是否具有所有项目服务权限.....	322
5.10.17 移除委托下的所有项目服务权限.....	324
5.11 企业项目管理.....	325
5.11.1 查询企业项目关联的用户组.....	326
5.11.2 查询企业项目关联用户组的权限.....	328
5.11.3 基于用户组为企业项目授权.....	332

5.11.4 删除企业项目关联用户组的权限.....	334
5.11.5 查询用户组关联的企业项目.....	336
5.11.6 查询用户直接关联的企业项目.....	337
5.11.7 查询企业项目直接关联用户.....	339
5.11.8 查询企业项目直接关联用户的权限.....	341
5.11.9 基于用户为企业项目授权.....	345
5.11.10 删除企业项目直接关联用户的权限.....	347
5.11.11 基于委托为企业项目授权.....	349
5.11.12 删除企业项目关联委托的权限.....	351
5.12 安全设置.....	353
5.12.1 修改账号操作保护策略.....	353
5.12.2 查询账号操作保护策略.....	357
5.12.3 修改账号密码策略.....	360
5.12.4 查询账号密码策略.....	365
5.12.5 修改账号登录策略.....	367
5.12.6 查询账号登录策略.....	371
5.12.7 修改账号控制台访问策略.....	374
5.12.8 查询账号控制台访问策略.....	378
5.12.9 修改账号接口访问策略.....	381
5.12.10 查询账号接口访问策略.....	384
5.12.11 查询 IAM 用户的 MFA 绑定信息列表.....	387
5.12.12 查询指定 IAM 用户的 MFA 绑定信息.....	389
5.12.13 查询 IAM 用户的登录保护状态信息列表.....	392
5.12.14 查询指定 IAM 用户的登录保护状态信息.....	394
5.12.15 修改 IAM 用户的登录保护状态信息.....	397
5.12.16 绑定 MFA 设备.....	399
5.12.17 解绑 MFA 设备.....	401
5.12.18 创建 MFA 设备.....	403
5.12.19 删除 MFA 设备.....	405
5.13 联邦身份认证管理.....	406
5.13.1 通过联邦认证获取 token.....	406
5.13.1.1 SP initiated 方式.....	406
5.13.1.2 IdP initiated 方式.....	409
5.13.2 身份提供商.....	415
5.13.2.1 查询身份提供商列表.....	415
5.13.2.2 查询身份提供商详情.....	418
5.13.2.3 创建身份提供商.....	421
5.13.2.4 修改 SAML 身份提供商配置.....	424
5.13.2.5 删除 SAML 身份提供商.....	427
5.13.2.6 创建 OpenID Connect 身份提供商配置.....	429
5.13.2.7 修改 OpenID Connect 身份提供商配置.....	434
5.13.2.8 查询 OpenID Connect 身份提供商配置.....	438

5.13.3 映射.....	442
5.13.3.1 查询映射列表.....	442
5.13.3.2 查询映射详情.....	446
5.13.3.3 注册映射.....	450
5.13.3.4 更新映射.....	456
5.13.3.5 删除映射.....	461
5.13.4 协议.....	463
5.13.4.1 查询协议列表.....	463
5.13.4.2 查询协议详情.....	466
5.13.4.3 注册协议.....	468
5.13.4.4 更新协议.....	471
5.13.4.5 删除协议.....	473
5.13.5 Metadata.....	475
5.13.5.1 查询 Metadata 文件.....	475
5.13.5.2 查询 Keystone 的 Metadata 文件.....	477
5.13.5.3 导入 Metadata 文件.....	479
5.13.6 Token.....	481
5.13.6.1 获取联邦认证 unscoped token(IdP initiated).....	481
5.13.6.2 获取联邦认证 scoped token.....	486
5.13.6.3 获取联邦认证 token(OpenID Connect ID token 方式).....	493
5.13.6.4 获取联邦认证 unscoped token(OpenID Connect ID token 方式).....	501
5.13.7 查询联邦用户可以访问的账号列表.....	507
5.13.8 查询联邦用户可以访问的项目列表.....	509
5.14 自定义身份代理.....	512
5.14.1 获取自定义身份代理登录票据.....	512
5.15 版本信息管理.....	517
5.15.1 查询 Keystone API 的版本信息.....	517
5.15.2 查询 Keystone API 的 3.0 版本信息.....	519
5.16 服务和终端节点.....	521
5.16.1 查询服务列表.....	521
5.16.2 查询服务详情.....	524
5.16.3 查询服务目录.....	527
5.16.4 查询终端节点列表.....	529
5.16.5 查询终端节点详情.....	532
6 历史 API.....	536
6.1 查询企业项目关联的用户组.....	536
6.2 查询企业项目已关联用户组的权限.....	538
6.3 基于用户组为企业项目授权.....	541
6.4 删除企业项目关联的用户组权限.....	543
7 权限及授权项.....	545
7.1 权限及授权项说明.....	545
7.2 授权项.....	546

8 附录.....	560
8.1 状态码.....	560
8.2 错误码.....	562
8.3 获取账号、IAM 用户、项目、用户组、区域、委托的名称和 ID.....	575
A 修订记录.....	578

1 使用前必读

1.1 概述

欢迎使用统一身份认证（Identity and Access Management，简称IAM）。IAM是提供用户身份认证、权限分配、访问控制等功能的身管理服务，可以帮助您安全地控制对华为云资源的访问。您可以使用IAM创建以及管理用户，并使用权限来允许或拒绝他们对华为云资源的访问。

IAM除了支持界面控制台操作外，还提供API供您调用，您可以使用本文档提供的API对IAM进行相关操作，如创建用户、创建用户组、获取Token等。在调用IAM的API之前，请确保已经充分了解IAM的相关概念，详细信息请参见：[IAM产品介绍](#)。

1.2 调用说明

统一身份认证服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见[如何调用API](#)。

同时统一身份认证服务还提供多种编程语言的SDK供您使用，SDK的使用方法请参见<https://developer.huaweicloud.com/intl/zh-cn/sdk?IAM>。

1.3 终端节点

终端节点即调用API的**请求地址**，不同服务在不同区域的终端节点不同，您可以从[地区](#)和[终端节点](#)中查询所有的终端节点。

IAM的终端节点如[表1](#)所示。IAM是全局级服务，数据全局一份，在全局项目中存储，IAM所有的API都可以使用全局服务的Endpoint调用；除了全局区域外，为了配合其他区域级云服务的API/CLI访问，IAM在其他区域（除全局服务外的所有区域）提供部分API，请您根据[约束与限制](#)，选择对应区域的终端节点调用API。

表 1-1 IAM 的终端节点

区域名称	区域	终端节点（Endpoint）
全局	global	iam.myhuaweicloud.com

区域名称	区域	终端节点 (Endpoint)
华北-北京一	cn-north-1	iam.cn-north-1.myhuaweicloud.com
华北-北京二	cn-north-2	iam.cn-north-2.myhuaweicloud.com
华北-北京四	cn-north-4	iam.cn-north-4.myhuaweicloud.com
华东-上海一	cn-east-3	iam.cn-east-3.myhuaweicloud.com
华东-上海二	cn-east-2	iam.cn-east-2.myhuaweicloud.com
华南-广州	cn-south-1	iam.cn-south-1.myhuaweicloud.com
华南-深圳	cn-south-2	iam.cn-south-2.myhuaweicloud.com
西南-贵阳一	cn-southwest-2	iam.cn-southwest-2.myhuaweicloud.com
中国-香港	ap-southeast-1	iam.ap-southeast-1.myhuaweicloud.com
亚太-曼谷	ap-southeast-2	iam.ap-southeast-2.myhuaweicloud.com
亚太-新加坡	ap-southeast-3	iam.ap-southeast-3.myhuaweicloud.com
亚太-雅加达	ap-southeast-4	iam.ap-southeast-4.myhuaweicloud.com
非洲-约翰内斯堡	af-south-1	iam.af-south-1.myhuaweicloud.com

区域名称	区域	终端节点 (Endpoint)
拉美-圣地亚哥	la-south-2	iam.la-south-2.myhuaweicloud.com
欧洲-都柏林	eu-west-101	iam.myhuaweicloud.eu
欧洲-巴黎	eu-west-0	iam.eu-west-0.myhuaweicloud.com
土耳其-伊斯坦布尔	tr-west-1	iam.tr-west-1.myhuaweicloud.com
中东-阿布扎比-OP5	ae-ad-1	iam.ae-ad-1.myhuaweicloud.com
亚太-吉隆坡-OP6	my-kualalumpur-1	iam.my-kualalumpur-1.myhuaweicloud.com

1.4 参数说明

使用IAM API涉及的参数对应应在控制台名称及如何获取，如表1所示。

表 1-2 参数说明

API参数名称	控制台中文名称	控制台英文名称	如何从控制台获取
domain	账号	Account	获取账号名称和ID
domain_id/租户ID	账号ID	Account ID	
domain_name/租户名	账号名	Account name	
user	IAM用户	IAM user	获取IAM用户名称和ID
user_id	IAM用户ID	IAM user ID	
user_name	IAM用户名	IAM user name	
group	用户组	User group	获取用户组名称和ID
group_id	用户组ID	User group ID	

API参数名称	控制台中文名称	控制台英文名称	如何从控制台获取
group_name	用户组名称	User group name	
project	项目	Project	获取项目名称和ID
project_id	项目ID	Project ID	
project_name	项目名称	Project Name	
agency	委托	Agency	获取委托名称和ID
agency_id	委托ID	Agency ID	
agency_name	委托名称	Agency Name	

1.5 基本概念

使用API涉及的常用概念

- 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管理工作，而是创建用户并使用他们进行日常管理工作。
- 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）**

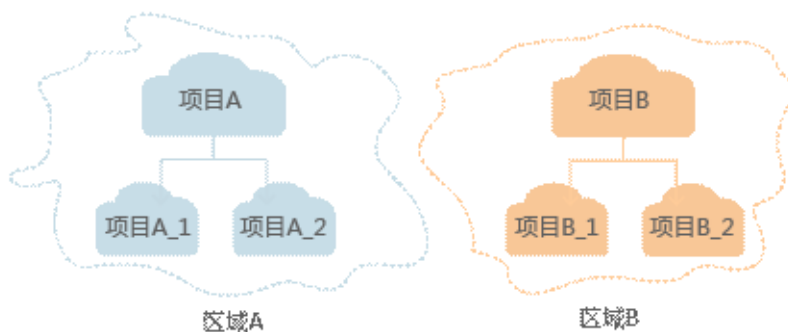
从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

详情请参见[区域和可用区](#)。
- 可用区（AZ, Availability Zone）**

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**

华为云的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，并在子项目中购买资源，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资源，使得资源的权限控制更加精确。

图 1-1 项目隔离模型



- 企业项目
企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，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《[企业管理服务用户指南](#)》。

2 API 概览

Token 管理

接口	说明
获取IAM用户Token (使用密码)	该接口可以用于通过用户名/密码的方式进行认证来获取IAM用户Token。
获取IAM用户Token (使用密码+虚拟MFA)	该接口可以用于在IAM用户开启了登录保护功能，并选择通过虚拟MFA验证时，通过用户名/密码+虚拟MFA的方式进行认证来获取IAM用户token。
获取委托Token	该接口可以用于获取委托方的token。
校验Token的有效性	该接口可以用于 管理员 校验本账号中IAM用户token的有效性，或IAM用户校验自己token的有效性

访问密钥管理

接口	说明
获取委托的临时访问密钥和securitytoken	该接口可以用于通过委托来获取临时访问密钥（临时AK/SK）和securitytoken。
获取用户的临时访问密钥和securitytoken	该接口可以用于通过token来获取临时AK/SK和securitytoken。
创建永久访问密钥	该接口可以用于 管理员 给IAM用户创建永久访问密钥，或IAM用户给自己创建永久访问密钥。
查询所有永久访问密钥	该接口可以用于 管理员 查询IAM用户的所有永久访问密钥，或IAM用户查询自己的所有永久访问密钥。
查询指定永久访问密钥	该接口可以用于 管理员 查询IAM用户的指定永久访问密钥，或IAM用户查询自己的指定永久访问密钥。
修改指定永久访问密钥	该接口可以用于 管理员 修改IAM用户的指定永久访问密钥，或IAM用户修改自己的指定永久访问密钥。

接口	说明
删除指定永久访问密钥	该接口可以用于 管理员 删除IAM用户的指定永久访问密钥，或IAM用户删除自己的指定永久访问密钥。

区域管理

接口	说明
查询区域列表	该接口可以用于查询区域列表。
查询区域详情	该接口可以用于查询区域详情。

项目管理

接口	说明
查询指定条件下的项目列表	该接口可以用于查询指定条件下的项目列表。
查询指定IAM用户的项目列表	该接口可以用于 管理员 查询指定IAM用户的项目列表，或IAM用户查询自己的项目列表。
查询IAM用户可以访问的项目列表	该接口可以用于查询IAM用户可以访问的项目列表。
创建项目	该接口可以用于 管理员 创建项目。
修改项目信息	该接口可以用于 管理员 修改指定项目信息。
查询项目详情	该接口可以用于查询指定项目详情。
设置项目状态	该接口可以用于 管理员 设置指定项目状态。项目状态包括：正常、冻结。
查询项目详情与状态	该接口可以用于 管理员 查询指定项目详情与状态。
查询项目配额	该接口可以用于查询指定项目配额。

账号管理

接口	说明
查询IAM用户可以访问的账号详情	该接口可以用于查询IAM用户可以访问的账号详情。
查询账号密码强度策略	该接口可以用于查询账号密码强度策略，查询结果包括密码强度策略的正则表达式及其描述。

接口	说明
按条件查询账号密码强度策略	该接口可以用于按条件查询账号密码强度策略，查询结果包括密码强度策略的正则表达式及其描述。
查询账号配额	该接口可以用于查询账号配额。

IAM 用户管理

接口	说明
管理员查询IAM用户列表	该接口可以用于 管理员 查询IAM用户列表。
查询IAM用户详情（推荐）	该接口可以用于 管理员 查询IAM用户详情，或IAM用户查询自己的用户详情。（可以查询手机号、邮箱）
查询IAM用户详情	该接口可以用于 管理员 查询IAM用户详情，或IAM用户查询自己的用户详情。（不可以查询手机号、邮箱）
查询IAM用户所属用户组	该接口可以用于 管理员 查询IAM用户所属用户组，或IAM用户查询自己所属用户组。
管理员查询用户组所包含的IAM用户	该接口可以用于 管理员 查询用户组中所包含的IAM用户。
管理员创建IAM用户（推荐）	该接口可以用于 管理员 创建IAM用户。
管理员创建IAM用户	该接口可以用于 管理员 创建IAM用户。
修改IAM用户密码	该接口可以用于IAM用户修改自己的密码。
修改IAM用户信息（推荐）	该接口可以用于IAM用户修改自己的用户信息。
管理员修改IAM用户信息（推荐）	该接口可以用于 管理员 修改IAM用户信息。
管理员修改IAM用户信息	该接口可以用于 管理员 修改IAM用户信息。
管理员删除IAM用户	该接口可以用于 管理员 删除指定IAM用户。
查询IAM用户的MFA绑定信息列表	该接口可以用于 管理员 查询IAM用户的MFA绑定信息列表。
查询指定IAM用户的MFA绑定信息	该接口可以用于 管理员 查询指定IAM用户的MFA绑定信息，或IAM用户查询自己的MFA绑定信息。
查询IAM用户的登录保护状态信息列表	该接口可以用于 管理员 查询IAM用户的登录保护状态列表。
查询指定IAM用户的登录保护状态信息	该接口可以用于 管理员 查询指定IAM用户的登录保护状态信息，或IAM用户查询自己的登录保护状态信息。

接口	说明
修改IAM用户的登录保护状态信息	该接口可以用于 管理员 修改IAM用户的登录保护状态信息。
绑定MFA设备	该接口可以用于IAM用户绑定MFA设备。
解绑MFA设备	该接口可以用于IAM用户解绑MFA设备。
创建MFA设备	接口可以用于IAM用户创建MFA设备。
删除MFA设备	该接口可以用于 管理员 删除MFA设备。

用户组管理

接口	说明
查询用户组列表	该接口可以用于 管理员 查询用户组列表。
查询用户组详情	该接口可以用于 管理员 查询用户组详情。
创建用户组	该接口可以用于 管理员 创建用户组。
更新用户组	该接口可以用于 管理员 更新用户组信息。
删除用户组	该接口可以用于 管理员 删除用户组。
查询IAM用户是否在用户组中	该接口可以用于 管理员 查询IAM用户是否在用户组中。
添加IAM用户到用户组	该接口可以用于 管理员 添加IAM用户到用户组。
移除用户组中的IAM用户	该接口可以用于 管理员 移除用户组中的IAM用户。

权限管理

接口	说明
查询权限列表	该接口可以用于 管理员 查询权限列表。
查询权限详情	该接口可以用于 管理员 查询权限详情。
查询全局服务中的用户组权限	该接口可以用于 管理员 查询全局服务中的用户组权限。
查询项目服务中的用户组权限	该接口可以用于 管理员 查询项目服务中的用户组权限。
为用户组授予全局服务权限	该接口可以用于 管理员 为用户组授予全局服务权限。
为用户组授予项目服务权限	该接口可以用于 管理员 为用户组授予项目服务权限。

接口	说明
查询用户组是否拥有全局服务权限	该接口可以用于 管理员 查询用户组是否拥有全局服务权限。
查询用户组是否拥有项目服务权限	该接口可以用于 管理员 查询用户组是否拥有项目服务权限。
查询用户组的所有项目权限列表	该接口可以用于 管理员 查询用户组所有项目服务权限列表。
查询用户组是否拥有所有项目指定权限	该接口可以用于 管理员 查询用户组是否拥有所有项目指定权限。
移除用户组的所有项目服务权限	该接口可以用于 管理员 移除用户组的所有项目服务权限。
移除用户组的全局服务权限	该接口可以用于 管理员 移除用户组的全局服务权限。
移除用户组的项目服务权限	该接口可以用于 管理员 移除用户组的项目服务权限。
为用户组授予所有项目服务权限	该接口可以用于 管理员 为用户组授予所有项目服务权限。

自定义策略管理

接口	说明
查询自定义策略列表	该接口可以用于 管理员 查询自定义策略列表。
查询自定义策略详情	该接口可以用于 管理员 查询自定义策略详情。
创建云服务自定义策略	该接口可以用于 管理员 创建云服务自定义策略。
创建委托自定义策略	该接口可以用于 管理员 创建委托自定义策略。
修改云服务自定义策略	该接口可以用于 管理员 修改云服务自定义策略。
修改委托自定义策略	该接口可以用于 管理员 修改委托自定义策略。
删除自定义策略	该接口可以用于 管理员 删除自定义策略。

委托管理

接口	说明
查询指定条件下的委托列表	该接口可以用于 管理员 查询指定条件下的委托列表。
查询委托详情	该接口可以用于 管理员 查询委托详情。

接口	说明
创建委托	该接口可以用于 管理员 创建委托。
修改委托	该接口可以用于 管理员 修改委托。
删除委托	该接口可以用于 管理员 删除委托。
查询全局服务中的委托权限	该接口可以用于 管理员 查询全局服务中的委托权限。
查询项目服务中的委托权限	该接口可以用于 管理员 查询项目服务中的委托权限。
为委托授予全局服务权限	该接口可以用于 管理员 为委托授予全局服务权限。
为委托授予项目服务权限	该接口可以用于 管理员 为委托授予项目服务权限。
查询委托是否拥有全局服务权限	该接口可以用于 管理员 查询委托是否拥有全局服务权限。
查询委托是否拥有项目服务权限	该接口可以用于 管理员 查询委托是否拥有项目服务权限。
移除委托的全局服务权限	该接口可以用于 管理员 移除委托的全局服务权限。
移除委托的项目服务权限	该接口可以用于 管理员 移除委托的项目服务权限。
查询委托下的所有项目服务权限列表	该接口可以用于 管理员 查询委托所有项目服务权限列表。
为委托授予所有项目服务权限	该接口可以用于 管理员 为委托授予所有项目服务权限。
检查委托下是否具有所有项目服务权限	该接口可以用于 管理员 检查委托是否具有所有项目服务权限。
移除委托下的所有项目服务权限	该接口可以用于 管理员 移除委托的所有项目服务权限。

企业项目管理

接口	说明
查询企业项目关联的用户组	该接口用于查询指定ID的企业项目所关联的用户组。
查询企业项目关联用户组的权限	该接口用于查询指定ID的企业项目所关联用户组的权限，适用于待查询的企业项目已关联了用户组。
基于用户组为企业项目授权	该接口用于给指定ID的企业项目授权，建立企业项目、用户组和权限的绑定关系。

接口	说明
删除企业项目关联用户组的权限	该接口提供删除某个企业项目关联的用户组权限。
查询用户组关联的企业项目	该接口可用于查询用户组所关联的企业项目。
查询用户直接关联的企业项目	该接口可用于查询用户所关联的企业项目。
查询企业项目直接关联用户	该接口可用于查询企业项目直接关联用户。
查询企业项目直接关联用户的权限	该接口可用于查询企业项目直接关联用户的权限。
基于用户为企业项目授权	该接口可用于基于用户为企业项目授权。
删除企业项目直接关联用户的权限	该接口可用于删除企业项目直接关联用户的权限，

安全设置

接口	说明
修改账号操作保护策略	该接口可以用于 管理员 修改账号操作保护策略。
查询账号操作保护策略	该接口可以用于查询账号操作保护策略。
修改账号密码策略	该接口可以用于 管理员 修改账号密码策略。
查询账号密码策略	该接口可以用于查询账号密码策略。
修改账号登录策略	该接口可以用于 管理员 修改账号登录策略。
查询账号登录策略	该接口可以用于查询账号登录策略。
修改账号控制台访问策略	该接口可以用于 管理员 修改账号控制台访问策略。
查询账号控制台访问策略	该接口可以用于查询账号控制台访问控制策略。
修改账号接口访问策略	该接口可以用于 管理员 修改账号接口访问策略。
查询账号接口访问策略	该接口可以用于查询账号接口访问控制策略。

联邦身份认证管理

接口	说明
通过联邦认证获取Token (SP initiated方式)	通过Openstack Client和ShibbolethECP Client获取联邦认证Token。

接口	说明
通过联邦认证获取 Token (IdP initiated 方式)	以“Client4ShibbolethIdP”脚本为例，介绍IdP initiated方式获取联邦认证Token的方法。
查询身份提供商列表	该接口可以用于查询身份提供商列表。
查询身份提供商详情	该接口可以用于查询身份提供商详情。
创建身份提供商	该接口可以用于 管理员 注册身份提供商。
修改SAML身份提供商配置	该接口可以用于 管理员 更新身份提供商。
删除SAML身份提供商	该接口可以用于 管理员 删除身份提供商。
查询映射列表	该接口可以用于查询映射列表。
查询映射详情	该接口可以用于查询映射详情。
注册映射	该接口可以用于 管理员 注册映射。
更新映射	该接口可以用于 管理员 更新映射。
删除映射	该接口可以用于 管理员 删除映射。
查询协议列表	该接口可以用于查询协议列表。
查询协议详情	该接口可以用于查询协议详情。
注册协议	该接口可以用于 管理员 注册协议（将协议关联到某一身份提供商）。
更新协议	该接口可以用于 管理员 更新协议。
删除协议	该接口可以用于 管理员 删除协议。
查询Metadata文件	该接口可以用于 管理员 查询身份提供商导入到IAM中的Metadata文件。
查询Keystone的Metadata文件	该接口可以用于查询keystone的Metadata文件。
导入Metadata文件	该接口可以用于 管理员 导入Metadata文件。
获取联邦认证Unscoped token(IdP initiated)	该接口可以用于通过IdP initiated的联邦认证方式获取unscoped token。
获取联邦认证scoped token	该接口可以用于通过联邦认证方式获取scoped token。
获取联邦认证 token(OpenID Connect ID token方式)	该接口可以用于通过OpenID Connect ID token方式获取联邦认证token。

接口	说明
获取联邦认证unscoped token(OpenID Connect ID token方式)	该接口可以用于通过OpenID Connect ID token方式获取联邦认证unscoped token。
查询联邦用户可以访问的账号列表	该接口用于查询联邦用户可以访问的账号列表。

自定义身份代理

接口	说明
获取自定义身份代理登录票据	该接口用于获取自定义身份代理登录票据logintoken。

版本信息管理

接口	说明
查询Keystone API的版本信息	该接口用于查询Keystone API的版本信息。
查询Keystone API的3.0版本信息	该接口用于查询Keystone API的3.0版本的信息。

服务和终端节点

接口	说明
查询服务列表	该接口可以用于查询服务列表。
查询服务详情	该接口可以用于查询服务详情。
查询服务目录	该接口可以用于查询请求头中X-Auth-Token对应的服务目录。
查询终端节点列表	该接口可以用于查询终端节点列表。
查询终端节点详情	该接口可以用于查询终端节点详情。

3 如何调用 API

3.1 构造请求

本节介绍REST API请求的组成，以调用[获取IAM用户Token（使用密码）](#)接口说明如何调用API，该API获取用户的Token，Token是用户的访问令牌，承载身份与权限信息，Token可以用于调用其他API时鉴权。

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	承载REST服务端点的服务器域名或IP，不同服务在不同区域，Endpoint不同，可以从 使用前必读 中获取。例如IAM服务在“中国-香港”区域的Endpoint为iam.ap-southeast-1.myhuaweicloud.com。
resource-path	资源路径，即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
query-string	查询参数，可选，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“中国-香港”区域的Token，则需使用“中国-香港”区域的Endpoint（iam.ap-southeast-1.myhuaweicloud.com），并在[获取IAM用户Token（使用密码）](#)的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

https://v3/auth/tokens

https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens

📖 说明

为查看方便，每个具体API的URI，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，而Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

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IAM用户Token（使用密码）](#)的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

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。

- **Content-Type**: 消息体的类型（格式），必选，默认取值为“application/json”。
- **X-Auth-Token**: 用户Token，可选，当使用Token方式认证时，必须填充该字段。X-Auth-Token是调用[获取IAM用户Token（使用密码）](#)接口返回的响应值，该接口功能为获取Token，因此调用该接口时，不用填写本字段。

📖 说明

公有云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IAM用户Token（使用密码）](#)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。

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

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。

对于[获取IAM用户Token（使用密码）](#)接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中*username*为用户名，*******为用户的登录密码，*domainname*为用户所属的账号名称，如果是账号本身获取token，*username*和*domainname*填为一致，*xxxxxxxxxxxxxxxxxxxx*为project的ID，获取方法请参见[获取账号、IAM用户、项目、用户组、区域、委托的名称和ID](#)。

📖 说明

scope参数定义了Token的作用范围，取值为project或domain，示例中取值为project，表示获取的Token仅能访问指定project下的资源，取值为domain时，表示获取的token可以访问指定账号下所有资源，scope参数的详细说明，请参见：[获取IAM用户Token（使用密码）](#)。

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "*****",
          "domain": {
            "name": "domainname"
          }
        }
      }
    }
  },
  "scope": {
    "project": {
      "id": "xxxxxxxxxxxxxxxxxxxx"
    }
  }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用[curl](#)、[Postman](#)或直接编写代码等方式发送请求调用API。对于[获取IAM用户Token（使用密码）](#)接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他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认证通用请求。
- （推荐）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，需要使用同一个Token鉴权时，可以缓存起来，避免频繁调用。

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。

Token可通过调用[获取IAM用户Token（使用密码）](#)接口获取，调用本服务API需要全局级别的Token，即调用[获取IAM用户Token（使用密码）](#)接口时，请求body中auth.scope的取值需要选择domain，如下所示。

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "domain": {
            "name": "IAMDomain"
          },
          "name": "IAMUser",
          "password": "IAMPassword"
        }
      }
    },
    "scope": {
      "domain": {
        "name": "IAMDomain"
      }
    }
  }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为获取到的Token。例如Token值为“ABCDEFJ....”，则调用接口时将“X-Auth-Token: ABCDEFJ....”加到请求消息头即可，如下所示。

```
GET https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

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签名认证方式可以避免因缓存的Token失效导致的API调用失败的问题。

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。


```
],  
  "catalog": [  
    {  
      "endpoints": [  
        {  
          "region_id": "ap-southeast-1",  
          .....  
        }  
      ]  
    }  
  ]  
}
```

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": "The format of message is error",  
  "error_code": "AS.0001"  
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

4 快速入门

4.1 密钥定期自动化轮换

场景描述

企业用户通常都会使用访问密钥（AK/SK）的方式对云上资源的进行API访问，但是访问密钥需要做到定期的自动轮换，以降低密钥泄露等潜在的安全风险。

本章节指导用户如何使用API调用的方式轮换访问密钥，您可进一步通过编程手段完成定期自动轮换工作。

前提条件

[账号管理员](#)操作其他IAM用户的访问密钥时，需要拥有Security Administrator权限，IAM用户操作自己的访问密钥无需任何权限。

总体思路

定期轮换访问密钥（AK/SK）时，步骤如下：

1. 创建AK/SK；
2. 查询您所有AK/SK的创建时间（或指定AK/SK的创建时间），判断使用时间是否需要轮换；
3. 更换新的AK/SK。
4. 删除需要轮换的AK/SK；

涉及的接口如下：

- [创建永久访问密钥](#)
- [查询所有永久访问密钥](#)
- [查询指定永久访问密钥](#)
- [删除指定永久访问密钥](#)

步骤 1：创建永久 AK/SK

URI: POST /v3.0/OS-CREDENTIAL/credentials

API文档详情请参见：[创建永久访问密钥](#)

- 请求示例

POST <https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials>

```
{
  "credential": {
    "description": "IAMDescription",
    "user_id": "07609fb9358010e21f7bc003751..."
  }
}
```

- 响应示例

```
{
  "credential": {
    "access": "P83EVBZJMXCYTMUII...",
    "create_time": "2020-01-08T06:25:19.014028Z",
    "user_id": "07609fb9358010e21f7bc003751...",
    "description": "IAMDescription",
    "secret": "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
    "status": "active"
  }
}
```

步骤 2：查询 AK/SK 的创建时间（或查询指定 AK/SK 的创建时间）

- 查询所有AK/SK的创建时间。

URI: GET [/v3.0/OS-CREDENTIAL/credentials](#)

API文档详情请参见：[查询所有永久访问密钥](#)

- 请求示例

1) IAM用户查询自己所有AK/SK的创建时间。

GET <https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials>

2) 管理员查询IAM用户所有AK/SK的创建时间。（待查询的用户ID为:076...）

GET https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials?user_id=076...

- 响应示例

```
{
  "credentials": [
    {
      "access": "LOSZM4YRVLKOY9E8X...",
      "create_time": "2020-01-08T06:26:08.123059Z",
      "user_id": "07609fb9358010e21f7bc0037...",
      "description": "",
      "status": "active"
    },
    {
      "access": "P83EVBZJMXCYTMU...",
      "create_time": "2020-01-08T06:25:19.014028Z",
      "user_id": "07609fb9358010e21f7bc003751...",
      "description": "",
      "status": "active"
    }
  ]
}
```

- 查询指定AK/SK的创建时间。

URI: GET [/v3.0/OS-CREDENTIAL/credentials/{access_key}](#)

API文档详情请参见：[查询指定永久访问密钥](#)

- 请求示例

GET https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials/{access_key}

- 响应示例

```
{
  "credential": {
```

```
"last_use_time": "2020-01-08T06:26:08.123059Z",  
"access": "LOSZM4YRVLKOY9E8...",  
"create_time": "2020-01-08T06:26:08.123059Z",  
"user_id": "07609fb9358010e21f7bc00375....",  
"description": "",  
"status": "active"  
}  
}
```

步骤 3: 更换新的 AK/SK

更换新的AK/SK，请重复[步骤1 创建永久AK/SK](#)。

步骤 4: 删除需要轮换的 AK/SK

URI: DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}

API文档详情请参见: [删除指定永久访问密钥](#)

- 请求示例
DELETE https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials/{access_key}
- 响应示例
该接口无返回体，状态码为204表示删除成功。

4.2 企业管理华为云上多租户的联邦认证

场景描述

部分企业级用户在公有云上存在多账号，并且通过企业级IDP系统联邦登录至公有云对不同账号进行操作，需要提前通过API自动配置联邦认证。

本章节指导用户如何使用API调用的方式自动配置联邦认证。

前提条件

账号[账号管理员](#)进行注册或导入操作需要拥有Security Administrator权限。

总体思路

进行华为云上多租户的联邦认证，步骤如下：

1. 注册身份提供商；
2. 注册映射；
3. 注册协议；
4. 导入Metadata文件；
5. 联邦登录。

涉及的接口如下：

- [注册身份提供商](#)
- [注册映射](#)
- [注册协议](#)

- [导入Metadata文件](#)

步骤 1：注册身份提供商

URI: PUT /v3/OS-FEDERATION/identity_providers/{id}

API文档详情请参见：[创建身份提供商](#)

- 请求示例

```
PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{id}
```

```
{
  "identity_provider":{
    "description":"Stores ACME identities.",
    "enabled":true
  }
}
```

- 响应示例

```
{
  "identity_provider": {
    "remote_ids": [],
    "enabled": true,
    "id": "ACME",
    "links": {
      "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",
      "protocols": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
    },
    "description": "Stores ACME identities."
  }
}
```

步骤 2：注册映射

URI: PUT /v3/OS-FEDERATION/mappings/{id}

API文档详情请参见：[注册映射](#)

- 请求示例

```
PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/{id}
```

```
{
  "mapping":{
    "rules":[
      {
        "local":[
          {
            "user":{
              "name":"LocalUser"
            }
          },
          {
            "group":{
              "name":"LocalGroup"
            }
          }
        ],
        "remote":[
          {
            "type":"UserName"
          },
          {
            "not_any_of":[
              "Contractor",
              "Guest"
            ]
          }
        ]
      }
    ]
  }
}
```

```
        "type": "orgPersonType"
      }
    ]
  }
}
```

- 响应示例

```
{
  "mapping": {
    "id": "ACME",
    "links": {
      "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/ACME"
    },
    "rules": [
      {
        "local": [
          {
            "user": {
              "name": "LocalUser"
            }
          },
          {
            "group": {
              "name": "LocalGroup"
            }
          }
        ],
        "remote": [
          {
            "type": "UserName"
          },
          {
            "not_any_of": [
              "Contractor",
              "Guest"
            ],
            "type": "orgPersonType"
          }
        ]
      }
    ]
  }
}
```

步骤 3: 注册协议

URI: PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

API文档详情请参见: [注册协议](#)

- 请求示例

PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

```
{
  "protocol": {
    "mapping_id": "ACME"
  }
}
```

- 响应示例

```
{
  "protocol": {
    "id": "saml",
    "links": {
      "identity_provider": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",

```

```
"self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/
protocols/saml"
  },
  "mapping_id": "ACME"
}
}
```

步骤 4: 导入 metadata 文件

URI: POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

API文档详情请参见: [导入Metadata文件](#)

- 请求示例

POST https://iam.myhuaweicloud.com/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

```
{
  "domain_id": "d78cbac186b744899480f25bd022....",
  "metadata": "$metadataContent",
  "xaccount_type": ""
}
```

- 响应示例

```
{
  "message": "Import metadata successful"
}
```

步骤 5: 联邦登录

完成云上多租户联邦认证配置。联邦登录详情参考: [身份提供商](#)。

4.3 对 IAM 用户的权限进行安全审计

场景描述

企业级用户通常需要对公有云上IAM用户的权限定期进行安全审计, 以确定IAM用户的权限未超出规定的范围。例如: 除账号和审计员用户以外的所有IAM用户都不应该具有任何IAM的管理权限。此安全审计往往是系统定期自动检查, 所以需要使用API来完成。

本章节指导用户如何使用API调用的方式对IAM用户的权限进行安全审计, 您可进一步通过编程手段完成定期安全审计工作。

前提条件

审计员对IAM用户的权限进行安全审计时, 需要拥有IAM ReadOnlyAccess (推荐) 或 Security Administrator权限。

总体思路

对IAM用户的权限进行安全审计, 步骤如下:

1. 查询用户组列表;
2. 查询全局服务中的用户组权限;
3. 查询项目服务中的用户组权限;

4. 确定需要审计的权限，查询用户组中的IAM用户，进行安全审计。

涉及的接口如下：

- [查询用户组列表](#)
- [查询全局服务中的用户组权限](#)
- [查询项目服务中的用户组权限](#)
- [管理员查询用户组所包含的IAM用户](#)

步骤 1：查询用户组列表

URI: GET /v3/groups

API文档详情请参见：[查询用户组列表](#)

- 请求示例
GET https://iam.myhuaweicloud.com/v3/groups

- 响应示例

```
{
  "groups": [
    {
      "create_time": 1536293929624,
      "description": "IAMDescription",
      "domain_id": "d78cbac186b744899480f25bd022....",
      "id": "5b050baea9db472c88cbae67e8d6....",
      "links": {
        "self": "https://iam.myhuaweicloud.com/v3/groups/5b050baea9db472c88cbae67e8d6...."
      },
      "name": "IAMGroupA"
    },
    {
      "create_time": 1578107542861,
      "description": "IAMDescription",
      "domain_id": "d78cbac186b744899480f25bd022....",
      "id": "07609e7eb200250a3f7dc003cb7a....",
      "links": {
        "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb7a...."
      },
      "name": "IAMGroupB"
    }
  ],
  "links": {
    "self": "https://iam.myhuaweicloud.com/v3/groups"
  }
}
```

步骤 2：查询全局服务中的用户组权限

URI: GET /v3/domains/{domain_id}/groups/{group_id}/roles

API文档详情请参见：[查询全局服务中的用户组权限](#)

- 请求示例
GET https://iam.myhuaweicloud.com/v3/domains/{domain_id}/groups/{group_id}/roles

- 响应示例

```
{
  "links": {
    "self": "https://iam.myhuaweicloud.com/v3/domains/d78cbac186b744899480f25bd022f468/
groups/077d71374b8025173f61c003ea0a11ac/roles"
  },
  "roles": [
    {

```

```

"catalog":"CDN",
"description":"Allow Query Domains",
"description_cn":"查询域名信息",
"display_name":"CDN Domain Viewer",
"flag":"fine_grained",
"id":"db4259cce0ce47c9903dfdc195eb...",
"links":{
  "self":"https://iam.myhuaweicloud.com/v3/roles/db4259cce0ce47c9903dfdc195eb..."
},
"name":"system_all_11",
"policy":{
  "Statement":[
    {
      "Action":[
        "cdn:configuration:queryDomains",
        "cdn:configuration:queryOriginServerInfo",
        "cdn:configuration:queryOriginConfInfo",
        "cdn:configuration:queryHttpsConf",
        "cdn:configuration:queryCacheRule",
        "cdn:configuration:queryReferConf",
        "cdn:configuration:queryChargeMode",
        "cdn:configuration:queryCacheHistoryTask",
        "cdn:configuration:queryIpAcl",
        "cdn:configuration:queryResponseHeaderList"
      ],
      "Effect":"Allow"
    }
  ],
  "Version":"1.1"
},
"type":"AX"
}
]
}

```

步骤 3：查询项目服务中的用户组权限

URI: GET /v3/projects/{project_id}/groups/{group_id}/roles

API文档详情请参见：[查询项目服务中的用户组权限](#)

- 请求示例

GET https://iam.myhuaweicloud.com/v3/projects/{project_id}/groups/{group_id}/roles

- 响应示例

```

{
  "links":{
    "self":"https://iam.myhuaweicloud.com/v3/projects/065a7c66da0010992ff7c0031e5a.../groups/077d71374b8025173f61c003ea0a.../roles"
  },
  "roles":[
    {
      "catalog":"AOM",
      "description":"AOM read only",
      "description_cn":"应用运维管理服务只读权限",
      "display_name":"AOM Viewer",
      "flag":"fine_grained",
      "id":"75cfe22af2b3498d82b655fbb39d...",
      "links":{
        "self":"https://iam.myhuaweicloud.com/v3/roles/75cfe22af2b3498d82b655fbb39d..."
      },
      "name":"system_all_30",
      "policy":{
        "Statement":[
          {
            "Action":[
              "aom:*.list",
              "aom:*.get",
              "apm:*.list",

```

```
        "apm:*:get"
      ],
      "Effect": "Allow"
    }
  ],
  "Version": "1.1"
},
"type": "XA"
}
]
```

步骤 4：确定需要审计的权限，查询用户组中的 IAM 用户，进行安全审计

URI: GET /v3/groups/{group_id}/users

API文档详情请参见：[管理员查询用户组所包含的IAM用户](#)

- 请求示例

GET https://iam.myhuaweicloud.com/v3/groups/{group_id}/users

- 响应示例

```
{
  "links": {
    "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb7a..../users"
  },
  "users": [
    {
      "description": "--",
      "domain_id": "d78cbac186b744899480f25bd022....",
      "enabled": true,
      "id": "07609fb9358010e21f7bc003751c....",
      "last_project_id": "065a7c66da0010992ff7c0031e5a....",
      "links": {
        "self": "https://iam.myhuaweicloud.com/v3/users/07609fb9358010e21f7bc003751c...."
      },
      "name": "IAMUserA",
      "pwd_status": true
    },
    {
      "description": "",
      "domain_id": "d78cbac186b744899480f25bd022....",
      "enabled": true,
      "id": "076837351e80251c1f0fc003afe4....",
      "last_project_id": "065a7c66da0010992ff7c0031e5a....",
      "links": {
        "self": "https://iam.myhuaweicloud.com/v3/users/076837351e80251c1f0fc003afe4...."
      },
      "name": "IAMUserB",
      "pwd_status": true
    }
  ]
}
```

5 API

5.1 Token 管理

5.1.1 获取 IAM 用户 Token（使用密码）

功能介绍

该接口可以用于通过用户名/密码的方式进行认证来获取IAM用户的Token。Token是系统颁发给IAM用户的访问令牌，承载用户的身份、权限等信息。调用IAM以及其他云服务的接口时，可以使用本接口获取的IAM用户Token进行鉴权。但强烈推荐您使用[AK/SK签名认证方式](#)调用API，可以避免因缓存的Token失效导致的API调用失败的问题。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

接口使用导航：

[IAM用户获取Token](#)

[判断当前账号是华为账号还是华为云账号](#)

[华为账号获取Token](#)

[华为云账号获取Token](#)

[第三方系统用户获取Token](#)

[Token有效期说明](#)

[获取Token常见问题](#)

[其他相关操作](#)

- **IAM用户获取Token**
无特殊要求，请按照[请求参数](#)说明获取Token。
- **判断当前账号是华为账号还是华为云账号**
华为账号不支持直接获取账号Token，排查是否为华为账号请参见：[怎么知道当前登录华为云使用的是“华为账号”还是“华为云账号”？](#)

- **华为账号获取Token**

华为账号获取token请参见以下步骤：[创建一个IAM用户](#)，[授予该用户必要的权限](#)，使用创建的IAM用户，获取IAM用户Token。
- **华为云账号获取Token**

无特殊要求，请按照[请求参数](#)说明获取Token。
- **第三方系统用户获取Token**

如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请先在华为云的登录页面，通过“忘记密码”功能，设置[华为云账号密码](#)。
- **Token有效期说明**
 - Token的有效期为**24小时**。建议进行缓存，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。重新获取Token，不影响已有Token有效性。
 - 如果在Token有效期内进行如下操作，**当前Token最长30分钟失效**。
 - 删除/停用IAM用户。
 - 修改IAM用户密码、访问密钥。
 - IAM用户权限发生变化（如账号欠费无法访问云服务、申请公测通过、IAM用户权限被修改等）。
 - 使用Token调用云服务API时，返回“**The token must be updated**”，则Token过期，需要客户端重新获取Token。
- **获取Token常见问题**

用户名或密码错误：请排查输入的用户名和密码是否正确。用户名密码正确但是仍旧报错，请排查[当前获取Token的账号是否为华为账号](#)，华为账号不支持直接获取Token，请新建IAM用户并授权，使用IAM用户获取Token。

没有API访问权限：调用API前，请确保已[开启编程访问](#)。

Token是否可以被篡改：Token生成时加入了签名防篡改的机制，Token被修改后无法通过验签，防止Token被伪造。
- **其他相关操作**
 - 如果您开启了登录保护并设置登录保护为MFA验证，请参考[获取IAM用户Token（使用密码+虚拟MFA）](#)获取IAM用户Token。
 - 如果需要获取具有Security Administrator权限的Token，请参见：[如何获取Security Administrator权限的Token](#)。
 - 通过Postman获取用户Token示例请参见：[如何通过Postman获取用户Token](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3/auth/tokens

表 5-1 Query 参数

参数	是否必选	参数类型	描述
nocatalog	否	String	如果设置该参数，返回的响应体中将不显示catalog信息。任何非空字符串都将解释为true，并使该字段生效。

请求参数

表 5-2 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

表 5-3 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-4 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。
scope	是	Object	Token的使用范围，取值为project或domain，二选一即可。 说明 <ul style="list-style-type: none"> 如果您将scope设置为domain，该Token适用于全局级服务；如果将scope设置为project，该Token适用于项目级服务。 如果您将scope同时设置为project和domain，将以project参数为准，获取到项目级服务的Token。 如果您将scope置空，将获取到全局级服务的Token。建议您按需要填写Token使用范围。

表 5-5 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为 ["password"]。
password	是	Object	<p>IAM用户密码认证信息。</p> <p>说明</p> <ul style="list-style-type: none"> user.name和user.domain.name可以在界面控制台“我的凭证”中查看，具体获取方法请参见：获取账号、IAM用户、项目、用户组、区域、委托的名称和ID。 该接口提供了锁定机制用于防止暴力破解，调用时，请确保用户名密码正确，输错一定次数（管理员可设置该规则，方法请参见：账号锁定策略）将被锁定。

表 5-6 auth.identity.password

参数	是否必选	参数类型	描述
user	是	Object	需要获取Token的IAM用户信息。

表 5-7 auth.identity.password.user

参数	是否必选	参数类型	描述
domain	是	Object	IAM用户所属账号信息。了解 账号与IAM用户的关系 。
name	是	String	IAM用户名。
password	是	String	<p>IAM用户的登录密码。</p> <p>说明</p> <ul style="list-style-type: none"> 务必保证密码输入正确，避免获取Token失败。 如果您的华为云账号已升级为华为账号，将不支持获取账号Token，建议您为自己创建一个IAM用户，授予该用户必要的权限，获取IAM用户Token。 如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请在华为云的登录页面，通过“忘记密码”功能，设置华为云账号密码，并在password中输入新设置的密码。

表 5-8 auth.identity.password.user.domain

参数	是否必选	参数类型	描述
name	是	String	IAM用户所属账号名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

表 5-9 auth.scope

参数	是否必选	参数类型	描述
domain	否	Object	取值为domain时，表示获取的Token可以作用于全局服务，全局服务不区分项目或区域，如OBS服务。如需了解服务作用范围，请参考 系统权限 。domain支持id和name，二选一即可，建议选择“domain_id”。
project	否	Object	取值为project时，表示获取的Token可以作用于项目级服务，仅能访问指定project下的资源，如ECS服务。如需了解服务作用范围，请参考 系统权限 。project支持id和name，二选一即可。

表 5-10 auth.scope.domain

参数	是否必选	参数类型	描述
id	否	String	IAM用户所属账号ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。当auth.scope选择了domain时，获取的Token可以作用于全局服务，id和name需要二选一。
name	否	String	IAM用户所属账号名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。当auth.scope选择了domain时，获取的Token可以作用于全局服务，id和name需要二选一。

表 5-11 auth.scope.project

参数	是否必选	参数类型	描述
id	否	String	表示IAM用户所属账号的项目ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。当auth.scope选择了project时，获取的Token可以作用于项目级服务，id和name需要二选一。每个区域的项目ID有所不同，需要根据业务所在的区域使用对应的项目ID。
name	否	String	表示IAM用户所属账号的项目名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。当auth.scope选择了project时，获取的Token可以作用于项目级服务，id和name需要二选一。

请求示例

- 获取IAM用户名为“IAMUser”，IAM用户密码为“IAMPassword”，所属租户名为“IAMDomain”，作用范围为项目“ap-southeast-1”，且返回的响应体中将不显示catalog信息的Token。IAM用户名、所属账号名可以在界面控制台“我的凭证”中查看，具体获取方法请参见：[获取账号、IAM用户、项目、用户组、区域、委托的名称和ID](#)。

POST https://iam.myhuaweicloud.com/v3/auth/tokens?nocatalog=true

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "domain": {
            "name": "IAMDomain" //IAM用户所属账号名
          },
          "name": "IAMUser", //IAM用户名
          "password": "IAMPassword" //IAM用户密码
        }
      }
    },
    "scope": {
      "project": {
        "name": "ap-southeast-1" //项目名称
      }
    }
  }
}
```

- 获取IAM用户名为“IAMUser”，IAM用户密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为整个账号的Token。IAM用户名、所属账号名可以在界面控制台“我的凭证”中查看，具体获取方法请参见：[获取账号、IAM用户、项目、用户组、区域、委托的名称和ID](#)。

POST https://iam.myhuaweicloud.com/v3/auth/tokens

```
{
  "auth": {
```

```

"identity": {
  "methods": [
    "password"
  ],
  "password": {
    "user": {
      "domain": {
        "name": "IAMDomain" //IAM用户所属账号名
      },
      "name": "IAMUser", //IAM用户名
      "password": "IAMPassword" //IAM用户密码
    }
  }
},
"scope": {
  "domain": {
    "name": "IAMDomain" //IAM用户所属账号名
  }
}
}

```

响应参数

表 5-12 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的Token，小于32KB。

表 5-13 响应 Body 参数

参数	参数类型	描述
Token	Object	获取到的Token信息。

表 5-14 Token

参数	参数类型	描述
catalog	Array of objects	服务目录信息。
domain	Object	获取Token的IAM用户所属的账号信息。如果获取Token时请求体中scope参数设置为domain，则返回该字段。
expires_at	String	Token过期时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。

参数	参数类型	描述
issued_at	String	Token下发时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如： 2023-06-28T08:56:33.710000Z。
methods	Array of strings	获取Token的方式。
project	Object	获取Token的IAM用户所属账号的项目信息。如果获取Token时请求体中scope参数设置为project，则返回该字段。
roles	Array of objects	Token的权限信息。
user	Object	获取Token的IAM用户信息。

表 5-15 Token.catalog

参数	参数类型	描述
endpoints	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-16 Token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

表 5-17 Token.domain

参数	参数类型	描述
name	String	账号名称。
id	String	账号ID。

表 5-18 Token.project

参数	参数类型	描述
domain	Object	项目所属账号信息。
id	String	项目ID。
name	String	项目名称。

表 5-19 Token.project.domain

参数	参数类型	描述
id	String	账号ID。
name	String	账号名称。

表 5-20 Token.roles

参数	参数类型	描述
name	String	权限名称。
id	String	权限ID。默认显示为0，非真实权限ID。

表 5-21 Token.user

参数	参数类型	描述
name	String	IAM用户名。
id	String	IAM用户ID。
password_expires_at	String	密码过期时间，“ ”表示密码不过期。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
domain	Object	IAM用户所属的账号信息。

表 5-22 Token.user.domain

参数	参数类型	描述
name	String	IAM用户所属账号名称。
id	String	IAM用户所属账号ID。

响应示例

状态码为 201 时:

创建成功。

- 获取IAM用户名为“IAMUser”，IAM用户密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为项目“ap-southeast-1”，且返回的响应体中将不显示catalog信息的Token。

响应Header参数（获取到的Token）：

X-Subject-Token:MIlatAYJKoZihvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数：

```
{
  "token": {
    "catalog": [],
    "expires_at": "2020-01-04T09:05:22.701000Z",
    "issued_at": "2020-01-03T09:05:22.701000Z",
    "methods": [
      "password"
    ],
  },
  "project": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "aa2d97d7e62c4b7da3ffdfc11551f...",
    "name": "ap-southeast-1"
  },
  "roles": [
    {
      "id": "0",
      "name": "te_admin"
    },
    {
      "id": "0",
      "name": "op_gated_Video_Campus"
    }
  ],
  "user": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "7116d09f88fa41908676fdd4b039e...",
    "name": "IAMUser",
    "password_expires_at": ""
  }
}
```

- 获取IAM用户名为“IAMUser”，IAM用户密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为整个账号的Token。

响应Header参数（获取到的Token）：

X-Subject-Token:MIlatAYJKoZihvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数：

```
{
```



```

"token": {
  "catalog": [
    {
      "endpoints": [
        {
          "id": "33e1cbdd86d34e89a63cf8ad16a5f...",
          "interface": "public",
          "region": "*",
          "region_id": "*",
          "url": "https://iam.myhuaweicloud.com/v3.0"
        }
      ],
      "id": "100a6a3477f1495286579b819d399...",
      "name": "iam",
      "type": "iam"
    },
    {
      "endpoints": [
        {
          "id": "29319cf2052d4e94bcf438b55d143...",
          "interface": "public",
          "region": "*",
          "region_id": "*",
          "url": "https://bss.sample.domain.com/v1.0"
        }
      ],
      "id": "c6db69fabbd549908adcb861c7e47...",
      "name": "bssv1",
      "type": "bssv1"
    }
  ],
  "domain": {
    "id": "d78cbac186b744899480f25bd022f...",
    "name": "IAMDomain"
  },
  "expires_at": "2020-01-04T09:08:49.965000Z",
  "issued_at": "2020-01-03T09:08:49.965000Z",
  "methods": [
    "password"
  ],
  "roles": [
    {
      "id": "0",
      "name": "te_admin"
    },
    {
      "id": "0",
      "name": "secu_admin"
    },
    {
      "id": "0",
      "name": "te_agency"
    }
  ],
  "user": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "7116d09f88fa41908676fdd4b039e...",
    "name": "IAMUser",
    "password_expires_at": ""
  }
}

```

状态码为 400 时:

参数无效。请排查body体是否符合json语法。

```
{
  "error": {
    "code": 400,
    "message": "The request body is invalid",
    "title": "Bad Request"
  }
}
```

状态码为 401 时:

认证失败。

- 如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请在华为云的登录页面，通过“忘记密码”功能，设置**华为云账号密码**，并在password中输入新设置的密码。
- 如果您的华为云账号已升级为华为账号，直接使用华为账号名和密码获取Token，系统会提示密码错误。建议您为自己创建一个IAM用户，授予该用户必要的权限，获取IAM用户Token。

```
{
  "error": {
    "code": 401,
    "message": "The username or password is wrong.",
    "title": "Unauthorized"
  }
}
```

返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
500	内部服务错误。
503	服务不可用。

错误码

无

5.1.2 获取 IAM 用户 Token（使用密码+虚拟 MFA）

功能介绍

该接口可以用于通过用户名/密码+虚拟MFA的方式进行认证，在IAM用户开启了的**登录保护功能**，并选择通过虚拟MFA验证时获取IAM用户Token。Token是系统颁发给用户的访问令牌，承载用户的身份、权限等信息。调用IAM以及其他云服务的接口时，可以使用本接口获取的Token进行鉴权。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

接口使用导航：

[IAM用户获取Token](#)

[判断当前账号是华为账号还是华为云账号](#)

[华为账号获取Token](#)

[华为云账号获取Token](#)

[第三方系统用户获取Token](#)

[Token有效期说明](#)

[获取Token常见问题](#)

[其他相关操作](#)

- **IAM用户获取Token**

无特殊要求，请按照[请求参数](#)说明获取Token。

- **判断当前账号是华为账号还是华为云账号**

华为账号不支持直接获取账号Token，排查是否为华为账号请参见：[怎么知道当前登录华为云使用的是“华为账号”还是“华为云账号”？](#)

- **华为账号获取Token**

华为账号获取token请参见以下步骤：[创建一个IAM用户](#)，[授予该用户必要的权限](#)，使用创建的IAM用户，获取IAM用户Token。

- **华为云账号获取Token**

无特殊要求，请按照[请求参数](#)说明获取Token。

- **第三方系统用户获取Token**

如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请先在华为云的登录页面，通过“忘记密码”功能，设置[华为云账号密码](#)。

- **Token有效期说明**

- Token的有效期为**24小时**。建议进行缓存，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。重新获取Token，不影响已有Token有效性。

- 如果在Token有效期内进行如下操作，**当前Token最长30分钟失效**。

- 删除/停用IAM用户。
- 修改IAM用户密码、访问密钥。
- IAM用户权限发生变化（如账号欠费无法访问云服务、申请公测通过、IAM用户权限被修改等）。

- 使用Token调用云服务API时，返回“**The token must be updated**”，则Token过期，需要客户端重新获取Token。

- **获取Token常见问题**

用户名或密码错误：请排查输入的用户名和密码是否正确。用户名密码正确但是仍旧报错，请排查[当前获取Token的账号是否为华为账号](#)，华为账号不支持直接获取Token，请新建IAM用户并授权，使用IAM用户获取Token。

没有API访问权限：调用API前，请确保已[开启编程访问](#)。

- **相关操作**
 - 如果需要获取具有Security Administrator权限的Token，请参见：[如何获取 Security Administrator权限的Token](#)。
 - 通过Postman获取用户Token示例请参见：[如何通过Postman获取用户Token](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3/auth/tokens

表 5-23 Query 参数

参数	是否必选	参数类型	描述
nocatalog	否	String	如果设置该参数，返回的响应体中将不显示catalog信息。任何非空字符串都将解释为true，并使该字段生效。

请求参数

表 5-24 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

表 5-25 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-26 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。
scope	是	Object	Token的使用范围，取值为project或domain，二选一即可。 说明 <ul style="list-style-type: none"> 如果您将scope设置为domain，该Token适用于全局级服务；如果将scope设置为project，该Token适用于项目级服务。 如果您将scope同时设置为project和domain，将以project参数为准，获取到项目级服务的Token。 如果您将scope置空，将获取到全局级服务的Token。建议您按需要填写Token使用范围。

表 5-27 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为["password", "totp"]。 取值范围： <ul style="list-style-type: none"> password totp
password	是	Object	用户密码认证信息。 说明 <ul style="list-style-type: none"> user.name和user.domain.name可以在界面控制台“我的凭证”中查看，具体获取方法请参见：获取账号、IAM用户、项目、用户组、区域、委托的名称和ID。 该接口提供了锁定机制用于防止暴力破解，调用时，请确保用户名密码正确，输错一定次数（管理员可设置该规则，方法请参见：账号锁定策略）将被锁定。
totp	是	Object	totp认证信息，仅在您已开启虚拟MFA方式的登录保护功能时需要填写该参数。

表 5-28 auth.identity.password

参数	是否必选	参数类型	描述
user	是	Object	需要获取Token的IAM用户信息。

表 5-29 auth.identity.password.user

参数	是否必选	参数类型	描述
domain	是	Object	IAM用户所属账号信息。了解 账号与IAM用户的关系 。
name	是	String	IAM用户名。
password	是	String	IAM用户的登录密码。 说明 <ul style="list-style-type: none"> 务必保证密码输入正确，避免获取Token失败。 如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请在华为云的登录页面，通过“忘记密码”功能，设置华为云账号密码，并在password中输入新设置的密码。

表 5-30 auth.identity.password.user.domain

参数	是否必选	参数类型	描述
name	是	String	IAM用户所属账号名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

表 5-31 auth.identity.totp

参数	是否必选	参数类型	描述
user	是	Object	IAM用户信息。该IAM用户已开启登录保护，并选择以虚拟MFA方式进行身份验证，开启/关闭登录保护方法请参见： 操作保护 。

表 5-32 auth.identity.totp.user

参数	是否必选	参数类型	描述
id	是	String	已开启虚拟MFA方式的登录保护的IAM用户ID。
passcode	是	String	虚拟MFA验证码，在MFA应用程序中获取动态验证码，获取方法请参见： 如何获取虚拟MFA验证码 。 说明 务必保证验证码输入正确，避免获取Token失败。

表 5-33 auth.scope

参数	是否必选	参数类型	描述
domain	否	Object	取值为domain时，表示获取的Token可以作用于全局服务，全局服务不区分项目或区域，如OBS服务。如需了解服务作用范围，请参考 系统权限 。domain支持id和name，二选一即可，建议选择“domain.id”。
project	否	Object	取值为project时，表示获取的Token可以作用于项目级服务，仅能访问指定project下的资源，如ECS服务。如需了解服务作用范围，请参考 系统权限 。project支持id和name，二选一即可。

表 5-34 auth.scope.domain

参数	是否必选	参数类型	描述
id	否	String	IAM用户所属账号ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。
name	否	String	IAM用户所属账号名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

表 5-35 auth.scope.project

参数	是否必选	参数类型	描述
id	否	String	IAM用户所属账号的项目id，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。
name	否	String	IAM用户所属账号的项目名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

请求示例

- 示例1：获取IAM用户名为“IAMUser”，密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为整个账号的Token。IAM用户名、所属账号名可以在界面控制台“我的凭证”中查看，具体获取方法请参见：[获取账号、IAM用户、项目、用户组、区域、委托的名称和ID](#)。

POST https://iam.myhuaweicloud.com/v3/auth/tokens

```
{
  "auth": {
    "identity": {
      "methods": [
        "password",
        "totp"
      ],
      "password": {
        "user": {
          "name": "IAMUser", //IAM用户名
          "password": "IAMPassword", //IAM用户密码
          "domain": {
            "name": "IAMDomain" //IAM用户所属账号名
          }
        }
      }
    },
    "totp": {
      "user": {
        "id": "7116d09f88fa41908676fdd4b039e...", //IAM用户ID
        "passcode": "*****" //虚拟MFA验证码
      }
    }
  },
  "scope": {
    "domain": {
      "name": "IAMDomain" //IAM用户所属账号名
    }
  }
}
```

- 示例2：获取IAM用户名为“IAMUser”，密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为项目“ap-southeast-1”，且返回的响应体中将不显示catalog信息的Token。IAM用户名、所属账号名可以在界面控制台“我的凭证”中查看，具体获取方法请参见：[获取账号、IAM用户、项目、用户组、区域、委托的名称和ID](#)。

POST https://iam.myhuaweicloud.com/v3/auth/tokens?nocatalog=true

```
{
  "auth": {
    "identity": {
      "methods": [
        "password",
```



```

    "totp"
  ],
  "password": {
    "user": {
      "name": "IAMUser",           //IAM用户名
      "password": "IAMPassword", //IAM用户密码
      "domain": {
        "name": "IAMDomain"      //IAM用户所属账号名
      }
    }
  },
  "totp": {
    "user": {
      "id": "7116d09f88fa41908676fdd4b039e...", //IAM用户ID
      "passcode": "*****"                       //虚拟MFA验证码
    }
  },
  "scope": {
    "project": {
      "name": "ap-southeast-1" //项目名称
    }
  }
}

```

响应参数

表 5-36 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的Token。

表 5-37 响应 Body 参数

参数	参数类型	描述
token	Object	获取到的Token信息。

表 5-38 token

参数	参数类型	描述
catalog	Array of objects	服务目录信息。
domain	Object	获取Token的IAM用户所属的账号信息。如果获取Token时请求体中scope参数设置为domain，则返回该字段。
expires_at	String	Token过期时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如： 2023-06-28T08:56:33.710000Z。

参数	参数类型	描述
mfa_authn_at	String	MFA验证时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如： 2023-06-28T08:56:33.710000Z。
issued_at	String	Token下发时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如： 2023-06-28T08:56:33.710000Z。
methods	Array of strings	获取Token的方式。
project	Object	获取Token的IAM用户所属账号的项目信息。如果获取Token时请求体中scope参数设置为project，则返回该字段。
roles	Array of objects	Token的权限信息。
user	Object	获取Token的IAM用户信息。

表 5-39 token.catalog

参数	参数类型	描述
endpoints	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-40 token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

表 5-41 token.domain

参数	参数类型	描述
name	String	账号名称。
id	String	账号ID。

表 5-42 token.project

参数	参数类型	描述
domain	Object	项目所属账号信息。
id	String	项目ID。
name	String	项目名称。

表 5-43 token.project.domain

参数	参数类型	描述
id	String	账号ID。
name	String	账号名称。

表 5-44 token.roles

参数	参数类型	描述
name	String	权限名称。
id	String	权限ID。默认显示为0，非真实权限ID。

表 5-45 token.user

参数	参数类型	描述
name	String	IAM用户名。
id	String	IAM用户ID。
password_expires_at	String	密码过期时间，“”表示密码不过期。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
domain	Object	IAM用户所属的账号信息。

表 5-46 token.user.domain

参数	参数类型	描述
name	String	IAM用户所属账号名称。
id	String	IAM用户所属账号ID。

响应示例

状态码为 201 时:

创建成功。

- 示例 1: 获取IAM用户名为 “IAMUser”，密码为 “IAMPassword”，所属账号名为 “IAMDomain”，作用范围为整个账号的Token。

响应Header参数 (获取到的Token) :

X-Subject-Token:MIlatAYJKoZihvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
  "token": {
    "expires_at": "2020-01-04T09:08:49.965000Z",
    "mfa_authn_at": "2020-01-03T09:08:49.965000Z",
    "methods": [
      "password",
      "totp"
    ],
    "catalog": [
      {
        "endpoints": [
          {
            "id": "33e1cbdd86d34e89a63cf8ad16a5f...",
            "interface": "public",
            "region": "*",
            "region_id": "*",
            "url": "https://iam.myhuaweicloud.com/v3.0"
          }
        ],
        "id": "100a6a3477f1495286579b819d399...",
        "name": "iam",
        "type": "iam"
      },
      {
        "endpoints": [
          {
            "id": "29319cf2052d4e94bcf438b55d143...",
            "interface": "public",
            "region": "*",
            "region_id": "*",
            "url": "https://bss.sample.domain.com/v1.0"
          }
        ],
        "id": "c6db69fabbd549908adcb861c7e47...",
        "name": "bssv1",
        "type": "bssv1"
      }
    ],
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "roles": [
      {
        "id": "0",
        "name": "te_admin"
      }
    ]
  }
}
```

```

    },
    {
      "id": "0",
      "name": "secu_admin"
    },
    {
      "id": "0",
      "name": "te_agency"
    }
  ],
  "issued_at": "2020-01-03T09:08:49.965000Z",
  "user": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "7116d09f88fa41908676fdd4b039e...",
    "name": "IAMUser",
    "password_expires_at": ""
  }
}

```

- 示例 2: 获取IAM用户名为“IAMUser”，密码为“IAMPassword”，所属账号名为“IAMDomain”，作用范围为项目“ap-southeast-1”，且返回的响应体中将不显示catalog信息的Token。

响应Header参数（获取到的Token）：

X-Subject-Token:MIlatAYJKoZlIhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数：

```

{
  "token": {
    "expires_at": "2020-01-04T09:05:22.701000Z",
    "mfa_authn_at": "2020-01-03T09:05:22.701000Z",
    "methods": [
      "password",
      "totp"
    ],
  },
  "catalog": [],
  "roles": [
    {
      "id": "0",
      "name": "te_admin"
    },
    {
      "id": "0",
      "name": "op_gated_OBS_file_protocol"
    },
    {
      "id": "0",
      "name": "op_gated_Video_Campus"
    }
  ],
  "project": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "aa2d97d7e62c4b7da3ffdfc11551f...",
    "name": "ap-southeast-1"
  },
  "issued_at": "2020-01-03T09:05:22.701000Z",
  "user": {
    "domain": {
      "id": "d78cbac186b744899480f25bd022f...",
      "name": "IAMDomain"
    },
    "id": "7116d09f88fa41908676fdd4b039e...",
    "name": "IAMUser",
    "password_expires_at": ""
  }
}

```

```
}  
}  
}
```

状态码为 400 时:

参数无效。

```
{  
  "error": {  
    "code": 400,  
    "message": "The request body is invalid",  
    "title": "Bad Request"  
  }  
}
```

状态码为 401 时:

认证失败。

- 如果您是第三方系统用户，直接使用联邦认证的用户名和密码获取Token，系统会提示密码错误。请在华为云的登录页面，通过“忘记密码”功能，设置**华为云账号密码**，并在password中输入新设置的密码。
- 如果您的华为云账号已升级为华为账号，直接使用华为账号名和密码获取Token，系统会提示密码错误。建议您为自己创建一个IAM用户，授予该用户必要的权限，获取IAM用户Token。

```
{  
  "error": {  
    "code": 401,  
    "message": "The username or password is wrong.",  
    "title": "Unauthorized"  
  }  
}
```

返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
500	内部服务错误。
503	服务不可用。

错误码

无

5.1.3 获取委托 Token

功能介绍

该接口可以用于获取委托方的token。

例如：A账号希望B账号管理自己的某些资源，所以A账号创建了委托给B账号，则A账号为委托方，B账号为被委托方。那么B账号可以通过该接口获取委托token。B账号仅能使用该token管理A账号的委托资源，不能管理自己账号中的资源。如果B账号需要管理自己账号中的资源，则需要获取自己的用户token。详情请参考：[委托其他账号管理资源](#)。

token是系统颁发给用户的访问令牌，承载用户的身份、权限等信息。调用IAM以及其他云服务的接口时，可以使用本接口获取的token进行鉴权。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

说明

- token的有效期为24小时，建议进行缓存，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。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3/auth/tokens

表 5-47 Query 参数

参数	是否必选	参数类型	描述
nocatalog	否	String	如果设置该参数，返回的响应体中将不显示catalog信息。任何非空字符串都将解释为true，并使该字段生效。

请求参数

表 5-48 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	被委托方B账号中的IAM用户token，且该token具有Agent Operator权限。

表 5-49 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-50 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。
scope	是	Object	token的使用范围，需要填写委托方A的project或domain，填写其中任一即可。 说明 <ul style="list-style-type: none"> 如果您将scope设置为domain，该Token适用于全局级服务；如果将scope设置为project，该Token适用于项目级服务。 如果您将scope同时设置为project和domain，将以project参数为准，获取到项目级服务的Token。 如果您将scope置空，将获取到全局级服务的Token。建议您按需要填写Token使用范围。

表 5-51 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	token的获取方式，该字段内容为["assume_role"]。 取值范围： <ul style="list-style-type: none"> assume_role
assume_role	是	Object	assume_role的具体信息。

表 5-52 auth.identity.assume_role

参数	是否必选	参数类型	描述
domain_id	否	String	委托方A的账号ID。“domain_id”与“domain_name”至少填写一个，建议选择“domain_id”。 委托方A可以参考 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ID。
domain_name	否	String	委托方A的账号名称。“domain_id”与“domain_name”至少填写一个，建议选择“domain_id”。 您可以在IAM控制台委托列表中查看委托方A的账号名称。
agency_name	是	String	委托方A创建的委托名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

表 5-53 auth.scope

参数	是否必选	参数类型	描述
domain	否	Object	取值为domain时，表示获取的Token可以作用于全局服务，全局服务不区分项目或区域，如OBS服务。如需了解服务作用范围，请参考 系统权限 。domain支持id和name，二选一即可，建议选择“domain_id”。
project	否	Object	取值为project时，表示获取的Token可以作用于项目级服务，仅能访问指定project下的资源，如ECS服务。如需了解服务作用范围，请参考 系统权限 。project支持id和name，二选一即可。

表 5-54 auth.scope.domain

参数	是否必选	参数类型	描述
id	否	String	委托方A的账号ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。id和name，二选一即可。

参数	是否必选	参数类型	描述
name	否	String	委托方A的账号名，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。id和name，二选一即可。

表 5-55 auth.scope.project

参数	是否必选	参数类型	描述
id	否	String	委托方A项目的ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。id和name，二选一即可。
name	否	String	委托方A项目的名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。id和name，二选一即可。

请求示例

- 由被委托方B（账号名为IAMDomainB）中的IAM用户B（用户名IAMUserB，请求头中的X-Auth-Token字段需要填写IAMUserB的用户token，且该token需要具有Agent Operator权限），获取委托方A（账号名为IAMDomainA）创建的委托名为IAMAgency，作用范围为委托方A的项目“ap-southeast-1”，且返回的响应体中将不显示catalog信息的token。

```
POST https://iam.myhuaweicloud.com/v3/auth/tokens?nocatalog=true
{
  "auth": {
    "identity": {
      "methods": [
        "assume_role"
      ],
      "assume_role": {
        "domain_name": "IAMDomainA", //委托方IAM用户A所属账号名称
        "agency_name": "IAMAgency" //委托方IAM用户A创建的委托名称
      }
    },
    "scope": {
      "project": {
        "name": "ap-southeast-1" //项目名称
      }
    }
  }
}
```

- 由被委托方B（账号名为IAMDomainB）中的IAM用户B（用户名IAMUserB，请求头中的X-Auth-Token字段需要填写IAMUserB的用户token，且该token需要具有Agent Operator权限），获取委托方A（账号名为IAMDomainA）创建的委托名为IAMAgency，作用范围为委托方A整个账号的token。

```
POST https://iam.myhuaweicloud.com/v3/auth/tokens
{
  "auth": {
```

```

"identity": {
  "methods": [
    "assume_role"
  ],
  "assume_role": {
    "domain_name": "IAMDomainA",           //委托方IAM用户A所属账号名称
    "agency_name": "IAMAgency"          //委托方IAM用户A创建的委托名称
  }
},
"scope": {
  "domain": {
    "name": "IAMDomainA"                 //委托方IAM用户A所属账号名称
  }
}
}

```

响应参数

表 5-56 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的token。

表 5-57 响应 Body 参数

参数	参数类型	描述
token	Object	token信息列表。

表 5-58 token

参数	参数类型	描述
methods	Array of strings	获取token的方式。
expires_at	String	token到期时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
issued_at	String	token下发时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
assumed_by	Object	被委托方B的相关信息。
catalog	Array of objects	服务目录信息。

参数	参数类型	描述
domain	Object	委托方A的账号信息。如果获取token时请求体中scope参数设置为domain，则返回该字段。
project	Object	委托方A的项目信息。如果获取token时请求体中scope参数设置为project，则返回该字段。
roles	Array of objects	委托token的权限信息。
user	Object	委托方A所创建的委托的信息。

表 5-59 token.assumed_by

参数	参数类型	描述
user	Object	被委托方B中IAM用户的用户信息。

表 5-60 token.assumed_by.user

参数	参数类型	描述
name	String	被委托方B中IAM用户的用户名。
id	String	被委托方B中IAM用户的用户ID。
domain	Object	被委托方B的账号信息。
password_expires_at	String	被委托方B中IAM用户的密码过期时间，“ ”表示密码不过期。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。

表 5-61 token.assumed_by.user.domain

参数	参数类型	描述
name	String	被委托方B的账号名称。
id	String	被委托方B的账号ID。

表 5-62 token.catalog

参数	参数类型	描述
endpoints	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-63 token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

表 5-64 token.domain

参数	参数类型	描述
name	String	委托方A的账号名称。
id	String	委托方A的账号ID。

表 5-65 token.project

参数	参数类型	描述
name	String	委托方A的项目名称。
id	String	委托方A的项目ID。
domain	Object	委托方A的账号信息。

表 5-66 token.project.domain

参数	参数类型	描述
name	String	委托方A的账号名称。
id	String	委托方A的账号ID。

表 5-67 token.roles

参数	参数类型	描述
name	String	权限名称。
id	String	权限ID。默认显示为0，非真实权限ID。

表 5-68 token.user

参数	参数类型	描述
name	String	委托方A账号名/委托名。
id	String	委托ID。
domain	Object	委托方A的账号信息。

表 5-69 token.user.domain

参数	参数类型	描述
id	String	委托方A的账号ID。
name	String	委托方A的账号名称。

响应示例

状态码为 201 时:

创建成功。

示例1: 由被委托方B (账号名为IAMDomainB) 中的IAM用户B (用户名IAMUserB, 请求头中的X-Auth-Token字段需要填写IAMUserB的用户token, 且该token需要具有Agent Operator权限), 获取委托方A (账号名为IAMDomainA) 创建的委托名为IAMAgency, 作用范围为委托方A整个账号的token。

示例2: 由被委托方B (账号名为IAMDomainB) 中的IAM用户B (用户名IAMUserB, 请求头中的X-Auth-Token字段需要填写IAMUserB的用户token, 且该token需要具有Agent Operator权限), 获取委托方A (账号名为IAMDomainA) 创建的委托名为IAMAgency, 作用范围为委托方A的项目“ap-southeast-1”, 且返回的响应体中将不显示catalog信息的token。

- 示例 1

响应Header参数:

X-Subject-Token:MIlatAYJKoZIhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
  "token": {
    "expires_at": "2020-01-05T05:05:17.429000Z",
    "methods": [
      "assume_role"
    ],
    "catalog": [
      {
        "endpoints": [
          {
            "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
            "interface": "public",
            "region": "*",
            "region_id": "*",
            "url": "https://iam.myhuaweicloud.com/v3.0"
          }
        ],
        "id": "100a6a3477f1495286579b819d399e36",
        "name": "iam",
        "type": "iam"
      }
    ],
    "domain": {
      "id": "d78cbac186b744899480f25bd022f468",
      "name": "IAMDomainA"
    },
    "roles": [
      {
        "id": "0",
        "name": "op_gated_eip_ipv6"
      },
      {
        "id": "0",
        "name": "op_gated_rds_mcs"
      }
    ],
    "issued_at": "2020-01-04T05:05:17.429000Z",
    "user": {
      "domain": {
        "id": "d78cbac186b744899480f25bd022f468",
        "name": "IAMDomainA"
      },
      "id": "0760a9e2a60026664f1fc0031f9f205e",
      "name": "IAMDomainA/IAMAgency"
    },
    "assumed_by": {
      "user": {
        "domain": {
          "id": "a2cd82a33fb043dc9304bf72a0f38f00",
          "name": "IAMDomainB"
        },
        "id": "0760a0bdee8026601f44c006524b17a9",
        "name": "IAMUserB",
        "password_expires_at": ""
      }
    }
  }
}
```

- 示例 2

响应Header参数:

X-Subject-Token:MIlatAYJKoZIhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
  "token": {
```

```
"expires_at": "2020-01-05T06:49:28.094000Z",
"methods": [
  "assume_role"
],
"catalog": [],
"roles": [
  {
    "id": "0",
    "name": "op_gated_eip_ipv6"
  },
  {
    "id": "0",
    "name": "op_gated_rds_mcs"
  }
],
"project": {
  "domain": {
    "id": "d78cbac186b744899480f25bd022f468",
    "name": "IAMDomainA"
  },
  "id": "aa2d97d7e62c4b7da3ffdfc11551f878",
  "name": "ap-southeast-1"
},
"issued_at": "2020-01-04T06:49:28.094000Z",
"user": {
  "domain": {
    "id": "d78cbac186b744899480f25bd022f468",
    "name": "IAMDomainA"
  },
  "id": "0760a9e2a60026664f1fc0031f9f205e",
  "name": "IAMDomainA/IAMAgency"
},
"assumed_by": {
  "user": {
    "domain": {
      "id": "a2cd82a33fb043dc9304bf72a0f38f00",
      "name": "IAMDomainB"
    },
    "id": "0760a0bdee8026601f44c006524b17a9",
    "name": "IAMUserB",
    "password_expires_at": ""
  }
}
}
```

状态码为 400 时:

参数无效。

```
{
  "error": {
    "code": 400,
    "message": "The request body is invalid",
    "title": "Bad Request"
  }
}
```

状态码为 401 时:

认证失败。

```
{
  "error": {
    "code": 401,
    "message": "The X-Auth-Token is invalid!",
    "title": "Unauthorized"
  }
}
```


状态码为 403 时:

没有操作权限。

- 可能原因：被委托方B中用户B的用户token（即X-Auth-Token填写的token）缺少Agent Operator权限，请添加权限。

```
{
  "error": {
    "code": 403,
    "message": "You have no right to do this action",
    "title": "Forbidden"
  }
}
```

返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。 可能原因：被委托方B中用户B的用户token（即X-Auth-Token填写的token）缺少Agent Operator权限，请添加权限。
404	未找到相应的资源。
500	内部服务错误。
503	服务不可用。

错误码

无

5.1.4 校验 Token 的有效性

功能介绍

该接口可以用于[管理员](#)校验本账号中IAM用户token的有效性，或IAM用户校验自己token的有效性。管理员仅能校验本账号中IAM用户token的有效性，不能校验其他账号中IAM用户token的有效性。如果被校验的token有效，则返回该token的详细信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

GET /v3/auth/tokens

表 5-70 Query 参数

参数	是否必选	参数类型	描述
nocatalog	否	String	如果设置该参数，返回的响应体中将不显示catalog参数。任何非空字符串都将解释为true，并使该字段生效。

请求参数

表 5-71 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	管理员 校验本账号中IAM用户的token的有效性：拥有Security Administrator权限的token。 IAM用户校验自己token的有效性：该IAM用户的token（无需特殊权限）。
X-Subject-Token	是	String	待校验的token。

请求示例

校验Token的有效性。

GET https://iam.myhuaweicloud.com/v3/auth/tokens

响应参数

表 5-72 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	已校验的token。

表 5-73 响应 Body 参数

参数	参数类型	描述
token	Object	获取到的token信息。

表 5-74 token

参数	参数类型	描述
catalog	Array of objects	服务目录信息。
domain	Object	被校验token的IAM用户所属的账号信息。如果获取token时请求体中scope参数设置为domain，则返回该字段。
expires_at	String	token过期时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
issued_at	String	token下发时间。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
methods	Array of strings	获取token的方式。
project	Object	被校验token的IAM用户所属账号的项目信息。如果获取token时请求体中scope参数设置为project，则返回该字段。
roles	Array of objects	token的权限信息。
user	Object	获取token的IAM用户信息。

表 5-75 token.catalog

参数	参数类型	描述
endpoints	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-76 token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

表 5-77 token.domain

参数	参数类型	描述
name	String	账号名称。
id	String	账号ID。

表 5-78 token.project

参数	参数类型	描述
domain	Object	项目所属账号信息。
id	String	项目ID。
name	String	项目名称。

表 5-79 token.project.domain

参数	参数类型	描述
id	String	账号ID。
name	String	账号名称。

表 5-80 token.roles

参数	参数类型	描述
name	String	权限名称。
id	String	权限ID。默认显示为0，非真实权限ID。

表 5-81 token.user

参数	参数类型	描述
name	String	IAM用户名。
id	String	IAM用户ID。
password_expires_at	String	密码过期时间，“ ”表示密码不过期。 说明 UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
domain	Object	IAM用户所属的账号信息。

表 5-82 token.user.domain

参数	参数类型	描述
name	String	IAM用户所属账号名称。
id	String	IAM用户所属账号ID，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。

响应示例

状态码为 200 时:

请求成功。

响应Header参数:

X-Subject-Token:MIlatAYJKoZlhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
  "token": {
    "expires_at": "2020-01-04T09:08:49.965000Z",
    "methods": [
      "password"
    ],
    "catalog": [
      {
        "endpoints": [
          {
            "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
            "interface": "public",
            "region": "*",
            "region_id": "*",
            "url": "https://iam.myhuaweicloud.com/v3.0"
          }
        ]
      }
    ],
    "id": "100a6a3477f1495286579b819d399e36",
    "name": "iam",
    "type": "iam"
  },
  {
    "endpoints": [
      {
```

```
        "id": "29319cf2052d4e94bcf438b55d143832",
        "interface": "public",
        "region": "*",
        "region_id": "*",
        "url": "https://bss.sample.domain.com/v1.0"
      }
    ],
    "id": "c6db69fabbd549908adcb861c7e47ca4",
    "name": "bssv1",
    "type": "bssv1"
  }
],
"domain": {
  "id": "d78cbac186b744899480f25bd022f468",
  "name": "IAMDomain"
},
"roles": [
  {
    "id": "0",
    "name": "te_admin"
  },
  {
    "id": "0",
    "name": "secu_admin"
  },
  {
    "id": "0",
    "name": "te_agency"
  }
],
"issued_at": "2020-01-03T09:08:49.965000Z",
"user": {
  "domain": {
    "id": "d78cbac186b744899480f25bd022f468",
    "name": "IAMDomain"
  },
  "id": "7116d09f88fa41908676fdd4b039e95b",
  "name": "IAMUser",
  "password_expires_at": ""
}
}
```

状态码为 404 时:

未找到相应的资源。

```
{
  "error": {
    "code": 404,
    "message": "X-Subject-Token is invalid in the request",
    "title": "Not Found"
  }
}
```

返回值

返回值	描述
200	请求成功。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。

返回值	描述
500	内部服务错误。

错误码

无

5.2 访问密钥管理

5.2.1 获取委托的临时访问密钥和 securitytoken

功能介绍

该接口可以用于通过委托来获取临时访问密钥（临时AK/SK）和securitytoken。

临时AK/SK和securitytoken是系统颁发给IAM用户的临时访问令牌，有效期可在15分钟至24小时范围内设置，过期后需要重新获取。临时AK/SK和securitytoken遵循权限最小化原则。鉴权时，临时AK/SK和securitytoken必须同时使用，请求头中需要添加“x-security-token”字段，使用方法详情请参考：[使用临时AK/SK做签名](#)

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

请求参数

表 5-83 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段填为“application/json;charset=utf8”。
Authorization	否	String	X-Auth-Token和Authorization二选一，推荐使用Authorization方式，AK/SK签名认证后会生成Authorization Header。更多信息请参考 AK/SK签名认证算法详解 。

参数	是否必选	参数类型	描述
X-Auth-Token	否	String	X-Auth-Token和Authorization二选一，拥有Agent Operator权限的token。

表 5-84 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-85 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。

表 5-86 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为 ["assume_role"]。
assume_role	是	Object	assume_role的具体信息。
policy	否	Object	<p>用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅OBS服务支持该限制）。</p> <p>如果填写此参数，则临时访问密钥和securitytoken的权限为：委托具有的权限和policy参数限制的权限交集。policy参数的字符个数不大于2048。</p> <p>关于IAM策略的格式和语法，请参考：策略。</p>

表 5-87 auth.identity.assume_role

参数	是否必选	参数类型	描述
agency_name	是	String	委托名称，获取方式请参见： 获取账号、IAM用户、项目、用户组、区域、委托的名称和ID 。
domain_id	否	String	委托方的账号ID。“domain_id”与“domain_name”至少填写一个，建议选择“domain_id”。
domain_name	否	String	委托方的账号名。“domain_id”与“domain_name”至少填写一个，建议选择“domain_id”。
duration_seconds	否	Integer	AK/SK和securitytoken的有效期限，时间单位为秒。取值范围：15分钟～24小时，默认为15分钟。
session_user	否	Object	委托方对应的企业用户信息。

表 5-88 auth.identity.assume_role.session_user

参数	是否必选	参数类型	描述
name	否	String	委托方对应的企业用户名。 用户名需满足如下规则：长度5~64之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且只能以字母开头。

表 5-89 auth.identity.policy

参数	是否必选	参数类型	描述
Version	是	String	权限版本号，创建自定义策略时，该字段值填为“1.1”。 说明 1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。
Statement	是	Array of objects	授权语句，描述自定义策略的具体内容，不超过8个。

表 5-90 auth.identity.policy.Statement

参数	是否必选	参数类型	描述
Action	是	Array of strings	<p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p>说明</p> <ul style="list-style-type: none"> 格式为：服务名:资源类型:操作，例：vpc:ports:create。 服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。
Effect	是	String	<p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> Allow Deny
Condition	否	Map<String,Map<String,Array<String>>>	<p>限制条件。了解更多相关参数，请参考：配置自定义策略。</p> <p>说明</p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": { "StringEquals": { "obs:prefix": ["public"] } } </pre>
Resource	否	Array of strings	<p>资源。规则如下：</p> <p>说明</p> <ul style="list-style-type: none"> 格式为“服务名:region:domainId:资源类型:资源路径”，资源类型支持通配符号*，通配符号*表示所有。如"obs:*:*:bucket:*":表示所有的OBS桶。 region字段为*或用户可访问的region。service必须存在且resource属于对应service。

响应参数

表 5-91 响应 Body 参数

参数	参数类型	描述
credential	Object	认证结果信息。

表 5-92 credential

参数	参数类型	描述
expires_at	String	AK/SK和securitytoken的过期时间。响应参数为UTC时间格式。
access	String	获取的AK。
secret	String	获取的SK。
securitytoken	String	securitytoken是将所获的AK、SK等信息进行加密后的字符串。

请求示例

- 填写"session_user"参数，即委托方对应的企业用户信息，包含委托方对应的企业用户名。

POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens

```
{
  "auth": {
    "identity": {
      "methods": [
        "assume_role"
      ],
      "assume_role": {
        "domain_name": "IAMDomainA",
        "agency_name": "IAMAgency",
        "duration_seconds": 3600,
        "session_user": {
          "name": "SessionUserName"
        }
      }
    }
  }
}
```

- 填写"policy"参数，即用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅适用限制OBS服务的权限）。如果填写此参数，则临时访问密钥和securitytoken的权限为：委托具有的权限和policy参数限制的权限交集。

POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens

```
{
  "auth": {
    "identity": {
      "methods": [
        "assume_role"
      ],
      "policy": {
        "Version": "1.1",
```

```

    "Statement": [{
      "Effect": "allow",
      "Action": [
        "obs:object:*"
      ],
      "Resource": ["obs:*:*:object:*"],
      "Condition": {
        "StringEquals": {
          "obs:prefix": ["public"]
        }
      }
    }
  ],
  "assume_role": {
    "domain_name": "IAMDomainA",
    "agency_name": "IAMAgency",
    "duration_seconds": 3600
  }
}
}
}
}

```

- 不填写"session_user"和policy参数。

```

POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
    "identity": {
      "methods": [
        "assume_role"
      ],
      "assume_role": {
        "domain_name": "IAMDomainA",
        "agency_name": "IAMAgency",
        "duration_seconds": 3600
      }
    }
  }
}

```

响应示例

状态码为 201 时:

创建成功。

无论session_user填写与否，返回都是相同的。若填写了session_user，则在securitytoken中包含了所填写的session_user信息。

```

{
  "credential": {
    "access": "E6DX0TF2ZREQ4Z...",
    "expires_at": "2020-01-08T02:56:19.587000Z",
    "secret": "w9ePum0qdfac39ErLD0UdjofYkqort6lw....",
    "securitytoken": "gQpjb1ub3J0aCO..."
  }
}

```

返回值

返回值	描述
201	创建成功。
400	参数无效。

返回值	描述
401	认证失败。
403	没有操作权限。
500	内部服务错误。

错误码

无

5.2.2 获取用户的临时访问密钥和 securitytoken

功能介绍

该接口可以用于通过token来获取临时AK/SK和securitytoken。临时AK/SK和securitytoken是系统颁发给IAM用户的临时访问令牌，有效期可在15分钟至24小时范围内设置，过期后需要重新获取。临时AK/SK和securitytoken遵循权限最小化原则。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

使用获取到的临时AK/SK和securitytoken作为凭证访问云服务，临时AK/SK和securitytoken两者必须**同时使用**，请求头中需要添加“x-security-token”字段，使用方法详情请参考：[使用临时AK/SK做签名](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

请求参数

表 5-93 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段填为“application/json;charset=utf8”。
Authorization	否	String	X-Auth-Token和Authorization二选一，推荐使用Authorization方式，AK/SK签名认证后会生成Authorization Header。更多信息请参考 AK/SK签名认证算法详解 。

参数	是否必选	参数类型	描述
X-Auth-Token	否	String	X-Auth-Token和Authorization二选一，推荐使用Authorization方式。IAM用户Token或联邦用户的Token或委托Token。通过调用 获取IAM用户Token或委托Token ，在参数X-Subject-Token中可以获取对应的Token。

表 5-94 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-95 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。

表 5-96 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为["token"]。
token	否	Object	临时访问密钥和securitytoken的有效期。
policy	否	Object	用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅OBS服务支持该限制）。 如果填写此参数，则临时访问密钥和securitytoken的权限为：原Token具有的权限和policy参数限制的权限交集。 policy参数的字符个数不大于2048。 关于IAM策略的格式和语法，请参考： 策略 。

表 5-97 auth.identity.policy

参数	是否必选	参数类型	描述
Version	是	String	权限版本号，创建自定义策略时，该字段值填为“1.1”。 说明 1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。
Statement	是	Array of objects	授权语句，描述自定义策略的具体内容。

表 5-98 auth.identity.policy.Statement

参数	是否必选	参数类型	描述
Action	是	Array of strings	授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。 说明 <ul style="list-style-type: none"> 格式为：服务名:资源类型:操作，例：vpc:ports:create。 服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。
Effect	是	String	作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。 取值范围： <ul style="list-style-type: none"> Allow Deny
Condition	否	Map<String,Map<String,Array<String>>>	限制条件。了解更多相关参数，请参考： 策略语法 。 说明 以请求示例中的Condition为例：当账号名（DomainName）等于DomainNameExample时，该策略才会生效。 <pre> "Condition": { "StringEquals": { "g:DomainName": ["DomainNameExample"] } } </pre>

参数	是否必选	参数类型	描述
Resource	否	Array of strings	<p>资源。规则如下：</p> <p>说明</p> <ul style="list-style-type: none"> 格式为“服务名:region:domainId:资源类型:资源路径”，资源类型支持通配符*，通配符*表示所有。如"obs:*:bucket:*": 表示所有的OBS桶。支持IAM资源粒度授权的云服务，请参考支持IAM资源粒度授权的云服务。 region字段为*或用户可访问的region。service必须存在且resource属于对应service。 其中，服务名、region、domainId、资源类型的格式为：由字母、数字、下划线、连字符、星号组成，长度为1到50个字符；资源路径的格式为：由除分号、竖线、波浪线、反引号、大括号、中括号、尖括号以外的任意字符组成，长度为1到1200个字符。

表 5-99 auth.identity.token

参数	是否必选	参数类型	描述
id	否	String	即token，若请求Header中不传X-Auth-Token，则须填此参数。
duration_seconds	否	Integer	<p>临时访问密钥和securitytoken的有效期限，时间单位为秒。</p> <p>取值范围：15分钟 ~ 24小时，默认为15分钟。</p>

响应参数

表 5-100 响应 Body 参数

参数	参数类型	描述
credential	Object	认证结果信息。

表 5-101 credential

参数	参数类型	描述
expires_at	String	AK/SK和securitytoken的过期时间。响应参数为UTC时间格式。
access	String	获取的AK。
secret	String	获取的SK。
securitytoken	String	securitytoken是将所获的AK、SK等信息进行加密后的字符串。

请求示例

- 填写"token"参数。包含tokenId（即token）和临时访问密钥和securitytoken的有效期。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
    "identity": {
      "methods": [
        "token"
      ],
      "token": {
        "id": "MIIElgYJKoZlIhvc...",
        "duration_seconds": "900"
      }
    }
  }
}
```

- 不填写“token”参数（请求头中需要X-Auth-Token）。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
    "identity": {
      "methods": [
        "token"
      ]
    }
  }
}
```

- 填写“policy”参数。即用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅适用限制OBS服务的权限）。如果填写此参数，则临时访问密钥和securitytoken的权限为：原Token具有的权限和policy参数限制的权限交集。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
    "identity": {
      "methods": [
        "token"
      ],
      "policy": {
        "Version": "1.1",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": [
              "obs:object:GetObject"
            ]
          }
        ]
      }
    }
  }
}
```

```

"Resource": [
  "OBS:*:object:*"
],
"Condition": {
  "StringEquals": {
    "g:DomainName": [
      "DomainNameExample" //示例，表示限制条件值，根据实际情况填写
    ]
  }
}
}
]
},
"token": {
  "duration_seconds": 900
}
}
}

```

响应示例

状态码为 201 时:

创建成功。

```

{
  "credential": {
    "access": "NZFAT5VNWEJDGZ4PZ...",
    "expires_at": "2020-01-08T03:50:07.574000Z",
    "secret": "riEoWsy3qO0BvgwfkolVgCUvzgpjBBcvdq...",
    "securitytoken": "gQpjbi1ub3J0aC00jD4Ej..."
  }
}

```

返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
500	内部服务错误。

错误码

无

5.2.3 获取联邦用户的临时访问密钥和 securitytoken

功能介绍

该接口可以用于通过token来获取临时AK/SK和securitytoken。临时AK/SK和securitytoken是系统颁发给IAM用户的临时访问令牌，有效期可在15分钟至24小时范围内设置，过期后需要重新获取。临时AK/SK和securitytoken遵循权限最小化原则。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

使用获取到的临时AK/SK和securitytoken作为凭证访问云服务，临时AK/SK和securitytoken两者必须**同时使用**，请求头中需要添加“x-security-token”字段，使用方法详情请参考：[使用临时AK/SK做签名](#)。

调试

您可以在[API Explorer](#)中调试该接口。

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

请求参数

表 5-102 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段填为“application/json;charset=utf8”。
X-Auth-Token	是	String	联邦用户只能使用X-Auth-Token获取securitytoken。

表 5-103 请求 Body 参数

参数	是否必选	参数类型	描述
auth	是	Object	认证信息。

表 5-104 auth

参数	是否必选	参数类型	描述
identity	是	Object	认证参数。

表 5-105 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为["token"]。
token	否	Object	临时访问密钥和securitytoken的有效期。
policy	否	Object	<p>用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅OBS服务支持该限制）。</p> <p>如果填写此参数，则临时访问密钥和securitytoken的权限为：原Token具有的权限和policy参数限制的权限交集。</p> <p>policy参数的字符个数不大于2048。</p> <p>关于IAM策略的格式和语法，请参考：策略。</p>

表 5-106 auth.identity.policy

参数	是否必选	参数类型	描述
Version	是	String	<p>权限版本号，创建自定义策略时，该字段值填为“1.1”。</p> <p>说明</p> <p>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</p>
Statement	是	Array of objects	授权语句，描述自定义策略的具体内容。

表 5-107 auth.identity.policy.Statement

参数	是否必选	参数类型	描述
Action	是	Array of strings	<p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p>说明</p> <ul style="list-style-type: none"> 格式为：服务名:资源类型:操作，例：vpc:ports:create。 服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符*，无需罗列全部授权项。
Effect	是	String	<p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> Allow Deny
Condition	否	Map<String,Map<String,Array<String>>>	<p>限制条件。了解更多相关参数，请参考：策略语法。</p> <p>说明</p> <p>以请求示例中的Condition为例：当账号名（DomainName）等于DomainNameExample时，该策略才会生效。</p> <pre> "Condition": { "StringEquals": { "g:DomainName": ["DomainNameExample"] } } </pre>
Resource	否	Array of strings	<p>资源。规则如下：</p> <p>说明</p> <ul style="list-style-type: none"> 格式为“服务名:region:domainId:资源类型:资源路径”，资源类型支持通配符*，通配符*表示所有。如"obs:*:*:bucket:*":表示所有的OBS桶。支持IAM资源粒度授权的云服务，请参考支持IAM资源粒度授权的云服务。 region字段为*或用户可访问的region。service必须存在且resource属于对应service。 其中，服务名、region、domainId、资源类型的格式为：由字母、数字、下划线、连字符、星号组成，长度为1到50个字符；资源路径的格式为：由除分号、竖线、波浪线、反引号、大括号、中括号、尖括号以外的任意字符组成，长度为1到1200个字符。

表 5-108 auth.identity.token

参数	是否必选	参数类型	描述
id	否	String	即token，若请求Header中不传X-Auth-Token，则须填此参数。
duration_seconds	否	Integer	临时访问密钥和securitytoken的有效期，时间单位为秒。 取值范围：15分钟 ~ 24小时，默认为15分钟。

响应参数

表 5-109 响应 Body 参数

参数	参数类型	描述
credential	Object	认证结果信息。

表 5-110 credential

参数	参数类型	描述
expires_at	String	AK/SK和securitytoken的过期时间。响应参数为UTC时间格式。
access	String	获取的AK。
secret	String	获取的SK。
securitytoken	String	securitytoken是将所获的AK、SK等信息进行加密后的字符串。

请求示例

- 填写"token"参数。包含tokenId（即token）和临时访问密钥和securitytoken的有效期。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
    "identity": {
      "methods": [
        "token"
      ],
      "token": {
        "id": "MIIElgYJKoZihvc...",
        "duration_seconds": "900"
      }
    }
  }
}
```

- ```

 }
 }
}

```
- 不填写“token”参数（请求头中需要X-Auth-Token）。  
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens  

```

{
 "auth": {
 "identity": {
 "methods": [
 "token"
]
 }
 }
}

```
  - 填写“policy”参数。即用户自定义策略的信息，用于限制获取到的临时访问密钥和securitytoken的权限（当前仅适用限制OBS服务的权限）。如果填写此参数，则临时访问密钥和securitytoken的权限为：原Token具有的权限和policy参数限制的权限交集。  
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/securitytokens  

```

{
 "auth": {
 "identity": {
 "methods": [
 "token"
],
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:object:GetObject"
],
 "Resource": [
 "OBS:*:*:object:*"
],
 "Condition": {
 "StringEquals": {
 "g:DomainName": [
 "DomainNameExample"
]
 }
 }
 }
]
 }
 },
 "token": {
 "duration_seconds": 900
 }
 }
}

```

//示例，表示限制条件值，根据实际情况填写

## 响应示例

**状态码为 201 时:**

创建成功。

```

{
 "credential": {
 "access": "NZFAT5VNWEJDGZ4PZ...",
 "expires_at": "2020-01-08T03:50:07.574000Z",
 "secret": "riEoWsy3qO0BvgwfkolVgCUvzgpjBBcvdq...",
 "securitytoken": "gQpjb1ub3J0aC00jD4Ej..."
 }
}

```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 201 | 创建成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.2.4 创建永久访问密钥

### 功能介绍

该接口可以用于[管理员](#)给IAM用户创建永久访问密钥，或IAM用户给自己创建永久访问密钥。

访问密钥（Access Key ID/Secret Access Key，简称AK/SK），是您通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，不用于登录控制台。系统通过AK识别访问用户的身份，通过SK进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。在控制台创建访问密钥的方式请参见：[访问密钥](#)。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-CREDENTIAL/credentials

### 请求参数

表 5-111 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                    |
|--------------|------|--------|---------------------------------------|
| Content-Type | 是    | String | 该字段填为“application/json;charset=utf8”。 |



| 参数           | 是否必选 | 参数类型   | 描述                                                                                                              |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 给IAM用户创建永久访问密钥：请参见 <a href="#">授权项</a> 。IAM用户给自己创建永久访问密钥：请求体中user_id所对应IAM用户的token（无需特殊权限）。 |

表 5-112 请求 Body 参数

| 参数                         | 是否必选 | 参数类型   | 描述    |
|----------------------------|------|--------|-------|
| <a href="#">credential</a> | 是    | Object | 认证信息。 |

表 5-113 credential

| 参数          | 是否必选 | 参数类型   | 描述                                                                              |
|-------------|------|--------|---------------------------------------------------------------------------------|
| user_id     | 是    | String | 待创建访问密钥（AK/SK）的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| description | 否    | String | 访问密钥描述信息。                                                                       |

## 响应参数

表 5-114 响应 Body 参数

| 参数                         | 参数类型   | 描述      |
|----------------------------|--------|---------|
| <a href="#">credential</a> | Object | 认证结果信息。 |

表 5-115 credential

| 参数          | 参数类型   | 描述                                                                                                                                     |
|-------------|--------|----------------------------------------------------------------------------------------------------------------------------------------|
| create_time | String | 创建访问密钥时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照 <a href="#">ISO-8601</a> ，如：<br>2023-06-28T08:56:33.710000Z。 |
| access      | String | 创建的AK。                                                                                                                                 |

| 参数          | 参数类型   | 描述                                                                                                      |
|-------------|--------|---------------------------------------------------------------------------------------------------------|
| secret      | String | 创建的SK。                                                                                                  |
| status      | String | 访问密钥状态。<br>取值范围： <ul style="list-style-type: none"> <li>• active: 启用</li> <li>• inactive: 停用</li> </ul> |
| user_id     | String | IAM用户ID。                                                                                                |
| description | String | 访问密钥描述信息。                                                                                               |

## 请求示例

给IAM用户创建永久访问密钥（用户ID为：07609fb9358010e21f7bc003751c....）

```
POST https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials
{
 "credential": {
 "description": "IAMDescription",
 "user_id": "07609fb9358010e21f7bc003751c..."
 }
}
```

## 响应示例

**状态码为 201 时:**

创建成功。

```
{
 "credential": {
 "access": "P83EVBZJMXYTMUII...",
 "create_time": "2020-01-08T06:25:19.014028Z",
 "user_id": "07609fb9358010e21f7bc003751...",
 "description": "IAMDescription",
 "secret": "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
 "status": "active"
 }
}
```

**状态码为 400 时:**

参数无效。（包括密钥数量已达到上限。）

```
{
 "error": {
 "message": "akSkNumExceed",
 "code": 400,
 "title": "Bad Request",
 "error_msg": null,
 "error_code": null
 }
}
```

## 返回值

| 返回值 | 描述                  |
|-----|---------------------|
| 201 | 创建成功。               |
| 400 | 参数无效。（包括密钥数量已达到上限。） |
| 401 | 认证失败。               |
| 403 | 没有操作权限。             |
| 500 | 内部服务错误。             |

## 错误码

无

## 5.2.5 查询所有永久访问密钥

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户的所有永久访问密钥，或IAM用户查询自己的所有永久访问密钥。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-CREDENTIAL/credentials

表 5-116 Query 参数

| 参数      | 是否必选 | 参数类型   | 描述           |
|---------|------|--------|--------------|
| user_id | 否    | String | 待查询的IAM用户ID。 |

## 请求参数

表 5-117 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                |
|--------------|------|--------|---------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段填为 “application/json;charset=utf8”。                                                            |
| X-Auth-Token | 是    | String | IAM用户查询自己的所有永久访问密钥：该IAM用户的token（无需特殊权限）。<br><b>管理员</b> 查询IAM用户的所有永久访问密钥：请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-118 响应 Body 参数

| 参数                 | 参数类型             | 描述        |
|--------------------|------------------|-----------|
| <b>credentials</b> | Array of objects | 认证结果信息列表。 |

表 5-119 credentials

| 参数          | 参数类型   | 描述                                                                                                                                 |
|-------------|--------|------------------------------------------------------------------------------------------------------------------------------------|
| user_id     | String | IAM用户ID。                                                                                                                           |
| access      | String | 查询的AK。                                                                                                                             |
| status      | String | 访问密钥状态。<br>取值范围：<br><ul style="list-style-type: none"> <li>active：启用</li> <li>inactive：停用</li> </ul>                               |
| create_time | String | 访问密钥创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照 <a href="#">ISO-8601</a> ，如：2023-06-28T08:56:33.710000Z。 |
| description | String | 访问密钥描述信息。                                                                                                                          |

## 请求示例

- IAM用户查询自己的所有永久访问密钥。  
GET <https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials>

- 管理员查询IAM用户的所有永久访问密钥。（待查询的用户ID为：07609fb9358010e21f7bc003751c...）  
GET https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials?  
user\_id=07609fb9358010e21f7bc0037....

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "credentials": [
 {
 "access": "LOSZM4YRVLKOY9E8X...",
 "create_time": "2020-01-08T06:26:08.123059Z",
 "user_id": "07609fb9358010e21f7bc0037...",
 "description": "",
 "status": "active"
 },
 {
 "access": "P83EVBZJMXCYTMU...",
 "create_time": "2020-01-08T06:25:19.014028Z",
 "user_id": "07609fb9358010e21f7bc003751...",
 "description": "",
 "status": "active"
 }
]
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.2.6 查询指定永久访问密钥

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户的指定永久访问密钥，或IAM用户查询自己的指定永久访问密钥。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-CREDENTIAL/credentials/{access\_key}

表 5-120 路径参数

| 参数         | 是否必选 | 参数类型   | 描述        |
|------------|------|--------|-----------|
| access_key | 是    | String | 待查询的指定AK。 |

## 请求参数

表 5-121 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                        |
|--------------|------|--------|---------------------------------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段填为 “application/json;charset=utf8”。                                                                                    |
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户的指定永久访问密钥：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己的指定永久访问密钥：URL中access_key所属IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-122 响应 Body 参数

| 参数                         | 参数类型   | 描述      |
|----------------------------|--------|---------|
| <a href="#">credential</a> | Object | 认证结果信息。 |

表 5-123 credential

| 参数      | 参数类型   | 描述       |
|---------|--------|----------|
| user_id | String | IAM用户ID。 |
| access  | String | 查询的AK。   |

| 参数            | 参数类型   | 描述                                                                                                                                     |
|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------------|
| status        | String | 访问密钥状态。<br>取值范围： <ul style="list-style-type: none"> <li>active：启用</li> <li>inactive：停用</li> </ul>                                      |
| create_time   | String | 访问密钥创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。                       |
| last_use_time | String | 访问密钥的使用时间，如果密钥没有使用过，则返回密钥的创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。 |
| description   | String | 访问密钥描述信息。                                                                                                                              |

## 请求示例

IAM用户查询自己的指定永久访问密钥。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials/{access_key}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "credential": {
 "last_use_time": "2020-01-08T06:26:08.123059Z",
 "access": "LOSZM4YRVLK0Y9E8...",
 "create_time": "2020-01-08T06:26:08.123059Z",
 "user_id": "07609fb9358010e21f7bc003751...",
 "description": "",
 "status": "active"
 }
}
```

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 200 | 请求成功。 |
| 400 | 参数无效。 |
| 401 | 认证失败。 |

| 返回值 | 描述        |
|-----|-----------|
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.2.7 修改指定永久访问密钥

### 功能介绍

该接口可以用于[管理员](#)修改IAM用户的指定永久访问密钥，或IAM用户修改自己的指定永久访问密钥。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-CREDENTIAL/credentials/{access\_key}

表 5-124 路径参数

| 参数         | 是否必选 | 参数类型   | 描述        |
|------------|------|--------|-----------|
| access_key | 是    | String | 待修改的指定AK。 |

### 请求参数

表 5-125 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                    |
|--------------|------|--------|---------------------------------------|
| Content-Type | 是    | String | 该字段填为“application/json;charset=utf8”。 |



| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                |
|--------------|------|--------|-------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <b>管理员</b> 修改IAM用户的指定永久访问密钥：请参见 <a href="#">授权项</a> 。<br>IAM用户修改自己的指定永久访问密钥：URL中access_key所对应IAM用户的token（无需特殊权限）。 |

表 5-126 请求 Body 参数

| 参数                | 是否必选 | 参数类型   | 描述    |
|-------------------|------|--------|-------|
| <b>credential</b> | 是    | Object | 认证信息。 |

表 5-127 credential

| 参数          | 是否必选 | 参数类型   | 描述                                                                                                |
|-------------|------|--------|---------------------------------------------------------------------------------------------------|
| status      | 否    | String | 访问密钥状态。<br>取值范围： <ul style="list-style-type: none"> <li>active：启用</li> <li>inactive：停用</li> </ul> |
| description | 否    | String | 访问密钥描述信息。                                                                                         |

## 响应参数

表 5-128 响应 Body 参数

| 参数                | 参数类型   | 描述    |
|-------------------|--------|-------|
| <b>credential</b> | Object | 认证信息。 |

表 5-129 credential

| 参数      | 参数类型   | 描述       |
|---------|--------|----------|
| user_id | String | IAM用户ID。 |
| access  | String | 修改的AK。   |

| 参数          | 参数类型   | 描述                                                                                                                                 |
|-------------|--------|------------------------------------------------------------------------------------------------------------------------------------|
| status      | String | 访问密钥状态。<br>取值范围： <ul style="list-style-type: none"> <li>● active：启用</li> <li>● inactive：停用</li> </ul>                              |
| create_time | String | 访问密钥创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照 <a href="#">ISO-8601</a> ，如：2023-06-28T08:56:33.710000Z。 |
| description | String | 访问密钥描述信息。                                                                                                                          |

## 请求示例

IAM用户修改自己的指定永久访问密钥状态为“不启用”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials/{access_key}
{
 "credential": {
 "status": "inactive",
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "credential": {
 "status": "inactive",
 "access": "LOSZM4YRVLK0Y9...",
 "create_time": "2020-01-08T06:26:08.123059Z",
 "user_id": "07609fb9358010e21f7bc00375..."
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

| 返回值 | 描述      |
|-----|---------|
| 500 | 内部服务错误。 |

## 错误码

无

## 5.2.8 删除指定永久访问密钥

### 功能介绍

该接口可以用于[管理员](#)删除IAM用户的指定永久访问密钥，或IAM用户删除自己的指定永久访问密钥。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 说明

删除操作无法恢复，为保证业务连续性，建议确认访问密钥一周以上未使用后，进行删除操作。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

DELETE /v3.0/OS-CREDENTIAL/credentials/{access\_key}

表 5-130 路径参数

| 参数         | 是否必选 | 参数类型   | 描述        |
|------------|------|--------|-----------|
| access_key | 是    | String | 待删除的指定AK。 |

## 请求参数

表 5-131 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                    |
|--------------|------|--------|---------------------------------------|
| Content-Type | 是    | String | 该字段填为“application/json;charset=utf8”。 |

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                |
|--------------|------|--------|-------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <b>管理员</b> 删除IAM用户的指定永久访问密钥：请参见 <a href="#">授权项</a> 。<br>IAM用户删除自己的指定永久访问密钥：URL中access_key所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

无

## 请求示例

删除指定永久访问密钥。

DELETE https://iam.myhuaweicloud.com/v3.0/OS-CREDENTIAL/credentials/{access\_key}

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.3 区域管理

## 5.3.1 查询区域列表

### 功能介绍

该接口可以用于查询账号可以访问的区域列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/regions

### 请求参数

表 5-132 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                         |
|--------------|------|--------|------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                    |
| X-Auth-Token | 是    | String | IAM用户的token（无需特殊权限）。如果token中没有私有region信息，则查询结果不返回私有region。 |

### 响应参数

表 5-133 响应 Body 参数

| 参数                      | 参数类型             | 描述      |
|-------------------------|------------------|---------|
| <a href="#">links</a>   | Object           | 资源链接信息。 |
| <a href="#">regions</a> | Array of objects | 区域信息列表。 |

表 5-134 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |

| 参数   | 参数类型   | 描述                    |
|------|--------|-----------------------|
| next | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-135 regions

| 参数               | 参数类型   | 描述                          |
|------------------|--------|-----------------------------|
| description      | String | 区域描述信息。                     |
| parent_region_id | String | null.                       |
| <b>links</b>     | Object | 区域的资源链接信息。                  |
| <b>locales</b>   | Object | 区域名，受区域信息注册影响，不一定返回对象中所有字段。 |
| id               | String | 区域ID。                       |
| type             | String | 区域类型。                       |

表 5-136 regions.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-137 regions.locales

| 参数    | 参数类型   | 描述           |
|-------|--------|--------------|
| zh-cn | String | 区域的中文名称。     |
| en-us | String | 区域的英文名称。     |
| pt-br | String | 区域的葡萄牙语名称。   |
| es-us | String | 区域的美国西班牙语名称。 |
| es-es | String | 区域的西班牙语名称。   |

## 请求示例

查询区域列表。

```
GET https://iam.myhuaweicloud.com/v3/regions
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "regions": [
 {
 "parent_region_id": null,
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/regions/ap-southeast-1"
 },
 "type": "public",
 "id": "ap-southeast-1",
 "locales": {
 "zh-cn": " "中国-香港" ",
 "en-us": "ap-southeast-1"
 }
 },
 {
 "parent_region_id": null,
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/regions/la-south-2"
 },
 "type": "public",
 "id": "la-south-2",
 "locales": {
 "pt-br": "AL-Santiago",
 "zh-cn": "拉美-圣地亚哥",
 "en-us": "LA-Santiago",
 "es-us": "AL-Santiago de Chile1",
 "es-es": "LA-Santiago"
 }
 }
],
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/regions",
 "previous": null,
 "next": null
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |

| 返回值 | 描述     |
|-----|--------|
| 503 | 服务不可用。 |

## 错误码

无

## 5.3.2 查询区域详情

### 功能介绍

该接口可以用于查询区域详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/regions/{region\_id}

表 5-138 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                             |
|-----------|------|--------|--------------------------------------------------------------------------------|
| region_id | 是    | String | 待查询的区域ID。可以使用 <a href="#">查询区域列表</a> 接口获取，控制台获取方法请参见： <a href="#">获取区域ID</a> 。 |

### 请求参数

表 5-139 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | IAM用户token(无需特殊权限)。                     |



## 响应参数

表 5-140 响应 Body 参数

| 参数                     | 参数类型   | 描述    |
|------------------------|--------|-------|
| <a href="#">region</a> | Object | 区域信息。 |

表 5-141 region

| 参数                      | 参数类型   | 描述                          |
|-------------------------|--------|-----------------------------|
| description             | String | 区域描述信息。                     |
| parent_region_id        | String | 预埋字段，当前无实际意义，返回null。        |
| <a href="#">links</a>   | Object | 区域的资源链接信息。                  |
| <a href="#">locales</a> | Object | 区域名，受区域信息注册影响，不一定返回对象中所有字段。 |
| id                      | String | 区域ID。                       |
| type                    | String | 区域类型。                       |

表 5-142 region.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-143 region.locales

| 参数    | 参数类型   | 描述           |
|-------|--------|--------------|
| zh-cn | String | 区域的中文名称。     |
| en-us | String | 区域的英文名称。     |
| pt-br | String | 区域的葡萄牙语名称。   |
| es-us | String | 区域的美国西班牙语名称。 |
| es-es | String | 区域的西班牙语名称。   |

## 请求示例

查询区域详情。

GET https://iam.myhuaweicloud.com/v3/regions/{region\_id}

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "region": {
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/regions/la-south-2"
 },
 "type": "public",
 "id": "la-south-2",
 "locales": {
 "pt-br": "AL-Santiago",
 "zh-cn": "拉美-圣地亚哥",
 "en-us": "LA-Santiago",
 "es-us": "AL-Santiago de Chile1",
 "es-es": "LA-Santiago"
 }
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.4 项目管理

## 5.4.1 查询指定条件下的项目列表

### 功能介绍

该接口可以用于查询指定条件下的项目列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/projects

表 5-144 Query 参数

| 参数        | 是否必选 | 参数类型    | 描述                                                                                                                                           |
|-----------|------|---------|----------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 否    | String  | 项目所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                            |
| enabled   | 否    | Boolean | 项目是否启用。                                                                                                                                      |
| is_domain | 否    | Boolean | 该字段无需填写。                                                                                                                                     |
| name      | 否    | String  | 项目名称，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                |
| page      | 否    | Integer | 分页查询时数据的页数，查询值最小为1。需要与per_page同时存在。                                                                                                          |
| parent_id | 否    | String  | 如果查询自己创建的项目，则此处应填为所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处应填为账号ID。<br>获取项目ID和账号ID，请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| per_page  | 否    | Integer | 分页查询时每页的数据个数，取值范围为[1,5000]。需要与page同时存在。                                                                                                      |

## 请求参数

表 5-145 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-146 响应 Body 参数

| 参数                       | 参数类型             | 描述      |
|--------------------------|------------------|---------|
| <a href="#">links</a>    | Object           | 资源链接信息。 |
| <a href="#">projects</a> | Array of objects | 项目信息列表。 |

表 5-147 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-148 projects

| 参数                    | 参数类型    | 描述       |
|-----------------------|---------|----------|
| is_domain             | Boolean | false.   |
| description           | String  | 项目描述信息。  |
| <a href="#">links</a> | Object  | 项目的资源链接。 |
| enabled               | Boolean | 项目是否可用。  |
| id                    | String  | 项目ID。    |

| 参数        | 参数类型   | 描述                                                                     |
|-----------|--------|------------------------------------------------------------------------|
| parent_id | String | 如果查询自己创建的项目，则此处返回所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。 |
| domain_id | String | 项目所属账号ID。                                                              |
| name      | String | 项目名称。如ap-southeast-1、MOS等，其中MOS为OBS内置项目。                               |

表 5-149 projects.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询指定条件下的项目列表。

```
GET https://iam.myhuaweicloud.com/v3/projects
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "projects": [
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd022...",
 "name": "ap-southeast-1",
 "description": "",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects/06f1c15e6f0010672f86c003006c5f17"
 },
 "id": "06f1c15e6f0010672f86c00300...",
 "enabled": true
 },
 {
 "domain_id": "d78cbac186b744899480f25bd...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd0...",
 "name": "",
 "description": "",
 "links": {
 "next": null,
```

```
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects/065a7c66da0010992ff7c0031e5a...",
 },
 "id": "065a7c66da0010992ff7c0031e5a...",
 "enabled": true
}
],
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects"
}
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.4.2 查询指定 IAM 用户的项目列表

### 功能介绍

该接口可以用于[管理员](#)查询指定IAM用户的项目列表，或IAM用户查询自己的项目列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/users/{user\_id}/projects

表 5-150 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-151 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                      |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                                                                                                 |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br><a href="#">管理员</a> 查询指定IAM用户的项目列表：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自身项目列表：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-152 响应 Body 参数

| 参数                       | 参数类型             | 描述      |
|--------------------------|------------------|---------|
| <a href="#">links</a>    | Object           | 资源链接信息。 |
| <a href="#">projects</a> | Array of objects | 项目信息列表。 |

表 5-153 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-154 projects

| 参数           | 参数类型    | 描述                                                                     |
|--------------|---------|------------------------------------------------------------------------|
| is_domain    | Boolean | false.                                                                 |
| description  | String  | 项目描述信息。                                                                |
| <b>links</b> | Object  | 项目的资源链接。                                                               |
| enabled      | Boolean | 项目是否可用。                                                                |
| id           | String  | 项目ID。                                                                  |
| parent_id    | String  | 如果查询自己创建的项目，则此处返回所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。 |
| domain_id    | String  | 项目所属账号ID。                                                              |
| name         | String  | 项目名称。                                                                  |

表 5-155 projects.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询指定IAM用户的项目列表。

GET https://iam.myhuaweicloud.com/v3/users/{user\_id}/projects

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "projects": [
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd0...",
 "name": "ap-southeast-1",
 "description": "",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects/06f1cd8ea9800ff02f26c003d93..."
 }
 }
]
}
```



```

 },
 "id": "06f1cd8ea9800ff02f26c003d93...",
 "enabled": true
 },
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd0...",
 "name": "MOS",
 "description": "",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects/babf0605d15b4f9fbcacc6a8ee0f8d84"
 },
 "id": "babf0605d15b4f9fbcacc6a8ee0f8d84",
 "enabled": true
 }
],
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/7116d09f88fa41908676fdd4b039e95b/projects"
}
}

```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

### 5.4.3 查询 IAM 用户可以访问的项目列表

#### 功能介绍

该接口可以用于查询IAM用户可以访问的项目列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/auth/projects

## 请求参数

表 5-156 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | IAM用户的token（无需特殊权限）。                    |

## 响应参数

表 5-157 响应 Body 参数

| 参数                       | 参数类型             | 描述      |
|--------------------------|------------------|---------|
| <a href="#">links</a>    | Object           | 资源链接信息。 |
| <a href="#">projects</a> | Array of objects | 项目信息列表。 |

表 5-158 links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-159 projects

| 参数                    | 参数类型    | 描述       |
|-----------------------|---------|----------|
| is_domain             | Boolean | false.   |
| description           | String  | 项目描述信息。  |
| <a href="#">links</a> | Object  | 项目的资源链接。 |
| enabled               | Boolean | 项目是否可用。  |

| 参数        | 参数类型   | 描述                                                                     |
|-----------|--------|------------------------------------------------------------------------|
| id        | String | 项目ID。                                                                  |
| parent_id | String | 如果查询自己创建的项目，则此处返回所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。 |
| domain_id | String | 项目所属账号ID。                                                              |
| name      | String | 项目名称。                                                                  |

表 5-160 projects.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

查询IAM用户可以访问的项目列表。

GET <https://iam.myhuaweicloud.com/v3/auth/projects>

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "projects": [
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd022...",
 "name": "af-south-1",
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/06f1cbbaf280106b2f14c00313a9d065"
 },
 "id": "06f1cbbaf280106b2f14c00313a9...",
 "enabled": true
 },
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd022...",
 "name": "",
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/065a7c66da0010992ff7c0031e5a5e7d"
 },
 "id": "065a7c66da0010992ff7c0031e5a5e7d",
 "enabled": true
 }
],
}
```

```
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/auth/projects"
}
```

#### 说明

- 当授权给项目级服务时，则返回已授权的项目列表。
- 当授权给所有资源时，则返回用户下的所有项目。
- 当授权给全局服务或未授权时，则返回的项目为空。

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

### 5.4.4 创建项目

#### 功能介绍

该接口可以用于[管理员](#)创建项目。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3/projects

## 请求参数

表 5-161 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-162 请求 Body 参数

| 参数                      | 是否必选 | 参数类型   | 描述    |
|-------------------------|------|--------|-------|
| <a href="#">project</a> | 是    | Object | 项目信息。 |

表 5-163 project

| 参数          | 是否必选 | 参数类型   | 描述                                                                                                                                 |
|-------------|------|--------|------------------------------------------------------------------------------------------------------------------------------------|
| name        | 是    | String | 项目名称。必须以存在的“区域ID_”开头，长度小于等于64。例如区域“中国-香港”的区域ID为“ap-southeast-1”，在其下创建项目时，项目名应填“ap-southeast-1_IAMProject”                          |
| parent_id   | 是    | String | 区域对应的项目ID，例如区域“中国-香港”区域对应的项目ID为：<br>04dd42abe48026ad2fa3c01ad7fa.....，<br>获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| domain_id   | 否    | String | 项目所属账号ID。                                                                                                                          |
| description | 否    | String | 项目描述信息，长度小于等于255字符。                                                                                                                |

## 响应参数

表 5-164 响应 Body 参数

| 参数                      | 参数类型   | 描述    |
|-------------------------|--------|-------|
| <a href="#">project</a> | Object | 项目信息。 |

表 5-165 project

| 参数                    | 参数类型    | 描述                                                                     |
|-----------------------|---------|------------------------------------------------------------------------|
| is_domain             | Boolean | false.                                                                 |
| description           | String  | 项目描述信息。                                                                |
| <a href="#">links</a> | Object  | 项目的资源链接。                                                               |
| enabled               | Boolean | 项目是否可用。                                                                |
| id                    | String  | 项目ID。                                                                  |
| parent_id             | String  | 区域对应的项目ID，例如区域“中国-香港”区域对应的项目ID为：<br>04dd42abe48026ad2fa3c01ad7fa.....。 |
| domain_id             | String  | 项目所属账号ID。                                                              |
| name                  | String  | 项目名称。                                                                  |

表 5-166 project.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

创建一个名为“ap-southeast-1\_IAMProject”且在中国-香港的项目，项目所属账号ID是d78cbac186b744899480f25bd0...

```
POST https://iam.myhuaweicloud.com/v3/projects
{
 "project": {
 "name": "ap-southeast-1_IAMProject",
 "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
 "domain_id": "d78cbac186b744899480f25bd0...",
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "project": {
 "is_domain": false,
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/07707ab14980265e2f5fc003a021bbc3"
 },
 "enabled": true,
 "id": "07707ab14980265e2f5fc003a021bbc3",
 "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
 "domain_id": "d78cbac186b744899480f25bd02...",
 "name": "ap-southeast-1_IAMProject"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 201 | 创建成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 409 | 资源冲突。   |

## 错误码

无

## 5.4.5 修改项目信息

### 功能介绍

该接口可以用于[管理员](#)修改项目信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PATCH /v3/projects/{project\_id}

表 5-167 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                |
|------------|------|--------|-------------------------------------------------------------------|
| project_id | 是    | String | 待修改的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-168 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-169 请求 Body 参数

| 参数                      | 是否必选 | 参数类型   | 描述         |
|-------------------------|------|--------|------------|
| <a href="#">project</a> | 是    | Object | 需要修改的项目信息。 |

表 5-170 project

| 参数          | 是否必选 | 参数类型   | 描述                                                                                                                                     |
|-------------|------|--------|----------------------------------------------------------------------------------------------------------------------------------------|
| name        | 否    | String | 项目名称，必须以存在的“区域ID_”开头，长度小于等于64。项目所属区域不能改变，即原项目名为“ap-southeast-1_IAMProject”时，新项目名只能以“ap-southeast-1_”开头。<br>“name”与“description”至少填写一个。 |
| description | 否    | String | 项目描述，长度小于等于255字符。<br>“name”与“description”至少填写一个。                                                                                       |



## 响应参数

表 5-171 响应 Body 参数

| 参数             | 参数类型   | 描述    |
|----------------|--------|-------|
| <b>project</b> | Object | 项目信息。 |

表 5-172 project

| 参数           | 参数类型    | 描述                                                                     |
|--------------|---------|------------------------------------------------------------------------|
| is_domain    | Boolean | false.                                                                 |
| description  | String  | 项目描述信息。                                                                |
| extra        | Object  | 项目的其他信息。                                                               |
| <b>links</b> | Object  | 项目的资源链接。                                                               |
| enabled      | Boolean | 项目是否可用。                                                                |
| id           | String  | 项目ID。                                                                  |
| parent_id    | String  | 区域对应的项目ID，例如区域“中国-香港”区域对应的项目ID为：<br>04dd42abe48026ad2fa3c01ad7fa.....。 |
| domain_id    | String  | 项目所属账号ID。                                                              |
| name         | String  | 项目名称。                                                                  |

表 5-173 project.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

修改项目的名称为“ap-southeast-1\_IAMNewProject”，描述修改为“IAMDescription”。

```
PATCH https://iam.myhuaweicloud.com/v3/projects/{project_id}
{
 "project": {
 "name": "ap-southeast-1_IAMNewProject",
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "project": {
 "is_domain": false,
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/07707ab14980265e2f5fc003a021bbc3"
 },
 "extra": {},
 "enabled": true,
 "id": "07707ab14980265e2f5fc003a021bbc3",
 "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
 "domain_id": "d78cbac186b744899480f25bd...",
 "name": "ap-southeast-1_IAMNewProject"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 409 | 资源冲突。   |

## 错误码

无

## 5.4.6 查询项目详情

### 功能介绍

该接口可以用于查询项目详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/projects/{project\_id}

表 5-174 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                                                                                                          |
|------------|------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id | 是    | String | 待查询的项目ID，获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> 。 |

## 请求参数

表 5-175 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | IAM用户的token（无需特殊权限）。                    |

## 响应参数

表 5-176 响应 Body 参数

| 参数                      | 参数类型   | 描述    |
|-------------------------|--------|-------|
| <a href="#">project</a> | Object | 项目信息。 |

表 5-177 project

| 参数                    | 参数类型    | 描述                                                                     |
|-----------------------|---------|------------------------------------------------------------------------|
| is_domain             | Boolean | false.                                                                 |
| description           | String  | 项目描述信息。                                                                |
| <a href="#">links</a> | Object  | 项目的资源链接。                                                               |
| enabled               | Boolean | 项目是否可用。                                                                |
| id                    | String  | 项目ID。                                                                  |
| parent_id             | String  | 如果查询自己创建的项目，则此处返回所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。 |
| domain_id             | String  | 项目所属账号ID。                                                              |

| 参数   | 参数类型   | 描述    |
|------|--------|-------|
| name | String | 项目名称。 |

表 5-178 project.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询项目详情。

GET https://iam.myhuaweicloud.com/v3/projects/{project\_id}

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "project": {
 "is_domain": false,
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/2e93d63d8d2249f5a4ac5e2c78586a6e"
 },
 "enabled": true,
 "id": "2e93d63d8d2249f5a4ac5e2c78586a6e",
 "parent_id": "44c0781c83484eb9a4a5d4d233522cea",
 "domain_id": "44c0781c83484eb9a4a5d4d23...",
 "name": "MOS"
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.4.7 设置项目状态

### 功能介绍

该接口可以用于[管理员](#)设置项目状态。项目状态包括：正常、冻结。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3-ext/projects/{project\_id}

表 5-179 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                  |
|------------|------|--------|---------------------------------------------------------------------|
| project_id | 是    | String | 待设置状态的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-180 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-181 请求 Body 参数

| 参数                      | 是否必选 | 参数类型   | 描述    |
|-------------------------|------|--------|-------|
| <a href="#">project</a> | 是    | Object | 项目信息。 |

表 5-182 project

| 参数     | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                      |
|--------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| status | 是    | String | 项目的状态信息，参数的值为"suspended"或"normal"。<br><ul style="list-style-type: none"> <li>status值为"suspended"时，会将项目设置为冻结状态。</li> <li>status值为"normal"时，会将项目设置为正常（解冻）状态。</li> </ul> 取值范围： <ul style="list-style-type: none"> <li>suspended</li> <li>normal</li> </ul> |

## 响应参数

无

## 请求示例

设置项目状态为“冻结”状态。

```
PUT https://iam.myhuaweicloud.com/v3-ext/projects/{project_id}
{
 "project": {
 "status": "suspended"
 }
}
```

## 响应示例

无

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 204 | 设置成功。 |
| 400 | 参数无效。 |
| 401 | 认证失败。 |

| 返回值 | 描述        |
|-----|-----------|
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.4.8 查询项目详情与状态

### 功能介绍

该接口可以用于[管理员](#)查询项目详情与状态。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3-ext/projects/{project\_id}

表 5-183 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                |
|------------|------|--------|-------------------------------------------------------------------|
| project_id | 是    | String | 待查询的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-184 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |

| 参数           | 是否必选 | 参数类型   | 描述                                 |
|--------------|------|--------|------------------------------------|
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的 token。 |

## 响应参数

表 5-185 响应 Body 参数

| 参数             | 参数类型   | 描述    |
|----------------|--------|-------|
| <b>project</b> | Object | 项目信息。 |

表 5-186 project

| 参数          | 参数类型    | 描述                                                                     |
|-------------|---------|------------------------------------------------------------------------|
| domain_id   | String  | 项目所属账号ID。                                                              |
| is_domain   | Boolean | false.                                                                 |
| parent_id   | String  | 如果查询自己创建的项目，则此处返回所属区域的项目ID。<br>如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。 |
| name        | String  | 项目名称。                                                                  |
| description | String  | 项目描述信息。                                                                |
| id          | String  | 项目ID。                                                                  |
| enabled     | Boolean | 项目是否可用。                                                                |
| status      | String  | 项目状态。                                                                  |

## 请求示例

查询项目详情与状态。

```
GET https://iam.myhuaweicloud.com/v3-ext/projects/{project_id}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "project": {
```



```

 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "aa2d97d7e62c4b7da3ffdfc11551...",
 "name": "ap-southeast-1_IAMProject",
 "description": "IAMDescription",
 "id": "07707ab14980265e2f5fc003a02...",
 "enabled": true,
 "status": "normal"
 }
}

```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.4.9 查询项目配额

### 功能介绍

该接口可以用于查询项目配额。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-QUOTA/projects/{project\_id}

表 5-187 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                              |
|------------|------|--------|-----------------------------------------------------------------|
| project_id | 是    | String | 待查询的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> |

## 请求参数

表 5-188 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                 |
|--------------|------|--------|------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的token。或IAM用户的token。（无需特殊权限，但token的scope需为URL中的project。） |

## 响应参数

表 5-189 响应 Body 参数

| 参数                     | 参数类型   | 描述      |
|------------------------|--------|---------|
| <a href="#">quotas</a> | object | 账号配额信息。 |

表 5-190 quotas

| 参数                        | 参数类型             | 描述   |
|---------------------------|------------------|------|
| <a href="#">resources</a> | Array of objects | 资源信息 |

表 5-191 resources

| 参数    | 参数类型    | 描述     |
|-------|---------|--------|
| max   | Integer | 配额最大值。 |
| min   | Integer | 配额最小值。 |
| quota | Integer | 当前配额。  |
| type  | String  | 配额类型。  |

| 参数   | 参数类型    | 描述      |
|------|---------|---------|
| used | Integer | 已使用的配额。 |

## 请求示例

查询项目配额。

GET https://iam.myhuaweicloud.com/v3.0/OS-QUOTA/projects/{project\_id}

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "quotas": {
 "resources": [
 {
 "max": 50,
 "min": 0,
 "quota": 10,
 "type": "project",
 "used": 4
 }
]
 }
}
```

### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.5 账号管理

### 5.5.1 查询 IAM 用户可以访问的账号详情

#### 功能介绍

该接口可以用于查询IAM用户可以访问的账号详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/auth/domains

#### 请求参数

表 5-192 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | IAM用户的token（无需特殊权限）。                    |

## 响应参数

表 5-193 响应 Body 参数

| 参数             | 参数类型             | 描述      |
|----------------|------------------|---------|
| <b>domains</b> | Array of objects | 账号信息列表。 |
| <b>links</b>   | Object           | 资源链接信息。 |

表 5-194 domains

| 参数           | 参数类型    | 描述                               |
|--------------|---------|----------------------------------|
| enabled      | Boolean | 是否启用账号，true为启用，false为停用，默认为true。 |
| id           | String  | 账号ID。                            |
| name         | String  | 账号名。                             |
| <b>links</b> | Object  | 账号的资源链接信息。                       |
| description  | String  | 账号的描述信息。                         |

表 5-195 domains.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-196 links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

查询IAM用户可以访问的账号详情。

```
GET https://iam.myhuaweicloud.com/v3/auth/domains
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "domains": [
 {
 "description": "",
 "enabled": true,
 "id": "d78cbac186b744899480f25bd022f468",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/domains/d78cbac186b744899480f25bd022f468"
 },
 "name": "IAMDomain"
 }
],
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/auth/domains"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 405 | 不允许的方法。 |
| 413 | 请求体过大。  |
| 500 | 内部服务错误。 |
| 503 | 服务不可用。  |

## 错误码

无

## 5.5.2 查询账号密码强度策略

### 功能介绍

该接口可以用于查询账号密码强度策略，查询结果包括密码强度策略的正则表达式及其描述。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/domains/{domain\_id}/config/security\_compliance

表 5-197 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                                                                                                          |
|-----------|------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> 。 |

## 请求参数

表 5-198 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | URL中domain_id所对应账号中IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-199 响应 Body 参数

| 参数                     | 参数类型   | 描述    |
|------------------------|--------|-------|
| <a href="#">config</a> | Object | 配置信息。 |

表 5-200 config

| 参数                                  | 参数类型   | 描述        |
|-------------------------------------|--------|-----------|
| <a href="#">security_compliance</a> | Object | 密码强度策略信息。 |

表 5-201 config.security\_compliance

| 参数                         | 参数类型   | 描述            |
|----------------------------|--------|---------------|
| password_regex             | String | 密码强度策略的正则表达式。 |
| password_regex_description | String | 密码强度策略的描述。    |

## 请求示例

查询账号密码强度策略。

```
GET https://iam.myhuaweicloud.com/v3/domains/{domain_id}/config/security_compliance
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "config": {
 "security_compliance": {
 "password_regex": "^(?![A-Z]*$)(?![a-z]*$)(?![\\d]*$)(?![\\W]*$)\\S{6,32}$",
 "password_regex_description": "The password must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters, and be a length between 6 and 32."
 }
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

### 5.5.3 按条件查询账号密码强度策略

#### 功能介绍

该接口可以用于按条件查询账号密码强度策略，查询结果包括密码强度策略的正则表达式及其描述。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。



## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/domains/{domain\_id}/config/security\_compliance/{option}

表 5-202 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                |
|-----------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                 |
| option    | 是    | String | 查询条件。该字段内容为：<br>password_regex或<br>password_regex_description。<br>password_regex：密码强度策略的正则表达式；password_regex_description：密码强度策略的描述。<br>取值范围： <ul style="list-style-type: none"> <li>password_regex</li> <li>password_regex_description</li> </ul> |

## 请求参数

表 5-203 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | URL中domain_id所对应账号中IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-204 响应 Body 参数

| 参数                     | 参数类型   | 描述    |
|------------------------|--------|-------|
| <a href="#">config</a> | Object | 配置信息。 |

表 5-205 config

| 参数                         | 参数类型   | 描述                                                |
|----------------------------|--------|---------------------------------------------------|
| password_regex             | String | 密码强度策略的正则表达式。(当option为password_regex时返回)          |
| password_regex_description | String | 密码强度策略的描述。(当option为password_regex_description时返回) |

## 请求示例

- 按照条件查询账号密码强度策略，option为password\_regex。  
GET https://iam.myhuaweicloud.com/v3/domains/{domain\_id}/config/security\_compliance/password\_regex
- 按照条件查询账号密码强度策略，option为password\_regex\_description。  
GET https://iam.myhuaweicloud.com/v3/domains/{domain\_id}/config/security\_compliance/password\_regex\_description

## 响应示例

状态码为 200 时:

请求成功。

示例1: option为password\_regex。

示例2: option为password\_regex\_description。

- 示例 1
 

```
{
 "config": {
 "password_regex": "^(?:[A-Z]*$)(?![a-z]*$)(?![\\d]*$)(?![\\W]*$)\\S{6,32}$"
```
- 示例 2
 

```
{
 "config": {
 "password_regex_description": "The password must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters, and be a length between 6 and 32."
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

| 返回值 | 描述      |
|-----|---------|
| 405 | 不允许的方法。 |
| 413 | 请求体过大。  |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.5.4 查询账号配额

### 功能介绍

该接口可以用于查询账号配额。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-QUOTA/domains/{domain\_id}

表 5-206 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                              |
|-----------|------|--------|-----------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> |

表 5-207 Query 参数

| 参数   | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type | 否    | String | <p>查询配额的类型，如果不填写此参数，则返回所有类型配额。取值范围如下：</p> <ul style="list-style-type: none"> <li>• user: IAM用户配额</li> <li>• group: 用户组配额</li> <li>• idp: 身份提供商配额</li> <li>• agency: 委托配额</li> <li>• policy: 自定义策略配额</li> <li>• assignment_group_mp: 一个用户组基于IAM项目可绑定的权限配额</li> <li>• assignment_agency_mp: 一个委托可绑定的权限配额</li> <li>• assignment_group_ep: 一个用户组基于企业项目可绑定的权限配额</li> <li>• assignment_user_ep: 一个用户基于企业项目可绑定的权限配额</li> <li>• mapping: 账号中所有身份提供商映射规则配额</li> </ul> |

## 请求参数

表 5-208 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                    |
|--------------|------|--------|-----------------------|
| X-Auth-Token | 是    | String | IAM用户的token。（无需特殊权限。） |

## 响应参数

状态码为 200 时:

表 5-209 响应 Body 参数

| 参数                     | 参数类型   | 描述      |
|------------------------|--------|---------|
| <a href="#">quotas</a> | Object | 账号配额信息。 |

表 5-210 quotas

| 参数               | 参数类型             | 描述    |
|------------------|------------------|-------|
| <b>resources</b> | Array of objects | 资源信息。 |

表 5-211 resources

| 参数    | 参数类型    | 描述                                                  |
|-------|---------|-----------------------------------------------------|
| max   | Integer | 配额最大值。                                              |
| min   | Integer | 配额最小值。                                              |
| quota | Integer | 当前配额。                                               |
| type  | String  | 配额类型。                                               |
| used  | Integer | 已使用的配额。<br>其中身份提供商映射规则mapping已使用数量为<br>用户自行设置，暂不返回。 |

## 请求示例

查询账号配额。

GET [https://iam.myhuaweicloud.com/v3.0/OS-QUOTA/domains/{domain\\_id}](https://iam.myhuaweicloud.com/v3.0/OS-QUOTA/domains/{domain_id})

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "quotas": {
 "resources": [
 {
 "max": 1000,
 "min": 50,
 "quota": 50,
 "type": "user",
 "used": 10
 },
 {
 "max": 300,
 "min": 10,
 "quota": 20,
 "type": "group",
 "used": 8
 },
 {
 "max": 20,
 "min": 10,
 "quota": 10,
 "type": "idp",
 "used": 9
 }
]
 }
}
```

```

 },
 {
 "max" : 300,
 "min" : 10,
 "quota" : 50,
 "type" : "agency",
 "used" : 12
 },
 {
 "max" : 300,
 "min" : 128,
 "quota" : 200,
 "type" : "policy",
 "used" : 8
 },
 {
 "max" : 500,
 "min" : 50,
 "quota" : 200,
 "type" : "assignment_group_mp",
 "used" : 8
 },
 {
 "max" : 500,
 "min" : 50,
 "quota" : 200,
 "type" : "assignment_agency_mp",
 "used" : 8
 },
 {
 "max" : 5000,
 "min" : 50,
 "quota" : 500,
 "type" : "assignment_group_ep",
 "used" : 8
 },
 {
 "max" : 5000,
 "min" : 50,
 "quota" : 500,
 "type" : "assignment_user_ep",
 "used" : 8
 },
 {
 "max" : 100,
 "min" : 10,
 "quota" : 10,
 "type" : "mapping",
 "used" : null
 }
]
}

```

#### 状态码为 400 时:

参数无效。

```

{
 "error_msg" : "Request parameter %(key)s is invalid.",
 "error_code" : "IAM.0007"
}

```

#### 状态码为 403 时:

没有操作权限。

- 示例 1

```

{
 "error_msg" : "You are not authorized to perform the requested action.",
}

```

```
"error_code" : "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
 "error_code" : "IAM.0003"
}
```

#### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg" : "Could not find %(target)s: %(target_id)s.",
 "error_code" : "IAM.0004"
}
```

#### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
 "error_code" : "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.6 IAM 用户管理

### 5.6.1 管理员查询 IAM 用户列表

#### 功能介绍

该接口可以用于[管理员](#)查询IAM用户列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/users

表 5-212 Query 参数

| 参数                  | 是否必选 | 参数类型    | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id           | 否    | String  | IAM用户所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                                                                        |
| enabled             | 否    | Boolean | 是否启用IAM用户，true为启用，false为停用，默认为true。                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| name                | 否    | String  | IAM用户名。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| password_expires_at | 否    | String  | <p>密码过期时间。该值为null表示未设置密码过期时间。</p> <p>格式为：<br/>password_expires_at={operator}:{timestamp}。</p> <p>timestamp格式为：YYYY-MM-DDTHH:mm:ssZ。示例：<br/>password_expires_at=lt:2016-12-08T22:02:00Z</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>operator取值范围：lt, lte, gt, gte, eq, neq。</li> <li>lt：过期时间小于timestamp。</li> <li>lte：过期时间小于等于timestamp。</li> <li>gt：过期时间大于timestamp。</li> <li>gte：过期时间大于等于timestamp。</li> <li>eq：过期时间等于timestamp。</li> <li>neq：过期时间不等于timestamp。</li> </ul> |

## 请求参数

表 5-213 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |



| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-214 响应 Body 参数

| 参数                    | 参数类型             | 描述         |
|-----------------------|------------------|------------|
| <a href="#">links</a> | Object           | 资源链接信息。    |
| <a href="#">users</a> | Array of objects | IAM用户信息列表。 |

表 5-215 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-216 users

| 参数                    | 参数类型    | 描述                                                                                                                   |
|-----------------------|---------|----------------------------------------------------------------------------------------------------------------------|
| name                  | String  | IAM用户名。                                                                                                              |
| <a href="#">links</a> | Object  | IAM用户的资源链接信息。                                                                                                        |
| domain_id             | String  | IAM用户所属账号ID。                                                                                                         |
| enabled               | Boolean | IAM用户是否启用。true表示启用，false表示停用，默认为true。                                                                                |
| id                    | String  | IAM用户ID。                                                                                                             |
| password_expires_at   | String  | IAM用户密码过期时间，“null”表示密码不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |
| description           | String  | IAM用户描述信息。                                                                                                           |

| 参数              | 参数类型    | 描述                                                                                                                                                          |
|-----------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access_mode     | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default: 默认访问模式，编程访问和管理控制台访问。</li> <li>• programmatic: 编程访问。</li> <li>• console: 管理控制台访问。</li> </ul> |
| pwd_status      | Boolean | IAM用户密码状态。true: 需要修改密码，false: 正常。如果密码未设置，此字段可能不返回。                                                                                                          |
| last_project_id | String  | IAM用户退出系统前，在控制台最后访问的项目ID，如果用户无访问记录，此字段可能不返回。                                                                                                                |
| pwd_strength    | String  | IAM用户的密码强度。high: 密码强度高；mid: 密码强度中等；low: 密码强度低。如果用户未设置密码，此字段可能不返回。                                                                                           |

表 5-217 users.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

管理员查询IAM用户列表。

GET <https://iam.myhuaweicloud.com/v3/users>

### 说明

如需缩小查询范围，可以增加路径参数，如：

GET [https://iam.myhuaweicloud.com/v3/users?domain\\_id=d78cbac186b744899480f25bd02...&enabled=true](https://iam.myhuaweicloud.com/v3/users?domain_id=d78cbac186b744899480f25bd02...&enabled=true)

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users"
 },
 "users": [
```

```
{
 "domain_id": "d78cbac186b744899480f25bd02...",
 "name": "IAMUserA",
 "description": "IAMDescriptionA",
 "password_expires_at": null,
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/07667db96a00265f1fc0c003a3..."
 },
 "id": "07667db96a00265f1fc0c003a...",
 "enabled": true
},
{
 "pwd_status": true,
 "domain_id": "d78cbac186b744899480f25bd02...",
 "last_project_id": "065a7c66da0010992ff7c0031e5a...",

 "name": "IAMUserB",
 "description": "IAMDescriptionB",
 "password_expires_at": null,
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/07609fb9358010e21f7bc003751c7..."
 },
 "id": "07609fb9358010e21f7bc003751c7...",
 "enabled": true
}
]
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 资源冲突。     |
| 500 | 请求体过大。    |
| 503 | 服务不可用。    |

## 错误码

无

## 5.6.2 查询 IAM 用户详情（推荐）

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户详情，或IAM用户查询自己的详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-USER/users/{user\_id}

表 5-218 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-219 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                         |
|--------------|------|--------|------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户详情：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己的详情：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

### 响应参数

表 5-220 响应 Body 参数

| 参数                   | 参数类型   | 描述       |
|----------------------|--------|----------|
| <a href="#">user</a> | Object | IAM用户信息。 |

表 5-221 user

| 参数              | 参数类型    | 描述                                                                |
|-----------------|---------|-------------------------------------------------------------------|
| enabled         | Boolean | IAM用户是否启用。true表示启用，false表示停用，默认为true。                             |
| id              | String  | IAM用户ID。                                                          |
| domain_id       | String  | IAM用户所属账号ID。                                                      |
| name            | String  | IAM用户名。                                                           |
| links           | Object  | IAM用户的资源链接信息。                                                     |
| xuser_id        | String  | IAM用户在外部系统中的ID。                                                   |
| xuser_type      | String  | IAM用户在外部系统中的类型。                                                   |
| areacode        | String  | IAM用户手机号的国家码。                                                     |
| email           | String  | IAM用户邮箱。                                                          |
| phone           | String  | IAM用户手机号。                                                         |
| pwd_status      | Boolean | IAM用户密码状态。true：需要修改密码，false：正常。如果密码未设置，此字段可能不返回。                  |
| pwd_create_time | String  | IAM用户密码创建更新时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DD HH:mm:ss。      |
| modify_pwd_time | String  | IAM用户更新时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DD HH:mm:ss。          |
| update_time     | String  | IAM用户更新时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DD HH:mm:ss。          |
| create_time     | String  | IAM用户创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DD HH:mm:ss。          |
| last_login_time | String  | IAM用户最后登录时间或认证访问时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DD HH:mm:ss。 |
| pwd_strength    | String  | IAM用户密码强度。结果为Low/Medium/Strong/None，分别表示密码强度低/中/高/无。              |
| is_domain_owner | Boolean | IAM用户是否为账号。                                                       |

| 参数          | 参数类型   | 描述                                                                                                                                                           |
|-------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access_mode | String | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default: 默认访问模式, 编程访问和管理控制台访问。</li> <li>• programmatic: 编程访问。</li> <li>• console: 管理控制台访问。</li> </ul> |
| description | String | IAM用户描述信息。                                                                                                                                                   |

表 5-222 user.links

| 参数       | 参数类型   | 描述                     |
|----------|--------|------------------------|
| self     | String | 资源链接地址。                |
| previous | String | 前一邻接资源链接地址, 不存在时为null。 |
| next     | String | 后一邻接资源链接地址, 不存在时为null。 |

## 请求示例

查询IAM用户详情, 包括查询IAM用户的手机号、邮箱等信息。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user_id}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "user": {
 "pwd_strength": "Strong",
 "create_time": "2020-07-08 02:19:03.0",
 "pwd_create_time": "2022-10-13 07:35:12.0",
 "modify_pwd_time": "2022-10-13 07:35:12.0",
 "last_login_time": null,
 "areacode": "",
 "enabled": true,
 "domain_id": "086ba757f90089cf0fe5c000dbe7f...",
 "xuser_id": "",
 "pwd_status": false,
 "update_time": null,
 "phone": "-",
 "is_domain_owner": false,
 "access_mode": "default",
 "name": "autotest1",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3.0/OS-USER/users/093f75808b8089ba1f6dc000c7cac..."
 },
 },
 "id": "093f75808b8089ba1f6dc000c7cac...",
 "xuser_type": "",
 "email": ""
}
```

```
"description" : "aaa"
}
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 500 | 内部服务错误。   |

## 错误码

请参考[错误码](#)。

## 5.6.3 查询 IAM 用户详情

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户详情，或IAM用户查询自己的用户详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

该接口无法查询IAM用户的手机号、邮箱等信息。如需查询上述信息，请参见：[查询IAM用户详情（推荐）](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/users/{user\_id}

表 5-223 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-224 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                         |
|--------------|------|--------|------------------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                                                                    |
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户详情：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己的详情：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-225 响应 Body 参数

| 参数                   | 参数类型   | 描述       |
|----------------------|--------|----------|
| <a href="#">user</a> | Object | IAM用户信息。 |

表 5-226 user

| 参数                    | 参数类型    | 描述                                                                                                                   |
|-----------------------|---------|----------------------------------------------------------------------------------------------------------------------|
| name                  | String  | IAM用户名。                                                                                                              |
| <a href="#">links</a> | Object  | IAM用户的资源链接信息。                                                                                                        |
| domain_id             | String  | IAM用户所属账号ID。                                                                                                         |
| enabled               | Boolean | IAM用户是否启用。true表示启用，false表示停用，默认为true。                                                                                |
| id                    | String  | IAM用户ID。                                                                                                             |
| password_expires_at   | String  | IAM用户密码过期时间，“null”表示密码不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |
| description           | String  | IAM用户描述信息。                                                                                                           |



| 参数              | 参数类型    | 描述                                                                                                                                                           |
|-----------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access_mode     | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default: 默认访问模式, 编程访问和管理控制台访问。</li> <li>• programmatic: 编程访问。</li> <li>• console: 管理控制台访问。</li> </ul> |
| pwd_status      | Boolean | IAM用户密码状态。true: 需要修改密码, false: 正常。如果密码未设置, 此字段可能不返回。                                                                                                         |
| last_project_id | String  | IAM用户退出系统前, 在控制台最后访问的项目ID, 如果用户无访问记录, 此字段可能不返回。                                                                                                              |

表 5-227 user.links

| 参数       | 参数类型   | 描述                     |
|----------|--------|------------------------|
| self     | String | 资源链接地址。                |
| previous | String | 前一邻接资源链接地址, 不存在时为null。 |
| next     | String | 后一邻接资源链接地址, 不存在时为null。 |

## 请求示例

查询IAM用户详情, 无法查询IAM用户的手机号、邮箱等信息。

```
GET https://iam.myhuaweicloud.com/v3/users/{user_id}
```

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "user": {
 "pwd_status": true,
 "domain_id": "d78cbac186b744899480f25bd02...",
 "last_project_id": "065a7c66da0010992ff7c0031e5a5...",
 "name": "IAMUser",
 "description": "--",
 "password_expires_at": null,
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/07609fb9358010e21f7bc003751..."
 },
 "id": "7116d09f88fa41908676fdd4b039...",
 "access_mode": "console",
 "enabled": true
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 资源冲突。     |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.6.4 查询 IAM 用户所属用户组

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户所属用户组，或IAM用户查询自己所属用户组。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/users/{user\_id}/groups

表 5-228 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-229 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                              |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                                                                         |
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户所属用户组：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己所属用户组：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-230 响应 Body 参数

| 参数                     | 参数类型             | 描述       |
|------------------------|------------------|----------|
| <a href="#">groups</a> | Array of objects | 用户组信息列表。 |
| <a href="#">links</a>  | Object           | 资源链接信息。  |

表 5-231 groups

| 参数                    | 参数类型   | 描述          |
|-----------------------|--------|-------------|
| description           | String | 用户组描述信息。    |
| id                    | String | 用户组ID。      |
| domain_id             | String | 用户组所属账号ID。  |
| name                  | String | 用户组名称。      |
| <a href="#">links</a> | Object | 用户组的资源链接信息。 |
| create_time           | Long   | 用户组创建时间。    |

表 5-232 groups.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-233 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询IAM用户所属用户组。

GET [https://iam.myhuaweicloud.com/v3/users/{user\\_id}/groups](https://iam.myhuaweicloud.com/v3/users/{user_id}/groups)

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "groups": [
 {
 "domain_id": "d78cbac186b744899480f25bd0...",
 "create_time": 1578107542861,
 "name": "IAMGroup",
 "description": "",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb..."
 },
 "id": "07609e7eb200250a3f7dc003cb7..."
 }
],
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/076837351e80251c1f0fc003afe43.../groups"
 }
}
```

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 200 | 请求成功。 |

| 返回值 | 描述        |
|-----|-----------|
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 资源冲突。     |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.6.5 管理员查询用户组所包含的 IAM 用户

### 功能介绍

该接口可以用于[管理员](#)查询用户组中所包含的IAM用户。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/groups/{group\_id}/users

表 5-234 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                 |
|----------|------|--------|--------------------------------------------------------------------|
| group_id | 是    | String | 待查询的用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-235 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-236 响应 Body 参数

| 参数                    | 参数类型             | 描述         |
|-----------------------|------------------|------------|
| <a href="#">links</a> | Object           | 用户组资源的链接。  |
| <a href="#">users</a> | Array of objects | IAM用户信息列表。 |

表 5-237 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-238 users

| 参数                    | 参数类型    | 描述                                 |
|-----------------------|---------|------------------------------------|
| name                  | String  | IAM用户名。                            |
| <a href="#">links</a> | Object  | IAM用户的资源链接信息。                      |
| domain_id             | String  | IAM用户所属账号ID。                       |
| enabled               | Boolean | 用户是否启用。true表示启用，false表示停用，默认为true。 |
| id                    | String  | IAM用户ID。                           |

| 参数                  | 参数类型    | 描述                                                                                                                                                       |
|---------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| password_expires_at | String  | 密码过期时间，“null”表示密码不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                          |
| description         | String  | IAM用户描述信息。                                                                                                                                               |
| access_mode         | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default：默认访问模式，编程访问和管理控制台访问。</li> <li>• programmatic：编程访问。</li> <li>• console：管理控制台访问。</li> </ul> |
| pwd_status          | Boolean | IAM用户密码状态。true：需要修改密码，false：正常。如果密码未设置，此字段可能不返回。                                                                                                         |
| last_project_id     | String  | IAM用户退出华为云前，在控制台最后访问的项目ID，如果用户无访问记录，此字段可能不返回。                                                                                                            |
| pwd_strength        | String  | IAM用户的密码强度。high：密码强度高；mid：密码强度中等；low：密码强度低。如果用户未设置密码，此字段可能不返回。                                                                                           |

表 5-239 users.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

管理员查询用户组所包含的IAM用户。

GET https://iam.myhuaweicloud.com/v3/groups/{group\_id}/users

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "links": {
 "next": null,
 "previous": null,

```

```
 "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb7a4e2d/users"
 },
 "users": [
 {
 "pwd_status": true,
 "domain_id": "d78cbac186b744899480f25bd...",
 "last_project_id": "065a7c66da0010992ff7c0031e...",
 "name": "IAMUserA",
 "description": "--",
 "password_expires_at": null,
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/07609fb9358010e21f7bc00375..."
 },
 "id": "07609fb9358010e21f7bc003751c7...",
 "enabled": true
 },
 {
 "pwd_status": true,
 "domain_id": "d78cbac186b744899480f25bd022...",
 "last_project_id": "065a7c66da0010992ff7c0031e5a...",
 "name": "IAMUserB",
 "description": "",
 "password_expires_at": null,
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/users/076837351e80251c1f0fc003af..."
 },
 "id": "076837351e80251c1f0fc003afe43...",
 "enabled": true
 }
]
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.6.6 管理员创建 IAM 用户（推荐）

### 功能介绍

该接口可以用于[管理员](#)创建IAM用户。



该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

POST /v3.0/OS-USER/users

## 请求参数

表 5-240 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-241 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">user</a> | 是    | Object | IAM用户信息。 |

表 5-242 user

| 参数        | 是否必选 | 参数类型   | 描述                                                                    |
|-----------|------|--------|-----------------------------------------------------------------------|
| name      | 是    | String | IAM用户名，长度1~64之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且不能以数字或空格开头。            |
| domain_id | 是    | String | IAM用户所属的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| password  | 否    | String | IAM用户密码。                                                              |
| email     | 否    | String | IAM用户邮箱，需符合邮箱格式，长度小于等于255位。                                           |

| 参数          | 是否必选 | 参数类型    | 描述                                                                                                                                                                                                                                                          |
|-------------|------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| areacode    | 否    | String  | 国家码。必须与手机号同时存在。                                                                                                                                                                                                                                             |
| phone       | 否    | String  | IAM用户手机号，纯数字，长度小于等于32位。必须与国家码同时存在。                                                                                                                                                                                                                          |
| enabled     | 否    | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                                                                                                                         |
| pwd_status  | 否    | Boolean | IAM用户首次登录是否重置密码，默认需要重置。                                                                                                                                                                                                                                     |
| xuser_type  | 否    | String  | IAM用户在外部系统中的类型。长度小于等于64位。xuser_type如果存在，则需要与同一租户中的xaccount_type、xdomain_type校验，须与xuser_id同时存在。xuser_type取值当前仅支持TenantIdp。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。 |
| xuser_id    | 否    | String  | IAM用户在外部系统中的ID。长度小于等于128位，须与xuser_type同时存在。使用API设置外部身份ID后，由于时延IAM控制台暂无法实时显示，请稍后刷新查看。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。                                      |
| access_mode | 否    | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>default：默认访问模式，编程访问和管理控制台访问。</li> <li>programmatic：编程访问。</li> <li>console：管理控制台访问。</li> </ul>                                                                                                          |
| description | 否    | String  | IAM用户描述信息。                                                                                                                                                                                                                                                  |

## 响应参数

表 5-243 响应 Body 参数

| 参数                   | 参数类型   | 描述       |
|----------------------|--------|----------|
| <a href="#">user</a> | Object | IAM用户信息。 |

表 5-244 user

| 参数              | 参数类型    | 描述                                                                                                                                                       |
|-----------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| status          | Integer | IAM用户状态信息。                                                                                                                                               |
| pwd_status      | Boolean | IAM用户首次登录是否重置密码。                                                                                                                                         |
| xuser_id        | String  | IAM用户在外部系统中的ID。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。        |
| xuser_type      | String  | 用户在外部系统中的类型。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。           |
| access_mode     | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default：默认访问模式，编程访问和管理控制台访问。</li> <li>• programmatic：编程访问。</li> <li>• console：管理控制台访问。</li> </ul> |
| description     | String  | IAM用户描述信息。                                                                                                                                               |
| name            | String  | IAM用户名，长度1~32之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且不能以数字或空格开头。                                                                                               |
| phone           | String  | IAM用户手机号，纯数字，长度小于等于32位。必须与国家码同时存在。                                                                                                                       |
| is_domain_owner | Boolean | IAM用户是否为账号 <a href="#">管理员</a> 。                                                                                                                         |
| domain_id       | String  | IAM用户所属账号ID。                                                                                                                                             |
| enabled         | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                      |
| areacode        | String  | 国家码。                                                                                                                                                     |

| 参数                  | 参数类型   | 描述                                                                                                              |
|---------------------|--------|-----------------------------------------------------------------------------------------------------------------|
| email               | String | IAM用户邮箱。                                                                                                        |
| create_time         | String | IAM用户创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。            |
| xdomain_id          | String | 运营主体的客户编码。                                                                                                      |
| xdomain_type        | String | 运营主体。                                                                                                           |
| default_project_id  | String | 用户默认的项目ID。                                                                                                      |
| id                  | String | IAM用户ID。长度为32字符。                                                                                                |
| password_expires_at | String | 密码过期时间，“null”表示密码不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |

## 请求示例

管理员创建一个名为“IAMUser”的IAM用户，用户的邮箱地址是IAMEmail@huawei.com，手机号码是0012312345678910，使用默认访问模式，可以编程访问和管理控制台访问。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-USER/users
{
 "user": {
 "domain_id": "d78cbac186b744899480f25...",
 "name": "IAMUser",
 "password": "IAMPassword@",
 "email": "IAMEmail@huawei.com",
 "areacode": "00123",
 "phone": "12345678910",
 "enabled": true,
 "pwd_status": false,
 "xuser_type": "",
 "xuser_id": "",
 "access_mode": "default",
 "description": "IAMDescription"
 }
}
```

## 响应示例

**状态码为 201 时:**

创建成功。

```
{
 "user": {
 "pwd_status": false,
 "xuser_id": "",
 "xuser_type": "",
 "access_mode": "default",
 "description": "IAMDescription",
```

```

"name": "IAMUser",
"phone": "12345678910",
"is_domain_owner": false,
"enabled": true,
"domain_id": "d78cbac186b744899480f25bd...",
"areacode": "00123",
"email": "IAMEmail@huaweixample.com",
"create_time": "2020-01-06T08:05:16.000000",
"xdomain_id": "",
"xdomain_type": "",
"id": "07664aec578026691f00c003a...",
"status": null,
"password_expires_at": null,
"default_project_id": null
}

```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 201 | 创建成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 409 | 资源冲突。     |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

## 5.6.7 管理员创建 IAM 用户

### 功能介绍

该接口可以用于[管理员](#)创建IAM用户。IAM用户首次登录时需要修改密码。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

使用该接口创建IAM用户时，不能预置IAM用户的手机号码和邮箱，如需预置上述信息，请参见：[管理员创建IAM用户（推荐）](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

POST /v3/users

## 请求参数

表 5-245 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-246 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述    |
|----------------------|------|--------|-------|
| <a href="#">user</a> | 是    | Object | 用户信息。 |

表 5-247 user

| 参数        | 是否必选 | 参数类型   | 描述                                                         |
|-----------|------|--------|------------------------------------------------------------|
| name      | 是    | String | IAM用户名，长度1~64之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且不能以数字或空格开头。 |
| domain_id | 否    | String | IAM用户所属账号ID。                                               |

| 参数          | 是否必选 | 参数类型    | 描述                                                                                                                                                                              |
|-------------|------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| password    | 否    | String  | IAM用户密码。<br><ul style="list-style-type: none"> <li>系统默认密码最小长度为8位字符，在8-32位之间支持用户自定义密码长度。</li> <li>至少包含以下四种字符中的两种：大写字母、小写字母、数字和特殊字符。</li> <li>必须满足账户设置中<b>密码策略</b>的要求。</li> </ul> |
| enabled     | 否    | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                                             |
| description | 否    | String  | IAM用户描述信息。                                                                                                                                                                      |

## 响应参数

表 5-248 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>user</b> | Object | IAM用户信息。 |

表 5-249 user

| 参数                  | 参数类型    | 描述                                                                                                              |
|---------------------|---------|-----------------------------------------------------------------------------------------------------------------|
| enabled             | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                             |
| id                  | String  | IAM用户ID。                                                                                                        |
| domain_id           | String  | IAM用户所属账号ID。                                                                                                    |
| name                | String  | IAM用户名。                                                                                                         |
| <b>links</b>        | Object  | IAM用户的资源链接信息。                                                                                                   |
| pwd_status          | Boolean | IAM用户密码状态。true：需要修改密码，false：正常；如果密码未设置，此字段可能不返回。                                                                |
| password_expires_at | String  | 密码过期时间，“null”表示密码不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |

| 参数          | 参数类型   | 描述         |
|-------------|--------|------------|
| description | String | IAM用户描述信息。 |

表 5-250 user.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

管理员创建一个名为“IAMUser”的用户。

```
POST https://iam.myhuaweicloud.com/v3/users
{
 "user": {
 "name": "IAMUser",
 "domain_id": "d78cbac186b744899480f25bd02...",
 "enabled": true,
 "password": "IAMPassword@",
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "user": {
 "description": "IAMDescription",
 "name": "IAMUser",
 "enabled": true,
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/users/076598a17b0010e21fdec003f3a2aa45"
 },
 "domain_id": "d78cbac186b744899480f25b...",
 "id": "076598a17b0010e21fdec003f3a2a...",
 "password_expires_at": null,
 "domain_id": "54a636f5a39c4e13809489dbcaa8e6b0",
 "pwd_status": false
 }
}
```

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 201 | 创建成功。 |
| 400 | 参数无效。 |
| 401 | 认证失败。 |



| 返回值 | 描述        |
|-----|-----------|
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 409 | 资源冲突。     |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

## 5.6.8 修改 IAM 用户密码

### 功能介绍

该接口可以用于IAM用户修改自己的密码。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3/users/{user\_id}/password

表 5-251 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                     |
|---------|------|--------|------------------------------------------------------------------------|
| user_id | 是    | String | 待修改密码的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-252 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | URL中user_id所对应IAM用户的token（无需特殊权限）。      |

表 5-253 请求 Body 参数

| 参数          | 是否必选 | 参数类型   | 描述       |
|-------------|------|--------|----------|
| <b>user</b> | 是    | Object | IAM用户信息。 |

表 5-254 user

| 参数                | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                          |
|-------------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| password          | 是    | String | IAM用户的新密码。 <ul style="list-style-type: none"> <li>系统默认密码最小长度为8位字符，在8-32位之间支持用户自定义密码长度。</li> <li>至少包含以下四种字符中的两种：大写字母、小写字母、数字和特殊字符。</li> <li>不能包含手机号和邮箱。</li> <li>必须满足用户所属账号的<b>密码策略</b>要求。</li> <li>新密码不能与当前密码相同。</li> </ul> |
| original_password | 是    | String | IAM用户的原密码。                                                                                                                                                                                                                  |

## 响应参数

无

## 请求示例

IAM用户将自己的原始密码 “IAMOriginalPassword@” 修改为 “IAMNewPassword@”。

```
POST https://iam.myhuaweicloud.com/v3/users/{user_id}/password
{
 "user": {
 "password": "IAMNewPassword@",
 "original_password": "IAMOriginalPassword@"
 }
}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 修改成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

无

## 5.6.9 修改 IAM 用户信息（推荐）

### 功能介绍

该接口可以用于IAM用户修改自己的用户信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PUT /v3.0/OS-USER/users/{user\_id}/info

表 5-255 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                     |
|---------|------|--------|------------------------------------------------------------------------|
| user_id | 是    | String | 待修改信息的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-256 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | URL中user_id所对应IAM用户的token（无需特殊权限）。      |

表 5-257 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">user</a> | 是    | Object | IAM用户信息。 |

表 5-258 user

| 参数     | 是否必选 | 参数类型   | 描述                                |
|--------|------|--------|-----------------------------------|
| email  | 否    | String | IAM用户的新邮箱，符合邮箱格式，长度小于等于255位。      |
| mobile | 否    | String | IAM用户的国家码+新手机号，手机号为纯数字，长度小于等于32位。 |

## 响应参数

无

## 请求示例

IAM用户修改自己的邮箱地址为“IAMEmail@huawei.com”，手机号码为“0852-123456789”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user_id}/info
{
 "user": {
 "email": "IAMEmail@huawei.com",
 "mobile": "0852-123456789"
 }
}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 修改成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 409 | 资源冲突。     |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

## 5.6.10 管理员修改 IAM 用户信息（推荐）

### 功能介绍

该接口可以用于[管理员](#)修改IAM用户信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PUT /v3.0/OS-USER/users/{user\_id}

表 5-259 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                     |
|---------|------|--------|------------------------------------------------------------------------|
| user_id | 是    | String | 待修改信息的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-260 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的token。       |

表 5-261 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">user</a> | 是    | Object | IAM用户信息。 |

表 5-262 user

| 参数   | 是否必选 | 参数类型   | 描述                                                          |
|------|------|--------|-------------------------------------------------------------|
| name | 否    | String | 新IAM用户名，长度1~32之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且不能以数字或空格开头。 |

| 参数         | 是否必选 | 参数类型    | 描述                                                                                                                                                                                                                                           |
|------------|------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| password   | 否    | String  | <p>IAM用户新密码。</p> <ul style="list-style-type: none"> <li>系统默认密码最小长度为8位字符，在8-32位之间支持用户自定义密码长度。</li> <li>至少包含以下四种字符中的两种：大写字母、小写字母、数字和特殊字符。</li> <li>必须满足账户设置中<b>密码策略</b>的要求。</li> <li>新密码不能与当前密码相同。</li> </ul>                                  |
| email      | 否    | String  | IAM用户新邮箱，需符合邮箱格式，长度小于等于255字符。                                                                                                                                                                                                                |
| areacode   | 否    | String  | 国家码。必须与手机号同时存在。                                                                                                                                                                                                                              |
| phone      | 否    | String  | IAM用户新手机号，纯数字，长度小于等于32位。必须与国家码同时存在。                                                                                                                                                                                                          |
| enabled    | 否    | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                                                                                                          |
| pwd_status | 否    | Boolean | IAM用户密码状态。true：需要修改密码，false：正常。如果密码未设置，此字段可能不返回。                                                                                                                                                                                             |
| xuser_type | 否    | String  | <p>IAM用户在外部系统中的类型。长度小于等于64位。xuser_type如果存在，则需要与同一租户中的xaccount_type、xdomain_type校验，须与xuser_id同时存在。</p> <p><b>说明</b><br/>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。</p> |
| xuser_id   | 否    | String  | <p>IAM用户在外部系统中的ID。长度小于等于128位，必须与xuser_type同时存在。使用API设置外部身份ID后，由于时延IAM控制台暂无法实时显示，请稍后刷新查看。</p> <p><b>说明</b><br/>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。</p>          |

| 参数          | 是否必选 | 参数类型   | 描述                                                                                                                                                     |
|-------------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| access_mode | 否    | String | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>default: 默认访问模式, 编程访问和管理控制台访问。</li> <li>programmatic: 编程访问。</li> <li>console: 管理控制台访问。</li> </ul> |
| description | 否    | String | IAM用户新描述信息。                                                                                                                                            |

## 响应参数

表 5-263 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>user</b> | Object | IAM用户信息。 |

表 5-264 user

| 参数              | 参数类型    | 描述                                                                                                                                                   |
|-----------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| pwd_status      | Boolean | IAM用户密码状态。true: 需要修改密码, false: 正常。如果密码未设置, 此字段可能不返回。                                                                                                 |
| create_time     | String  | IAM用户的创建时间<br><b>说明</b><br>UTC时间, 格式为YYYY-MM-DDTHH:mm:ss.ssssss, 日期和时间戳格式如: 2023-06-28T08:56:33.710000。                                              |
| xdomain_id      | String  | IAM用户在外部系统中的ID。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统, xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值, 无法在华为云获取, 请咨询企业管理员。 |
| xdomain_type    | String  | IAM用户在外部系统中的类型。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统, xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值, 无法在华为云获取, 请咨询企业管理员。 |
| is_domain_owner | Boolean | IAM用户是否为账号 <b>管理员</b> 。                                                                                                                              |



| 参数                 | 参数类型    | 描述                                                                                                                                                          |
|--------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| xuser_id           | String  | IAM用户在外部系统中的ID。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。           |
| xuser_type         | String  | IAM用户在外部系统中的类型。<br><b>说明</b><br>外部系统指与华为云对接的外部企业管理系统，xaccount_type、xaccount_id、xdomain_type、xdomain_id、xuser_type、xuser_id等参数值，无法在华为云获取，请咨询企业管理员。           |
| access_mode        | String  | IAM用户访问方式。<br><ul style="list-style-type: none"> <li>• default: 默认访问模式，编程访问和管理控制台访问。</li> <li>• programmatic: 编程访问。</li> <li>• console: 管理控制台访问。</li> </ul> |
| description        | String  | IAM用户的新描述信息。                                                                                                                                                |
| name               | String  | IAM用户新用户名，长度1~32之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-、_）且不能以数字或空格开头。                                                                                               |
| phone              | String  | IAM用户新手机号，纯数字，长度小于等于32位。必须与国家码同时存在。                                                                                                                         |
| domain_id          | String  | IAM用户所属账号ID。                                                                                                                                                |
| enabled            | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                         |
| areacode           | String  | 国家码。                                                                                                                                                        |
| email              | String  | IAM用户新邮箱。                                                                                                                                                   |
| id                 | String  | IAM用户ID。                                                                                                                                                    |
| <b>links</b>       | Object  | IAM用户的资源链接信息。                                                                                                                                               |
| password_expire_at | String  | 密码过期时间。当值为“null”时，不返回。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                            |

表 5-265 user.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

管理员修改名为“IAMUser”的邮箱地址为“IAMEmail@huawei.com”，手机号码为“085212345678910”，密码为IAMPassword@。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user_id}
{
 "user": {
 "email": "IAMEmail@huawei.com",
 "areacode": "0852",
 "phone": "12345678910",
 "enabled": true,
 "name": "IAMUser",
 "password": "IAMPassword@",
 "pwd_status": false,
 "xuser_type": "",
 "xuser_id": "",
 "access_mode": "default",
 "description": "IAMDescription"
 }
}
```

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "user": {
 "description": "IAMDescription",
 "areacode": "0852",
 "enabled": true,
 "pwd_status": false,
 "xuser_id": "",
 "access_mode": "default",
 "domain_id": "d78cbac186b744899480f25bd0...",
 "phone": "12345678910",
 "name": "IAMUser",
 "links": {
 "self": "https://iam.myhuaweicloud.com/3.0/OS-USER/users/076934ff9f0010cd1f0bc003..."
 },
 "id": "076934ff9f0010cd1f0bc0031019...",
 "xuser_type": "",
 "email": "IAMEmail@huawei.com",
 "create_time": "2024-03-28T03:42:08.000000",
 "is_domain_owner": false,
 "xdomain_id": "30086000630940966",
 "xdomain_type": ""
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |

| 返回值 | 描述        |
|-----|-----------|
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 409 | 资源冲突。     |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

## 5.6.11 管理员修改 IAM 用户信息

### 功能介绍

该接口可以用于[管理员](#)修改IAM用户信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

该接口无法修改手机号、邮箱等信息。如需修改手机号、邮箱等信息，请使用接口：[管理员修改IAM用户信息（推荐）](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PATCH /v3/users/{user\_id}

表 5-266 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                     |
|---------|------|--------|------------------------------------------------------------------------|
| user_id | 是    | String | 待修改信息的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-267 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-268 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">user</a> | 是    | Object | IAM用户信息。 |

表 5-269 user

| 参数          | 是否必选 | 参数类型    | 描述                                                                                                                                                                                                                                |
|-------------|------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id   | 否    | String  | IAM用户所属账号ID。                                                                                                                                                                                                                      |
| name        | 否    | String  | IAM用户新用户名，长度1~32之间，只能包含如下字符：大小写字母、空格、数字或特殊字符（-_.）且不能以数字或空格开头。                                                                                                                                                                     |
| password    | 否    | String  | IAM用户密码。 <ul style="list-style-type: none"> <li>系统默认密码最小长度为8位字符，在8-32位之间支持用户自定义密码长度。</li> <li>至少包含以下四种字符中的两种：大写字母、小写字母、数字和特殊字符。</li> <li>不能包含手机号和邮箱。</li> <li>必须满足账户设置中<a href="#">密码策略</a>的要求。</li> <li>新密码不能与当前密码相同。</li> </ul> |
| enabled     | 否    | Boolean | 是否启用IAM用户。true为启用，false为停用，默认为true。                                                                                                                                                                                               |
| description | 否    | String  | IAM用户新描述信息。                                                                                                                                                                                                                       |

| 参数         | 是否必选 | 参数类型    | 描述                               |
|------------|------|---------|----------------------------------|
| pwd_status | 否    | Boolean | IAM用户密码状态。true:需要修改密码, false:正常。 |

## 响应参数

表 5-270 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>user</b> | Object | IAM用户信息。 |

表 5-271 user

| 参数                  | 参数类型    | 描述                                                                                                                  |
|---------------------|---------|---------------------------------------------------------------------------------------------------------------------|
| name                | String  | IAM用户名。                                                                                                             |
| domain_id           | String  | IAM用户所属账号ID。                                                                                                        |
| enabled             | Boolean | IAM用户是否启用。true表示启用, false表示停用, 默认为true。                                                                             |
| id                  | String  | IAM用户ID。                                                                                                            |
| password_expires_at | String  | 密码过期时间, “null”表示密码不过期。<br><b>说明</b><br>UTC时间, 格式为YYYY-MM-DDTHH:mm:ss.ssssss, 日期和时间戳格式如: 2023-06-28T08:56:33.710000。 |
| description         | String  | IAM用户描述信息, 若无描述信息, 此字段可能不返回。                                                                                        |
| pwd_status          | Boolean | IAM用户密码状态。true: 需要修改密码, false: 正常。如果密码未设置, 此字段可能不返回。                                                                |
| last_project_id     | String  | IAM用户退出华为云前, 在控制台最后访问的项目ID, 如果用户无访问记录, 此字段可能不返回。                                                                    |
| <b>links</b>        | Object  | IAM用户的资源链接信息。                                                                                                       |

表 5-272 user.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

管理员修改名为“IAMUser”的IAM用户的密码为“IAMPassword@”。

```
PATCH https://iam.myhuaweicloud.com/v3/users/{user_id}
{
 "user": {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "name": "IAMUser",
 "password": "IAMPassword@",
 "enabled": true,
 "pwd_status": false,
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "user": {
 "pwd_status": false,
 "description": "IAMDescription",
 "name": "IAMUser",
 "enabled": true,
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/users/07609fb9358010e21f7bc003751c7..."
 },
 "id": "07609fb9358010e21f7bc003751c7...",
 "domain_id": "d78cbac186b744899480f25bd02..."
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 409 | 资源冲突。     |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

## 5.6.12 管理员删除 IAM 用户

### 功能介绍

该接口可以用于[管理员](#)删除指定IAM用户。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3/users/{user\_id}

表 5-273 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待删除的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-274 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

### 响应参数

无

## 请求示例

管理员删除IAM用户。

```
DELETE https://iam.myhuaweicloud.com/v3/users/{user_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 405 | 不允许的方法。   |
| 413 | 请求体过大。    |
| 500 | 内部服务错误。   |
| 503 | 服务不可用。    |

## 错误码

请参考[错误码](#)。

# 5.7 用户组管理

## 5.7.1 查询用户组列表

### 功能介绍

该接口可以用于[管理员](#)查询用户组列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。



## URI

GET /v3/groups

表 5-275 Query 参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                        |
|-----------|------|--------|---------------------------------------------------------------------------|
| domain_id | 否    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。        |
| name      | 否    | String | 用户组名，长度1~128字符之间，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-276 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-277 响应 Body 参数

| 参数                     | 参数类型             | 描述       |
|------------------------|------------------|----------|
| <a href="#">groups</a> | Array of objects | 用户组信息列表。 |
| <a href="#">links</a>  | Object           | 资源链接信息。  |

表 5-278 groups

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| description | String | 用户组描述信息。 |

| 参数           | 参数类型   | 描述          |
|--------------|--------|-------------|
| id           | String | 用户组ID。      |
| domain_id    | String | 用户组所属账号ID。  |
| name         | String | 用户组名。       |
| <b>links</b> | Object | 用户组的资源链接信息。 |
| create_time  | Long   | 用户组创建时间。    |

表 5-279 groups.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-280 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询用户组列表。

GET <https://iam.myhuaweicloud.com/v3/groups>

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "groups": [
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "create_time": 1536293929624,
 "name": "IAMGroupA",
 "description": "IAMDescription",
 "links": {
 "next": null,
 "previous": null,

```

```

 "self": "https://iam.myhuaweicloud.com/v3/groups/5b050baea9db472c88cbae67..."
 },
 "id": "5b050baea9db472c88cbae6..."
},
{
 "domain_id": "d78cbac186b744899480f25...",
 "create_time": 1578107542861,
 "name": "IAMGroupB",
 "description": "IAMDescription",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb7a4e2d"
 },
 "id": "07609e7eb200250a3f7dc003cb..."
}
],
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/groups"
}
}

```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |

## 错误码

无

## 5.7.2 查询用户组详情

### 功能介绍

该接口可以用于[管理员](#)查询用户组详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/groups/{group\_id}

表 5-281 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                 |
|----------|------|--------|--------------------------------------------------------------------|
| group_id | 是    | String | 待查询的用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-282 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-283 响应 Body 参数

| 参数                    | 参数类型   | 描述     |
|-----------------------|--------|--------|
| <a href="#">group</a> | Object | 用户组信息。 |

表 5-284 group

| 参数                    | 参数类型   | 描述          |
|-----------------------|--------|-------------|
| description           | String | 用户组描述信息。    |
| id                    | String | 用户组ID。      |
| domain_id             | String | 用户组所属账号ID。  |
| name                  | String | 用户组名。       |
| <a href="#">links</a> | Object | 用户组的资源链接信息。 |
| create_time           | Long   | 用户组创建时间。    |

表 5-285 group.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

## 请求示例

查询用户组详情。

```
GET https://iam.myhuaweicloud.com/v3/groups/{group_id}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "group": {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "create_time": 1578107542861,
 "name": "IAMGroup",
 "description": "",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/groups/07609e7eb200250a3f7dc003cb7a..."
 }
 },
 "id": "07609e7eb200250a3f7dc003cb7..."
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.7.3 创建用户组

### 功能介绍

该接口可以用于[管理员](#)创建用户组。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3/groups

### 请求参数

表 5-286 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-287 请求 Body 参数

| 参数                    | 是否必选 | 参数类型   | 描述     |
|-----------------------|------|--------|--------|
| <a href="#">group</a> | 是    | Object | 用户组信息。 |

表 5-288 group

| 参数          | 是否必选 | 参数类型   | 描述                                                                 |
|-------------|------|--------|--------------------------------------------------------------------|
| description | 否    | String | 用户组描述信息，长度小于等于255字符。                                               |
| domain_id   | 否    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

| 参数   | 是否必选 | 参数类型   | 描述                |
|------|------|--------|-------------------|
| name | 是    | String | 用户组名，长度1~128字符之间。 |

## 响应参数

表 5-289 响应 Body 参数

| 参数           | 参数类型   | 描述     |
|--------------|--------|--------|
| <b>group</b> | Object | 用户组信息。 |

表 5-290 group

| 参数           | 参数类型   | 描述          |
|--------------|--------|-------------|
| description  | String | 用户组描述信息。    |
| id           | String | 用户组ID。      |
| domain_id    | String | 用户组所属账号ID。  |
| name         | String | 用户组名。       |
| <b>links</b> | Object | 用户组的资源链接信息。 |
| create_time  | Long   | 用户组创建时间。    |

表 5-291 group.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

创建名为“IAMGroup”的用户组。

```
POST https://iam.myhuaweicloud.com/v3/groups
{
 "group": {
 "description": "IAMDescription",
 "domain_id": "d78cbac186b744899480f25bd0...",
 "name": "IAMGroup"
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "group": {
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/groups/077a4c7bcd8010d53fb7c003e9d966c2"
 },
 "id": "077a4c7bcd8010d53fb7c003e9d966c2",
 "create_time": 1578969208707,
 "domain_id": "d78cbac186b744899480f25bd0...",
 "name": "IAMGroup"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 201 | 创建成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 409 | 资源冲突。   |

## 错误码

无

## 5.7.4 更新用户组

### 功能介绍

该接口可以用于[管理员](#)更新用户组信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PATCH /v3/groups/{group\_id}



表 5-292 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                 |
|----------|------|--------|--------------------------------------------------------------------|
| group_id | 是    | String | 待更新的用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-293 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-294 请求 Body 参数

| 参数                    | 是否必选 | 参数类型   | 描述     |
|-----------------------|------|--------|--------|
| <a href="#">group</a> | 是    | Object | 用户组信息。 |

表 5-295 group

| 参数          | 是否必选 | 参数类型   | 描述                                                                 |
|-------------|------|--------|--------------------------------------------------------------------|
| description | 否    | String | 用户组描述信息，长度小于等于255字符。name与description至少填写一个。                        |
| domain_id   | 否    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| name        | 否    | String | 用户组名，长度1~128字符。name与description至少填写一个。                             |

## 响应参数

表 5-296 响应 Body 参数

| 参数           | 参数类型   | 描述     |
|--------------|--------|--------|
| <b>group</b> | Object | 用户组信息。 |

表 5-297 group

| 参数           | 参数类型   | 描述          |
|--------------|--------|-------------|
| description  | String | 用户组描述信息。    |
| id           | String | 用户组ID。      |
| domain_id    | String | 用户组所属账号ID。  |
| name         | String | 用户组名。       |
| <b>links</b> | Object | 用户组的资源链接信息。 |
| create_time  | Long   | 用户组创建时间。    |

表 5-298 group.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

修改用户组的名称为“IAMGroup”，描述修改为“IAMDescription”。

```
PATCH https://iam.myhuaweicloud.com/v3/groups/{group_id}
{
 "group": {
 "description": "IAMDescription",
 "domain_id": "d78cbac186b744899480f25bd02...",
 "name": "IAMGroup"
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "group": {
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/groups/077a4da48a00251f3f9dc0032103400f"
 }
 }
}
```

```
},
"id": "077a4da48a00251f3f9dc0032103400f",
"create_time": 1578969360636,
"domain_id": "d78cbac186b744899480f25bd...",
"name": "IAMGroup"
}
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 409 | 资源冲突。     |
| 501 | 接口没有实现。   |

## 错误码

无

## 5.7.5 删除用户组

### 功能介绍

该接口可以用于[管理员](#)删除用户组。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3/groups/{group\_id}

表 5-299 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                                                                                                           |
|----------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group_id | 是    | String | 待删除的用户组ID，获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> 。 |

## 请求参数

表 5-300 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

删除用户组。

```
DELETE https://iam.myhuaweicloud.com/v3/groups/{group_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.7.6 查询 IAM 用户是否在用户组中

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户是否在用户组中。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

HEAD /v3/groups/{group\_id}/users/{user\_id}

表 5-301 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                   |
|----------|------|--------|----------------------------------------------------------------------|
| group_id | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。       |
| user_id  | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-302 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

查询IAM用户是否在用户组中。

```
HEAD https://iam.myhuaweicloud.com/v3/groups/{group_id}/users/{user_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述                       |
|-----|--------------------------|
| 204 | 查询成功。（该IAM用户在此用户组中）      |
| 400 | 参数无效。                    |
| 401 | 认证失败。                    |
| 403 | 没有操作权限。                  |
| 404 | 未找到相应的资源。（该IAM用户不在此用户组中） |

## 错误码

无

## 5.7.7 添加 IAM 用户到用户组

### 功能介绍

该接口可以用于[管理员](#)添加IAM用户到用户组。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

```
PUT /v3/groups/{group_id}/users/{user_id}
```

表 5-303 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                    |
|----------|------|--------|-----------------------------------------------------------------------|
| group_id | 是    | String | 用户组ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。       |
| user_id  | 是    | String | 待添加的IAM用户ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-304 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                         |
|--------------|------|--------|------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为 “application/json;charset=utf8”                    |
| X-Auth-Token | 是    | String | 访问令牌, 承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

添加IAM用户到用户组。

```
PUT https://iam.myhuaweicloud.com/v3/groups/{group_id}/users/{user_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 204 | 添加成功。 |
| 400 | 参数无效。 |
| 401 | 认证失败。 |

| 返回值 | 描述        |
|-----|-----------|
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.7.8 移除用户组中的 IAM 用户

### 功能介绍

该接口可以用于[管理员](#)移除用户组中的IAM用户。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3/groups/{group\_id}/users/{user\_id}

表 5-305 路径参数

| 参数       | 是否必选 | 参数类型   | 描述                                                                        |
|----------|------|--------|---------------------------------------------------------------------------|
| group_id | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。            |
| user_id  | 是    | String | 待从用户组中移除的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-306 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |



| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除用户组中的IAM用户。

```
DELETE https://iam.myhuaweicloud.com/v3/groups/{group_id}/users/{user_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述                       |
|-----|--------------------------|
| 204 | 移除成功。                    |
| 400 | 参数无效。                    |
| 401 | 认证失败。                    |
| 403 | 没有操作权限。                  |
| 404 | 未找到相应的资源。（该IAM用户不在此用户组中） |

## 错误码

无

# 5.8 权限管理

## 5.8.1 查询权限列表

### 功能介绍

该接口可以用于[管理员](#)查询权限列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/roles

表 5-307 Query 参数

| 参数              | 是否必选 | 参数类型    | 描述                                                                                                                                                                                            |
|-----------------|------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id       | 否    | String  | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。<br><b>说明</b> <ul style="list-style-type: none"> <li>如果填写此参数，则返回账号下所有自定义策略。</li> <li>如果不填写此参数，则返回所有系统权限（包含系统策略和系统角色）。</li> </ul> |
| permission_type | 否    | String  | 区分系统权限类型的参数。当domain_id参数为空时生效。 <ul style="list-style-type: none"> <li>policy：返回系统策略</li> <li>role：返回系统角色。</li> </ul>                                                                          |
| name            | 否    | String  | 系统内部呈现的权限名称。如云目录服务CCS普通用户权限CCS User的name为ccs_user。<br><b>建议您传参display_name，不传name参数。</b>                                                                                                      |
| display_name    | 否    | String  | 权限名称或过滤条件。该参数可以传入控制台或 <a href="#">系统权限</a> 显示的权限名称。 <ul style="list-style-type: none"> <li>权限名称：如传参为ECS FullAccess，则返回该权限相关信息。</li> <li>过滤条件：如传参为Administrator，则返回满足条件的所有管理员权限。</li> </ul>    |
| page            | 否    | Integer | 分页查询时数据的页数，查询值最小为1。需要与per_page同时存在。传入domain_id参数查询自定义策略时，可配套使用。                                                                                                                               |
| per_page        | 否    | Integer | 分页查询时每页的数据个数，取值范围为[1,300]，默认值为300。需要与page同时存在。<br>不传page和per_page参数时，每页最多返回300个权限。                                                                                                            |

| 参数      | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                                                                      |
|---------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type    | 否    | String | 过滤权限的显示模式。取值范围：domain，project，all。type为domain时，返回type=AA或AX的权限；type为project时，返回type=AA或XA的权限；type为all时返回type为AA、AX、XA的权限。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> </ul> |
| catalog | 否    | String | 权限所在目录。catalog值精确匹配策略的catalog字段(可以过滤服务的策略、或者自定义策略)。                                                                                                                                                                                                                                                     |

## 请求参数

表 5-308 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-309 响应 Body 参数

| 参数                    | 参数类型             | 描述       |
|-----------------------|------------------|----------|
| <a href="#">links</a> | Object           | 资源链接信息。  |
| <a href="#">roles</a> | Array of objects | 权限信息列表。  |
| total_number          | Integer          | 返回权限的总数。 |

表 5-310 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接。                 |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-311 roles

| 参数             | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id      | String | 权限所属账号ID。                                                                                                                                                                                                                                                                   |
| flag           | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                           |
| description_cn | String | 权限的中文描述信息，仅在创建时中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                                                                                                            |
| catalog        | String | 权限所在目录。                                                                                                                                                                                                                                                                     |
| name           | String | 系统内部呈现的权限名称。如云目录服务CCS普通用户权限CCS User的名称为ccs_user。<br>携带在用户的token中，云服务根据该名称来判断用户是否有权访问。                                                                                                                                                                                       |
| description    | String | 权限描述信息。                                                                                                                                                                                                                                                                     |
| <b>links</b>   | Object | 权限的资源链接信息。                                                                                                                                                                                                                                                                  |
| id             | String | 权限ID。                                                                                                                                                                                                                                                                       |
| display_name   | String | 权限名称。                                                                                                                                                                                                                                                                       |
| type           | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b>  | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |

| 参数           | 参数类型   | 描述                                                                                                 |
|--------------|--------|----------------------------------------------------------------------------------------------------|
| updated_time | String | 权限更新时间，仅在查询账号下所有自定义策略时，返回更新时间，查询系统权限时不返回此字段。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。 |
| created_time | String | 权限创建时间，仅在查询账号下所有自定义策略时，返回创建时间，查询系统权限时不返回此字段。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。 |

表 5-312 roles.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-313 roles.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                   |
|------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。                                                                                                                                                           |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                      |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-314 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-315 roles.policy.Statement

| 参数        | 参数类型             | 描述                                                                                                                                                                                                                                                                                                                                                    |
|-----------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>• 服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符*，无需罗列全部授权项。</li> <li>• 当自定义策略为委托自定义策略时，该字段值为：<code>"Action": ["iam:agencies:assume"]</code>。</li> </ul>                        |
| Effect    | String           | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>                                                                                                                                                                                             |
| Condition | Object           | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b></p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                                                                    |
| Resource  | Object           | <p>资源。如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例：“obs:::bucket:*”。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<code>"Resource": {"uri": ["iam/agencies/07805acaba800fdd4fbd00b8f888c7c"]}</code>。</li> </ul> |

表 5-316 roles.policy.Statement.Condition.operator

| 参数        | 参数类型             | 描述                                                                        |
|-----------|------------------|---------------------------------------------------------------------------|
| attribute | Array of strings | <p>条件键。key为与运算符有对应关系的合法属性，value为长度不超过10的字符串数组。</p> <p>该参数类型为自定义字符串数组。</p> |

## 请求示例

查询权限列表。

```
GET https://iam.myhuaweicloud.com/v3/roles
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "roles": [{
 "domain_id": null,
 "description_cn": "漏洞扫描服务 (VSS) 管理员, 拥有该服务下的所有权限",
 "catalog": "VulnScan",
 "name": "wscn_adm",
 "description": "Vulnerability Scan Service administrator of tasks and reports.",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/0af84c1502f447fa9c2fa18083fbb87e"
 },
 "id": "0af84c1502f447fa9c2fa18083fbb87e",
 "display_name": "VSS Administrator",
 "type": "XA",
 "policy": {
 "Version": "1.0",
 "Statement": [{
 "Action": ["WebScan:*:*"],
 "Effect": "Allow"
 }],
 "Depends": [{
 "catalog": "BASE",
 "display_name": "Server Administrator"
 }, {
 "catalog": "BASE",
 "display_name": "Tenant Guest"
 }]
 }
 }, {
 "domain_id": null,
 "flag": "fine_grained",
 "description_cn": "微服务引擎服务管理员权限",
 "catalog": "CSE",
 "name": "system_all_34",
 "description": "All permissions of CSE service.",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/0b5ea44ebdc64a24a9c372b2317f7e39"
 },
 "id": "0b5ea44ebdc64a24a9c372b2317f7e39",
 "display_name": "CSE Admin",
 "type": "XA",
 "policy": {
 "Version": "1.1",
 "Statement": [{
 "Action": ["cse:*:*", "ecs:*:*", "evs:*:*", "vpc:*:*"],
 "Effect": "Allow"
 }]
 }
 }],
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles"
 }
}
```

```
},
"total_number" : 300
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |

## 错误码

无

## 5.8.2 查询权限详情

### 功能介绍

该接口可以用于[管理员](#)查询权限详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/roles/{role\_id}

表 5-317 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                     |
|---------|------|--------|----------------------------------------|
| role_id | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。 |



## 请求参数

表 5-318 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-319 响应 Body 参数

| 参数                   | 参数类型   | 描述    |
|----------------------|--------|-------|
| <a href="#">role</a> | Object | 权限信息。 |

表 5-320 role

| 参数                    | 参数类型   | 描述                                                                                     |
|-----------------------|--------|----------------------------------------------------------------------------------------|
| domain_id             | String | 权限所属账号ID。                                                                              |
| flag                  | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                      |
| description_cn        | String | 权限的中文描述信息，仅在创建时传入了description_cn参数，响应体中才会返回此字段。                                        |
| catalog               | String | 权限所在目录。                                                                                |
| name                  | String | 系统内部呈现的权限名称。如云目录服务CCS普通用户权限CCS User的名称为ccs_user。<br>携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。 |
| description           | String | 权限描述信息。                                                                                |
| <a href="#">links</a> | Object | 权限的资源链接信息。                                                                             |
| id                    | String | 权限ID。                                                                                  |
| display_name          | String | 权限名称。                                                                                  |

| 参数            | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|---------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type          | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b> | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time  | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |
| created_time  | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

表 5-321 role.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-322 role.policy

| 参数               | 参数类型             | 描述              |
|------------------|------------------|-----------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。      |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。 |

| 参数      | 参数类型   | 描述                                                                                                                                                                                  |
|---------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version | String | <p>权限版本号。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-323 role.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-324 role.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                                                                     |
|--------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | <p>授权项, 指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为: 服务名:资源类型:操作, 例: vpc:ports:create。</li> <li>服务名为产品名称, 例如ecs、evs和vpc等, 服务名仅支持小写。资源类型和操作没有大小写, 要求支持通配符号*, 无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时, 该字段值为: "Action": ["iam:agencies:assume"]。</li> </ul> |
| Effect | String           | <p>作用。包含两种: 允许 ( Allow ) 和拒绝 ( Deny ), 既有Allow又有Deny的授权语句时, 遵循Deny优先的原则。</p> <p>取值范围:</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                        |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                                                      |
|-----------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Object | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b><br/>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                                                                         |
| Resource  | Object | <p>资源。如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs:::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<code>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</code>。</li> </ul> |

## 请求示例

查询权限详情。

```
GET https://iam.myhuaweicloud.com/v3/roles/{role_id}
```

## 响应示例

状态码为 200 时:

请求成功。

```

{
 "role": {
 "domain_id": null,
 "description_cn": "漏洞扫描服务（VSS）管理员，拥有该服务下的所有权限",
 "catalog": "VulnScan",
 "name": "wscn_admin",
 "description": "Vulnerability Scan Service administrator of tasks and reports.",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/0af84c1502f447fa9c2fa18083fbb87e"
 },
 "id": "0af84c1502f447fa9c2fa18083fbb87e",
 "display_name": "VSS Administrator",
 "type": "XA",
 "policy": {
 "Version": "1.0",
 "Statement": [
 {
 "Action": [
 "WebScan:*"
]
 }
]
 }
 }
}

```

```

 "Effect": "Allow"
 }
],
 "Depends": [
 {
 "catalog": "BASE",
 "display_name": "Server Administrator"
 },
 {
 "catalog": "BASE",
 "display_name": "Tenant Guest"
 }
]
 }
}

```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.3 查询租户授权信息

### 功能介绍

该接口用于查询指定账号中的授权记录。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-PERMISSION/role-assignments

表 5-325 Query 参数

| 参数                           | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id                    | 是    | String | 待查询账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                              |
| role_id                      | 否    | String | 策略ID。                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| subject                      | 否    | String | 授权主体，取值范围：user、group、agency。该参数与subject.user_id、subject.group_id、subject.agency_id只能选择一个。                                                                                                                                                                                                                                                                                                                                                     |
| subject.user_id              | 否    | String | 授权的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                           |
| subject.group_id             | 否    | String | 授权的用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                             |
| subject.agency_id            | 否    | String | 授权的委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                              |
| scope                        | 否    | String | 授权范围，取值范围：project、domain、enterprise_project。该参数与scope.project_id、scope.domain_id、scope.enterprise_projects_id只能选择一个。<br><b>说明</b> <ul style="list-style-type: none"> <li>如需查看全局服务授权记录，scope取值domain或填写scope.domain_id。</li> <li>如需查看基于所有资源的授权记录，scope取值为domain，且is_inherited取值为true。</li> <li>如需查看基于项目的授权记录，scope取值为project或填写scope.project_id。</li> <li>如需查看基于企业项目的授权记录，scope取值为enterprise_project或填写scope.enterprise_project_id。</li> </ul> |
| scope.project_id             | 否    | String | 授权的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                              |
| scope.domain_id              | 否    | String | 待查询账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                                                                                                                                                                                                                                              |
| scope.enterprise_projects_id | 否    | String | 授权的企业项目ID，获取方式请参见： <a href="#">如何获取企业项目ID</a> 。                                                                                                                                                                                                                                                                                                                                                                                               |

| 参数            | 是否必选 | 参数类型    | 描述                                                                                                                            |
|---------------|------|---------|-------------------------------------------------------------------------------------------------------------------------------|
| is_inherited  | 否    | Boolean | 是否包含基于所有项目授权的记录，默认为false。当参数scope=domain或者scope.domain_id存在时生效。true: 查询基于所有项目授权的记录。false: 查询基于全局服务授权的记录。                      |
| include_group | 否    | Boolean | 是否包含基于IAM用户所属用户组授权的记录，默认为true。当参数subject=user或者subject.user_id存在时生效。true: 查询基于IAM用户授权、IAM用户所属用户组授权的记录。false: 仅查询基于IAM用户授权的记录。 |
| page          | 否    | Integer | 分页查询时数据的页数，查询值最小为1。需要与per_page同时存在。                                                                                           |
| per_page      | 否    | Integer | 分页查询时每页的数据个数，取值范围为[1,50]，需要与page同时存在。                                                                                         |

## 请求参数

表 5-326 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                    |
|--------------|------|--------|-------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-327 响应 Body 参数

| 参数                               | 参数类型                                | 描述          |
|----------------------------------|-------------------------------------|-------------|
| total_num                        | Long                                | 返回授权记录的总条数。 |
| <a href="#">role_assignments</a> | Array of RoleAssignmentBody objects | 授权信息。       |

表 5-328 role\_assignments

| 名称            | 类型                            | 描述                                      |
|---------------|-------------------------------|-----------------------------------------|
| <b>user</b>   | RoleUserAssignmentId object   | 授权用户信息。仅在授权主体，取值为user时返回此字段。            |
| <b>role</b>   | RoleAssignmentId object       | 授权策略信息。                                 |
| <b>group</b>  | RoleGroupAssignmentId object  | 授权用户组信息。仅在授权主体，取值为 <b>group</b> 时返回此字段。 |
| <b>agency</b> | RoleAgencyAssignmentId object | 授权委托信息。仅在授权主体，取值为agency时返回此字段。          |
| <b>scope</b>  | RoleAssignmentScope object    | 授权作用的范围。                                |
| is_inherited  | Boolean                       | 是否基于所有项目授权。                             |

表 5-329 role\_assignments.user

| 参数 | 参数类型   | 描述       |
|----|--------|----------|
| id | String | IAM用户ID。 |

表 5-330 role\_assignments.role

| 名称 | 类型     | 描述    |
|----|--------|-------|
| id | String | 权限ID。 |

表 5-331 role\_assignments.group

| 名称 | 类型     | 描述     |
|----|--------|--------|
| id | String | 用户组ID。 |

表 5-332 role\_assignments.agency

| 名称 | 类型     | 描述    |
|----|--------|-------|
| id | String | 委托ID。 |



表 5-333 role\_assignments.scope

| 名称                        | 类型                                       | 描述                                           |
|---------------------------|------------------------------------------|----------------------------------------------|
| <b>project</b>            | RoleProjectAssignmentId object           | 基于IAM项目授权的信息。仅授权范围选择project时返回此字段。           |
| <b>domain</b>             | RoleDomainAssignmentId object            | 基于全局服务或所有项目授权的信息。仅授权范围选择domain时返回此字段。        |
| <b>enterprise_project</b> | RoleEnterpriseProjectAssignmentId object | 基于企业项目授权的信息。仅授权范围选择enterprise_project时返回此字段。 |

表 5-334 role\_assignments.scope.project

| 名称 | 类型     | 描述       |
|----|--------|----------|
| id | String | IAM项目ID。 |

表 5-335 role\_assignments.scope.domain

| 名称 | 类型     | 描述      |
|----|--------|---------|
| id | String | 全局服务ID。 |

表 5-336 role\_assignments.scope.enterprise\_project

| 名称 | 类型     | 描述      |
|----|--------|---------|
| id | String | 企业项目ID。 |

## 请求示例

查询租户授权信息。

GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/role-assignments?{domain\_id}

## 响应示例

状态码为200时：

请求成功。

```
{
 "role_assignments":{
 "group":{
 "id":"07609e7eb200250a3f7dc003cb7a4e2d"
 },
 },
}
```

```

 "is_inherited":true,
 "role":{
 "id":"11e5c42d20cc349a2b9e2f8afd253f50c"
 },
 "scope":{
 "domain":{
 "id":"d78cbac186b744899480f25bd022f468"
 }
 }
 },
 "total_num":1
}

```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |

## 错误码

请参见[错误码](#)。

## 5.8.4 查询全局服务中的用户组权限

### 功能介绍

该接口可以用于[管理员](#)查询全局服务中的用户组权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/domains/{domain\_id}/groups/{group\_id}/roles

表 5-337 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

| 参数       | 是否必选 | 参数类型   | 描述                                                             |
|----------|------|--------|----------------------------------------------------------------|
| group_id | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-338 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-339 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">links</a> | Object           | 资源链接信息。 |
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |

表 5-340 links

| 参数       | 参数类型   | 描述                     |
|----------|--------|------------------------|
| self     | String | 资源链接。                  |
| previous | String | 前一个邻接资源链接地址，不存在时为null。 |
| next     | String | 后一个邻接资源链接地址，不存在时为null。 |

表 5-341 roles

| 参数             | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id      | String | 权限所属账号ID。                                                                                                                                                                                                                                                                   |
| flag           | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                           |
| description_cn | String | 权限的中文描述信息。仅在创建时中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                                                                                                            |
| catalog        | String | 权限所在目录。                                                                                                                                                                                                                                                                     |
| name           | String | 系统内部呈现的权限名称。如云目录服务CCS普通用户权限CCS User的name为ccs_user。<br>携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。                                                                                                                                                                                    |
| description    | String | 权限描述信息。                                                                                                                                                                                                                                                                     |
| <b>links</b>   | Object | 权限的资源链接信息。                                                                                                                                                                                                                                                                  |
| id             | String | 权限ID。                                                                                                                                                                                                                                                                       |
| display_name   | String | 权限名称。                                                                                                                                                                                                                                                                       |
| type           | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b>  | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time   | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |
| created_time   | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

表 5-342 roles.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-343 roles.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                     |
|------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。                                                                                                                                                             |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                        |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-344 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-345 roles.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                                                          |
|--------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | 授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：<br/>vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul> |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                             |
|-----------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Effect    | String | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br>取值范围：<br><ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>                                                                                                                                                                              |
| Condition | Object | 限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。<br><b>说明</b><br>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。<br><pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } } </pre>                                                                                                             |
| Resource  | Object | 资源，如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：<br><b>说明</b> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为："Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}。</li> </ul> |

## 请求示例

查询全局服务中的用户组权限。

GET https://iam.myhuaweicloud.com/v3/domains/{domain\_id}/groups/{group\_id}/roles

## 响应示例

状态码为 200 时:

请求成功。

```

{
 "roles": [
 {
 "domain_id": null,
 "flag": "fine_grained",
 "description_cn": "查询域名信息",
 "catalog": "CDN",
 "name": "system_all_11",
 "description": "Allow Query Domains",
 "links": {
 "next": null,

```

```

 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/db4259cce0ce47c9903dfdc195eb453b"
 },
 "id": "db4259cce0ce47c9903dfdc195eb453b",
 "display_name": "CDN Domain Viewer",
 "type": "AX",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "cdn:configuration:queryDomains",
 "cdn:configuration:queryOriginServerInfo",
 "cdn:configuration:queryOriginConfInfo",
 "cdn:configuration:queryHttpsConf",
 "cdn:configuration:queryCacheRule",
 "cdn:configuration:queryReferConf",
 "cdn:configuration:queryChargeMode",
 "cdn:configuration:queryCacheHistoryTask",
 "cdn:configuration:queryIpAcl",
 "cdn:configuration:queryResponseHeaderList"
],
 "Effect": "Allow"
 }
]
 }
},
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/domains/d78cbac186b744899480f25bd022f468/groups/077d71374b8025173f61c003ea0a11ac/roles"
}
}

```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.5 查询项目服务中的用户组权限

### 功能介绍

该接口可以用于[管理员](#)查询项目服务中的用户组权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/projects/{project\_id}/groups/{group\_id}/roles

表 5-346 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                             |
|------------|------|--------|----------------------------------------------------------------|
| group_id   | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| project_id | 是    | String | 项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。  |

## 请求参数

表 5-347 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-348 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">links</a> | Object           | 资源链接信息。 |
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |



表 5-349 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接。                 |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-350 roles

| 参数                     | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id              | String | 权限所属账号ID。                                                                                                                                                                                                                                                                   |
| flag                   | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                           |
| description_cn         | String | 权限的中文描述信息。仅在创建时中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                                                                                                            |
| catalog                | String | 权限所在目录。                                                                                                                                                                                                                                                                     |
| name                   | String | 系统内部呈现的权限名称。如云目录服务CCS普通用户权限CCS User的名称为ccs_user。携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。                                                                                                                                                                                          |
| description            | String | 权限描述信息。                                                                                                                                                                                                                                                                     |
| <a href="#">links</a>  | Object | 权限的资源链接信息。                                                                                                                                                                                                                                                                  |
| id                     | String | 权限ID。                                                                                                                                                                                                                                                                       |
| display_name           | String | 权限名称。                                                                                                                                                                                                                                                                       |
| type                   | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <a href="#">policy</a> | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time           | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

| 参数           | 参数类型   | 描述                                                                |
|--------------|--------|-------------------------------------------------------------------|
| created_time | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：<br>1687913793000。 |

表 5-351 roles.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-352 roles.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                   |
|------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。                                                                                                                                                           |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                      |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-353 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限名称。   |

表 5-354 roles.policy.Statement

| 参数        | 参数类型             | 描述                                                                                                                                                                                                                                                                                                                                      |
|-----------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：<br/>vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul>                  |
| Effect    | String           | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                                                   |
| Condition | Object           | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b></p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } } </pre>                                                                                                          |
| Resource  | object           | <p>资源，如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<br/>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</li> </ul> |

## 请求示例

查询项目服务中的用户组权限。

GET [https://iam.myhuaweicloud.com/v3/projects/{project\\_id}/groups/{group\\_id}/roles](https://iam.myhuaweicloud.com/v3/projects/{project_id}/groups/{group_id}/roles)

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "roles": [
 {
 "domain_id": null,
 "flag": "fine_grained",
 "description_cn": "应用运维管理服务只读权限",
 "catalog": "AOM",
 "name": "system_all_30",
 "description": "AOM read only",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/75cfe22af2b3498d82b655fbb39de498"
 },
 "id": "75cfe22af2b3498d82b655fbb39de498",
 "display_name": "AOM Viewer",
 "type": "XA",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "aom:*:list",
 "aom:*:get",
 "apm:*:list",
 "apm:*:get"
],
 "Effect": "Allow"
 }
]
 }
 }
],
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/projects/065a7c66da0010992ff7c0031e5a5e7d/groups/077d71374b8025173f61c003ea0a11ac/roles"
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.6 为用户组授予全局服务权限

### 功能介绍

该接口可以用于[管理员](#)为用户组授予全局服务权限。权限作用范围请参见：[系统权限](#)。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3/domains/{domain\_id}/groups/{group\_id}/roles/{role\_id}

表 5-355 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                                                                                 |
|-----------|------|--------|------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                 |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                     |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。<br><b>说明</b><br>如果您需要给用户组授予包含OBS操作的自定义策略，请分别创建作用范围为全局服务、区域级项目，其他参数相同的2个自定义策略，并将2个策略同时授予用户组。 |

### 请求参数

表 5-356 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为用户组授予全局服务权限。

```
PUT https://iam.myhuaweicloud.com/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 授权成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 409 | 资源冲突。     |

## 错误码

无

## 5.8.7 为用户组授予项目服务权限

### 功能介绍

该接口可以用于[管理员](#)为用户组授予项目服务权限。权限作用范围请参见：[系统权限](#)。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PUT /v3/projects/{project\_id}/groups/{group\_id}/roles/{role\_id}

表 5-357 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                   |
|------------|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group_id   | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                                                                                                       |
| project_id | 是    | String | 为用户组授权的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。<br>请确保该项目与用户组中IAM用户待授权、使用的IAM项目一致。<br><b>说明</b><br>如果您需要给用户组授予包含OBS操作的自定义策略，请使用 <a href="#">查询指定条件下的项目列表</a> 获取名为“MOS”的项目ID，为用户组授予该项目的OBS自定义策略。 |
| role_id    | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                                                                                                                                                                               |

## 请求参数

表 5-358 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为用户组授予项目服务权限。

```
PUT https://iam.myhuaweicloud.com/v3/projects/{project_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 授权成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 409 | 资源冲突。     |

## 错误码

无

## 5.8.8 查询用户组是否拥有全局服务权限

### 功能介绍

该接口可以用于[管理员](#)查询用户组是否拥有全局服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

```
HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```



表 5-359 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                             |

## 请求参数

表 5-360 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

查询用户组是否拥有全局服务权限。

```
HEAD https://iam.myhuaweicloud.com/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述            |
|-----|---------------|
| 204 | 查询成功。（具有指定权限） |

| 返回值 | 描述        |
|-----|-----------|
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.9 查询用户组是否拥有项目服务权限

### 功能介绍

该接口可以用于[管理员](#)查询用户组是否拥有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

HEAD /v3/projects/{project\_id}/groups/{group\_id}/roles/{role\_id}

表 5-361 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                             |
|------------|------|--------|----------------------------------------------------------------|
| group_id   | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| project_id | 是    | String | 项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。  |
| role_id    | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                         |

## 请求参数

表 5-362 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

查询用户组是否拥有项目服务权限。

```
HEAD https://iam.myhuaweicloud.com/v3/projects/{project_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述            |
|-----|---------------|
| 204 | 查询成功。（具有指定权限） |
| 400 | 参数无效。         |
| 401 | 认证失败。         |
| 403 | 没有操作权限。       |
| 404 | 未找到相应的资源。     |

## 错误码

无

### 5.8.10 查询用户组的所有项目权限列表

#### 功能介绍

该接口可以用于[管理员](#)查询用户组所有项目服务权限列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/OS-INHERIT/domains/{domain\_id}/groups/{group\_id}/roles/  
inherited\_to\_projects

表 5-363 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                             |
|-----------|------|--------|----------------------------------------------------------------|
| domain_id | 是    | String | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。  |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-364 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                |
|--------------|------|--------|-----------------------------------|
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的token。 |

## 响应参数

状态码为 200 时：

表 5-365 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">links</a> | object           | 资源链接信息。 |
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |

表 5-366 roles

| 参数             | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flag           | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                           |
| description_cn | String | 权限的中文描述信息。仅在创建时中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                                                                                                            |
| catalog        | String | 权限所在目录。                                                                                                                                                                                                                                                                     |
| name           | String | 权限名。携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。                                                                                                                                                                                                                                      |
| description    | String | 权限描述信息。                                                                                                                                                                                                                                                                     |
| <b>links</b>   | object | 权限的资源链接信息。                                                                                                                                                                                                                                                                  |
| id             | String | 权限ID。                                                                                                                                                                                                                                                                       |
| display_name   | String | 权限展示名。                                                                                                                                                                                                                                                                      |
| type           | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b>  | object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time   | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |
| created_time   | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

表 5-367 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-368 roles.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                   |
|------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。                                                                                                                                                           |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                      |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-369 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-370 roles.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                                                             |
|--------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | 授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<code>"Action": ["iam:agencies:assume"]</code>。</li> </ul> |
| Effect | String           | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br><b>枚举值：</b> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                               |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                                        |
|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Object | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b><br/>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                                                           |
| Resource  | Object | <p>资源，如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为："Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}。</li> </ul> |

## 请求示例

查询用户组的所有项目权限列表。

```
GET https://iam.myhuaweicloud.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/
inherited_to_projects
```

## 响应示例

**状态码： 200**

请求成功。

```

{
 "roles": [{
 "description_cn": "漏洞扫描服务（VSS）管理员，拥有该服务下的所有权限",
 "catalog": "VulnScan",
 "name": "wscn_adm",
 "description": "Vulnerability Scan Service administrator of tasks and reports.",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/0af84c1502f447fa9c2fa18083fbb..."
 },
 "id": "0af84c1502f447fa9c2fa18083fbb...",
 "display_name": "VSS Administrator",
 "type": "XA",
 "policy": {
 "Version": "1.0",
 "Statement": [{
 "Action": ["WebScan:*:*"],
 "Effect": "Allow"
 }],
 "Depends": [{

```

```

 "catalog": "BASE",
 "display_name": "Server Administrator"
 }, {
 "catalog": "BASE",
 "display_name": "Tenant Guest"
 }
]
}, {
 "flag": "fine_grained",
 "description_cn": "微服务引擎服务管理员权限",
 "catalog": "CSE",
 "name": "system_all_34",
 "description": "All permissions of CSE service.",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles/0b5ea44ebdc64a24a9c372b2317f7..."
 },
 "id": "0b5ea44ebdc64a24a9c372b2317f7...",
 "display_name": "CSE Admin",
 "type": "XA",
 "policy": {
 "Version": "1.1",
 "Statement": [{
 "Action": ["cse:*:*", "ecs:*:*", "evs:*:*", "vpc:*:*"],
 "Effect": "Allow"
 }
]
}
},
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles"
}
}

```

## 状态码

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |

## 错误码

请参见[错误码](#)。

### 5.8.11 查询用户组是否拥有所有项目指定权限

#### 功能介绍

该接口可以用于[管理员](#)查询用户组是否拥有所有项目指定权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。



## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

HEAD /v3/OS-INHERIT/domains/{domain\_id}/groups/{group\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-371 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。      |

## 请求参数

表 5-372 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                |
|--------------|------|--------|-----------------------------------|
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的token。 |

## 响应参数

无

## 请求示例

查询用户组是否拥有所有项目指定权限。

```
HEAD https://iam.myhuaweicloud.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

无

## 状态码

| 状态码 | 描述       |
|-----|----------|
| 204 | 查询成功。    |
| 401 | 认证失败。    |
| 403 | 没有操作权限。  |
| 404 | 未找到相应资源。 |

## 错误码

请参见[错误码](#)。

### 5.8.12 移除用户组的所有项目服务权限

#### 功能介绍

该接口可以用于[管理员](#)移除用户组的所有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

DELETE /v3/OS-INHERIT/domains/{domain\_id}/groups/{group\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-373 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。      |

## 请求参数

表 5-374 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                |
|--------------|------|--------|-----------------------------------|
| X-Auth-Token | 是    | String | 拥有Security Administrator权限的token。 |

## 响应参数

无

## 请求示例

移除用户组的所有项目服务权限。

```
DELETE https://iam.myhuaweicloud.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

### 状态码： 403

请求未授权。

- 示例 1

```
{
 "error_code": "IAM.0002",
 "error_msg": "You are not authorized to perform the requested action."
}
```
- 示例 2

```
{
 "error_code": "IAM.0003",
 "error_msg": "Policy doesn't allow %(actions)s to be performed."
}
```

### 状态码： 500

Internal Server Error

```
{
 "error_code": "IAM.0006",
 "error_msg": "An unexpected error prevented the server from fulfilling your request."
}
```

## 状态码

| 返回值 | 描述       |
|-----|----------|
| 204 | 请求成功。    |
| 401 | 认证失败。    |
| 403 | 请求未授权。   |
| 404 | 未找到相应资源。 |

| 返回值 | 描述      |
|-----|---------|
| 500 | 内部服务错误。 |

## 错误码

请参见[错误码](#)。

### 5.8.13 移除用户组的全局服务权限

#### 功能介绍

该接口可以用于[管理员](#)移除用户组的全局服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

DELETE /v3/domains/{domain\_id}/groups/{group\_id}/roles/{role\_id}

表 5-375 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| group_id  | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                             |

## 请求参数

表 5-376 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除用户组的全局服务权限。

```
DELETE https://iam.myhuaweicloud.com/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 移除成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.14 移除用户组的项目服务权限

### 功能介绍

该接口可以用于[管理员](#)移除用户组的项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

DELETE /v3/projects/{project\_id}/groups/{group\_id}/roles/{role\_id}

表 5-377 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                             |
|------------|------|--------|----------------------------------------------------------------|
| group_id   | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| project_id | 是    | String | 项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。  |
| role_id    | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                         |

## 请求参数

表 5-378 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除用户组的项目服务权限。

DELETE https://iam.myhuaweicloud.com/v3/projects/{project\_id}/groups/{group\_id}/roles/{role\_id}

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 移除成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

## 错误码

无

## 5.8.15 为用户组授予所有项目服务权限

### 功能介绍

该接口可以用于[管理员](#)为用户组授予所有项目服务权限，权限作用范围包括全局服务和所有IAM项目。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3/OS-INHERIT/domains/{domain\_id}/groups/{group\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-379 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                 |
|-----------|------|--------|--------------------------------------------------------------------|
| domain_id | 是    | String | 用户组所属账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

| 参数       | 是否必选 | 参数类型   | 描述                                                             |
|----------|------|--------|----------------------------------------------------------------|
| group_id | 是    | String | 用户组ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id  | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                         |

## 请求参数

表 5-380 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为用户组授予所有项目服务权限。

```
PUT https://iam.myhuaweicloud.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

无

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 204 | 授权成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |



| 返回值 | 描述        |
|-----|-----------|
| 404 | 未找到相应的资源。 |

## 5.9 自定义策略管理

### 5.9.1 查询自定义策略列表

#### 功能介绍

该接口可以用于[管理员](#)查询自定义策略列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3.0/OS-ROLE/roles

表 5-381 Query 参数

| 参数       | 是否必选 | 参数类型    | 描述                                     |
|----------|------|---------|----------------------------------------|
| page     | 否    | Integer | 分页查询时数据的页数，查询值最小为1。需要与per_page同时存在。    |
| per_page | 否    | Integer | 分页查询时每页的数据个数，取值范围为[1,300]。需要与page同时存在。 |

#### 请求参数

表 5-382 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                    |
|--------------|------|--------|-------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。               |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-383 响应 Body 参数

| 参数           | 参数类型             | 描述           |
|--------------|------------------|--------------|
| <b>links</b> | Object           | 资源链接信息。      |
| <b>roles</b> | Array of objects | 自定义策略信息列表。   |
| total_number | Integer          | 返回自定义策略的总条数。 |

表 5-384 links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-385 roles

| 参数             | 参数类型   | 描述                                                               |
|----------------|--------|------------------------------------------------------------------|
| domain_id      | String | 自定义策略所属账号ID。                                                     |
| updated_time   | String | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。 |
| created_time   | String | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。 |
| description_cn | String | 自定义策略的中文描述信息，仅创建自定义策略时传入了description_cn参数，响应体中才会返回此字段。           |
| catalog        | String | 自定义策略所在目录。                                                       |
| name           | String | 自定义策略名。                                                          |
| description    | String | 自定义策略的描述信息。                                                      |
| <b>links</b>   | Object | 自定义策略的资源链接信息。                                                    |

| 参数            | 参数类型   | 描述                                                                                                                                                                                 |
|---------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id            | String | 自定义策略ID。                                                                                                                                                                           |
| display_name  | String | 自定义策略展示名。                                                                                                                                                                          |
| type          | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| <b>policy</b> | Object | 自定义策略的具体内容。                                                                                                                                                                        |

表 5-386 roles.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-387 roles.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                     |
|------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                     |

表 5-388 roles.policy.Statement

| 参数        | 参数类型                                    | 描述                                                                                                                                                                                                                                                                                                                                                    |
|-----------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings                        | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<code>"Action": ["iam:agencies:assume"]</code>。</li> </ul>                             |
| Effect    | String                                  | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p>                                                                                                                                                                                                                                                                                    |
| Condition | Map<String, Map<String, Array<String>>> | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b></p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre>"Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }</pre>                                                                                                                          |
| Resource  | Object                                  | <p>资源，如果创建此策略时未传入此字段，则返回结果中也无此字段。</p> <p>规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>可填*的五段式：:::，例：“obs::bucket:*”。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<code>"Resource": {"uri": ["iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</code>。</li> </ul> |

## 请求示例

查询自定义策略列表。

GET <https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles>

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "roles": [{
```

```

"domain_id": "d78cbac186b744899480f25bd022f...",
"updated_time": "1579229246886",
"created_time": "1579229246886",
"description_cn": "中文描述",
"catalog": "CUSTOMED",
"name": "custom_d78cbac186b744899480f25bd022f468_1",
"description": "IAMDescription",
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/93879fd90f1046f69e6e0b31c94d2..."
},
},
{id": "93879fd90f1046f69e6e0b31c94d2...",
"display_name": "IAMCloudServicePolicy",
"type": "AX",
"policy": {
 "Version": "1.1",
 "Statement": [{
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": ["ap-southeast-1"]
 }
 },
 "Action": ["obs:bucket:GetBucketAcl"],
 "Resource": ["obs:*:bucket:*"],
 "Effect": "Allow"
 }]
}
}, {
"domain_id": "d78cbac186b744899480f25bd022f...",
"updated_time": "1579229242358",
"created_time": "1579229242358",
"description_cn": "中文描述",
"catalog": "CUSTOMED",
"name": "custom_d78cbac186b744899480f25bd022f468_0",
"description": "IAMDescription",
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/f67224e84dc849ab954ce29fb4f47..."
},
},
{id": "f67224e84dc849ab954ce29fb4f473...",
"display_name": "IAMAgencyPolicy",
"type": "AX",
"policy": {
 "Version": "1.1",
 "Statement": [{
 "Action": ["iam:agencies:assume"],
 "Resource": {
 "uri": ["/iam/agencies/07805acaba800fdd4fbd00b8f888..."]
 },
 "Effect": "Allow"
 }]
}
},
},
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/roles?domain_id=d78cbac186b744899480f25bd022f..."
},
"total_number": 300
}

```

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 200 | 请求成功。 |
| 400 | 参数无效。 |

| 返回值 | 描述      |
|-----|---------|
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.2 查询自定义策略详情

### 功能介绍

该接口可以用于[管理员](#)查询自定义策略详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-ROLE/roles/{role\_id}

表 5-389 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                             |
|---------|------|--------|------------------------------------------------|
| role_id | 是    | String | 待查询的自定义策略ID，获取方式请参见： <a href="#">自定义策略ID</a> 。 |

### 请求参数

表 5-390 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-391 响应 Body 参数

| 参数                   | 参数类型   | 描述       |
|----------------------|--------|----------|
| <a href="#">role</a> | Object | 自定义策略信息。 |

表 5-392 role

| 参数                    | 参数类型    | 描述                                                                   |
|-----------------------|---------|----------------------------------------------------------------------|
| domain_id             | String  | 自定义策略所属账号ID。                                                         |
| references            | Integer | 自定义策略的引用次数。                                                          |
| updated_time          | String  | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：<br>1687913793000。 |
| created_time          | String  | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：<br>1687913793000。 |
| description_cn        | String  | 自定义策略的中文描述信息，仅创建自定义策略时传入了description_cn参数，响应体中才会返回此字段。               |
| catalog               | String  | 自定义策略所在目录。                                                           |
| name                  | String  | 自定义策略名。                                                              |
| description           | String  | 自定义策略的描述信息。                                                          |
| <a href="#">links</a> | Object  | 自定义策略的资源链接信息。                                                        |
| id                    | String  | 自定义策略ID。                                                             |
| display_name          | String  | 自定义策略展示名。                                                            |

| 参数            | 参数类型   | 描述                                                                                                                                                                                     |
|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type          | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA, 不能同时在全局服务和区域级项目生效 (AA), 或者在全局服务和区域级项目都不生效 (XX)。</li> </ul> |
| <b>policy</b> | Object | 自定义策略的具体内容。                                                                                                                                                                            |

表 5-393 role.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-394 role.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                       |
|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句, 描述自定义策略的具体内容。                                                                                                                                                      |



表 5-395 role.policy.Statement

| 参数        | 参数类型                                  | 描述                                                                                                                                                                                                                                                                                                                                 |
|-----------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings                      | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：<br/>vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul>             |
| Effect    | String                                | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                                              |
| Condition | Map<String,Map<String,Array<String>>> | <p>限制条件。如果创建此策略未传入此字段，则返回结果中也无此字段。</p> <p><b>说明</b></p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } } </pre>                                                                                                     |
| Resource  | Object                                | <p>资源，如果创建此策略时未传入此字段，则返回结果中也无此字段。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>当该自定义策略为委托自定义策略时，该字段类型为Object，值为："Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</li> </ul> |

## 请求示例

查询自定义策略详情。

GET [https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles/{role\\_id}](https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles/{role_id})

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "role": {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "references": 0,
 "description_cn": "中文描述",
 "catalog": "CUSTOMED",
 "name": "custom_d78cbac186b744899480f25bd022f468_11",
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/a24a71dcc41f4da989c2a1c900b52d1a"
 },
 "id": "a24a71dcc41f4da989c2a1c900b52d1a",
 "display_name": "IAMCloudServicePolicy",
 "type": "AX",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": [
 "ap-southeast-1"
]
 }
 },
 "Action": [
 "obs:bucket:GetBucketAcl"
],
 "Resource": [
 "obs:*:*:bucket:*"
],
 "Effect": "Allow"
 }
]
 }
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.3 创建云服务自定义策略

### 功能介绍

该接口可以用于[管理员](#)创建云服务自定义策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-ROLE/roles

### 请求参数

表 5-396 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-397 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">role</a> | 是    | Object | 自定义策略信息。 |

表 5-398 role

| 参数           | 是否必选 | 参数类型   | 描述        |
|--------------|------|--------|-----------|
| display_name | 是    | String | 自定义策略展示名。 |

| 参数             | 是否必选 | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                                                                |
|----------------|------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type           | 是    | String | <p>自定义策略的作用范围。</p> <ul style="list-style-type: none"> <li>全局服务：AX</li> <li>区域级项目：XA</li> </ul> <p>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>如果您需要给用户组授予包含OBS操作的自定义策略，请分别创建作用范围为全局服务、区域级项目，其他参数相同的2个自定义策略，并将2个策略同时授予用户组。</li> <li>为保障最小授权范围，建议OBS自定义策略中不要包含其他云服务授权项。</li> </ul> |
| description    | 是    | String | 自定义策略的描述信息。                                                                                                                                                                                                                                                                                                                                                       |
| description_cn | 否    | String | 自定义策略的中文描述信息。                                                                                                                                                                                                                                                                                                                                                     |
| <b>policy</b>  | 是    | Object | 自定义策略的具体内容。                                                                                                                                                                                                                                                                                                                                                       |

表 5-399 role.policy

| 参数               | 是否必选 | 参数类型             | 描述                                                                                                                                                                                                   |
|------------------|------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | 是    | String           | <p>权限版本号，创建自定义策略时，该字段值填为“1.1”。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | 是    | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                                                   |

表 5-400 role.policy.Statement

| 参数        | 是否必选 | 参数类型                                  | 描述                                                                                                                                                                                                                                                                                                                                          |
|-----------|------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | 是    | Array of strings                      | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>一个自定义策略role.policy.Statement不能同时包含项目级服务和全局服务的action。查看服务权限作用范围请参考：<a href="#">系统权限</a>。</li> </ul> |
| Effect    | 是    | String                                | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p>取值范围：</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                                                       |
| Condition | 否    | Map<String,Map<String,Array<String>>> | <p>限制条件。了解更多相关参数，请参考：<a href="#">配置自定义策略</a>。</p> <p><b>说明</b></p> <p>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                                               |
| Resource  | 否    | Array of strings                      | <p>资源。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例：“obs::bucket:*”。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> </ul>                                                                                                                                                       |

## 响应参数

表 5-401 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>role</b> | Object | 自定义策略信息。 |

表 5-402 role

| 参数             | 参数类型   | 描述                                                                                                                                                                                 |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catalog        | String | 自定义策略所在目录。                                                                                                                                                                         |
| display_name   | String | 自定义策略展示名。                                                                                                                                                                          |
| description    | String | 自定义策略的描述信息。                                                                                                                                                                        |
| <b>links</b>   | Object | 自定义策略的资源链接信息。                                                                                                                                                                      |
| <b>policy</b>  | Object | 自定义策略的具体内容。                                                                                                                                                                        |
| description_cn | String | 自定义策略的中文描述信息，仅在请求中传入了 description_cn 参数，响应体中才会返回此字段。                                                                                                                               |
| domain_id      | String | 自定义策略所属账号ID。                                                                                                                                                                       |
| type           | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| id             | String | 自定义策略ID。                                                                                                                                                                           |
| name           | String | 自定义策略名。                                                                                                                                                                            |
| updated_time   | String | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |
| created_time   | String | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |

表 5-403 role.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-404 role.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                       |
|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句, 描述自定义策略的具体内容, 不超过8个。                                                                                                                                               |

表 5-405 role.policy.Statement

| 参数        | 参数类型                                    | 描述                                                                                                                                                                                                       |
|-----------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings                        | 授权项, 指对资源的具体操作权限。                                                                                                                                                                                        |
| Effect    | String                                  | 作用。包含两种: 允许 ( Allow ) 和拒绝 ( Deny ), 既有Allow又有Deny的授权语句时, 遵循Deny优先的原则。<br>取值范围: <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                     |
| Condition | Map<String, Map<String, Array<String>>> | 限制条件, 如果请求中未传入此字段, 则返回结果中也无此字段。                                                                                                                                                                          |
| Resource  | Array of strings                        | 资源, 如果请求中未传入此字段, 则返回结果中也无此字段。规则如下:<br><b>说明</b> <ul style="list-style-type: none"> <li>可填 * 的五段式: :::, 例: "obs:::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> </ul> |

## 请求示例

创建一个名为“IAMCloudServicePolicy”的自定义策略。策略表示仅允许以项目名称为“ap-southeast-1”开头的请求获取所有桶ACL的相关信息。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles
{
 "role": {
 "display_name": "IAMCloudServicePolicy",
 "type": "AX",
 "description": "IAMDescription",
 "description_cn": "中文描述",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:bucket:GetBucketAcl"
],
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": [
 "ap-southeast-1"
]
 }
 },
 "Resource": [
 "obs:*:bucket:*"
]
 }
]
 }
 }
}
```

## 响应示例

**状态码为 201 时:**

创建成功。

```
{
 "role": {
 "catalog": "CUSTOMED",
 "display_name": "IAMCloudServicePolicy",
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/93879fd90f1046f69e6e0b31c94d2615"
 },
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "obs:bucket:GetBucketAcl"
],
 "Resource": [
 "obs:*:bucket:*"
],
 "Effect": "Allow",
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": [
 "ap-southeast-1"
]
 }
 }
 }
]
 }
 },
 "description_cn": "中文描述",
 "domain_id": "d78cbac186b744899480f25bd...",
 "type": "AX",
}
```



```
"id": "93879fd90f1046f69e6e0b31c9...",
"name": "custom_d78cbac186b744899480f25bd022f468_1"
}
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 201 | 创建成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.4 创建委托自定义策略

### 功能介绍

该接口可以用于[管理员](#)创建委托自定义策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-ROLE/roles

### 请求参数

表 5-406 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-407 请求 Body 参数

| 参数          | 是否必选 | 参数类型   | 描述       |
|-------------|------|--------|----------|
| <b>role</b> | 是    | Object | 自定义策略信息。 |

表 5-408 role

| 参数             | 是否必选 | 参数类型   | 描述                                                                                                                                                                                 |
|----------------|------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| display_name   | 是    | String | 自定义策略展示名，长度1~128字符之间。                                                                                                                                                              |
| type           | 是    | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| description    | 是    | String | 自定义策略的描述信息。                                                                                                                                                                        |
| description_cn | 否    | String | 自定义策略的中文描述信息。                                                                                                                                                                      |
| <b>policy</b>  | 是    | Object | 自定义策略的具体内容。                                                                                                                                                                        |

表 5-409 role.policy

| 参数               | 是否必选 | 参数类型             | 描述                                                                                                                                                                                          |
|------------------|------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | 是    | String           | 权限版本号，创建自定义策略时，该字段值填为“1.1”。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | 是    | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                                          |

表 5-410 role.policy.Statement

| 参数              | 是否必选 | 参数类型             | 描述                                                                                                                                                                                                                                                                                         |
|-----------------|------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action          | 是    | Array of strings | <p>授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>当自定义策略为委托自定义策略时，该字段值为：<code>"Action": ["iam:agencies:assume"]</code>。</li> </ul> <p><b>取值范围：</b></p> <ul style="list-style-type: none"> <li>iam:agencies:assume</li> </ul> |
| Effect          | 是    | String           | <p>作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。</p> <p><b>取值范围：</b></p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                               |
| <b>Resource</b> | 否    | Object           | <p>委托资源。在有其他账号与您创建了多个委托关系，即您是被委托方，需要将委托中的权限授权给不同的用户组，这些用户组中的IAM用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托。例：</p> <pre>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</pre>                                                                                                   |

表 5-411 role.policy.Statement.Resource

| 参数  | 是否必选 | 参数类型             | 描述                                                                                                                                   |
|-----|------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| uri | 是    | Array of strings | <p>委托资源的URI，长度不超过128。格式为：<code>/iam/agencies/委托ID</code>。例：</p> <pre>"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]</pre> |

## 响应参数

表 5-412 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>role</b> | Object | 自定义策略信息。 |

表 5-413 role

| 参数             | 参数类型   | 描述                                                                                                                                                                                 |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catalog        | String | 自定义策略所在目录。                                                                                                                                                                         |
| display_name   | String | 自定义策略展示名。                                                                                                                                                                          |
| description    | String | 自定义策略的描述信息。                                                                                                                                                                        |
| <b>links</b>   | Object | 自定义策略的资源链接信息。                                                                                                                                                                      |
| <b>policy</b>  | Object | 自定义策略的具体内容。                                                                                                                                                                        |
| description_cn | String | 自定义策略的中文描述信息，仅在请求中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                 |
| domain_id      | String | 自定义策略所属账号ID。                                                                                                                                                                       |
| type           | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| id             | String | 自定义策略ID。                                                                                                                                                                           |
| name           | String | 自定义策略名。                                                                                                                                                                            |
| updated_time   | String | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |
| created_time   | String | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |

表 5-414 role.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-415 role.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                       |
|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句, 描述自定义策略的具体内容。                                                                                                                                                      |

表 5-416 role.policy.Statement

| 参数              | 参数类型             | 描述                                                                                                                                                                                                    |
|-----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action          | Array of strings | 授权项, 指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>当自定义策略为委托自定义策略时, 该字段值为: "Action": ["/iam:agencies:assume"]。</li> </ul>                          |
| Effect          | String           | 作用。包含两种: 允许 (Allow) 和拒绝 (Deny), 既有Allow又有Deny的授权语句时, 遵循Deny优先的原则。<br><b>取值范围:</b> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                               |
| <b>Resource</b> | Object           | 委托资源, 仅在创建请求中传递此字段, 才会返回此对象。在有其他账号与您创建了多个委托关系, 即您是被委托方, 需要将委托中的权限授权给不同的用户组, 这些用户组中的IAM用户进行角色切换时, 仅能切换到被授权的委托中, 不能切换其他委托。例:<br>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]} |

表 5-417 role.policy.Statement.Resource

| 参数  | 参数类型             | 描述                                                                                                         |
|-----|------------------|------------------------------------------------------------------------------------------------------------|
| uri | Array of strings | 委托资源的URI, 长度不超过128。格式为: /iam/agencies/委托ID。例:<br>"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"] |

## 请求示例

创建一个名为“IAMAgencyPolicy”的委托自定义策略。策略表示作用范围为全局服务，委托资源的URI是/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles
{
 "role": {
 "display_name": "IAMAgencyPolicy",
 "type": "AX",
 "description": "IAMDescription",
 "description_cn": "中文描述",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:agencies:assume"
],
 "Resource": {
 "uri": [
 "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
]
 }
 }
]
 }
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "role": {
 "catalog": "CUSTOMED",
 "display_name": "IAMAgencyPolicy",
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/f67224e84dc849ab954ce29fb4f47f8e"
 },
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "iam:agencies:assume"
],
 "Resource": {
 "uri": [
 "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
]
 },
 "Effect": "Allow"
 }
]
 },
 "description_cn": "中文描述",
 "domain_id": "d78cbac186b744899480f25bd02...",
 "type": "AX",
 "id": "f67224e84dc849ab954ce29fb4f47f8e",
 "name": "custom_d78cbac186b744899480f25bd022f468_0"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 201 | 创建成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.5 修改云服务自定义策略

### 功能介绍

该接口可以用于[管理员](#)修改云服务自定义策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PATCH /v3.0/OS-ROLE/roles/{role\_id}

表 5-418 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                             |
|---------|------|--------|------------------------------------------------|
| role_id | 是    | String | 待修改的自定义策略ID，获取方式请参见： <a href="#">自定义策略ID</a> 。 |

## 请求参数

表 5-419 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-420 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">role</a> | 是    | Object | 自定义策略信息。 |

表 5-421 role

| 参数                     | 是否必选 | 参数类型   | 描述                                                                                                                                                                                 |
|------------------------|------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| display_name           | 是    | String | 自定义策略展示名。                                                                                                                                                                          |
| type                   | 是    | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| description            | 是    | String | 自定义策略的描述信息。                                                                                                                                                                        |
| description_cn         | 否    | String | 自定义策略的中文描述信息。                                                                                                                                                                      |
| <a href="#">policy</a> | 是    | Object | 自定义策略的具体内容。                                                                                                                                                                        |



表 5-422 role.policy

| 参数               | 是否必选 | 参数类型             | 描述                                                                                                                                                                                        |
|------------------|------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | 是    | String           | 权限版本号，创建自定义策略时，该字段值填为“1.1”。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | 是    | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                                        |

表 5-423 role.policy.Statement

| 参数        | 是否必选 | 参数类型                                  | 描述                                                                                                                                                                                                                              |
|-----------|------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | 是    | Array of strings                      | 授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> </ul> |
| Effect    | 是    | String                                | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br>取值范围： <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                      |
| Condition | 否    | Map<String,Map<String,Array<String>>> | 限制条件。了解更多相关参数，请参考： <a href="#">配置自定义策略</a> 。<br><b>说明</b><br>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。<br><pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } } </pre> |

| 参数       | 是否必选 | 参数类型             | 描述                                                                                                                                                                         |
|----------|------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource | 否    | Array of strings | 资源。规则如下：<br><b>说明</b> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> </ul> |

## 响应参数

表 5-424 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>role</b> | Object | 自定义策略信息。 |

表 5-425 role

| 参数             | 参数类型   | 描述                                                                                                                                                                               |
|----------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catalog        | String | 自定义策略所在目录。                                                                                                                                                                       |
| display_name   | String | 自定义策略展示名。                                                                                                                                                                        |
| description    | String | 自定义策略的描述信息。                                                                                                                                                                      |
| <b>links</b>   | Object | 自定义策略的资源链接信息。                                                                                                                                                                    |
| <b>policy</b>  | Object | 自定义策略的具体内容。                                                                                                                                                                      |
| description_cn | String | 自定义策略的中文描述信息，仅在请求中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                               |
| domain_id      | String | 自定义策略所属账号ID。                                                                                                                                                                     |
| type           | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX：全局服务。</li> <li>XA：区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| id             | String | 自定义策略ID。                                                                                                                                                                         |
| name           | String | 自定义策略名。                                                                                                                                                                          |

| 参数           | 参数类型   | 描述                                                                   |
|--------------|--------|----------------------------------------------------------------------|
| updated_time | String | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：<br>1687913793000。 |
| created_time | String | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：<br>1687913793000。 |

表 5-426 role.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-427 role.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                     |
|------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                     |

表 5-428 role.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                         |
|--------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | 授权项，指对资源的具体操作权限。                                                                                                                           |
| Effect | String           | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br>取值范围： <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul> |

| 参数        | 参数类型                                  | 描述                                                                                                                                                                                                  |
|-----------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Map<String,Map<String,Array<String>>> | 限制条件，如果请求中未传入此字段，则返回结果中也无此字段。                                                                                                                                                                       |
| Resource  | Array of strings                      | 资源，如果请求中未传入此字段，则返回结果中也无此字段。规则如下：<br><b>说明</b> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例："obs:::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> </ul> |

## 请求示例

修改名为“IAMCloudServicePolicy”的自定义策略。策略修改为仅允许以项目名称为“ap-southeast-1”开头的请求获取所有桶ACL的相关信息。

PATCH https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles/{role\_id}

```
{
 "role": {
 "display_name": "IAMCloudServicePolicy",
 "type": "AX",
 "description": "IAMDescription",
 "description_cn": "中文描述",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:bucket:GetBucketAcl"
],
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": [
 "ap-southeast-1"
]
 }
 }
 }
],
 "Resource": [
 "obs::*:bucket:*"
]
 }
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "role": {
 "catalog": "CUSTOMED",
 "display_name": "IAMCloudServicePolicy",
 "description": "IAMDescription",
 "links": {
```

```

 "self": "https://iam.myhuaweicloud.com/v3/roles/93879fd90f1046f69e6e0b31c94d2615"
 },
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "obs:bucket:GetBucketAcl"
],
 "Resource": [
 "obs:*:bucket:*"
],
 "Effect": "Allow",
 "Condition": {
 "StringStartWith": {
 "g:ProjectName": [
 "ap-southeast-1"
]
 }
 }
 }
]
 },
 "description_cn": "中文描述",
 "domain_id": "d78cbac186b744899480f25bd0...",
 "type": "AX",
 "id": "93879fd90f1046f69e6e0b31c94d2615",
 "name": "custom_d78cbac186b744899480f25bd022f468_1"
}

```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.6 修改委托自定义策略

### 功能介绍

该接口可以用于[管理员](#)修改委托自定义策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PATCH /v3.0/OS-ROLE/roles/{role\_id}

表 5-429 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                             |
|---------|------|--------|------------------------------------------------|
| role_id | 是    | String | 待修改的自定义策略ID，获取方式请参见： <a href="#">自定义策略ID</a> 。 |

## 请求参数

表 5-430 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-431 请求 Body 参数

| 参数                   | 是否必选 | 参数类型   | 描述       |
|----------------------|------|--------|----------|
| <a href="#">role</a> | 是    | Object | 自定义策略信息。 |

表 5-432 role

| 参数           | 是否必选 | 参数类型   | 描述        |
|--------------|------|--------|-----------|
| display_name | 是    | String | 自定义策略展示名。 |

| 参数             | 是否必选 | 参数类型   | 描述                                                                                                                                                                                   |
|----------------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type           | 是    | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA, 不能同时在全局服务和区域级项目生效(AA), 或者在全局服务和区域级项目都不生效(XX)。</li> </ul> |
| description    | 是    | String | 自定义策略的描述信息。                                                                                                                                                                          |
| description_cn | 否    | String | 自定义策略的中文描述信息。                                                                                                                                                                        |
| <b>policy</b>  | 是    | Object | 自定义策略的具体内容。                                                                                                                                                                          |

表 5-433 role.policy

| 参数               | 是否必选 | 参数类型             | 描述                                                                                                                                                                                              |
|------------------|------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | 是    | String           | 权限版本号, 创建自定义策略时, 该字段值填为“1.1”。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | 是    | Array of objects | 授权语句, 描述自定义策略的具体内容。                                                                                                                                                                             |

表 5-434 role.policy.Statement

| 参数     | 是否必选 | 参数类型             | 描述                                                                                                                                                                                                                                                             |
|--------|------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | 是    | Array of strings | 授权项, 指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>当自定义策略为委托自定义策略时, 该字段值为: "Action": ["iam:agencies:assume"]。</li> </ul> <b>取值范围:</b> <ul style="list-style-type: none"> <li>iam:agencies:assume</li> </ul> |

| 参数              | 是否必选 | 参数类型   | 描述                                                                                                                                                                                   |
|-----------------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Effect          | 是    | String | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br>取值范围：<br><ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                        |
| <b>Resource</b> | 否    | Object | 委托资源。当有其他账号与您创建了多个委托关系，即您是被委托方，需要将委托中的权限授权给不同的用户组，这些用户组中的IAM用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托。例：<br><pre>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</pre> |

表 5-435 role.policy.Statement.Resource

| 参数  | 是否必选 | 参数类型             | 描述                                                                                                                  |
|-----|------|------------------|---------------------------------------------------------------------------------------------------------------------|
| uri | 是    | Array of strings | 委托资源的URI，长度不超过128。格式为：/iam/agencies/委托ID。例：<br><pre>"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]</pre> |

## 响应参数

表 5-436 响应 Body 参数

| 参数          | 参数类型   | 描述       |
|-------------|--------|----------|
| <b>role</b> | Object | 自定义策略信息。 |

表 5-437 role

| 参数           | 参数类型   | 描述            |
|--------------|--------|---------------|
| catalog      | String | 自定义策略所在目录。    |
| display_name | String | 自定义策略展示名。     |
| description  | String | 自定义策略的描述信息。   |
| <b>links</b> | Object | 自定义策略的资源链接信息。 |



| 参数             | 参数类型   | 描述                                                                                                                                                                                 |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>policy</b>  | Object | 自定义策略的具体内容。                                                                                                                                                                        |
| description_cn | String | 自定义策略的中文描述信息，仅在请求中传入了description_cn参数，响应体中才会返回此字段。                                                                                                                                 |
| domain_id      | String | 自定义策略所属账号ID。                                                                                                                                                                       |
| type           | String | 自定义策略的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX: 全局服务。</li> <li>XA: 区域级项目。</li> <li>自定义策略的显示模式只能为AX或者XA，不能同时在全局服务和区域级项目生效（AA），或者在全局服务和区域级项目都不生效（XX）。</li> </ul> |
| id             | String | 自定义策略ID。                                                                                                                                                                           |
| name           | String | 自定义策略名。                                                                                                                                                                            |
| updated_time   | String | 自定义策略更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |
| created_time   | String | 自定义策略创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                   |

表 5-438 role.links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

表 5-439 role.policy

| 参数               | 参数类型             | 描述                                                                                                                                                                     |
|------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |
| <b>Statement</b> | Array of objects | 授权语句，描述自定义策略的具体内容。                                                                                                                                                     |

表 5-440 role.policy.Statement

| 参数              | 参数类型             | 描述                                                                                                                                                                                           |
|-----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action          | Array of strings | 授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul>                |
| Effect          | String           | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br><b>取值范围：</b> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                            |
| <b>Resource</b> | Object           | 委托资源，仅在请求中传递此字段，才会返回此对象。在有其他账号与您创建了多个委托关系，即您是被委托方，需要将委托中的权限授权给不同的用户组，这些用户组中的IAM用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托。例：<br>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]} |

表 5-441 role.policy.Statement.Resource

| 参数  | 参数类型             | 描述                                                                                                       |
|-----|------------------|----------------------------------------------------------------------------------------------------------|
| uri | Array of strings | 委托资源的URI，长度不超过128。格式为：/iam/agencies/委托ID。例：<br>"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"] |

## 请求示例

修改名为“IAMAgencyPolicy”的委托自定义策略。策略表示作用范围为全局服务，委托资源的URI是/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c。

PATCH https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles/{role\_id}

```
{
 "role": {
 "display_name": "IAMAgencyPolicy",
 "type": "AX",
 "description": "IAMDescription",
 "description_cn": "中文描述",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:agencies:assume"
]
 }
]
 }
 }
}
```

```
],
 "Resource": {
 "uri": [
 "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
]
 }
 }
}
}
}
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "role": {
 "catalog": "CUSTOMED",
 "display_name": "IAMAgencyPolicy",
 "description": "IAMDescription",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/roles/f67224e84dc849ab954ce29fb4f47f8e"
 },
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "iam:agencies:assume"
],
 "Resource": {
 "uri": [
 "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
]
 },
 "Effect": "Allow"
 }
]
 },
 "description_cn": "中文描述",
 "domain_id": "d78cbac186b744899480f25b...",
 "type": "AX",
 "id": "f67224e84dc849ab954ce29fb4f47f8e",
 "name": "custom_d78cbac186b744899480f25bd022f468_0"
 }
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.9.7 删除自定义策略

### 功能介绍

该接口可以用于[管理员](#)删除自定义策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-ROLE/roles/{role\_id}

表 5-442 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                             |
|---------|------|--------|------------------------------------------------|
| role_id | 是    | String | 待删除的自定义策略ID，获取方式请参见： <a href="#">自定义策略ID</a> 。 |

### 请求参数

表 5-443 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-444 响应 Body 参数

| 参数      | 参数类型   | 描述    |
|---------|--------|-------|
| message | String | 响应信息。 |

## 请求示例

删除自定义策略。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-ROLE/roles/{role_id}
```

## 响应示例

```
{
 "message": "Delete success"
}
```

## 返回值

| 返回值 | 描述      |
|-----|---------|
| 200 | 删除成功。   |
| 400 | 参数无效。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 内部服务错误。 |

## 错误码

无

## 5.10 委托管理

### 5.10.1 查询指定条件下的委托列表

#### 功能介绍

该接口可以用于[管理员](#)查询指定条件下的委托列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-AGENCY/agencies

表 5-445 Query 参数

| 参数              | 是否必选 | 参数类型    | 描述                                                                                                                           |
|-----------------|------|---------|------------------------------------------------------------------------------------------------------------------------------|
| domain_id       | 是    | String  | 委托方账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。<br><b>说明</b><br>X-Auth-Token字段填写拥有策略权限的token时，domain_id非必选。 |
| name            | 否    | String  | 委托名，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                                 |
| trust_domain_id | 否    | String  | 被委托方账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。                                                            |
| page            | 否    | Integer | 分页查询时数据的页数，查询值最小为1。需要与per_page同时存在。                                                                                          |
| per_page        | 否    | Integer | 分页查询时每页的数据个数，取值范围为[1,500]。需要与page同时存在。                                                                                       |

## 请求参数

表 5-446 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | 拥有Security Administrator权限或策略权限的token。  |

## 响应参数

表 5-447 响应 Body 参数

| 参数              | 参数类型             | 描述      |
|-----------------|------------------|---------|
| <b>agencies</b> | Array of objects | 委托信息列表。 |

表 5-448 agencies

| 参数                | 参数类型   | 描述                                                                                                            |
|-------------------|--------|---------------------------------------------------------------------------------------------------------------|
| create_time       | String | 委托创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。             |
| description       | String | 委托描述信息。                                                                                                       |
| domain_id         | String | 委托方账号ID。                                                                                                      |
| duration          | String | 委托的期限。取值为"FOREVER"或“null”表示委托的期限为永久，取值为"ONEDAY"表示委托的期限为一天。                                                    |
| expire_time       | String | 委托过期时间。“null”表示不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |
| id                | String | 委托ID。                                                                                                         |
| name              | String | 委托名。                                                                                                          |
| agency_urn        | String | 委托URN。                                                                                                        |
| trust_domain_id   | String | 被委托方账号ID。                                                                                                     |
| trust_domain_name | String | 被委托方账号名。                                                                                                      |

## 请求示例

查询指定条件下的委托列表。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/agencies?domain_id=0ae9c6993a2e47bb8c4c7a9bb82...
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "agencies": [
 {
 "create_time": "2020-01-04T03:37:16.000000",
 "description": "",
 "domain_id": "d78cbac186b744899480f25b...8",
 "duration": "FOREVER",
 "expire_time": null,
 "id": "0760a9e2a60026664f1fc0031f9f2...",
 "name": "IAMAgency",
 "agency_urn": "iam::d78cbac186b744899480f25b...8:agency:IAMAgency",
 "trust_domain_id": "a2cd82a33fb043dc9304bf72...",
 "trust_domain_name": "IAMDomainB"
 }
]
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.2 查询委托详情

### 功能介绍

该接口可以用于[管理员](#)查询委托详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-AGENCY/agencies/{agency\_id}



表 5-449 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 待查询的委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-450 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                    |
|--------------|------|--------|-------------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                                                               |
| X-Auth-Token | 是    | String | 拥有iam:agencies:getAgency细粒度权限或Security Administrator权限的token。<br>了解更多细粒度权限，请参考： <a href="#">授权项</a> 。 |

## 响应参数

表 5-451 响应 Body 参数

| 参数                     | 参数类型   | 描述    |
|------------------------|--------|-------|
| <a href="#">agency</a> | object | 委托信息。 |

表 5-452 agency

| 参数          | 参数类型   | 描述                                                                                                |
|-------------|--------|---------------------------------------------------------------------------------------------------|
| create_time | String | 委托创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。 |
| description | String | 委托描述信息。                                                                                           |
| domain_id   | String | 委托方账号ID。                                                                                          |

| 参数                | 参数类型   | 描述                                                                                                                                                        |
|-------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| duration          | String | 委托的期限，单位为“小时”。 <ul style="list-style-type: none"> <li>FOREVER/null：表示委托的期限为永久。</li> <li>24：表示委托的期限为一天，即24小时。</li> <li>XXX：表示委托的期限为有限时间，如480小时。</li> </ul> |
| expire_time       | String | 委托过期时间。“null”表示不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                             |
| id                | String | 委托ID。                                                                                                                                                     |
| name              | String | 委托名。                                                                                                                                                      |
| agency_urn        | String | 委托URN。                                                                                                                                                    |
| trust_domain_id   | String | 被委托方账号ID。                                                                                                                                                 |
| trust_domain_name | String | 被委托方账号名。                                                                                                                                                  |

## 请求示例

查询委托详情。

GET https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/agencies/{agency\_id}

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "agency":{
 "create_time":"2020-01-04T03:37:16.000000",
 "description":"",
 "domain_id":"d78cbac186b744899480f25bd...8",
 "duration":"FOREVER",
 "id":"0760a9e2a60026664f1fc0031f9f205e",
 "name":"IAMAgency",
 "agency_urn": "iam::d78cbac186b744899480f25b...8:agency:IAMAgency",
 "trust_domain_id":"a2cd82a33fb043dc9304bf72...",
 "trust_domain_name":"IAMDomainB"
 }
}
```

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 200 | 请求成功。 |

| 返回值 | 描述        |
|-----|-----------|
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.3 创建委托

### 功能介绍

该接口可以用于[管理员](#)创建委托。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-AGENCY/agencies

### 请求参数

表 5-453 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-454 请求 Body 参数

| 参数            | 是否必选 | 参数类型   | 描述    |
|---------------|------|--------|-------|
| <b>agency</b> | 是    | object | 委托信息。 |

表 5-455 agency

| 参数                | 是否必选 | 参数类型   | 描述                                                                                                                                                                   |
|-------------------|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name              | 是    | String | 委托名，长度不大于64位。                                                                                                                                                        |
| domain_id         | 是    | String | 委托方账号ID。                                                                                                                                                             |
| trust_domain_id   | 否    | String | 被委托方账号ID。trust_domain_id和trust_domain_name至少填写一个，若都填写优先校验trust_domain_name。                                                                                          |
| trust_domain_name | 否    | String | 被委托方账号名。trust_domain_id和trust_domain_name至少填写一个，若都填写优先校验trust_domain_name。                                                                                           |
| description       | 否    | String | 委托描述信息，长度不大于255位。                                                                                                                                                    |
| duration          | 否    | String | 委托的期限，单位为“天”。默认为FOREVER。<br>取值范围： <ul style="list-style-type: none"> <li>FOREVER：表示委托的期限为永久。</li> <li>ONEDAY：表示委托的期限为一天。</li> <li>自定义天数：表示委托的期限为有限天数，如20。</li> </ul> |

## 响应参数

表 5-456 响应 Body 参数

| 参数            | 参数类型   | 描述    |
|---------------|--------|-------|
| <b>agency</b> | object | 委托信息。 |

表 5-457 agency

| 参数              | 参数类型   | 描述                                                                                                                                                        |
|-----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| create_time     | String | 委托创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                                         |
| description     | String | 委托描述信息。                                                                                                                                                   |
| domain_id       | String | 委托方账号ID。                                                                                                                                                  |
| duration        | String | 委托的期限，单位为“小时”。 <ul style="list-style-type: none"> <li>FOREVER/null：表示委托的期限为永久。</li> <li>24：表示委托的期限为一天，即24小时。</li> <li>XXX：表示委托的期限为有限时间，如480小时。</li> </ul> |
| expire_time     | String | 委托过期时间。“null”表示不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                             |
| id              | String | 委托ID。                                                                                                                                                     |
| name            | String | 委托名。                                                                                                                                                      |
| trust_domain_id | String | 被委托方账号ID。                                                                                                                                                 |

## 请求示例

创建一个名为“IAMAgency”的委托，被委托账号ID是c2cd82a33fb043dc9304bf72a...，账号名是IAMDomainB，委托的有效期限是永久。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/agencies
{
 "agency": {
 "name": "IAMAgency",
 "domain_id": "d78cbac186b744899480f25bd...",
 "trust_domain_id": "c2cd82a33fb043dc9304bf72a...",
 "trust_domain_name": "IAMDomainB",
 "duration": "FOREVER",
 "description": "IAMDescription"
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "agency": {
 "description": "IAMDescription",
 "trust_domain_id": "a2cd82a33fb043dc9304bf72a0f...",
 }
}
```

```
"id": "078ade0fc20010004f8fc0034fad529d",
"duration": "FOREVER",
"create_time": "2020-01-20T12:59:20.811642",
"expire_time": null,
"domain_id": "d78cbac186b744899480f25bd02...",
"name": "IAMAgency"
}
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 201 | 创建成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 409 | 资源冲突。     |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.4 修改委托

### 功能介绍

该接口可以用于[管理员](#)修改委托。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-AGENCY/agencies/{agency\_id}

表 5-458 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 待修改的委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-459 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-460 请求 Body 参数

| 参数                     | 是否必选 | 参数类型   | 描述    |
|------------------------|------|--------|-------|
| <a href="#">agency</a> | 是    | object | 委托信息。 |

表 5-461 agency

| 参数                | 是否必选 | 参数类型   | 描述                                                                                 |
|-------------------|------|--------|------------------------------------------------------------------------------------|
| trust_domain_id   | 否    | String | 被委托方账号ID。如果trust_domain_id和trust_domain_name都填写，则优先校验trust_domain_name。四个参数至少填写一个。 |
| trust_domain_name | 否    | String | 被委托方账号名。如果trust_domain_id和trust_domain_name都填写，则优先校验trust_domain_name。四个参数至少填写一个。  |
| description       | 否    | String | 委托描述信息，长度不大于255位。四个参数至少填写一个。                                                       |

| 参数       | 是否必选 | 参数类型   | 描述                                                                                                                                                                   |
|----------|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| duration | 否    | String | 委托的期限，单位为“天”。四个参数至少填写一个。<br>取值范围： <ul style="list-style-type: none"> <li>FOREVER：表示委托的期限为永久。</li> <li>ONEDAY：表示委托的期限为一天。</li> <li>自定义天数：表示委托的期限为有限天数，如20。</li> </ul> |

## 响应参数

表 5-462 响应 Body 参数

| 参数            | 参数类型   | 描述    |
|---------------|--------|-------|
| <b>agency</b> | object | 委托信息。 |

表 5-463 agency

| 参数          | 参数类型   | 描述                                                                                                                                                        |
|-------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| create_time | String | 委托创建时间。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                                         |
| description | String | 委托描述信息。                                                                                                                                                   |
| domain_id   | String | 委托方账号ID。                                                                                                                                                  |
| duration    | String | 委托的期限，单位为“小时”。 <ul style="list-style-type: none"> <li>FOREVER/null：表示委托的期限为永久。</li> <li>24：表示委托的期限为一天，即24小时。</li> <li>XXX：表示委托的期限为有限时间，如480小时。</li> </ul> |
| expire_time | String | 委托过期时间。“null”表示不过期。<br><b>说明</b><br>UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssss，日期和时间戳格式如：2023-06-28T08:56:33.710000。                                             |
| id          | String | 委托ID。                                                                                                                                                     |
| name        | String | 委托名。                                                                                                                                                      |



| 参数              | 参数类型   | 描述        |
|-----------------|--------|-----------|
| trust_domain_id | String | 被委托方账号ID。 |

## 请求示例

修改委托的有效时间为1天。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/agencies/{agency_id}
{
 "agency": {
 "trust_domain_id": "b2cd82a33fb043dc9304bf72...",
 "trust_domain_name": "IAMDomainB",
 "description": "IAMDescription",
 "duration": "ONEDAY"
 }
}
```

## 响应示例

状态码为 200 时:

修改成功。

```
{
 "agency": {
 "description": "IAMDescription",
 "trust_domain_id": "b2cd82a33fb043dc9304bf72a0...",
 "id": "0760a9e2a60026664f1fc0031f9f205e",
 "duration": "ONEDAY",
 "create_time": "2020-01-04T03:37:16.000000",
 "expire_time": "2020-01-21T13:06:11.241588",
 "domain_id": "d78cbac186b744899480f25...",
 "name": "IAMAgency"
 }
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 修改成功。     |
| 400 | 参数无效。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.5 删除委托

### 功能介绍

该接口可以用于[管理员](#)删除委托。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-AGENCY/agencies/{agency\_id}

表 5-464 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 待删除的委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-465 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

### 响应参数

无

### 请求示例

删除委托。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/agencies/{agency_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.6 查询全局服务中的委托权限

### 功能介绍

该接口可以用于[管理员](#)查询全局服务中的委托权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-AGENCY/domains/{domain\_id}/agencies/{agency\_id}/roles

表 5-466 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                               |
|-----------|------|--------|------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。    |
| domain_id | 是    | String | 委托方账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-467 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-468 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |

表 5-469 roles

| 参数                    | 参数类型   | 描述                                     |
|-----------------------|--------|----------------------------------------|
| domain_id             | String | 权限所属账号ID。                              |
| flag                  | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。      |
| description_cn        | String | 权限的中文描述信息。                             |
| catalog               | String | 权限所在目录。                                |
| name                  | String | 权限名。携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。 |
| description           | String | 权限描述信息。                                |
| <a href="#">links</a> | Object | 权限的资源链接信息。                             |
| id                    | String | 权限ID。                                  |
| display_name          | String | 权限展示名。                                 |

| 参数            | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|---------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type          | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b> | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time  | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |
| created_time  | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

表 5-470 roles.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-471 roles.policy

| 参数               | 参数类型             | 描述              |
|------------------|------------------|-----------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。      |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。 |

| 参数      | 参数类型   | 描述                                                                                                                                                                                  |
|---------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version | String | <p>权限版本号。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-472 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-473 roles.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                                                                     |
|--------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | <p>授权项, 指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为: 服务名:资源类型:操作, 例: vpc:ports:create。</li> <li>服务名为产品名称, 例如ecs、evs和vpc等, 服务名仅支持小写。资源类型和操作没有大小写, 要求支持通配符号*, 无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时, 该字段值为: "Action": ["iam:agencies:assume"]。</li> </ul> |
| Effect | String           | <p>作用。包含两种: 允许 ( Allow ) 和拒绝 ( Deny ), 既有Allow又有Deny的授权语句时, 遵循Deny优先的原则。</p> <p>取值范围:</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                        |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                                           |
|-----------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Object | <p>限制条件。了解更多相关参数，请参考：<a href="#">配置自定义策略</a>。</p> <p><b>说明</b><br/>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                                   |
| Resource  | Object | <p>资源。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs:::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<code>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</code>。</li> </ul> |

## 请求示例

查询全局服务中的委托权限。

GET `https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles`

## 响应示例

状态码为 200 时:

请求成功。

```

{
 "roles": [
 {
 "flag": "fine_grained",
 "display_name": "CDN Domain Viewer",
 "description": "Allow Query Domains",
 "name": "system_all_11",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "cdn:configuration:queryDomains",
 "cdn:configuration:queryOriginServerInfo",
 "cdn:configuration:queryOriginConfInfo",
 "cdn:configuration:queryHttpsConf",
 "cdn:configuration:queryCacheRule",
 "cdn:configuration:queryReferConf",
 "cdn:configuration:queryChargeMode",
 "cdn:configuration:queryCacheHistoryTask",
 "cdn:configuration:queryIpAcl",
 "cdn:configuration:queryResponseHeaderList"
]
 }
]
 }
 }
],
}

```

```
 "Effect": "Allow"
 }
]
 },
 "description_cn": "查询域名信息",
 "domain_id": null,
 "type": "AX",
 "catalog": "CDN",
 "id": "db4259cce0ce47c9903dfdc195eb453b"
}
]
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.7 查询项目服务中的委托权限

### 功能介绍

该接口可以用于[管理员](#)查询项目服务中的委托权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-AGENCY/projects/{project\_id}/agencies/{agency\_id}/roles



表 5-474 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                 |
|------------|------|--------|--------------------------------------------------------------------|
| agency_id  | 是    | String | 委托ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| project_id | 是    | String | 委托方的项目ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-475 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                         |
|--------------|------|--------|------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                    |
| X-Auth-Token | 是    | String | 访问令牌, 承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-476 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |

表 5-477 roles

| 参数             | 参数类型   | 描述                                 |
|----------------|--------|------------------------------------|
| domain_id      | String | 权限所属账号ID。                          |
| flag           | String | 该参数值为fine_grained时, 标识此权限为系统内置的策略。 |
| description_cn | String | 权限的中文描述信息。                         |
| catalog        | String | 权限所在目录。                            |

| 参数            | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|---------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name          | String | 权限名。携带在用户的token中，云服务根据该名称来判断用户是否有权限访问。                                                                                                                                                                                                                                      |
| description   | String | 权限描述信息。                                                                                                                                                                                                                                                                     |
| <b>links</b>  | Object | 权限的资源链接信息。                                                                                                                                                                                                                                                                  |
| id            | String | 权限ID。                                                                                                                                                                                                                                                                       |
| display_name  | String | 权限展示名。                                                                                                                                                                                                                                                                      |
| type          | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |
| <b>policy</b> | Object | 权限的具体内容。                                                                                                                                                                                                                                                                    |
| updated_time  | String | 权限更新时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |
| created_time  | String | 权限创建时间。<br><b>说明</b><br>UNIX时间戳格式，单位是毫秒，时间戳格式如：1687913793000。                                                                                                                                                                                                               |

表 5-478 roles.links

| 参数       | 参数类型   | 描述                    |
|----------|--------|-----------------------|
| self     | String | 资源链接地址。               |
| previous | String | 前一邻接资源链接地址，不存在时为null。 |
| next     | String | 后一邻接资源链接地址，不存在时为null。 |

表 5-479 roles.policy

| 参数             | 参数类型             | 描述         |
|----------------|------------------|------------|
| <b>Depends</b> | Array of objects | 该权限所依赖的权限。 |

| 参数               | 参数类型             | 描述                                                                                                                                                                     |
|------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                        |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-480 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-481 roles.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                     |
|--------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | 授权项，指对资源的具体操作权限。<br><b>说明</b> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul> |
| Effect | String           | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。<br>取值范围： <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                             |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                             |
|-----------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Object | <p>限制条件。了解更多相关参数，请参考：<a href="#">配置自定义策略</a>。</p> <p><b>说明</b><br/>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                     |
| Resource  | Object | <p>资源。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为："Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}。</li> </ul> |

## 请求示例

查询项目服务中的委托权限。

GET https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/projects/{project\_id}/agencies/{agency\_id}/roles

## 响应示例

状态码为 200 时:

请求成功。

```

{
 "roles": [
 {
 "domain_id": null,
 "flag": "fine_grained",
 "description_cn": "应用运维管理服务只读权限",
 "catalog": "AOM",
 "name": "system_all_30",
 "description": "AOM read only",
 "id": "75cfe22af2b3498d82b655fbb39de498",
 "display_name": "AOM Viewer",
 "type": "XA",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "aom:*:list",
 "aom:*:get",
 "apm:*:list",
 "apm:*:get"
],
 "Effect": "Allow"
 }
]
 }
 }
]
}

```

```
}
]
 }
 }
]
}
```

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.8 为委托授予全局服务权限

### 功能介绍

该接口可以用于[管理员](#)为委托授予全局服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

URL中role\_id对应的权限由黑名单控制，不能是te\_agency。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-AGENCY/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}

表 5-482 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。    |
| domain_id | 是    | String | 委托方账号ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 全局服务权限ID, 获取方式请参见: <a href="#">获取权限ID</a> 。                       |

## 请求参数

表 5-483 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                         |
|--------------|------|--------|------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                    |
| X-Auth-Token | 是    | String | 访问令牌, 承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为委托授予全局服务权限。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述    |
|-----|-------|
| 204 | 授权成功。 |

| 返回值 | 描述        |
|-----|-----------|
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.9 为委托授予项目服务权限

### 功能介绍

该接口可以用于[管理员](#)为委托授予项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

URL中role\_id对应的权限由黑名单控制，不能是secu\_admin、te\_agency。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-AGENCY/projects/{project\_id}/agencies/{agency\_id}/roles/{role\_id}

表 5-484 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                |
|------------|------|--------|-------------------------------------------------------------------|
| agency_id  | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| project_id | 是    | String | 委托方的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id    | 是    | String | 项目服务权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                        |

## 请求参数

表 5-485 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为委托授予项目服务权限。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 授权成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无



## 5.10.10 查询委托是否拥有全局服务权限

### 功能介绍

该接口可以用于[管理员](#)查询委托是否拥有全局服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

HEAD /v3.0/OS-AGENCY/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}

表 5-486 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                               |
|-----------|------|--------|------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。    |
| domain_id | 是    | String | 委托方账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 全局服务权限ID。获取方式请参见： <a href="#">获取权限ID</a> 。                       |

### 请求参数

表 5-487 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

查询委托是否拥有全局服务权限。

```
HEAD https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述            |
|-----|---------------|
| 204 | 查询成功。（具有指定权限） |
| 401 | 认证失败。         |
| 403 | 没有操作权限。       |
| 404 | 未找到相应的资源。     |
| 500 | 内部服务错误。       |

## 错误码

无

## 5.10.11 查询委托是否拥有项目服务权限

### 功能介绍

该接口可以用于[管理员](#)查询委托是否拥有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

```
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

表 5-488 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                 |
|------------|------|--------|--------------------------------------------------------------------|
| agency_id  | 是    | String | 委托ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| project_id | 是    | String | 委托方的项目ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id    | 是    | String | 项目服务权限ID, 获取方式请参见: <a href="#">获取权限ID</a> 。                        |

## 请求参数

表 5-489 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                      |
|--------------|------|--------|-----------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。 |
| X-Auth-Token | 是    | String | 已认证的拥有Security Administrator权限的token。   |

## 响应参数

无

## 请求示例

查询委托是否拥有项目服务权限。

```
HEAD https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述            |
|-----|---------------|
| 204 | 查询成功。(具有指定权限) |
| 401 | 认证失败。         |

| 返回值 | 描述        |
|-----|-----------|
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.12 移除委托的全局服务权限

### 功能介绍

该接口可以用于[管理员](#)移除委托的全局服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-AGENCY/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}

表 5-490 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                               |
|-----------|------|--------|------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。    |
| domain_id | 是    | String | 委托方账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 全局服务权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                       |

## 请求参数

表 5-491 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除委托的全局服务权限。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.13 移除委托的项目服务权限

### 功能介绍

该接口可以用于[管理员](#)移除委托的项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-AGENCY/projects/{project\_id}/agencies/{agency\_id}/roles/{role\_id}

表 5-492 路径参数

| 参数         | 是否必选 | 参数类型   | 描述                                                                |
|------------|------|--------|-------------------------------------------------------------------|
| agency_id  | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| project_id | 是    | String | 委托方的项目ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id    | 是    | String | 项目服务权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                        |

### 请求参数

表 5-493 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                   |
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除委托的项目服务权限。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

## 响应示例

无

## 返回值

| 返回值 | 描述        |
|-----|-----------|
| 204 | 删除成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

无

## 5.10.14 查询委托下的所有项目服务权限列表

### 功能介绍

该接口可以用于[管理员](#)查询委托所有项目服务权限列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

```
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/
inherited_to_projects
```

表 5-494 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。    |
| domain_id | 是    | String | 委托方账号ID, 获取方式请参见: <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-495 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                         |
|--------------|------|--------|------------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌, 承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-496 响应 Body 参数

| 参数                    | 参数类型             | 描述      |
|-----------------------|------------------|---------|
| <a href="#">roles</a> | Array of objects | 权限信息列表。 |
| <a href="#">links</a> | object           | 资源链接信息。 |

表 5-497 roles

| 参数                    | 参数类型   | 描述         |
|-----------------------|--------|------------|
| id                    | String | 权限ID。      |
| <a href="#">links</a> | object | 权限的资源链接信息。 |
| name                  | String | 权限名。       |



表 5-498 links

| 参数   | 参数类型   | 描述      |
|------|--------|---------|
| self | String | 资源链接地址。 |

## 请求示例

查询委托下的所有项目服务权限列表。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/
inherited_to_projects
```

## 响应示例

状态码为 200 时:

查询成功

```
{
 "roles": [
 {
 "name": "system_all_154",
 "links": {
 "self": "https://internal.iam.ctcclouddev.com/v3/roles/04570dfe267c45a3940e1ae9de868..."
 },
 "id": "04570dfe267c45a3940e1ae9de868..."
 },
 {
 "name": "test1_admin",
 "links": {
 "self": "https://internal.iam.ctcclouddev.com/v3/roles/1bf20f1adba94747a6e02e1be3810..."
 },
 "id": "1bf20f1adba94747a6e02e1be3810..."
 }
],
 "links": {
 "self": "https://internal.iam.ctcclouddev.com/v3.0/OSHERIT/domains/
05b09b4723001dc90f27c0008f8b1.../agencies/08c6652e86801d234f01c00078308.../roles/
inherited_to_projects"
 }
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 查询成功      |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.10.15 为委托授予所有项目服务权限

### 功能介绍

该接口可以用于[管理员](#)为委托授予所有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 接口约束

URL中role\_id对应的权限由黑名单控制，不能是te\_agency。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-INHERIT/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-499 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| domain_id | 是    | String | 委托方的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                            |

## 请求参数

表 5-500 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

为委托授予所有项目服务权限。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

无

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 204 | 授权成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.10.16 检查委托下是否具有所有项目服务权限

### 功能介绍

该接口可以用于[管理员](#)检查委托是否具有所有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

HEAD /v3.0/OS-INHERIT/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-501 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| domain_id | 是    | String | 委托方的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                            |

## 请求参数

表 5-502 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

检查委托下是否具有所有项目服务权限。

```
HEAD https://iam.myhuaweicloud.com/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

无

## 状态码

| 状态码 | 描述            |
|-----|---------------|
| 204 | 查询成功。（具有指定权限） |
| 401 | 认证失败。         |
| 403 | 没有操作权限。       |
| 404 | 未找到相应的资源。     |
| 500 | 内部服务错误。       |

## 错误码

请参见[错误码](#)。

### 5.10.17 移除委托下的所有项目服务权限

#### 功能介绍

该接口可以用于[管理员](#)移除委托的所有项目服务权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

DELETE /v3.0/OS-INHERIT/domains/{domain\_id}/agencies/{agency\_id}/roles/{role\_id}/inherited\_to\_projects

表 5-503 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| agency_id | 是    | String | 委托ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。     |
| domain_id | 是    | String | 委托方的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |
| role_id   | 是    | String | 权限ID，获取方式请参见： <a href="#">获取权限ID</a> 。                            |

## 请求参数

表 5-504 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

无

## 请求示例

移除委托下的所有项目服务权限。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

## 响应示例

无

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 204 | 移除成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.11 企业项目管理

## 5.11.1 查询企业项目关联的用户组

### 功能介绍

该接口可用于查询企业项目直接关联的用户组。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/groups

表 5-505 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述           |
|-----------------------|------|--------|--------------|
| enterprise_project_id | 是    | String | 待查询的企业项目的ID。 |

### 请求参数

表 5-506 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                                      |
|--------------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listGroupsOnEnterpriseProject细粒度权限或 Security Administrator权限的 token。同时要求 enterprise_project_id所属账号的domain_id与Token中的domain_id一致。 |

### 响应参数

状态码为 200 时：

表 5-507 响应 Body 参数

| 参数            | 参数类型             | 描述     |
|---------------|------------------|--------|
| <b>groups</b> | Array of objects | 用户组信息。 |

表 5-508 groups

| 参数          | 参数类型    | 描述       |
|-------------|---------|----------|
| createTime  | Integer | 用户组创建时间。 |
| description | String  | 用户组描述。   |
| domainId    | String  | 账号ID。    |
| id          | String  | 用户组ID。   |
| name        | String  | 用户组名称。   |

## 请求示例

查询企业项目关联的用户组。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups
```

## 响应示例

状态码： 200

请求成功。

```
{
 "groups": [{
 "createTime": 1552093271000,
 "description": null,
 "domainId": "dc7f62ae236c47b8836014c16d64d...",
 "id": "e6bde2403bda43e2813a1a6848963...",
 "name": "auth"
 }]
}
```

## 状态码

| 状态码 | 描述                |
|-----|-------------------|
| 200 | 请求成功。             |
| 400 | 请求参数出错。           |
| 401 | 认证失败。             |
| 403 | 没有操作权限。           |
| 404 | 找不到指定资源。          |
| 415 | Content type校验错误。 |
| 500 | 内部系统异常。           |



## 错误码

请参见[错误码](#)。

## 5.11.2 查询企业项目关联用户组的权限

### 功能介绍

该接口可用于查询企业项目直接关联用户组的权限

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles

表 5-509 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述         |
|-----------------------|------|--------|------------|
| enterprise_project_id | 是    | String | 待查询企业项目ID。 |
| group_id              | 是    | String | 待查询用户组ID。  |

### 请求参数

表 5-510 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                               |
|--------------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listRolesForGroupOnEnterpriseProject细粒度权限或Security Administrator 权限的token。同时要求 group_id所属账号的domain_id与Token中的domain_id一致。 |

### 响应参数

状态码为 200 时:

表 5-511 响应 Body 参数

| 参数           | 参数类型             | 描述    |
|--------------|------------------|-------|
| <b>roles</b> | Array of objects | 角色列表。 |

表 5-512 roles

| 参数             | 参数类型   | 描述                                                                                                                                                                                                                                                                          |
|----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catalog        | String | 权限所在目录。                                                                                                                                                                                                                                                                     |
| display_name   | String | 权限展示名称。                                                                                                                                                                                                                                                                     |
| description    | String | 权限的英文描述信息。                                                                                                                                                                                                                                                                  |
| description_cn | String | 权限的中文描述信息。                                                                                                                                                                                                                                                                  |
| domain_id      | String | 权限所属账号ID。                                                                                                                                                                                                                                                                   |
| flag           | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                           |
| id             | String | 权限ID。                                                                                                                                                                                                                                                                       |
| name           | String | 权限名称。                                                                                                                                                                                                                                                                       |
| <b>policy</b>  | object | 权限具体内容。                                                                                                                                                                                                                                                                     |
| type           | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或者在domain层和project层都不显示（XX）。</li> </ul> |

表 5-513 roles.policy

| 参数               | 参数类型             | 描述              |
|------------------|------------------|-----------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。      |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。 |

| 参数      | 参数类型   | 描述                                                                                                                                                                                  |
|---------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version | String | <p>权限版本号。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>1.0: 系统预置的角色。以服务为粒度, 提供有限的服务相关角色用于授权。</li> <li>1.1: 策略。IAM最新提供的一种细粒度授权的能力, 可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-514 roles.policy.Depends

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名。  |

表 5-515 roles.policy.Statement

| 参数     | 参数类型             | 描述                                                                                                                                                                                                                                                                                                                     |
|--------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action | Array of strings | <p>授权项, 指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>格式为: 服务名:资源类型:操作, 例: vpc:ports:create。</li> <li>服务名为产品名称, 例如ecs、evs和vpc等, 服务名仅支持小写。资源类型和操作没有大小写, 要求支持通配符号*, 无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时, 该字段值为: "Action": ["iam:agencies:assume"]。</li> </ul> |
| Effect | String           | <p>作用。包含两种: 允许 ( Allow ) 和拒绝 ( Deny ), 既有Allow又有Deny的授权语句时, 遵循Deny优先的原则。</p> <p>枚举值:</p> <ul style="list-style-type: none"> <li>Allow</li> <li>Deny</li> </ul>                                                                                                                                                         |

| 参数        | 参数类型   | 描述                                                                                                                                                                                                                                                                                                             |
|-----------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | Object | <p>限制条件。了解更多相关参数，请参考：<a href="#">配置自定义策略</a>。</p> <p><b>说明</b><br/>以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。</p> <pre> "Condition": {   "StringEquals": {     "obs:prefix": [       "public"     ]   } }                     </pre>                                                     |
| Resource  | Object | <p>资源。规则如下：</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>• region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>• 当该自定义策略为委托自定义策略时，该字段类型为Object，值为："Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}。</li> </ul> |

## 请求示例

查询企业项目关联用户组的权限。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles
```

## 响应示例

**状态码： 200**

请求成功

```

{
 "roles": [{
 "catalog": "CUSTOMED",
 "description": "u81eau5b9au4e49u6743u9...",
 "description_cn": null,
 "display_name": "XpBdkPYCCx",
 "domain_id": "0456fd5a278033120f37c006683ab...",
 "flag": null,
 "id": "5d1b6256331f4fb494534bf240698...",
 "name": "custom_policy1",
 "policy": {
 "Statement": [{
 "Action": ["aaa:a*b:baa*"],
 "Condition": null,
 "Effect": "deny",
 "Resource": null
 }, {
 "Action": ["aaa:a*b:bab*"],
 "Condition": null,
 "Effect": "Allow",
 "Resource": null
 }
]
 }
}

```

```
"Version": "1.1"
},
"type": "XA"
}]
}
```

## 状态码

| 状态码 | 描述                |
|-----|-------------------|
| 200 | 请求成功。             |
| 400 | 请求参数出错。           |
| 401 | 认证失败。             |
| 403 | 没有操作权限。           |
| 404 | 未找到相应的资源。         |
| 415 | Content type校验错误。 |
| 500 | 内部系统异常。           |

## 错误码

请参见[错误码](#)。

### 5.11.3 基于用户组为企业项目授权

#### 功能介绍

该接口用于给指定ID的企业项目授权，建立企业项目、用户组和权限的绑定关系。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles/{role\_id}

表 5-516 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |
| group_id              | 是    | String | 用户组ID。  |

| 参数      | 是否必选 | 参数类型   | 描述                                                                      |
|---------|------|--------|-------------------------------------------------------------------------|
| role_id | 是    | String | 角色ID。<br><b>说明</b><br>请确认该角色支持为企业项目授权。查看 <a href="#">支持企业项目授权的云服务</a> 。 |

## 请求参数

表 5-517 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                                        |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:grantRoleToGroupOnEnterpriseProject 细粒度权限或 Security Administrator 权限的 token。同时要求 group_id 所属账号的 domain_id 与 Token 中的 domain_id 一致。 |

## 响应参数

无

## 请求示例

基于用户组为企业项目授权。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 状态码

| 状态码 | 描述                 |
|-----|--------------------|
| 204 | 请求响应成功。            |
| 400 | 请求消息格式非法。          |
| 401 | token 认证失败。        |
| 403 | 禁止操作，权限不够。         |
| 415 | Content type 校验错误。 |

| 状态码 | 描述      |
|-----|---------|
| 500 | 内部系统异常。 |

## 错误码

请参见[错误码](#)。

## 5.11.4 删除企业项目关联用户组的权限

### 功能介绍

该接口用于删除企业项目关联用户组的权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles/{role\_id}

表 5-518 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |
| group_id              | 是    | String | 用户组ID。  |
| role_id               | 是    | String | 权限ID。   |

## 请求参数

表 5-519 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                                           |
|--------------|------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:revokeRoleFromGroupOnEnterpriseProject 细粒度权限或 Security Administrator 权限的 token。同时要求 group_id 所属账号的 domain_id 与 Token 中的 domain_id 一致。 |

## 响应参数

无

## 请求示例

删除企业项目关联用户组的权限。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}
```

## 响应示例

无

## 状态码

| 状态码 | 描述                 |
|-----|--------------------|
| 204 | 请求响应成功。            |
| 400 | 请求消息格式非法。          |
| 401 | token 认证失败。        |
| 403 | 禁止操作，权限不够。         |
| 404 | 操作资源不存在。           |
| 415 | Content type 校验错误。 |
| 500 | 内部系统异常。            |

## 错误码

请参见[错误码](#)。



## 5.11.5 查询用户组关联的企业项目

### 功能介绍

该接口可用于查询用户组所关联的企业项目。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-PERMISSION/groups/{group\_id}/enterprise-projects

表 5-520 路径参数

| 参数       | 是否必选 | 参数类型   | 描述        |
|----------|------|--------|-----------|
| group_id | 是    | String | 待查询用户组ID。 |

### 请求参数

表 5-521 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                          |
|--------------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listEnterpriseProjectsForGroup细粒度权限或 Security Administrator权限的 token。同时要求group_id所属账号的domain_id与Token中的 domain_id一致。 |

### 响应参数

状态码为 200 时：

表 5-522 响应 Body 参数

| 参数                                  | 参数类型             | 描述      |
|-------------------------------------|------------------|---------|
| <a href="#">enterprise-projects</a> | Array of objects | 企业项目信息。 |

表 5-523 enterprise-projects

| 参数        | 参数类型   | 描述    |
|-----------|--------|-------|
| projectId | String | 项目ID。 |

## 请求示例

查询用户组关联的企业项目。

GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/groups/{group\_id}/enterprise-projects

## 响应示例

状态码： 200

请求成功。

```
{
 "enterprise-projects" : [{
 "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
 }]
}
```

## 状态码

| 状态码 | 描述                |
|-----|-------------------|
| 200 | 请求成功。             |
| 400 | 请求参数出错。           |
| 401 | 认证失败。             |
| 403 | 没有操作权限。           |
| 404 | 未找到相应的资源。         |
| 415 | Content type校验错误。 |
| 500 | 内部系统异常。           |

## 错误码

请参见[错误码](#)。

## 5.11.6 查询用户直接关联的企业项目

### 功能介绍

该接口可用于查询用户直接关联的企业项目。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-PERMISSION/users/{user\_id}/enterprise-projects

表 5-524 路径参数

| 参数      | 是否必选 | 参数类型   | 描述       |
|---------|------|--------|----------|
| user_id | 是    | String | 待查询用户ID。 |

## 请求参数

表 5-525 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                                 |
|--------------|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listEnterpriseProjectsForUser 细粒度权限或 Security Administrator 权限的 token。同时要求 user_id 所属账号的 domain_id 与 Token 中的 domain_id 一致。 |

## 响应参数

状态码为 200 时:

表 5-526 响应 Body 参数

| 参数                                  | 参数类型             | 描述      |
|-------------------------------------|------------------|---------|
| <a href="#">enterprise-projects</a> | Array of objects | 企业项目信息。 |

表 5-527 enterprise-projects

| 参数        | 参数类型   | 描述    |
|-----------|--------|-------|
| projectId | String | 项目ID。 |

## 请求示例

查询用户直接关联的企业项目。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects
```

## 响应示例

**状态码： 200**

请求成功。

```
{
 "enterprise-projects" : [{
 "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
 }, {
 "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
 }]
}
```

## 状态码

| 状态码 | 描述                |
|-----|-------------------|
| 200 | 请求成功。             |
| 400 | 请求参数出错。           |
| 401 | 认证失败。             |
| 403 | 没有操作权限。           |
| 404 | 未找到相应的资源。         |
| 415 | Content type校验错误。 |
| 500 | 内部系统异常。           |

## 错误码

请参见[错误码](#)。

## 5.11.7 查询企业项目直接关联用户

### 功能介绍

该接口可用于查询企业项目直接关联的用户。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/users

表 5-528 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述         |
|-----------------------|------|--------|------------|
| enterprise_project_id | 是    | String | 待查询企业项目ID。 |

## 请求参数

表 5-529 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                          |
|--------------|------|--------|---------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listUsersForEnterpriseProject细粒度权限或 Security Administrator权限的 token。 |

## 响应参数

状态码： 200

表 5-530 响应 Body 参数

| 参数           | 参数类型             | 描述    |
|--------------|------------------|-------|
| <b>users</b> | Array of objects | 用户信息。 |

表 5-531 users

| 参数          | 参数类型    | 描述                                   |
|-------------|---------|--------------------------------------|
| domain_id   | String  | 授权用户所属账号ID。                          |
| id          | String  | 授权用户ID。                              |
| name        | String  | 授权用户名。                               |
| enabled     | Boolean | 授权用户是否启用，true表示启用，false表示停用，默认为true。 |
| description | String  | 授权用户描述信息。                            |

| 参数                  | 参数类型    | 描述                    |
|---------------------|---------|-----------------------|
| policy_num          | Integer | 授权用户的策略数。             |
| lastest_policy_time | Long    | 用户最近与企业项目关联策略的时间（毫秒）。 |

## 请求示例

查询企业项目直接关联用户。

GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/users

## 响应示例

**状态码： 200**

请求成功。

```
{
 "users": [{
 "domain_id": "d78cbac186b744899480f25bd02...",
 "id": "07667db96a00265f1fc0c003a...",
 "name": "IAMUserA",
 "enabled": true,
 "description": "IAMDescriptionA",
 "policy_num": 2,
 "lastest_policy_time": 1589874427000
 }]
}
```

## 状态码

| 状态码 | 描述       |
|-----|----------|
| 200 | 请求成功。    |
| 400 | 请求参数出错。  |
| 401 | 认证失败。    |
| 403 | 没有操作权限。  |
| 404 | 未找到相关资源。 |
| 500 | 系统异常。    |

## 5.11.8 查询企业项目直接关联用户的权限

### 功能介绍

该接口可用于查询企业项目直接关联用户的权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/users/{user\_id}/roles

表 5-532 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |
| user_id               | 是    | String | 用户ID。   |

## 请求参数

表 5-533 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                  |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:listRolesForUserOnEnterpriseProject 细粒度权限或 Security Administrator 权限的 token。 |

## 响应参数

状态码： 200

表 5-534 响应 Body 参数

| 参数                    | 参数类型             | 描述    |
|-----------------------|------------------|-------|
| <a href="#">roles</a> | Array of objects | 角色列表。 |

表 5-535 RolesItem

| 参数           | 参数类型   | 描述      |
|--------------|--------|---------|
| catalog      | String | 权限所在目录。 |
| display_name | String | 权限展示名称。 |

| 参数             | 参数类型   | 描述                                                                                                                                                                                                                                                                         |
|----------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description    | String | 权限的英文描述。                                                                                                                                                                                                                                                                   |
| description_cn | String | 权限的中文描述信息。                                                                                                                                                                                                                                                                 |
| domain_id      | String | 权限所属账号ID。                                                                                                                                                                                                                                                                  |
| flag           | String | 该参数值为fine_grained时，标识此权限为系统内置的策略。                                                                                                                                                                                                                                          |
| id             | String | 权限Id。                                                                                                                                                                                                                                                                      |
| name           | String | 权限名称。                                                                                                                                                                                                                                                                      |
| <b>policy</b>  | object | 权限具体内容。                                                                                                                                                                                                                                                                    |
| type           | String | 权限的显示模式。<br><b>说明</b> <ul style="list-style-type: none"> <li>AX表示在domain层显示。</li> <li>XA表示在project层显示。</li> <li>AA表示在domain和project层均显示。</li> <li>XX表示在domain和project层均不显示。</li> <li>自定义策略的显示模式只能为AX或者XA，不能在domain层和project层都显示（AA），或在domain层和project层都不显示（XX）。</li> </ul> |

表 5-536 RolePolicy

| 参数               | 参数类型             | 描述                                                                                                                                                                   |
|------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Depends</b>   | Array of objects | 该权限所依赖的权限。                                                                                                                                                           |
| <b>Statement</b> | Array of objects | 授权语句，描述权限的具体内容。                                                                                                                                                      |
| Version          | String           | 权限版本号。<br><b>说明</b> <ul style="list-style-type: none"> <li>1.0：系统预置的角色。以服务为粒度，提供有限的服务相关角色用于授权。</li> <li>1.1：策略。IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。</li> </ul> |

表 5-537 PolicyDepends

| 参数      | 参数类型   | 描述      |
|---------|--------|---------|
| catalog | String | 权限所在目录。 |



| 参数           | 参数类型   | 描述     |
|--------------|--------|--------|
| display_name | String | 权限展示名。 |

表 5-538 PolicyStatement

| 参数        | 参数类型             | 描述                                                                                                                                                                                                                                                                                                     |
|-----------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | Array of strings | 授权项，指对资源的具体操作权限。支持的授权项请参考各云服务《API参考》中“权限和授权项”章节。<br><b>说明</b> <ul style="list-style-type: none"> <li>格式为：服务名:资源类型:操作，例：vpc:ports:create。</li> <li>服务名为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。资源类型和操作没有大小写，要求支持通配符号*，无需罗列全部授权项。</li> <li>当自定义策略为委托自定义策略时，该字段值为：<br/>"Action": ["iam:agencies:assume"]。</li> </ul> |
| Effect    | String           | 作用。包含两种：允许（Allow）和拒绝（Deny），既有Allow又有Deny的授权语句时，遵循Deny优先的原则。                                                                                                                                                                                                                                            |
| Condition | Object           | 限制条件。                                                                                                                                                                                                                                                                                                  |
| Resource  | Object           | 资源。规则如下：<br><b>说明</b> <ul style="list-style-type: none"> <li>可填 * 的五段式：:::，例："obs::bucket:*"。</li> <li>region字段为*或用户可访问的region。service必须存在且resource属于对应service。</li> <li>当该自定义策略为委托自定义策略时，该字段类型为Object，值为：<br/>"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}</li> </ul>      |

## 请求示例

查询企业项目直接关联用户的权限。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles
```

## 响应示例

状态码： 200

请求成功。

```
{
 "roles": [{
 "display_name": "Customed ECS Viewer",
```

```

 "description": "The read-only permissions to all ECS resources, which can be used for statistics and survey.",
 "domain_id": "9698542758bc422088c0c3eabfc30d...",
 "catalog": "CUSTOMED",
 "policy": {
 "Version": "1.1",
 "Statement": [{
 "Action": ["ecs:*:get*", "ecs:*:list*", "ecs:blockDevice:use", "ecs:serverGroups:manage",
"ecs:serverVolumes:use", "evs:*:get*", "evs:*:list*", "vpc:*:get*", "vpc:*:list*", "ims:*:get*", "ims:*:list*"],
 "Effect": "Allow"
 }]
 },
 "id": "24e7a89bffe443979760c4e9715c1...",
 "type": "XA",
 "name": "custom_9698542758bc422088c0c3eabfc30..."
 }]
}

```

## 状态码

| 状态码 | 描述       |
|-----|----------|
| 200 | 请求成功。    |
| 400 | 请求参数出错。  |
| 401 | 认证失败。    |
| 403 | 没有操作权限。  |
| 404 | 找不到指定资源。 |
| 500 | 系统异常。    |

## 5.11.9 基于用户为企业项目授权

### 功能介绍

该接口可以基于用户为企业项目授权。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

```
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}
```

表 5-539 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |
| user_id               | 是    | String | 用户ID。   |
| role_id               | 是    | String | 权限ID。   |

## 请求参数

表 5-540 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                 |
|--------------|------|--------|----------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:grantRoleToUserOnEnterpriseProject 细粒度权限或 Security Administrator 权限的 token。 |

## 响应参数

无

## 请求示例

基于用户为企业项目授权。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}
```

## 响应示例

**状态码： 400**

请求参数出错。

```
{
 "error": {
 "message": "Illegal request",
 "code": 400,
 "title": "Bad Request"
 }
}
```

**状态码： 401**

认证失败。

```
{
 "error": {
 "message": "Authentication failed",
 "code": 401,
 }
}
```

```
"title" : "Unauthorized"
}
}
```

**状态码： 403**

没有操作权限。

```
{
 "error" : {
 "message" : "Forbidden operation",
 "code" : 403,
 "title" : "Forbidden"
 }
}
```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 204 | 请求成功。   |
| 400 | 请求参数出错。 |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 系统异常。   |

## 5.11.10 删除企业项目直接关联用户的权限

### 功能介绍

该接口可以用于删除企业项目直接关联用户的权限。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise\_project\_id}/users/{user\_id}/roles/{role\_id}

**表 5-541** 路径参数

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |

| 参数      | 是否必选 | 参数类型   | 描述    |
|---------|------|--------|-------|
| user_id | 是    | String | 用户ID。 |
| role_id | 是    | String | 权限ID。 |

## 请求参数

表 5-542 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                    |
|--------------|------|--------|-------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:revokeRoleFromUserOnEnterpriseProject 细粒度权限或 Security Administrator 权限的 token。 |

## 响应参数

无

## 请求示例

删除企业项目直接关联用户的权限。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}
```

## 响应示例

无

## 状态码

| 状态码 | 描述       |
|-----|----------|
| 204 | 请求成功。    |
| 400 | 请求参数出错。  |
| 401 | 认证失败。    |
| 403 | 没有操作权限。  |
| 404 | 找不到指定资源。 |
| 500 | 系统异常。    |

## 5.11.11 基于委托为企业项目授权

### 功能介绍

该接口可以基于委托为企业项目授权。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments

### 请求参数

表 5-543 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                               |
|--------------|------|--------|--------------------------------------------------------------------------------------------------|
| Content-Type | 是    | String | 该字段内容填为“application/json;charset=utf8”。                                                          |
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:grantRoleToAgencyOnEnterpriseProject细粒度权限或Security Administrator权限的token。 |

表 5-544 请求 Body 参数

| 参数                               | 是否必选 | 参数类型             | 描述                      |
|----------------------------------|------|------------------|-------------------------|
| <a href="#">role_assignments</a> | 是    | Array of objects | 委托在企业项目上的绑定关系，最多支持250条。 |

表 5-545 role\_assignments

| 参数        | 是否必选 | 参数类型   | 描述    |
|-----------|------|--------|-------|
| agency_id | 是    | String | 委托ID。 |

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| enterprise_project_id | 是    | String | 企业项目ID。 |
| role_id               | 是    | String | 策略ID。   |

## 响应参数

无

## 请求示例

基于委托为企业项目授权。

```
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments
{
 "role_assignments": [
 {
 "agency_id": "as0d9f8asdfsdfa09sd8f9aaa",
 "enterprise_project_id": "3asdfs0d9f8asdfsdfa09sd8f9aaa",
 "role_id": "5s0d9f8dafsdfsdfa09sd8f9aaa"
 }
]
}
```

## 响应示例

**状态码： 200**

请求成功。

**状态码： 400**

请求参数出错。

```
{
 "error": {
 "message": "Illegal request",
 "code": 400,
 "title": "Bad Request"
 }
}
```

**状态码： 401**

认证失败。

```
{
 "error": {
 "message": "Authentication failed",
 "code": 401,
 "title": "Unauthorized"
 }
}
```

**状态码： 403**

没有操作权限。

```
{
 "error": {
 "message": "Forbidden operation",
 "code": 403,
 "title": "Forbidden"
 }
}
```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 请求参数出错。 |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 系统异常。   |

## 5.11.12 删除企业项目关联委托的权限

### 功能介绍

该接口可以删除企业项目委托上的授权。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments

### 请求参数

表 5-546 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                   |
|--------------|------|--------|------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | 已认证的拥有 iam:permissions:revokeRoleFromAgencyOnEnterpriseProject 细粒度权限或Security Administrator权限的token。 |



表 5-547 请求 Body 参数

| 参数                               | 是否必选 | 参数类型             | 描述                      |
|----------------------------------|------|------------------|-------------------------|
| <a href="#">role_assignments</a> | 是    | Array of objects | 委托在企业项目上的绑定关系，最多支持250条。 |

表 5-548 role\_assignments

| 参数                    | 是否必选 | 参数类型   | 描述      |
|-----------------------|------|--------|---------|
| agency_id             | 是    | String | 委托ID。   |
| enterprise_project_id | 是    | String | 企业项目ID。 |
| role_id               | 是    | String | 策略ID。   |

## 响应参数

无

## 请求示例

删除企业项目关联委托的权限

```
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments
{
 "role_assignments": [
 {
 "agency_id": "as0d9f8asdfsdfa09sd8f9aaa",
 "enterprise_project_id": "3asdfs0d9f8asdfsdfa09sd8f9aaa",
 "role_id": "5s0d9f8dafsdfsdfa09sd8f9aaa"
 }
]
}
```

## 响应示例

**状态码： 204**

请求成功。

**状态码： 400**

请求参数出错。

```
{
 "error": {
 "message": "Illegal request",
 "code": 400,
 "title": "Bad Request"
 }
}
```

### 状态码： 401

认证失败。

```
{
 "error": {
 "message": "Authentication failed",
 "code": 401,
 "title": "Unauthorized"
 }
}
```

### 状态码： 403

没有操作权限。

```
{
 "error": {
 "message": "Forbidden operation",
 "code": 403,
 "title": "Forbidden"
 }
}
```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 204 | 请求成功。   |
| 400 | 请求参数出错。 |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 系统异常。   |

## 5.12 安全设置

### 5.12.1 修改账号操作保护策略

#### 功能介绍

该接口可以用于[管理员](#)修改账号操作保护策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/protect-policy

表 5-549 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                                                                                                          |
|-----------|------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 是    | String | 待修改的账号ID，获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> 。 |

## 请求参数

表 5-550 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-551 请求 Body 参数

| 参数                             | 是否必选 | 参数类型                       | 描述      |
|--------------------------------|------|----------------------------|---------|
| <a href="#">protect_policy</a> | 是    | ProtectPolicyOption object | 操作保护策略。 |

表 5-552 protect\_policy

| 参数                         | 是否必选 | 参数类型                 | 描述                                                                  |
|----------------------------|------|----------------------|---------------------------------------------------------------------|
| operation_protection       | 是    | boolean              | 是否开启操作保护，开启为"true"，不开启为"false"。                                     |
| <a href="#">allow_user</a> | 否    | AllowUserBody object | 管理员设置IAM子用户可以自主修改的属性。                                               |
| mobile                     | 否    | String               | 操作保护验证指定手机号码，admin_check为on、scene为mobile时，必须填写。示例：                  |
| admin_check                | 否    | String               | 是否指定人员验证。on为指定人员验证，必须填写scene参数。off为操作员验证。                           |
| email                      | 否    | String               | 操作保护验证指定邮件地址，admin_check为on、scene为email时，必须填写。示例:example@email.com。 |

| 参数    | 是否必选 | 参数类型   | 描述                                                |
|-------|------|--------|---------------------------------------------------|
| scene | 否    | String | 操作保护指定人员验证方式，admin_check为on时，必须填写。包括mobile、email。 |

表 5-553 protect\_policy.allow\_user

| 名称               | 是否必选 | 参数类型    | 描述                            |
|------------------|------|---------|-------------------------------|
| manage_accesskey | 否    | boolean | 是否允许子用户自行管理AK，取值范围true或false。 |
| manage_email     | 否    | boolean | 是否允许子用户自己修改邮箱，取值范围true或false。 |
| manage_mobile    | 否    | boolean | 是否允许子用户自己修改电话，取值范围true或false。 |
| manage_password  | 否    | boolean | 是否允许子用户自己修改密码，取值范围true或false。 |

## 响应参数

状态码： 200

表 5-554 响应 Body 参数

| 参数                    | 参数类型                            | 描述      |
|-----------------------|---------------------------------|---------|
| <b>protect_policy</b> | <b>protect_policy</b><br>object | 操作保护策略。 |

表 5-555 protect\_policy

| 参数                   | 参数类型                    | 描述                            |
|----------------------|-------------------------|-------------------------------|
| <b>allow_user</b>    | AllowUserBody<br>object | 用户可以自主修改的属性。                  |
| operation_protection | boolean                 | 是否开启操作保护，取值范围true或false。      |
| admin_check          | String                  | 是否指定人员验证。on为指定人员验证，off为操作员验证。 |
| scene                | String                  | 操作保护指定人员验证方式。                 |

表 5-556 protect\_policy.allow\_user

| 名称               | 类型      | 描述                            |
|------------------|---------|-------------------------------|
| manage_accesskey | boolean | 是否允许子用户自行管理AK，取值范围true或false。 |
| manage_email     | boolean | 是否允许子用户自己修改邮箱，取值范围true或false。 |
| manage_mobile    | boolean | 是否允许子用户自己修改电话，取值范围true或false。 |
| manage_password  | boolean | 是否允许子用户自己修改密码，取值范围true或false。 |

## 请求示例

修改账号操作保护策略，开启操作保护。

PUT https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/protect-policy

```
{
 "protect_policy": {
 "operation_protection": true
 }
}
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "protect_policy": {
 "allow_user": {
 "manage_mobile": true,
 "manage_accesskey": true,
 "manage_email": true,
 "manage_password": true
 },
 "operation_protection": true,
 "admin_check": "off",
 "scene": ""
 }
}
```

### 状态码为 400 时:

请求体异常。

- 示例 1

```
{
 "error_msg": "%(key)s' is a required property.",
 "error_code": "IAM.0072"
}
```

- 示例 2

```
{
 "error_msg": "Invalid input for field '%(key)s'. The value is '%(value)s'!",
}
```

```
"error_code" : "IAM.0073"
}
```

### 状态码为 403 时:

鉴权失败。

- 示例 1

```
{
 "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
 "error_code" : "IAM.0003"
}
```

- 示例 2

```
{
 "error_msg" : "You are not authorized to perform the requested action.",
 "error_code" : "IAM.0002"
}
```

### 状态码为 500 时:

系统异常。

```
{
 "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
 "error_code" : "IAM.0006"
}
```

## 状态码

| 状态码 | 描述     |
|-----|--------|
| 200 | 请求成功。  |
| 400 | 请求体异常。 |
| 401 | 认证失败。  |
| 403 | 鉴权失败。  |
| 500 | 系统异常。  |

## 错误码

请参见[错误码](#)。

## 5.12.2 查询账号操作保护策略

### 功能介绍

该接口可以用于查询账号操作保护策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/protect-policy

表 5-557 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-558 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

状态码： 200

表 5-559 响应 Body 参数

| 参数                             | 参数类型                                  | 描述      |
|--------------------------------|---------------------------------------|---------|
| <a href="#">protect_policy</a> | <a href="#">protect_policy</a> object | 操作保护策略。 |

表 5-560 protect\_policy

| 参数                         | 参数类型                 | 描述                              |
|----------------------------|----------------------|---------------------------------|
| <a href="#">allow_user</a> | AllowUserBody object | 用户可以自主修改的属性。                    |
| operation_protection       | boolean              | 是否开启操作保护，取值范围true或false。        |
| mobile                     | String               | 操作保护验证指定手机号码。示例:0852-123456789。 |

| 参数          | 参数类型   | 描述                                 |
|-------------|--------|------------------------------------|
| admin_check | String | 是否指定人员验证。on为指定人员验证，off为操作员验证。      |
| email       | String | 操作保护验证指定邮件地址。示例:example@email.com。 |
| scene       | String | 操作保护指定人员验证方式，包括mobile、email。       |

表 5-561 protect\_policy.allow\_user

| 名称               | 类型      | 描述                            |
|------------------|---------|-------------------------------|
| manage_accesskey | boolean | 是否允许子用户自行管理AK，取值范围true或false。 |
| manage_email     | boolean | 是否允许子用户自己修改邮箱，取值范围true或false。 |
| manage_mobile    | boolean | 是否允许子用户自己修改电话，取值范围true或false。 |
| manage_password  | boolean | 是否允许子用户自己修改密码，取值范围true或false。 |

## 请求示例

查询账号操作保护策略。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy
```

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "protect_policy": {
 "operation_protection": false
 }
}
```

**状态码为 403 时:**

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```



- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

**状态码为 404 时:**

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

**状态码为 500 时:**

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

### 5.12.3 修改账号密码策略

#### 功能介绍

该接口可以用于[管理员](#)修改账号密码策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/password-policy

表 5-562 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                            |
|-----------|------|--------|---------------------------------------------------------------|
| domain_id | 是    | String | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-563 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-564 请求 Body 参数

| 参数                              | 是否必选 | 参数类型   | 描述    |
|---------------------------------|------|--------|-------|
| <a href="#">password_policy</a> | 是    | object | 密码策略。 |

表 5-565 password\_policy

| 参数                                    | 是否必选 | 参数类型    | 描述                         |
|---------------------------------------|------|---------|----------------------------|
| maximum_consecutive_identical_chars   | 否    | Integer | 同一字符连续出现的最大次数，取值范围[0,32]。  |
| minimum_password_age                  | 否    | Integer | 密码最短使用时间(分钟)，取值范围[0,1440]。 |
| minimum_password_length               | 否    | Integer | 密码最小字符数，取值范围[8,32]。        |
| number_of_recent_passwords_disallowed | 否    | Integer | 密码不能与历史密码重复次数，取值范围[0,24]。  |

| 参数                              | 是否必选 | 参数类型    | 描述                               |
|---------------------------------|------|---------|----------------------------------|
| password_not_username_or_invert | 否    | Boolean | 密码是否可以用户名或用户名的反序。                |
| password_validity_period        | 否    | Integer | 密码有效期（天），取值范围[0,180]，设置0表示关闭该策略。 |
| password_char_combination       | 否    | Integer | 至少包含字符种类的个数，取值区间[2,4]。           |

## 响应参数

表 5-566 响应 Body 参数

| 参数                     | 参数类型   | 描述    |
|------------------------|--------|-------|
| <b>password_policy</b> | object | 密码策略。 |

表 5-567 password\_policy

| 参数                                    | 参数类型    | 描述             |
|---------------------------------------|---------|----------------|
| maximum_consecutive_identical_chars   | Integer | 同一字符连续出现的最大次数。 |
| maximum_password_length               | Integer | 密码最大字符数。       |
| minimum_password_age                  | Integer | 密码最短使用时间（分钟）。  |
| minimum_password_length               | Integer | 密码最小字符数。       |
| number_of_recent_passwords_disallowed | Integer | 密码不能与历史密码重复次数。 |

| 参数                              | 参数类型    | 描述                     |
|---------------------------------|---------|------------------------|
| password_not_username_or_invert | Boolean | 密码是否可以用户名或用户名的反序。      |
| password_requirements           | String  | 设置密码必须包含的字符要求。         |
| password_validity_period        | Integer | 密码有效期（天）。              |
| password_char_combination       | Integer | 至少包含字符种类的个数，取值区间[2,4]。 |

## 请求示例

修改账号的密码策略：密码最少为8个字符，密码不能与近2次历史密码重复，密码最短使用时间为20分钟，密码有效期为60天，同一字符连续出现的最大次数为3，密码不可以是用户名或用户名的反序，至少包含3种字符类型。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy
{
 "password_policy": {
 "minimum_password_length": 8,
 "number_of_recent_passwords_disallowed": 2,
 "minimum_password_age": 20,
 "password_validity_period": 60,
 "maximum_consecutive_identical_chars": 3,
 "password_not_username_or_invert": false,
 "password_char_combination": 3
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "password_policy": {
 "password_requirements": "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
 "minimum_password_age": 20,
 "minimum_password_length": 8,
 "maximum_password_length": 32,
 "number_of_recent_passwords_disallowed": 2,
 "password_validity_period": 60,
 "maximum_consecutive_identical_chars": 3,
 "password_not_username_or_invert": true,
 "password_char_combination": 3
 }
}
```

### 状态码为 400 时:

请求体异常。

- 示例 1

```
{
 "error_msg": "%(key)s' is a required property.",
 "error_code": "IAM.0072"
}
```

- 示例 2

```
{
 "error_msg": "Invalid input for field '%(key)s'. The value is '%(value)s'.",
 "error_code": "IAM.0073"
}
```

### 状态码为 403 时:

鉴权失败。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 500 时:

系统异常。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述     |
|-----|--------|
| 200 | 请求成功。  |
| 400 | 请求体异常。 |
| 401 | 认证失败。  |
| 403 | 鉴权失败。  |
| 500 | 系统异常。  |

## 错误码

请参见[错误码](#)。

## 5.12.4 查询账号密码策略

### 功能介绍

该接口可以用于查询账号密码策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/password-policy

表 5-568 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-569 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

### 响应参数

表 5-570 响应 Body 参数

| 参数                              | 参数类型   | 描述    |
|---------------------------------|--------|-------|
| <a href="#">password_policy</a> | object | 密码策略。 |

表 5-571 password\_policy

| 参数                                    | 参数类型    | 描述                     |
|---------------------------------------|---------|------------------------|
| maximum_consecutive_identical_chars   | Integer | 同一字符连续出现的最大次数。         |
| maximum_password_length               | Integer | 密码最大字符数。               |
| minimum_password_age                  | Integer | 密码最短使用时间（分钟）。          |
| minimum_password_length               | Integer | 密码最小字符数。               |
| number_of_recent_passwords_disallowed | Integer | 密码不能与历史密码重复次数。         |
| password_not_username_or_invert       | Boolean | 密码是否可以用户名或用户名的反序。      |
| password_requirements                 | String  | 设置密码必须包含的字符要求。         |
| password_validity_period              | Integer | 密码有效期（天）。              |
| password_char_combination             | Integer | 至少包含字符种类的个数，取值区间[2,4]。 |

## 请求示例

查询账号密码策略。

GET [https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain\\_id}/password-policy](https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy)

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "password_policy": {
 "password_requirements": "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
 "minimum_password_age": 20,
 "minimum_password_length": 8,
 "maximum_password_length": 32,
 "number_of_recent_passwords_disallowed": 2,
 "password_validity_period": 60,
 "maximum_consecutive_identical_chars": 3,
 "password_not_username_or_invert": true,
 "password_char_combination": 3
 }
}
```

```
}
}
```

#### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

#### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

#### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

### 5.12.5 修改账号登录策略

#### 功能介绍

该接口可以用于[管理员](#)修改账号登录策略。



该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/login-policy

表 5-572 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                            |
|-----------|------|--------|---------------------------------------------------------------|
| domain_id | 是    | String | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-573 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-574 请求 Body 参数

| 参数                           | 是否必选 | 参数类型   | 描述    |
|------------------------------|------|--------|-------|
| <a href="#">login_policy</a> | 是    | object | 登录策略。 |

表 5-575 login\_policy

| 参数                      | 是否必选 | 参数类型    | 描述                                   |
|-------------------------|------|---------|--------------------------------------|
| account_validity_period | 否    | Integer | 账号在该值设置的有效期（天）内未使用，则被停用，取值范围[0,240]。 |
| custom_info_for_login   | 否    | String  | 登录提示信息。                              |

| 参数                         | 是否必选 | 参数类型    | 描述                           |
|----------------------------|------|---------|------------------------------|
| lockout_duration           | 否    | Integer | 账号锁定时长（分钟），取值范围[15,30]。      |
| login_failed_times         | 否    | Integer | 限定时间内允许的最大登录失败次数，取值范围[3,10]。 |
| period_with_login_failures | 否    | Integer | 限定时间长度（分钟），取值范围[15,60]。      |
| session_timeout            | 否    | Integer | 登录会话失效时间（分钟），取值范围[15,1440]。  |
| show_recent_login_info     | 否    | Boolean | 显示最近一次的登录信息。取值范围true或false。  |

## 响应参数

表 5-576 响应 Body 参数

| 参数                  | 参数类型   | 描述    |
|---------------------|--------|-------|
| <b>login_policy</b> | object | 登录策略。 |

表 5-577 login\_policy

| 参数                         | 参数类型    | 描述                       |
|----------------------------|---------|--------------------------|
| account_validity_period    | Integer | 账号在该值设置的有效期（天）内未使用，则被停用。 |
| custom_info_for_login      | String  | 登录提示信息。                  |
| lockout_duration           | Integer | 账号锁定时长（分钟）。              |
| login_failed_times         | Integer | 限定时间内允许的最大登录失败次数。        |
| period_with_login_failures | Integer | 限定时间长度（分钟）。              |
| session_timeout            | Integer | 登录会话失效时间（分钟）。            |
| show_recent_login_info     | Boolean | 是否显示最近一次的登录信息。           |

## 请求示例

修改账号的登录策略：登录失败后账号锁定时长为15分钟，账号在99天内未使用则被停用，限定时间内登录失败次数为3次，登录会话失效时间为16分钟，显示最近一次的登录信息。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy
{
 "login_policy": {
 "custom_info_for_login": "",
 "period_with_login_failures": 15,
 "lockout_duration": 15,
 "account_validity_period": 99,
 "login_failed_times": 3,
 "session_timeout": 16,
 "show_recent_login_info": true
 }
}
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "login_policy": {
 "custom_info_for_login": "",
 "period_with_login_failures": 15,
 "lockout_duration": 15,
 "account_validity_period": 99,
 "login_failed_times": 3,
 "session_timeout": 16,
 "show_recent_login_info": true
 }
}
```

### 状态码为 400 时:

请求体异常。

- 示例 1

```
{
 "error_msg": "'%(key)s' is a required property.",
 "error_code": "IAM.0072"
}
```

- 示例 2

```
{
 "error_msg": "Invalid input for field '%(key)s'. The value is '%(value)s'.",
 "error_code": "IAM.0073"
}
```

### 状态码为 403 时:

鉴权失败。

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

### 状态码为 500 时:

系统异常。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述     |
|-----|--------|
| 200 | 请求成功。  |
| 400 | 请求体异常。 |
| 401 | 认证失败。  |
| 403 | 鉴权失败。  |
| 500 | 系统异常。  |

## 错误码

请参见[错误码](#)。

## 5.12.6 查询账号登录策略

### 功能介绍

该接口可以用于查询账号登录策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/login-policy

表 5-578 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-579 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-580 响应 Body 参数

| 参数                           | 参数类型   | 描述    |
|------------------------------|--------|-------|
| <a href="#">login_policy</a> | object | 登录策略。 |

表 5-581 login\_policy

| 参数                         | 参数类型    | 描述                       |
|----------------------------|---------|--------------------------|
| account_validity_period    | Integer | 账号在该值设置的有效期（天）内未使用，则被停用。 |
| custom_info_for_login      | String  | 登录提示信息。                  |
| lockout_duration           | Integer | 账号锁定时长（分钟）。              |
| login_failed_times         | Integer | 限定时间内允许的最大登录失败次数。        |
| period_with_login_failures | Integer | 限定时间长度（分钟）。              |
| session_timeout            | Integer | 登录会话失效时间（分钟）。            |
| show_recent_login_info     | Boolean | 是否显示最近一次的登录信息。           |

## 请求示例

查询账号登录策略。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "login_policy": {
 "custom_info_for_login": "",
 "period_with_login_failures": 15,
 "lockout_duration": 15,
 "account_validity_period": 99,
 "login_failed_times": 3,
 "session_timeout": 16,
 "show_recent_login_info": true
 }
}
```

### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

| 状态码 | 描述      |
|-----|---------|
| 500 | 内部服务错误。 |

## 错误码

请参见[错误码](#)。

## 5.12.7 修改账号控制台访问策略

### 功能介绍

该接口可以用于[管理员](#)修改账号控制台访问策略，策略修改后将对账号下所有IAM用户 and 联邦用户（SP方式）生效。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/console-acl-policy

表 5-582 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                            |
|-----------|------|--------|---------------------------------------------------------------|
| domain_id | 是    | String | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-583 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-584 请求 Body 参数

| 参数                                 | 是否必选 | 参数类型   | 描述         |
|------------------------------------|------|--------|------------|
| <a href="#">console_acl_policy</a> | 是    | object | 控制台访问控制策略。 |

表 5-585 console\_acl\_policy

| 参数                                     | 是否必选 | 参数类型             | 描述                                                                    |
|----------------------------------------|------|------------------|-----------------------------------------------------------------------|
| <a href="#">allow_address_netmasks</a> | 否    | Array of objects | 允许访问的IP地址或网段。<br>allow_address_netmasks与<br>allow_ip_ranges两个参数二选一即可。 |
| <a href="#">allow_ip_ranges</a>        | 否    | Array of objects | 允许访问的IP地址区间。<br>allow_address_netmasks与<br>allow_ip_ranges两个参数二选一即可。  |

表 5-586 allow\_address\_netmasks

| 参数              | 是否必选 | 参数类型   | 描述                         |
|-----------------|------|--------|----------------------------|
| address_netmask | 是    | String | IP地址或网段，例如:192.168.0.1/24。 |
| description     | 否    | String | 描述信息。                      |

表 5-587 allow\_ip\_ranges

| 参数          | 是否必选 | 参数类型   | 描述                                 |
|-------------|------|--------|------------------------------------|
| description | 否    | String | 描述信息。                              |
| ip_range    | 是    | String | IP地址区间，例如:0.0.0.0-255.255.255.255。 |



## 响应参数

表 5-588 响应 Body 参数

| 参数                              | 参数类型   | 描述             |
|---------------------------------|--------|----------------|
| <code>console_acl_policy</code> | object | Console访问控制策略。 |

表 5-589 console\_acl\_policy

| 参数                                    | 参数类型             | 描述                                     |
|---------------------------------------|------------------|----------------------------------------|
| <code>allow_addresses_netmasks</code> | Array of objects | 允许访问的IP地址或网段，仅在设置了允许访问的IP地址或网段才会返回此字段。 |
| <code>allow_ip_ranges</code>          | Array of objects | 允许访问的IP地址区间，仅在设置了允许访问的IP地址区间才会返回此字段。   |

表 5-590 allow\_address\_netmasks

| 参数                           | 参数类型   | 描述                         |
|------------------------------|--------|----------------------------|
| <code>address_netmask</code> | String | IP地址或网段，例如:192.168.0.1/24。 |
| <code>description</code>     | String | 描述信息。                      |

表 5-591 allow\_ip\_ranges

| 参数                       | 参数类型   | 描述                                 |
|--------------------------|--------|------------------------------------|
| <code>description</code> | String | 描述信息。                              |
| <code>ip_range</code>    | String | IP地址区间，例如:0.0.0.0-255.255.255.255。 |

## 请求示例

修改账号的控制台访问策略：允许访问的IP地址区间为“0.0.0.0-255.255.255.255”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy
{
 "console_acl_policy": {
 "allow_ip_ranges": [
 {
 "ip_range": "0.0.0.0-255.255.255.255"
 }
]
 }
}
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "console_acl_policy": {
 "allow_ip_ranges": [
 {
 "ip_range": "0.0.0.0-255.255.255.255",
 "description": ""
 }
]
 }
}
```

### 状态码为 400 时:

请求体异常。

- 示例 1

```
{
 "error_msg": "%(key)s' is a required property.",
 "error_code": "IAM.0072"
}
```

- 示例 2

```
{
 "error_msg": "Invalid input for field '%(key)s'. The value is '%(value)s'.",
 "error_code": "IAM.0073"
}
```

### 状态码为 500 时:

系统异常。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述     |
|-----|--------|
| 200 | 请求成功。  |
| 400 | 请求体异常。 |
| 401 | 认证失败。  |
| 403 | 鉴权失败。  |
| 500 | 系统异常。  |

## 错误码

请参见[错误码](#)。

## 5.12.8 查询账号控制台访问策略

### 功能介绍

该接口可以用于查询账号控制台访问控制策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/console-acl-policy

表 5-592 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                |
|-----------|------|--------|-------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-593 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

### 响应参数

表 5-594 响应 Body 参数

| 参数                                 | 参数类型   | 描述         |
|------------------------------------|--------|------------|
| <a href="#">console_acl_policy</a> | object | 控制台访问控制策略。 |

表 5-595 console\_acl\_policy

| 参数                                       | 参数类型             | 描述                                     |
|------------------------------------------|------------------|----------------------------------------|
| <a href="#">allow_addresses_netmasks</a> | Array of objects | 允许访问的IP地址或网段，仅在设置了允许访问的IP地址或网段才会返回此字段。 |
| <a href="#">allow_ip_ranges</a>          | Array of objects | 允许访问的IP地址区间，仅在设置了允许访问的IP地址区间才会返回此字段。   |

表 5-596 allow\_address\_netmasks

| 参数              | 参数类型   | 描述                         |
|-----------------|--------|----------------------------|
| address_netmask | String | IP地址或网段，例如：192.168.0.1/24。 |
| description     | String | 描述信息。                      |

表 5-597 allow\_ip\_ranges

| 参数          | 参数类型   | 描述                                |
|-------------|--------|-----------------------------------|
| description | String | 描述信息。                             |
| ip_range    | String | IP地址区间，例如0.0.0.0-255.255.255.255。 |

## 请求示例

查询账号控制台访问策略。

GET [https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain\\_id}/console-acl-policy](https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy)

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "console_acl_policy": {
 "allow_ip_ranges": [{
 "ip_range": "0.0.0.0-255.255.255.255",
 "description": ""
 }, {
 "ip_range": "0.0.0.0-255.255.255.255",
 "description": ""
 }],
 "allow_address_netmasks": [{
 "address_netmask": "192.168.0.1/24",
 "description": ""
 }, {
 "address_netmask": "192.168.0.1/24",
 "description": ""
 }]
 }
}
```

```
}
}
```

#### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

#### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

#### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.12.9 修改账号接口访问策略

### 功能介绍

该接口可以用于[管理员](#)修改账号接口访问策略，策略修改后将对该账号下所有IAM用户  
和联邦用户（SP方式）生效。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请  
参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/api-acl-policy

表 5-598 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                            |
|-----------|------|--------|---------------------------------------------------------------|
| domain_id | 是    | String | 账号ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

### 请求参数

表 5-599 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

表 5-600 请求 Body 参数

| 参数                             | 是否必选 | 参数类型   | 描述        |
|--------------------------------|------|--------|-----------|
| <a href="#">api_acl_policy</a> | 是    | object | 接口访问控制策略。 |

表 5-601 api\_acl\_policy

| 参数                                      | 是否必选 | 参数类型             | 描述                                                                    |
|-----------------------------------------|------|------------------|-----------------------------------------------------------------------|
| <a href="#">allow_address_net_masks</a> | 否    | Array of objects | 允许访问的IP地址或网段。<br>allow_address_netmasks与<br>allow_ip_ranges两个参数二选一即可。 |
| <a href="#">allow_ip_ranges</a>         | 否    | Array of objects | 允许访问的IP地址区间。<br>allow_address_netmasks与<br>allow_ip_ranges两个参数二选一即可。  |

表 5-602 allow\_address\_netmasks

| 参数              | 是否必选 | 参数类型   | 描述                         |
|-----------------|------|--------|----------------------------|
| address_netmask | 是    | String | IP地址或网段，例如:192.168.0.1/24。 |
| description     | 否    | String | 描述信息。                      |

表 5-603 allow\_ip\_ranges

| 参数          | 是否必选 | 参数类型   | 描述                                 |
|-------------|------|--------|------------------------------------|
| description | 否    | String | 描述信息。                              |
| ip_range    | 是    | String | IP地址区间，例如:0.0.0.0-255.255.255.255。 |

## 响应参数

表 5-604 响应 Body 参数

| 参数                             | 参数类型   | 描述        |
|--------------------------------|--------|-----------|
| <a href="#">api_acl_policy</a> | object | 接口访问控制策略。 |

表 5-605 api\_acl\_policy

| 参数                                     | 参数类型    | 描述                                     |
|----------------------------------------|---------|----------------------------------------|
| <a href="#">allow_address_netmasks</a> | objects | 允许访问的IP地址或网段，仅在设置了允许访问的IP地址或网段才会返回此字段。 |
| <a href="#">allow_ip_ranges</a>        | objects | 允许访问的IP地址区间，仅在设置了允许访问的IP地址区间才会返回此字段。   |

表 5-606 allow\_address\_netmasks

| 参数              | 参数类型   | 描述                         |
|-----------------|--------|----------------------------|
| address_netmask | String | IP地址或网段，例如:192.168.0.1/24。 |
| description     | String | 描述信息。                      |

表 5-607 allow\_ip\_ranges

| 参数          | 参数类型   | 描述                                 |
|-------------|--------|------------------------------------|
| description | String | 描述信息。                              |
| ip_range    | String | IP地址区间，例如:0.0.0.0-255.255.255.255。 |

## 请求示例

修改账号的接口访问策略：允许访问的IP地址区间为“0.0.0.0-255.255.255.255”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy
{
 "api_acl_policy": {
 "allow_ip_ranges": [
 {
 "description": "2",
 "ip_range": "0.0.0.0-255.255.255.255"
 }
]
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "api_acl_policy": {
 "allow_ip_ranges": [
 {
```



```

 "ip_range": "0.0.0.0-255.255.255.255",
 "description": "2"
 }
]
}
}

```

#### 状态码为 400 时:

请求体异常。

- 示例 1

```

{
 "error_msg": "%(key)s' is a required property.",
 "error_code": "IAM.0072"
}

```

- 示例 2

```

{
 "error_msg": "Invalid input for field '%(key)s'. The value is '%(value)s'.",
 "error_code": "IAM.0073"
}

```

#### 状态码为 500 时:

系统异常。

```

{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}

```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 400 | 请求体异常。  |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |
| 500 | 系统异常。   |

## 错误码

请参见[错误码](#)。

### 5.12.10 查询账号接口访问策略

#### 功能介绍

该接口可以用于查询账号接口访问控制策略。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain\_id}/api-acl-policy

表 5-608 路径参数

| 参数        | 是否必选 | 参数类型   | 描述                                                                                                                                                        |
|-----------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain_id | 是    | String | 待查询的账号ID，获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> |

## 请求参数

表 5-609 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-610 响应 Body 参数

| 参数                             | 参数类型   | 描述        |
|--------------------------------|--------|-----------|
| <a href="#">api_acl_policy</a> | object | 接口访问控制策略。 |

表 5-611 api\_acl\_policy

| 参数                                       | 参数类型             | 描述                                     |
|------------------------------------------|------------------|----------------------------------------|
| <a href="#">allow_addresses_netmasks</a> | Array of objects | 允许访问的IP地址或网段，仅在设置了允许访问的IP地址或网段才会返回此字段。 |
| <a href="#">allow_ip_ranges</a>          | Array of objects | 允许访问的IP地址区间，仅在设置了允许访问的IP地址区间才会返回此字段。   |

表 5-612 allow\_address\_netmasks

| 参数              | 参数类型   | 描述                         |
|-----------------|--------|----------------------------|
| address_netmask | String | IP地址或网段，例如:192.168.0.1/24。 |
| description     | String | 描述信息。                      |

表 5-613 allow\_ip\_ranges

| 参数          | 参数类型   | 描述                                |
|-------------|--------|-----------------------------------|
| ip_range    | String | IP地址区间，例如0.0.0.0-255.255.255.255。 |
| description | String | 描述信息。                             |

## 请求示例

查询账号接口访问策略。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy
```

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "api_acl_policy": {
 "allow_ip_ranges": [{
 "ip_range": "0.0.0.0-255.255.255.255",
 "description": ""
 }, {
 "ip_range": "0.0.0.0-255.255.255.255",
 "description": ""
 }],
 "allow_address_netmasks": [{
 "address_netmask": "192.168.0.1/24",
 "description": ""
 }, {
 "address_netmask": "192.168.0.1/24",
 "description": ""
 }]
 }
}
```

**状态码为 403 时:**

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

**状态码为 404 时:**

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

**状态码为 500 时:**

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

### 5.12.11 查询 IAM 用户的 MFA 绑定信息列表

#### 功能介绍

该接口可以用于[管理员](#)查询IAM用户的MFA绑定信息列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3.0/OS-MFA/virtual-mfa-devices

## 请求参数

表 5-614 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

## 响应参数

表 5-615 响应 Body 参数

| 参数                                  | 参数类型             | 描述           |
|-------------------------------------|------------------|--------------|
| <a href="#">virtual_mfa_devices</a> | Array of objects | 虚拟MFA设备信息列表。 |

表 5-616 virtual\_mfa\_devices

| 参数            | 参数类型   | 描述           |
|---------------|--------|--------------|
| serial_number | String | 虚拟MFA的设备序列号。 |
| user_id       | String | IAM用户ID。     |

## 请求示例

查询IAM用户的MFA绑定信息列表。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-MFA/virtual-mfa-devices
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "virtual_mfa_devices": [
 {
 "user_id": "16b26081f43d4c628c4bb88cf32e9...",
 "serial_number": "iam:16b26081f43d4c628c4bb88cf32e9..."
 },
 {
 "user_id": "47026081f43d4c628c4bb88cf32e9...",
 "serial_number": "iam:75226081f43d4c628c4bb88cf32e9..."
 }
]
}
```

### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.12.12 查询指定 IAM 用户的 MFA 绑定信息

### 功能介绍

该接口可以用于[管理员](#)查询指定IAM用户的MFA绑定信息，或IAM用户查询自己的MFA绑定信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-MFA/users/{user\_id}/virtual-mfa-device

表 5-617 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-618 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                    |
|--------------|------|--------|-----------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户的MFA绑定信息：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己的MFA绑定信息：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

表 5-619 响应 Body 参数

| 参数                                 | 参数类型   | 描述         |
|------------------------------------|--------|------------|
| <a href="#">virtual_mfa_device</a> | object | 虚拟MFA设备信息。 |

表 5-620 virtual\_mfa\_device

| 参数            | 参数类型   | 描述           |
|---------------|--------|--------------|
| serial_number | String | 虚拟MFA的设备序列号。 |
| user_id       | String | IAM用户ID。     |

## 请求示例

查询指定IAM用户的MFA绑定信息。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-MFA/users/{user_id}/virtual-mfa-device
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "virtual_mfa_device":
 {
 "user_id": "16b26081f43d4c628c4bb88cf32e9...",
 "serial_number": "iam:16b26081f43d4c628c4bb88cf32e9..."
 }
}
```

### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 200 | 请求成功。   |
| 401 | 认证失败。   |
| 403 | 没有操作权限。 |



| 状态码 | 描述        |
|-----|-----------|
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

## 5.12.13 查询 IAM 用户的登录保护状态信息列表

### 功能介绍

该接口可以用于[管理员](#)查询IAM用户的登录保护状态列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3.0/OS-USER/login-protects

### 请求参数

表 5-621 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                        |
|--------------|------|--------|-----------------------------------------------------------|
| X-Auth-Token | 是    | String | 访问令牌，承载用户的身份、权限等信息。<br>token所需权限请参见 <a href="#">授权项</a> 。 |

### 响应参数

表 5-622 响应 Body 参数

| 参数                             | 参数类型             | 描述                                             |
|--------------------------------|------------------|------------------------------------------------|
| <a href="#">login_protects</a> | Array of objects | 登录状态保护信息列表。<br><b>说明</b><br>只返回开启过登录保护的用户状态信息。 |

表 5-623 login\_protects

| 参数                  | 参数类型    | 描述                                   |
|---------------------|---------|--------------------------------------|
| enabled             | Boolean | IAM用户是否开启登录保护，开启为"true"，未开启为"false"。 |
| user_id             | String  | IAM用户ID。                             |
| verification_method | String  | IAM用户登录验证方式。                         |

## 请求示例

查询IAM用户的登录保护状态信息列表。

```
GET https://iam.myhuaweicloud.com/v3.0/OS-USER/login-protects
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "login_protects": [
 {
 "user_id": "75226081f43d4c628c4bb88cf32e9...",
 "enabled": true,
 "verification_method": "email"
 },
 {
 "user_id": "16b26081f43d4c628c4bb88cf32e9...",
 "enabled": true,
 "verification_method": "vmfa"
 },
 {
 "user_id": "56b26081f43d4c628c4bb88cf32e9...",
 "enabled": true,
 "verification_method": "sms"
 }
]
}
```

### 说明

对于从未开启过登录保护的IAM用户，该接口无法获取到其登录保护状态信息，只返回开启过登录保护的用户状态信息。

状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
}
```

```
"error_code" : "IAM.0003"
}
```

#### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg" : "Could not find %(target)s: %(target_id)s.",
 "error_code" : "IAM.0004"
}
```

#### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
 "error_code" : "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |
| 500 | 内部服务错误。   |

## 错误码

请参见[错误码](#)。

### 5.12.14 查询指定 IAM 用户的登录保护状态信息

#### 功能介绍

该接口可以用于[管理员](#)查询指定IAM用户的登录保护状态信息，或IAM用户查询自己的登录保护状态信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3.0/OS-USER/users/{user\_id}/login-protect

表 5-624 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                   |
|---------|------|--------|----------------------------------------------------------------------|
| user_id | 是    | String | 待查询的IAM用户ID，获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> 。 |

## 请求参数

表 5-625 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                      |
|--------------|------|--------|-------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <a href="#">管理员</a> 查询IAM用户的登录保护状态信息：请参见 <a href="#">授权项</a> 。<br>IAM用户查询自己的登录保护状态信息：URL中user_id所对应IAM用户的token（无需特殊权限）。 |

## 响应参数

状态码为 200 时:

表 5-626 响应 Body 参数

| 参数                            | 参数类型   | 描述        |
|-------------------------------|--------|-----------|
| <a href="#">login_protect</a> | object | 登录状态保护信息。 |

表 5-627 login\_protect

| 参数                  | 参数类型    | 描述                                   |
|---------------------|---------|--------------------------------------|
| enabled             | Boolean | IAM用户是否开启登录保护，开启为"true"，未开启为"false"。 |
| user_id             | String  | IAM用户ID。                             |
| verification_method | String  | IAM用户登录验证方式。                         |

## 请求示例

查询指定IAM用户的登录保护状态信息。

GET [https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user\\_id}/login-protect](https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user_id}/login-protect)

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "login_protect": {
 "user_id": "16b26081f43d4c628c4bb88cf32e9...",
 "enabled": true,
 "verification_method": "vmfa"
 }
}
```

### 状态码为 403 时:

没有操作权限。

- 示例 1

```
{
 "error_msg": "You are not authorized to perform the requested action.",
 "error_code": "IAM.0002"
}
```

- 示例 2

```
{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}
```

### 状态码为 404 时:

未找到相应的资源。

```
{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}
```

#### 说明

对于从未开启过登录保护的IAM用户，该接口无法获取到其登录保护状态信息，会返回IAM.0004错误码。

### 状态码为 500 时:

内部服务错误。

```
{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 401 | 认证失败。     |
| 403 | 没有操作权限。   |
| 404 | 未找到相应的资源。 |

| 状态码 | 描述      |
|-----|---------|
| 500 | 内部服务错误。 |

## 错误码

请参见[错误码](#)。

## 5.12.15 修改 IAM 用户的登录保护状态信息

### 功能介绍

该接口可以用于[管理员](#)修改IAM用户的登录保护状态信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-USER/users/{user\_id}/login-protect

表 5-628 路径参数

| 参数      | 是否必选 | 参数类型   | 描述                                                                                                                                                                                       |
|---------|------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user_id | 是    | String | 待修改登录保护状态信息的IAM用户ID（不支持修改自己的登录保护状态信息），获取方式请参见： <a href="#">获取账号</a> 、 <a href="#">IAM用户</a> 、 <a href="#">项目</a> 、 <a href="#">用户组</a> 、 <a href="#">区域</a> 、 <a href="#">委托的名称和ID</a> 。 |

### 请求参数

表 5-629 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                |
|--------------|------|--------|-----------------------------------|
| X-Auth-token | 是    | String | 拥有Security Administrator权限的token。 |

表 5-630 请求 Body 参数

| 参数                         | 是否必选 | 参数类型   | 描述        |
|----------------------------|------|--------|-----------|
| <code>login_protect</code> | 是    | object | 登录保护状态信息。 |

表 5-631 Login\_project

| 参数                               | 是否必选 | 参数类型    | 描述                                                |
|----------------------------------|------|---------|---------------------------------------------------|
| <code>enabled</code>             | 是    | Boolean | IAM用户是否开启登录保护，开启为"true"，未开启为"false"。              |
| <code>verification_method</code> | 是    | String  | IAM用户登录验证方式。手机验证为"sms"，邮箱验证为"email"，MFA验证为"vmfa"。 |

## 响应参数

状态码为 200 时：

表 5-632 响应 Body 参数

| 参数                         | 参数类型   | 描述        |
|----------------------------|--------|-----------|
| <code>login_protect</code> | object | 登录保护状态信息。 |

表 5-633 login\_protect

| 参数                               | 参数类型    | 描述                                                |
|----------------------------------|---------|---------------------------------------------------|
| <code>user_id</code>             | String  | 待修改登录保护状态信息的IAM用户ID。                              |
| <code>enabled</code>             | Boolean | IAM用户是否开启登录保护，开启为"true"，不开启为"false"。              |
| <code>verification_method</code> | String  | IAM用户登录验证方式。手机验证为"sms"，邮箱验证为"email"，MFA验证为"vmfa"。 |

## 请求示例

修改IAM用户的登录保护状态信息：开启登录保护，且登录验证方式为MFA验证。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-USER/users/{user_id}/login-protect
```

```
{
 "login_protect": {
```

```
"enabled" : true,
"verification_method" : "vmfa"
}
}
```

## 响应示例

**状态码：200**

请求成功。

```
{
 "login_protect" : {
 "user_id": "16b26081f43d4c628c4bb88cf32e9...",
 "enabled" : true,
 "verification_method" : "vmfa"
 }
}
```

## 状态码

| 状态码 | 描述        |
|-----|-----------|
| 200 | 请求成功。     |
| 400 | 请求校验异常。   |
| 401 | 认证失败。     |
| 403 | 请求未授权。    |
| 404 | 未找到相应的资源。 |
| 500 | 系统错误。     |

## 错误码

请参见[错误码](#)。

## 5.12.16 绑定 MFA 设备

### 功能介绍

该接口可以用于IAM用户为自己绑定MFA设备。启用MFA后不影响已获取Token的有效性，同时无法强制忽略MFA的二次认证。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-MFA/mfa-devices/bind



## 请求参数

表 5-634 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                    |
|--------------|------|--------|---------------------------------------|
| X-Auth-token | 是    | String | 请求Body中user_id所对应IAM用户的token（无需特殊权限）。 |

表 5-635 请求 Body 参数

| 参数                         | 是否必选 | 参数类型   | 描述                |
|----------------------------|------|--------|-------------------|
| user_id                    | 是    | String | 待绑定MFA设备的IAM用户ID。 |
| serial_number              | 是    | String | MFA设备序列号。         |
| authentication_code_first  | 是    | String | 第一组验证码。           |
| authentication_code_second | 是    | String | 第二组验证码。           |

## 响应参数

无

## 请求示例

绑定MFA设备，第一组验证码为“977931”，第二组验证码为“527347”，MFA设备序列号为“iam:09f6bd6a96801de40f01c00c85691...:mfa/{device\_name}”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-MFA/mfa-devices/bind
```

```
{
 "user_id": "09f99d8f6a001d4f1f01c00c31968...",
 "authentication_code_first": "977931",
 "authentication_code_second": "527347",
 "serial_number": "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}"
}
```

## 响应示例

状态码：204。

请求成功。

## 状态码

| 状态码 | 描述           |
|-----|--------------|
| 204 | 请求成功。        |
| 400 | 请求校验异常。      |
| 401 | 认证失败。        |
| 403 | 请求未授权。       |
| 404 | 无法找到请求资源。    |
| 409 | 保存请求资源时发生冲突。 |
| 500 | 系统错误。        |

## 错误码

请参见[错误码](#)。

## 5.12.17 解绑 MFA 设备

### 功能介绍

该接口可以用于管理员为IAM用户解绑MFA设备，或IAM用户为自己解绑MFA设备。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

PUT /v3.0/OS-MFA/mfa-devices/unbind

### 请求参数

表 5-636 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                                                                                                                                        |
|--------------|------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | 是    | String | <ul style="list-style-type: none"> <li><a href="#">管理员</a>为IAM用户解绑MFA设备：请参见<a href="#">授权项</a>。</li> <li>IAM用户为自己解绑MFA设备：请求Body中user_id所对应IAM用户的token（无需特殊权限）。</li> </ul> |

表 5-637 请求 Body 参数

| 参数                  | 是否必选 | 参数类型   | 描述                                                                                                                      |
|---------------------|------|--------|-------------------------------------------------------------------------------------------------------------------------|
| user_id             | 是    | String | 待解绑MFA设备的IAM用户ID。                                                                                                       |
| authentication_code | 是    | String | <ul style="list-style-type: none"> <li>管理员为IAM用户解绑MFA设备：填写6位任意验证码，不做校验。</li> <li>IAM用户为自己解绑MFA设备：填写虚拟MFA验证码。</li> </ul> |
| serial_number       | 是    | String | MFA设备序列号。                                                                                                               |

## 响应参数

无

## 请求示例

解绑序列号为“iam:09f6bd6a96801de40f01c00c85691...:mfa/{device\_name}”的MFA设备，验证码是“373658”。

```
PUT https://iam.myhuaweicloud.com/v3.0/OS-MFA/mfa-devices/unbind
```

```
{
 "user_id": "09f99d8f6a001d4f1f01c00c31968...",
 "authentication_code": "373658",
 "serial_number": "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}"
}
```

## 响应示例

状态码：204

请求成功。

## 状态码

| 状态码 | 描述           |
|-----|--------------|
| 204 | 请求成功。        |
| 400 | 请求校验异常。      |
| 401 | 认证失败。        |
| 403 | 请求未授权。       |
| 404 | 无法找到请求资源。    |
| 409 | 保存请求资源时发生冲突。 |
| 500 | 系统错误。        |

## 错误码

请参见[错误码](#)。

## 5.12.18 创建 MFA 设备

### 功能介绍

该接口可以用于IAM用户为自己创建MFA设备。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-MFA/virtual-mfa-devices

### 请求参数

表 5-638 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                    |
|--------------|------|--------|---------------------------------------|
| X-Auth-Token | 是    | String | 请求Body中user_id所对应IAM用户的token（无需特殊权限）。 |

表 5-639 请求 Body 参数

| 参数                                 | 是否必选 | 参数类型   | 描述          |
|------------------------------------|------|--------|-------------|
| <a href="#">virtual_mfa_device</a> | 是    | object | 创建的MFA设备信息。 |

表 5-640 virtual\_mfa\_device

| 参数      | 是否必选 | 参数类型   | 描述                         |
|---------|------|--------|----------------------------|
| name    | 是    | String | 设备名称。<br>最小长度：1<br>最大长度：64 |
| user_id | 是    | String | 创建MFA设备的IAM用户ID。           |

## 响应参数

状态码为 201 时:

表 5-641 响应 Body 参数

| 参数                              | 参数类型   | 描述        |
|---------------------------------|--------|-----------|
| <code>virtual_mfa_device</code> | object | 创建的MFA设备。 |

表 5-642 virtual\_mfa\_device

| 参数                              | 参数类型   | 描述                 |
|---------------------------------|--------|--------------------|
| <code>serial_number</code>      | String | MFA设备序列号。          |
| <code>base32_string_seed</code> | String | 密钥信息，用于第三方生成图片验证码。 |

## 请求示例

创建MFA设备。

POST <https://iam.myhuaweicloud.com/v3.0/OS-MFA/virtual-mfa-devices>

```
{
 "virtual_mfa_device": {
 "name": "{device_name}",
 "user_id": "09f99d8f6a001d4f1f01c00c31968..."
 }
}
```

## 响应示例

状态码: 201

请求成功。

```
{
 "virtual_mfa_device": {
 "serial_number": "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}",
 "base32_string_seed": "{string}"
 }
}
```

## 状态码

| 状态码 | 描述      |
|-----|---------|
| 201 | 请求成功。   |
| 400 | 请求校验异常。 |
| 401 | 认证失败。   |

| 状态码 | 描述     |
|-----|--------|
| 403 | 请求未授权。 |
| 500 | 系统错误。  |

## 错误码

请参见[错误码](#)。

## 5.12.19 删除 MFA 设备

### 功能介绍

该接口可以用于[管理员](#)删除自己的MFA设备。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

DELETE /v3.0/OS-MFA/virtual-mfa-devices

表 5-643 Query 参数

| 参数            | 是否必选 | 参数类型   | 描述                                                                      |
|---------------|------|--------|-------------------------------------------------------------------------|
| user_id       | 是    | String | 待删除MFA设备的IAM用户ID。获取方式请参见： <a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a> |
| serial_number | 是    | String | MFA设备序列号。                                                               |

### 请求参数

表 5-644 请求 Header 参数

| 参数           | 是否必选 | 参数类型   | 描述                                                       |
|--------------|------|--------|----------------------------------------------------------|
| X-Auth-Token | 是    | String | 请求Body中user_id所对应IAM用户且拥有Security Administrator权限的token。 |

## 响应参数

无

## 请求示例

删除MFA设备。

```
DELETE https://iam.myhuaweicloud.com/v3.0/OS-MFA/virtual-mfa-devices?
user_id=09f6bd85fc801de41f0cc00ce9172...&serial_number=iam:09f6bd6a96801de40f01c00c85691...mfa/
{device_name}
```

## 响应示例

状态码：204

请求成功。

## 状态码

| 状态码 | 描述     |
|-----|--------|
| 204 | 请求成功。  |
| 401 | 认证失败。  |
| 403 | 请求未授权。 |
| 500 | 系统错误。  |

## 错误码

请参见[错误码](#)。

## 5.13 联邦身份认证管理

### 5.13.1 通过联邦认证获取 token

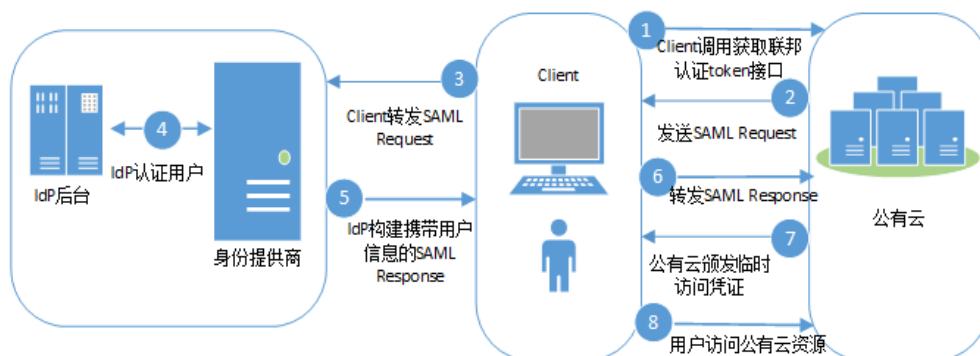
#### 5.13.1.1 SP initiated 方式

Openstack和Shibboleth是被广泛使用的一套开源联邦身份认证解决方案，提供了强大的单点登录能力，将用户连接到企业内外的各种应用服务。本章介绍通过Openstack Client和ShibbolethECP Client获取联邦认证Token的方法。

## 流程图

SP initiated联邦认证的流程如下图所示。

图 5-1 流程图（SP initiated 方式）



## 步骤说明

1. Client调用公有云系统提供的“通过SP initiated方式获取联邦token”接口。
2. 公有云系统根据URL中的用户及IdP信息查找Metadata文件，发送SAML Request，请求经过中间媒介Client。
3. Client对SAML Request进行重新封装后转发SAML Request给IdP。
4. 用户输入用户名和密码完成身份认证。
5. 用户认证成功后，IdP构建携带用户身份信息的断言发送SAML Response，请求经过中间媒介Client。
6. Client对SAML Response进行重新封装后转发SAML Response给公有云。
7. 公有云对断言进行校验和认证，并根据用户在身份提供商配置的身份转换规则生成临时访问凭证。
8. 用户根据分配的权限访问公有云资源。

## Openstack Client

统一命令行客户端工具的安装需要使用root权限，以下配置Openstack Client的操作只需要普通用户权限。

### 须知

接口调用操作应该在一个安全的网络环境中进行（在VPN或者在租户的云服务器中），如果在不安全的网络环境中，可能会受到中间人攻击。

- 步骤1** 使用文本编辑器创建环境变量文件，在文件中设置用户名、密码、区域、SAML协议版本、IAM地址和端口等信息。参数说明如表5-645所示。

示例如下：

```
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_TYPE=v3samlpassword
export OS_AUTH_URL=https://example:443/v3
export OS_IDENTITY_PROVIDER=idpid
export OS_PROTOCOL=saml
```



```
export OS_IDENTITY_PROVIDER_URL=https://idp.example.com/idp/profile/SAML2/SOAP/ECP
export OS_USERNAME=username
export OS_PASSWORD=userpassword
export OS_DOMAIN_NAME=example-domain-name
```

表 5-645 环境变量文件参数说明

| 参数名称                     | 说明                                                                                                                    |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------|
| OS_IDENTITY_API_VERSION  | 认证接口版本，固定值为“3”。                                                                                                       |
| OS_AUTH_TYPE             | 认证类型，固定值为v3samlpassword。                                                                                              |
| OS_AUTH_URL              | 格式为“https://IAM地址:端口号/接口版本”。 <ul style="list-style-type: none"> <li>端口号：固定值为“443”。</li> <li>接口版本：固定值为“v3”。</li> </ul> |
| OS_IDENTITY_PROVIDER     | 用户在本系统创建的身份提供商的名称。例如：Publiccloud-Shibboleth。                                                                          |
| OS_DOMAIN_NAME           | 待认证的租户名称。                                                                                                             |
| OS_PROTOCOL              | SAML协议版本，固定值为“saml”。                                                                                                  |
| OS_IDENTITY_PROVIDER_URL | Identity Provider处理通过客户端代理机制（ECP）发起的认证请求的地址。                                                                          |
| OS_USERNAME              | 用户在Identity Provide认证时使用的用户名。                                                                                         |
| OS_PASSWORD              | 用户在Identity Provide认证时使用的密码。                                                                                          |

**步骤2** 执行如下命令，设置环境变量。

```
source keystonerc
```

**步骤3** 执行如下命令，获取token。

```
openstack token issue
```

```
>>openstack token issue
command: token issue -> openstackclient.identity.v3.token.IssueToken (auth=True)
Using auth plugin: v3samlpassword
+-----+
| Field | Value
| expires | 2018-04-16T03:46:51+0000
| id | MIIDbQYJKoZIhvcNAQcCoIIDXjXXX...
| user_id | 9B7CJy5ME14f0fQKhb6HJVQdpXXX...
```

回显信息中id为获取到的联邦认证token

----结束

## Shibboleth ECP Client

**步骤1** 在Shibboleth IdP v3中配置metadata-providers.xml文件，并将metadata.xml文件放在对应路径下。

```
<MetadataProvider id="LocalMetadata1" xsi:type="FilesystemMetadataProvider" metadataFile="C:\Program Files (x86)\Shibboleth\IdP\metadata\web_metadata.xml"/>
<MetadataProvider id="LocalMetadata2" xsi:type="FilesystemMetadataProvider" metadataFile="C:\Program Files (x86)\Shibboleth\IdP\metadata\api_metadata.xml"/>
```

#### 说明

- MetadataProvider id: 下载的SP系统的元数据文件名称。
- metadataFile: SP的元数据文件在企业IdP系统中放置的路径。

### 步骤2 在Shibboleth IdP v3中配置attribute-filter.xml文件。

```
<afp:AttributeFilterPolicy id="example1">
 <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://auth.example.com/" />
 <afp:AttributeRule attributeID="eduPersonPrincipalName">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
 <afp:AttributeRule attributeID="uid">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
 <afp:AttributeRule attributeID="mail">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
</afp:AttributeFilterPolicy>

<afp:AttributeFilterPolicy id="example2">
 <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://iam.{region_id}.example.com" />
 <afp:AttributeRule attributeID="eduPersonPrincipalName">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
 <afp:AttributeRule attributeID="uid">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
 <afp:AttributeRule attributeID="mail">
 <afp:PermitValueRule xsi:type="basic:ANY" />
 </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

#### 说明

- AttributeFilterPolicy id: 下载的SP系统元数据文件名称。
- value: SP系统元数据文件中的EntityID。

### 步骤3 在ecp.py脚本中配置企业IdP系统的终端节点地址。

```
mapping from user friendly names or tags to IdP ECP endpoints
IDP_ENDPOINTS = {
 "idp1": "https://idp.example.com/idp/profile/SAML2/SOAP/ECP"
}
```

### 步骤4 执行ecp.py脚本获取联邦认证token。

```
>>>python ecp.py
Usage: ecp.py [options] IdP_tag target_url login
>>>python ecp.py -d idp1 https://iam.{region_id}.example.com/v3/OS-FEDERATION/identity_providers/
idp_example/protocols/saml/auth {username}
X-Subject-Token: MIIDbQYJKoZIhvcNAQcColIDXXX...
```

X-Subject-Token为获取到联邦认证token。

----结束

## 5.13.1.2 IdP initiated 方式

本章以“Client4ShibbolethIdP”脚本为例，介绍IdP initiated方式获取联邦认证Token的方法。“Client4ShibbolethIdP”脚本模拟用户在浏览器上登录企业IdP系统，通过

呈现浏览器提交的表单数据和客户端实现的对比，帮助用户开发本企业IdP系统的客户端脚本。

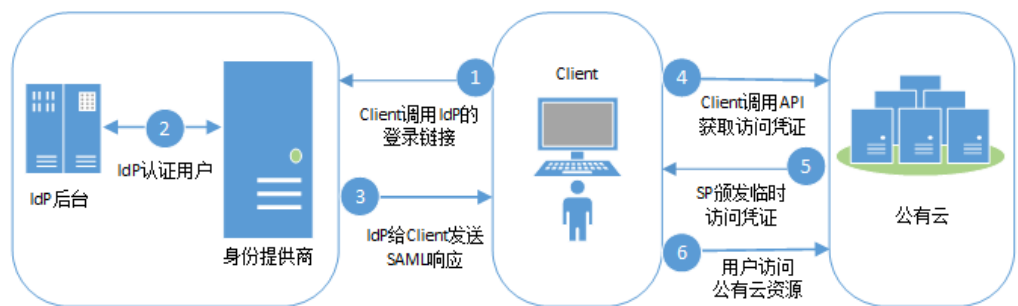
## 前提条件

- 企业IdP服务器支持IdP Initiated方式的联邦认证。
- 客户端需要安装python模块beautifulsoup4。

## 流程图

IdP initiated联邦认证的流程如下图所示。

图 5-2 流程图（IdP initiated 方式）



## 步骤说明

1. Client调用IdP提供的基于IdP initiated方式的登录链接，并在登录链接中设置公有云的地址，即公有云Metadata文件中的“entityID”。
2. Client获取IdP的登录页面，用户通过Client提交身份信息给IdP进行认证。
3. 用户认证成功后，IdP构建携带用户身份信息的断言发送SAML Response，请求经过中间媒介Client。
4. Client对SAML Response进行重新封装后转发SAML Response，调用公有云提供的“通过IdP initiated方式获取联邦token”接口。
5. 公有云对断言进行校验和认证，并根据用户在身份提供商配置的身份转换规则生成临时访问凭证。
6. 用户根据分配的权限访问公有云资源。

## 客户端实现

“Client4ShibbolethIdP.py”脚本（仅供参考），实现本企业IdP到本系统的API/CLI侧联邦认证的脚本。

脚本下载地址：

<https://obs-iam-download01.obs.cn-north-1.myhuaweicloud.com/non-ecp-script/Client4ShibbolethIdP.py>

**步骤1** 配置企业IdP的登录连接。

表 5-646 常用 IdP 产品的登录 URL

IdP	URL中标记SP的参数	登录URL示例
ADFS	logintorp	https://adfs-server.contoso.com/adfs/ls/IdpInitiatedSignon.aspx?logintorp=https://iam.example.com
Shibboleth	providerId	https://idp.example.org/idp/profile/SAML2/Unsolicited/SSO?providerId=iam.example.com
SimpleSAMLphp	spentityid	https://idp.example.org/simplesaml/saml2/idp/SSOService.php?spentityid=iam.example.com

配置完成后，在浏览器里输入登录URL，浏览器会呈现如下登录页面：

图 5-3 登录页面

**Our Identity Provider**  
(replace this placeholder with your organizational logo / label)

Username

Password

> Forgot your password?  
 > Need Help?

Don't Remember Login

Clear prior granting of permission for release of your information to this service.

Login

Client4ShibbolethIdP脚本实现：

```
import sys
import requests
import getpass
import re
from bs4 import BeautifulSoup
from urlparse import urlparse

SSL certificate verification: Whether or not strict certificate
verification is done, False should only be used for dev/test
sslverification = True

Get the federated credentials from the user
print "Username:",
username = raw_input()
```

```
password = getpass.getpass()
print ""

session = requests.Session()

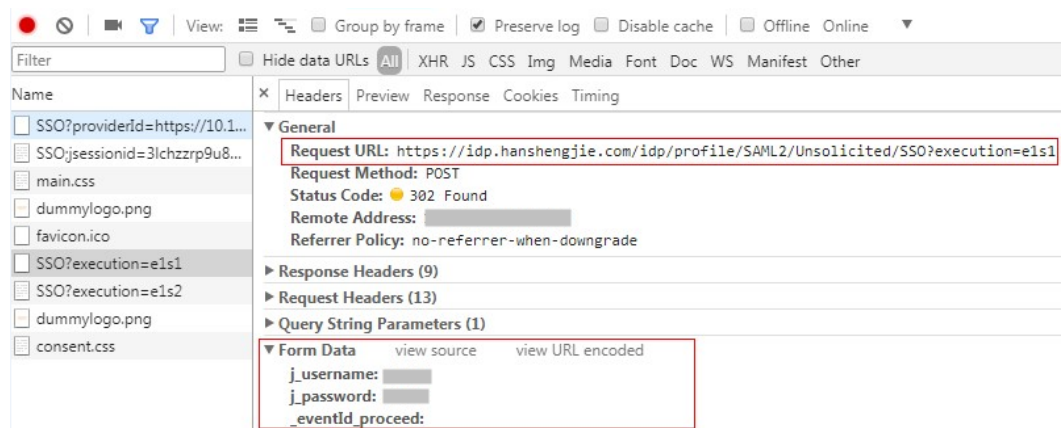
The initial url that starts the authentication process.
idp_entry_url = 'https://idp.example.com/idp/profile/SAML2/Unsolicited/SSO?providerId=https://iam.example.com'

Programmatically get the SAML assertion,open the initial IdP url# and follows all of the HTTP302
redirects, and gets the resulting# login page
formresponse = session.get(idp_entry_url, verify=sslverification)
Capture the idp_authform_submit_url,which is the final url after# all the 302s
idp_authform_submit_url = formresponse.url
```

**步骤2** 客户端提交认证信息。客户端通过beautifulsoup4模块解析登录页面，捕获用户信息输入框、请求action，构造请求的参数，发起向IdP的身份认证。

通过浏览器获取登录页面提交的所有表单数据。

图 5-4 认证信息 ( 1 )



Client4ShibbolethIdP脚本实现：

```
Parse the response and extract all the necessary values in order to build a dictionary of all of the form
values the IdP expects
formsoup = BeautifulSoup(formresponse.text.decode('utf8'), "lxml")
payload = {}

for inputtag in formsoup.find_all(re.compile('(INPUT|input)')):
 name = inputtag.get('name', "")
 value = inputtag.get('value', "")
 if "username" in name.lower():
 payload[name] = username
 elif "password" in name.lower():
 payload[name] = password
 else:
 payload[name] = value

for inputtag in formsoup.find_all(re.compile('(FORM|form)')):
 action = inputtag.get('action')
 if action:
 parsedurl = urlparse(idp_entry_url)
 idp_authform_submit_url = parsedurl.scheme + "://" + parsedurl.netloc + action

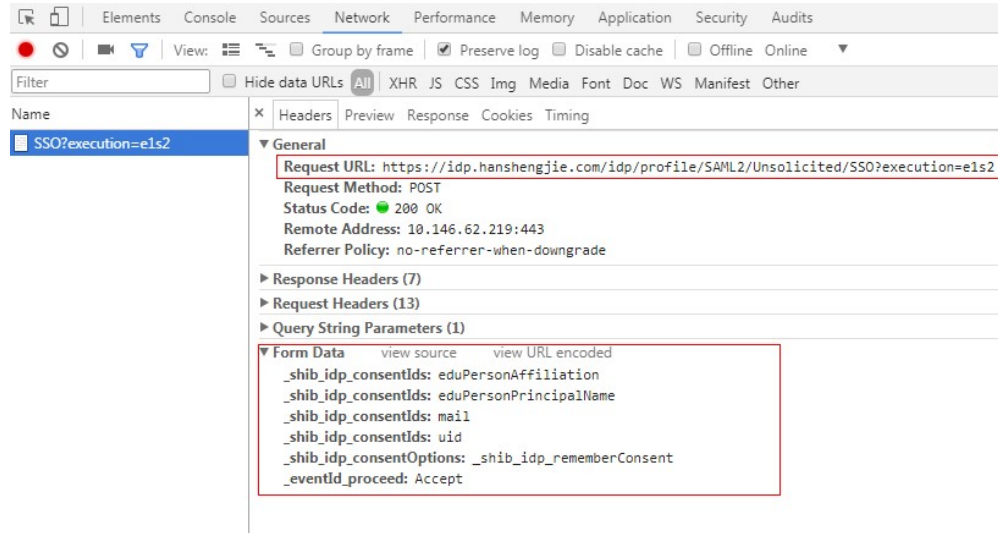
please test on browser first, add other parameters in payload
payload["_eventId_proceed"] = ""

formresponse = session.post(
 idp_authform_submit_url, data=payload, verify=sslverification)
```

**步骤3** 客户端解析下一页（部分企业IdP会有展示用户属性的页面）。

通过浏览器获取登录页面提交的所有表单数据。

**图 5-5** 认证信息（2）



**Client4ShibbolethIdP脚本实现：**

```
In shebbleth IdP v3, browser will show attributes page for user,# so we need parse the page
formsoup = BeautifulSoup(formresponse.text.decode('utf8'), "lxml")
payload = {}

Add other form data required from browser to payload
_shib_idp_consentsIds = []
for inputtag in formsoup.find_all(re.compile('input')):
 name = inputtag.get("name")
 value = inputtag.get("value")
 if name == "_shib_idp_consentsIds":
 _shib_idp_consentsIds.append(value)
payload["_shib_idp_consentsIds"] = _shib_idp_consentsIds
payload["_shib_idp_consentOptions"] = "_shib_idp_rememberConsent"
payload["_eventId_proceed"] = "Accept"

user can get the action url from the html file
nexturl = "https://idp.example.com/idp/profile/SAML2/Unsolicited/SSO?execution=e1s2"

for inputtag in formsoup.find_all(re.compile('(FORM|form)')):
 action = inputtag.get('action')
 if action:
 parsedurl = urlparse(idp_entry_url)
 nexturl = parsedurl.scheme + "://" + parsedurl.netloc + action

response = session.post(
 nexturl, data=payload, verify=sslverification)
```

**步骤4** 客户端解析IdP的响应。客户端提交用户信息给企业IdP系统认证，IdP认证用户信息成功后，发送响应给客户端，客户端解析出SAMLResponse参数。

**Client4ShibbolethIdP脚本实现：**

```
Decode the response and extract the SAML assertion
soup = BeautifulSoup(response.text.decode('utf8'), "lxml")
SAMLResponse = ""

Look for the SAMLResponse attribute of the input tag
for inputtag in soup.find_all('input'):
```

```
if (inputtag.get('name') == 'SAMLResponse'):
 SAMLResponse = inputtag.get('value')

Better error handling is required for production use.
if (SAMLResponse == ''):
 print 'Response did not contain a valid SAML assertion, please troubleshooting in Idp side.'
 sys.exit(0)
```

**步骤5** 获取Unscoped token。参考[获取联邦认证unscoped token\(IdP initiated\)](#)

Client4ShibbolethIdP脚本实现:

```
Set headers
headers = {}
headers["X-Idp-Id"] = "test_local_idp"

IAM API url: get unscoped token on IDP initiated mode
sp_unscoped_token_url = "https://iam.example.com/v3.0/OS-FEDERATION/tokens"

Set form data
payload = {}
payload["SAMLResponse"] = SAMLResponse
response = session.post(
 sp_unscoped_token_url, data=payload, headers=headers, verify=sslverification)

Debug only
print(response.text)
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
 sys.exit(1)

unscoped_token = response.headers.get("X-Subject-Token") if "X-Subject-Token" in response.headers.keys()
else None
if unscoped_token:
 print ">>>>>>X-Subject-Token: " + unscoped_token
```

**步骤6** 获取Scoped token。参考[获取联邦认证scoped token](#)

Client4ShibbolethIdP脚本实现:

```
payload = {
 "auth": {
 "identity": {
 "methods": ["token"],
 "token": {
 "id": unscoped_token
 }
 },
 "scope": {
 "project": {
 "name": "{region_id}_test1"
 }
 }
 }
}

sp_scoped_token_url = "https://10.120.171.90:31943/v3/auth/tokens"

response = session.post(
 sp_scoped_token_url, json=payload, verify=sslverification)

Debug only
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
 print response.text
 sys.exit(1)

scoped_token = response.text if response.status_code == 201 else None
if scoped_token:
 print ">>>>>>Scoped Token:" + scoped_token
```

**步骤7** 获取临时访问密钥。参考[获取用户的临时访问密钥和securitytoken](#)。

Client4ShibbolethIdP脚本实现：

```
Set form data
payload = {
 "auth": {
 "identity": {
 "methods": ["token"],
 "token": {
 "duration_seconds": "900"
 }
 }
 }
}

Set headers
headers = {}
headers["X-Auth-Token"] = unscoped_token

sp_STS_token_url = "https://10.120.171.90:31943/v3.0/OS-CREDENTIAL/securitytokens"

response = session.post(
 sp_STS_token_url, json=payload, headers=headers, verify=sslverification)

Debug only
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
 print response.text
 sys.exit(1)

sts_token = response.text if response.status_code == 201 else None
if sts_token:
 print ">>>>>>STS Token:" + sts_token
```

----结束

## 5.13.2 身份提供商

### 5.13.2.1 查询身份提供商列表

#### 功能介绍

该接口可以用于查询身份提供商列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/identity\_providers



## 请求参数

表 5-647 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-648 响应 Body 参数

参数	参数类型	描述
<a href="#">identity_providers</a>	Array of objects	身份提供商信息列表。
<a href="#">links</a>	Object	资源链接信息。

表 5-649 identity\_providers

参数	参数类型	描述
sso_type	String	身份提供商类型。当前支持如下两种： <ul style="list-style-type: none"> <li>virtual_user_sso：联邦登录跳转后映射为虚拟用户。</li> <li>iam_user_sso：联邦登录跳转后映射为实际存在的IAM用户。</li> </ul> 默认配置为virtual_user_sso类型。
id	String	身份提供商ID。
description	String	身份提供商描述信息。
enabled	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	Array of strings	身份提供商的联邦用户ID列表。
<a href="#">links</a>	Object	身份提供商的资源链接信息。

表 5-650 identity\_providers.links

参数	参数类型	描述
self	String	身份提供商的资源链接地址。
protocols	String	协议的资源链接地址。

表 5-651 links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

## 请求示例

查询身份提供商列表。

GET [https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity\\_providers](https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers)

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers",
 "previous": null,
 "next": null
 },
 "identity_providers": [
 {
 "remote_ids": [],
 "enabled": true,
 "id": "ACME",
 "sso_type": "iam_user_sso",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",
 "protocols": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
 },
 "description": "Stores ACME identities."
 }
]
}
```

## 返回值

返回值	描述
200	请求成功。

返回值	描述
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.2.2 查询身份提供商详情

#### 功能介绍

该接口可以用于查询身份提供商详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/identity\_providers/{id}

表 5-652 路径参数

参数	是否必选	参数类型	描述
id	是	String	待查询的身份提供商ID。

## 请求参数

表 5-653 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token（无需特殊权限）。

## 响应参数

表 5-654 响应 Body 参数

参数	参数类型	描述
<a href="#">identity_provider</a>	Object	身份提供商信息。

表 5-655 identity\_provider

参数	参数类型	描述
sso_type	String	身份提供商类型。当前支持如下两种： <ul style="list-style-type: none"> <li>virtual_user_sso：联邦登录跳转后映射为虚拟用户。</li> <li>iam_user_sso：联邦登录跳转后映射为实际存在的IAM用户。</li> </ul> 默认配置为virtual_user_sso类型。
id	String	身份提供商ID。
description	String	身份提供商描述信息。
enabled	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	Array of strings	身份提供商的联邦用户ID列表。
<a href="#">links</a>	Object	身份提供商的资源链接信息。

表 5-656 identity\_provider.links

参数	参数类型	描述
self	String	身份提供商的资源链接地址。
protocols	String	协议的资源链接地址。

## 请求示例

查询身份提供商详情。

GET https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity\_providers/{id}

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "identity_provider": {
 "remote_ids": [],
 "enabled": true,
 "id": "ACME",
 "sso_type": "iam_user_sso",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",
 "protocols": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
 },
 "description": "Stores ACME identities."
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.2.3 创建身份提供商

#### 功能介绍

该接口可以用于[管理员](#)创建身份提供商。请创建身份提供商后，注册协议并修改身份提供商配置。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3/OS-FEDERATION/identity\_providers/{id}

表 5-657 路径参数

参数	是否必选	参数类型	描述
id	是	String	身份提供商名称。

#### 请求参数

表 5-658 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-659 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">identity_provider</a>	是	Object	身份提供商信息。

表 5-660 identity\_provider

参数	是否必选	参数类型	描述
sso_type	否	String	<p>身份提供商类型。当前支持如下两种：</p> <ul style="list-style-type: none"> <li>virtual_user_sso：联邦登录跳转后映射为虚拟用户。</li> <li>iam_user_sso：联邦登录跳转后映射为实际存在的IAM用户。如果选择该类型，请确保您已在华为云创建IAM用户。</li> </ul> <p>默认配置为virtual_user_sso类型，同一个账号下两种类型不能同时存在，且iam_user_sso最多只能创建一个。</p>
description	否	String	身份提供商描述信息。
enabled	否	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。

## 响应参数

表 5-661 响应 Body 参数

参数	参数类型	描述
<a href="#">identity_provider</a>	Object	身份提供商信息。

表 5-662 identity\_provider

参数	参数类型	描述
sso_type	String	身份提供商类型。
id	String	身份提供商ID。
description	String	身份提供商描述信息。

参数	参数类型	描述
enabled	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	Array of strings	身份提供商的联邦用户ID列表。
<a href="#">links</a>	Object	身份提供商的资源链接信息。

表 5-663 identity\_provider.links

参数	参数类型	描述
self	String	身份提供商的资源链接地址。
protocols	String	协议的资源链接地址。

## 请求示例

创建身份提供商并且启用。

```
PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{id}
{
 "identity_provider": {
 "sso_type": "iam_user_sso",
 "description": "Stores ACME identities.",
 "enabled": true
 }
}
```

## 响应示例

状态码为 201 时:

请求成功。

```
{
 "identity_provider": {
 "remote_ids": [],
 "enabled": true,
 "id": "ACME",
 "sso_type": "iam_user_sso",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",
 "protocols": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
 },
 "description": "Stores ACME identities."
 }
}
```



## 返回值

返回值	描述
201	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
409	资源冲突。
413	请求体过大。
500	请求体过大。
503	服务不可用。

## 错误码

无

### 5.13.2.4 修改 SAML 身份提供商配置

#### 功能介绍

该接口可以用于[管理员](#)修改基于SAML协议的身份提供商配置。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PATCH /v3/OS-FEDERATION/identity\_providers/{id}

表 5-664 路径参数

参数	是否必选	参数类型	描述
id	是	String	待更新的身份提供商ID。

## 请求参数

表 5-665 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-666 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">identity_provider</a>	是	Object	身份提供商信息。

表 5-667 identity\_provider

参数	是否必选	参数类型	描述
description	否	String	身份提供商描述信息。
enabled	否	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。

## 响应参数

表 5-668 响应 Body 参数

参数	参数类型	描述
<a href="#">identity_provider</a>	Object	身份提供商信息。

表 5-669 identity\_provider

参数	参数类型	描述
sso_type	String	身份提供商类型。

参数	参数类型	描述
id	String	身份提供商ID。
description	String	身份提供商描述信息。
enabled	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	Array of strings	身份提供商的联邦用户ID列表。
<b>links</b>	Object	身份提供商的资源链接信息。

表 5-670 identity\_provider.links

参数	参数类型	描述
self	String	身份提供商的资源链接地址。
protocols	String	协议的资源链接地址。

## 请求示例

修改SAML身份提供商为不启用。

```
PATCH https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{id}
{
 "identity_provider": {
 "description": "Stores ACME identities.",
 "enabled": false
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "identity_provider": {
 "remote_ids": [],
 "enabled": false,
 "id": "ACME",
 "sso_type": "iam_user_sso",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME",
 "protocols": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
 },
 "description": "Stores ACME identities."
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
409	资源冲突。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.2.5 删除 SAML 身份提供商

#### 功能介绍

该接口可以用于[管理员](#)删除基于SAML协议的身份提供商。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

DELETE /v3/OS-FEDERATION/identity\_providers/{id}

表 5-671 路径参数

参数	是否必选	参数类型	描述
id	是	String	待删除的身份提供商ID。

## 请求参数

表 5-672 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

无

## 请求示例

删除SAML身份提供商。

```
DELETE https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{id}
```

## 响应示例

无

## 返回值

返回值	描述
204	删除成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

## 5.13.2.6 创建 OpenID Connect 身份提供商配置

### 功能介绍

该接口可以用于[管理员](#)在[创建身份提供商](#)，并[注册协议](#)（OIDC协议）后，创建 OpenID Connect 身份提供商配置。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

POST /v3.0/OS-FEDERATION/identity-providers/{idp\_id}/openid-connect-config

表 5-673 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。

### 请求参数

表 5-674 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-675 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">openid_connect_config</a>	是	object	OpenID Connect配置详情。

表 5-676 CreateOpenIDConnectConfig

参数	是否必选	参数类型	描述
access_mode	是	String	访问方式。 <ul style="list-style-type: none"> <li>program_console: 支持编程访问和管理控制台访问方式。</li> <li>program: 支持编程访问方式</li> </ul>
idp_url	是	String	OpenID Connect身份提供商标识，对应ID token中iss字段。 最小长度：10。最大长度：255。
client_id	是	String	在OpenID Connect身份提供商注册的客户端ID。 最小长度：5。最大长度：255。
authorization_endpoint	否	String	OpenID Connect身份提供商授权地址。 <b>访问方式为program_console必选。</b> 最小长度：10。最大长度：255。
scope	否	String	授权请求信息范围。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>openid</li> <li>email</li> <li>profile</li> </ul> <b>说明</b> <ul style="list-style-type: none"> <li>此字段必选值“openid”。</li> <li>最少1个值，最多10个值，之间使用空格分割。</li> </ul> 例如："openid"、"openid email"、"openid profile"、"openid email profile"。
response_type	否	String	授权请求返回的类型。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>id_token</li> </ul>
response_mode	否	String	授权请求返回方式。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>fragment</li> <li>form_post</li> </ul>

参数	是否必选	参数类型	描述
signing_key	是	String	<p>OpenID Connect身份提供商ID Token签名的公钥。</p> <p>最小长度：10。最大长度：30000。</p> <p>格式示例：</p> <pre> {   "keys": [     {       "kid": "d05ef20c4512645v1...",       "n": "cws_cnjiwsbwweolwn_vnl...",       "e": "AQAB",       "kty": "RSA",       "use": "sig",       "alg": "RS256"     }   ] } </pre>

## 响应参数

状态码为 201 时:

表 5-677 响应 Body 参数

参数	参数类型	描述
<a href="#">openid_connect_config</a>	object	OpenID Connect配置详情。

表 5-678 openid\_connect\_config

参数	参数类型	描述
access_mode	String	<p>访问方式。</p> <ul style="list-style-type: none"> <li>program_console: 支持编程访问和管理控制台访问方式。</li> <li>program: 支持编程访问方式。</li> </ul>
idp_url	String	OpenID Connect身份提供商标识。对应ID token中iss字段。
client_id	String	在OpenID Connect身份提供商注册的客户端ID。
authorization_endpoint	String	OpenID Connect身份提供商授权地址。 <b>访问方式为program方式时返回null。</b>



参数	参数类型	描述
scope	String	授权请求信息范围。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• openid</li> <li>• email</li> <li>• profile</li> </ul> <b>说明</b> <ul style="list-style-type: none"> <li>• 此字段必选值“openid”。</li> <li>• 最少1个值，最多10个值，之间使用空格分割。 例如：“openid”、“openid email”、“openid profile”、“openid email profile”。</li> </ul>
response_type	String	授权请求返回的类型。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• id_token</li> </ul>
response_mode	String	授权请求返回方式。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• fragment</li> <li>• form_post</li> </ul>
signing_key	String	OpenID Connect身份提供商ID Token签名的公钥。

## 请求示例

- 创建支持编程访问配置的OpenID Connect身份提供商。

POST /v3.0/OS-FEDERATION/identity-providers/{idp\_id}/openid-connect-config

```
{
 "openid_connect_config": {
 "access_mode": "program",
 "idp_url": "https://accounts.example.com",
 "client_id": "client_id_example",
 "signing_key": "{\"keys\": [{\"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\"}]}"
 }
}
```
- 创建支持编程访问和管理控制台访问配置的OpenID Connect身份提供商。

POST /v3.0/OS-FEDERATION/identity-providers/{idp\_id}/openid-connect-config

```
{
 "openid_connect_config": {
 "access_mode": "program_console",
 "idp_url": "https://accounts.example.com",
 "client_id": "client_id_example",
 "authorization_endpoint": "https://accounts.example.com/o/oauth2/v2/auth",
 "scope": "openid",
 }
}
```

```
"response_type" : "id_token",
"response_mode" : "form_post",
"signing_key" : "{ \"keys\": [{ \"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\" }] }"
```

## 响应示例

状态码为 201 时:

创建成功。

- 示例 1

```
{
 "openid_connect_config" : {
 "access_mode" : "program",
 "idp_url" : "https://accounts.example.com",
 "client_id" : "client_id_example",
 "signing_key" : "{ \"keys\": [{ \"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\" }] }"
```

- 示例 2

```
{
 "openid_connect_config" : {
 "access_mode" : "program_console",
 "idp_url" : "https://accounts.example.com",
 "client_id" : "client_id_example",
 "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
 "scope" : "openid",
 "response_type" : "id_token",
 "response_mode" : "form_post",
 "signing_key" : "{ \"keys\": [{ \"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\" }] }"
```

## 状态码

状态码	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
409	资源已存在。
500	系统内部错误。

## 错误码

请参见[错误码](#)。

### 5.13.2.7 修改 OpenID Connect 身份提供商配置

#### 功能介绍

该接口可以用于[管理员](#)修改OpenID Connect身份提供商配置。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3.0/OS-FEDERATION/identity-providers/{idp\_id}/openid-connect-config

表 5-679 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商ID。 最小长度：1。最大长度：64。

#### 请求参数

表 5-680 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-681 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">openid_connect_config</a>	是	object	OpenID Connect配置详情。

表 5-682 openid\_connect\_config

参数	是否必选	参数类型	描述
access_mode	否	String	访问方式。 <ul style="list-style-type: none"> <li>program_console: 支持编程访问和管理控制台访问方式。</li> <li>program: 支持编程访问方式</li> </ul>
idp_url	否	String	OpenID Connect身份提供商标识，对应ID token中iss字段。 最小长度：10。最大长度：255。
client_id	否	String	在OpenID Connect身份提供商注册的客户端ID。 最小长度：5。最大长度：255。
authorization_endpoint	否	String	OpenID Connect身份提供商授权地址。 <b>访问方式为program_console必选。</b> 最小长度：10。最大长度：255。
scope	否	String	授权请求信息范围。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>openid</li> <li>email</li> <li>profile</li> </ul> <b>说明</b> <ul style="list-style-type: none"> <li>此字段必选值“openid”。</li> <li>最少1个值，最多10个值，之间使用空格分割。</li> </ul> 例如：“openid”、“openid email”、“openid profile”、“openid email profile”。
response_type	否	String	授权请求返回的类型。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>id_token</li> </ul>
response_mode	否	String	授权请求返回方式。 <b>访问方式为program_console必选。</b> 枚举值： <ul style="list-style-type: none"> <li>fragment</li> <li>form_post</li> </ul>

参数	是否必选	参数类型	描述
signing_key	否	String	<p>OpenID Connect身份提供商ID Token签名的公钥。</p> <p>最小长度：10。最大长度：30000。</p> <p>格式示例：</p> <pre> {   "keys": [     {       "kid": "d05ef20c4512645v1...",       "n": "cws_cnjiwsbwveolwn_vnl...",       "e": "AQAB",       "kty": "RSA",       "use": "sig",       "alg": "RS256"     }   ] } </pre>

## 响应参数

状态码为 200 时:

表 5-683 响应 Body 参数

参数	参数类型	描述
<a href="#">openid_connect_config</a>	object	OpenID Connect配置详情。

表 5-684 OpenIDConnectConfig

参数	参数类型	描述
access_mode	String	<p>访问方式。</p> <ul style="list-style-type: none"> <li>program_console: 支持编程访问和管理控制台访问方式。</li> <li>program: 支持编程访问方式</li> </ul>
idp_url	String	OpenID Connect身份提供商标识，对应ID token中iss字段。
client_id	String	在OpenID Connect身份提供商注册的客户端ID。
authorization_endpoint	String	OpenID Connect身份提供商授权地址。 <b>访问方式为program方式时返回null。</b>

参数	参数类型	描述
scope	String	授权请求信息范围。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• openid</li> <li>• email</li> <li>• profile</li> </ul> <b>说明</b> <ul style="list-style-type: none"> <li>• 此字段必选值“openid”。</li> <li>• 最少1个值，最多10个值，之间使用空格分割。 例如：“openid”、“openid email”、“openid profile”、“openid email profile”。</li> </ul>
response_type	String	授权请求返回的类型。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• id_token</li> </ul>
response_mode	String	授权请求返回方式。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• fragment</li> <li>• form_post</li> </ul>
signing_key	String	OpenID Connect身份提供商ID Token签名的公钥。

## 请求示例

- 修改编程访问配置

```
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config
```

```
{
 "openid_connect_config": {
 "access_mode": "program",
 "idp_url": "https://accounts.example.com",
 "client_id": "client_id_example",
 "signing_key": "{\"keys\": [{\"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\"}]}"
 }
}
```

- 修改编程访问和管理控制台访问配置

```
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config
```

```
{
 "openid_connect_config": {
 "access_mode": "program_console",
 "idp_url": "https://accounts.example.com",
 "client_id": "client_id_example",
 "authorization_endpoint": "https://accounts.example.com/o/oauth2/v2/auth",
 "scope": "openid",
 }
}
```

```
"response_type" : "id_token",
"response_mode" : "form_post",
"signing_key" : "{ \"keys\": [{ \"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\" }] }"
```

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "openid_connect_config" : {
 "access_mode" : "program_console",
 "idp_url" : "https://accounts.example.com",
 "client_id" : "client_id_example",
 "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
 "scope" : "openid",
 "response_type" : "id_token",
 "response_mode" : "form_post",
 "signing_key" : "{ \"keys\": [{ \"key\": \"RSA\", \"e\": \"AQAB\", \"use\": \"sig\", \"n\": \"example\", \"kid\": \"kid_example\", \"alg\": \"RS256\" }] }"
 }
}
```

## 状态码

状态码	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
500	系统内部错误。

## 错误码

请参见[错误码](#)。

### 5.13.2.8 查询 OpenID Connect 身份提供商配置

#### 功能介绍

该接口可以用于[管理员](#)查询OpenID Connect身份提供商配置。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3.0/OS-FEDERATION/identity-providers/{idp\_id}/openid-connect-config

表 5-685 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商ID。 最小长度：1。最大长度：64。

## 请求参数

表 5-686 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

状态码为 200 时:

表 5-687 响应 Body 参数

参数	参数类型	描述
<a href="#">openid_connect_config</a>	object	OpenID Connect配置详情。

表 5-688 OpenIDConnectConfig

参数	参数类型	描述
access_mode	String	访问方式。 <ul style="list-style-type: none"> <li>• program_console: 支持编程访问和管理控制台访问方式。</li> <li>• program: 支持编程访问方式</li> </ul>



参数	参数类型	描述
idp_url	String	OpenID Connect身份提供商标识，对应ID token中iss字段。
client_id	String	在OpenID Connect身份提供商注册的客户端ID。
authorization_endpoint	String	OpenID Connect身份提供商授权地址。 <b>访问方式为program方式时返回null。</b>
scope	String	授权请求信息范围。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• openid</li> <li>• email</li> <li>• profile</li> </ul> <b>说明</b> <ul style="list-style-type: none"> <li>• 此字段必选值“openid”。</li> <li>• 最少1个值，最多10个值，之间使用空格分割。</li> </ul> 例如：“openid”、“openid email”、“openid profile”、“openid email profile”。
response_type	String	授权请求返回的类型。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• id_token</li> </ul>
response_mode	String	授权请求返回方式。 <b>访问方式为program方式时返回null。</b> 枚举值： <ul style="list-style-type: none"> <li>• fragment</li> <li>• form_post</li> </ul>
signing_key	String	OpenID Connect身份提供商ID Token签名的公钥。

## 请求示例

查询OpenID Connect身份提供商配置。

```
GET https://{address}/v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config
```

## 响应示例

**状态码为 200 时:**

创建成功。

```
{
 "openid_connect_config": {
```

```

"access_mode" : "program_console",
"idp_url" : "https://accounts.example.com",
"client_id" : "client_id_example",
"authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
"scope" : "openid",
"response_type" : "id_token",
"response_mode" : "form_post",
"signing_key" : "{\"keys\":{\"kt\":\"RSA\", \"e\":\"AQAB\", \"use\":\"sig\", \"n\":\"example\", \"kid\":\"kid_example\", \"alg\":\"RS256\"}}}"
}

```

#### 状态码为 400 时:

参数无效。

```

{
 "error_msg" : "Request body is invalid.",
 "error_code" : "IAM.0011"
}

```

#### 状态码为 401 时:

认证失败。

```

{
 "error_msg" : "Request parameter %(key)s is invalid.",
 "error_code" : "IAM.0007"
}

```

#### 状态码为 403 时:

没有操作权限。

```

{
 "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
 "error_code" : "IAM.0003"
}

```

#### 状态码为 404 时:

未找到相应的资源。

```

{
 "error_msg" : "Could not find %(target)s: %(target_id)s.",
 "error_code" : "IAM.0004"
}

```

#### 状态码为 500 时:

系统内部异常。

```

{
 "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
 "error_code" : "IAM.0006"
}

```

## 状态码

状态码	描述
200	请求成功。
400	参数无效。
401	认证失败。

状态码	描述
403	没有操作权限。
404	未找到相应的资源。
500	系统内部异常。

## 错误码

请参见[错误码](#)。

## 5.13.3 映射

### 5.13.3.1 查询映射列表

#### 功能介绍

该接口可以用于查询映射列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/mappings

#### 请求参数

表 5-689 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-690 响应 Body 参数

参数	参数类型	描述
<b>links</b>	Links object	资源链接信息。
<b>mappings</b>	Array of MappingResult objects	映射信息列表。

表 5-691 links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

表 5-692 mappings

参数	参数类型	描述
id	String	映射ID。
<b>links</b>	Object	映射的资源链接信息。
<b>rules</b>	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-693 mappings.links

参数	参数类型	描述
self	String	资源链接地址。

表 5-694 mappings.rules

参数	参数类型	描述
<b>local</b>	Array of RulesLocal objects	表示联邦用户在本系统中的用户信息。user:联邦用户在本系统中的用户名称。group:联邦用户在本系统中所属用户组。

参数	参数类型	描述
<b>remote</b>	Array<Object >	表示联邦用户在IdP中的用户信息。由断言属性及运算符组成的表达式，取值由断言决定。

表 5-695 mappings.rules.local

参数	参数类型	描述
<b>user</b>	user object	联邦用户在本系统中的用户名称
<b>group</b>	group object	联邦用户在本系统中所属用户组

表 5-696 mappings.rules.local.user

名称	类型	描述
name	String	联邦用户在本系统中的用户名称

表 5-697 mappings.rules.local.group

名称	类型	描述
name	String	联邦用户在本系统中所属用户组

表 5-698 mappings.rules.remote

参数	参数类型	描述
type	String	表示IdP断言（SAML协议）或ID token（OIDC协议）中的属性。
any_one_of	Array of strings	输入属性值中包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。在同一个remote数组元素中，any_one_of与not_any_of互斥，两者至多填写一个，不能同时填写。
not_any_of	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 请求示例

查询映射列表。

GET https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "mappings": [
 {
 "rules": [
 {
 "local": [
 {
 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
 "name": "LocalGroup"
 }
 }
],
 "remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
 }
],
 "id": "ACME",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/ACME"
 }
 }
],
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings",
 "previous": null,
 "next": null
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。

返回值	描述
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.3.2 查询映射详情

#### 功能介绍

该接口可以用于查询映射详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/mappings/{id}

表 5-699 路径参数

参数	是否必选	参数类型	描述
id	是	String	待查询的映射ID。

#### 请求参数

表 5-700 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-701 响应 Body 参数

参数	参数类型	描述
<a href="#">mapping</a>	Object	映射信息。

表 5-702 mapping

参数	参数类型	描述
id	String	映射ID。
<a href="#">links</a>	Object	映射的资源链接信息。
<a href="#">rules</a>	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-703 mapping.links

参数	参数类型	描述
self	String	资源链接地址。

表 5-704 mappings.rules

参数	参数类型	描述
<a href="#">local</a>	Array of RulesLocal objects	表示联邦用户在本系统中的用户信息。user:联邦用户在本系统中的用户名称。group:联邦用户在本系统中所属用户组。
<a href="#">remote</a>	Array<Object >	表示联邦用户在IdP中的用户信息。由断言属性及运算符组成的表达式，取值由断言决定。



表 5-705 mappings.rules.local

参数	参数类型	描述
<code>user</code>	user object	联邦用户在本系统中的用户名称
<code>group</code>	group object	联邦用户在本系统中所属用户组

表 5-706 mappings.rules.local.user

名称	类型	描述
name	String	联邦用户在本系统中的用户名称

表 5-707 mappings.rules.local.group

名称	类型	描述
name	String	联邦用户在本系统中所属用户组

表 5-708 mapping.rules.remote

参数	参数类型	描述
type	String	表示IdP断言（SAML协议）或ID token（OIDC协议）中的属性。
any_one_of	Array of strings	输入属性值中包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。在同一个remote数组元素中，any_one_of与not_any_of互斥，两者至多填写一个，不能同时填写。
not_any_of	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 请求示例

查询映射列表。

```
GET https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/{id}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "mapping": {
```

```

"rules": [
 {
 "local": [
 {
 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
 "name": "LocalGroup"
 }
 }
],
 "remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
 }
],
"id": "ACME",
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/ACME"
}
}

```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.3.3 注册映射

#### 功能介绍

该接口可以用于[管理员](#)注册映射。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3/OS-FEDERATION/mappings/{id}

表 5-709 路径参数

参数	是否必选	参数类型	描述
id	是	String	待注册的映射ID。

#### 请求参数

表 5-710 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-711 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">mapping</a>	是	Object	映射信息。

表 5-712 mapping

参数	是否必选	参数类型	描述
<b>rules</b>	是	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-713 mapping.rules

参数	是否必选	参数类型	描述
<b>local</b>	是	Array of RulesLocal objects	表示联邦用户在本系统中的用户信息。 user:联邦用户在本系统中的用户名称。 group:联邦用户在本系统中所属用户组。
<b>remote</b>	是	Array of objects	表示联邦用户在IdP中的用户信息。使用SAML协议时，由断言属性及运算符组成的表达式，取值由断言决定。使用OIDC协议时，取值由ID token决定。

表 5-714 mappings.rules.local

参数	是否必选	参数类型	描述
<b>user</b>	否	user object	联邦用户在本系统中的用户名称
<b>group</b>	否	group object	联邦用户在本系统中所属用户组

表 5-715 mappings.rules.local.user

名称	是否必选	类型	描述
name	是	String	联邦用户在本系统中的用户名称

表 5-716 mappings.rules.local.group

名称	是否必选	类型	描述
name	是	String	联邦用户在本系统中所属用户组

表 5-717 mapping.rules.remote

参数	是否必选	参数类型	描述
type	是	String	表示IdP断言（SAML协议）或ID token（OIDC协议）中的属性。
any_one_of	否	Array of strings	输入属性值中包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。在同一个remote数中，any_one_of与not_any_of互斥，两者至多填写一个，不能同时填写。
not_any_of	否	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 响应参数

表 5-718 响应 Body 参数

参数	参数类型	描述
<b>mapping</b>	Object	映射信息。

表 5-719 mapping

参数	参数类型	描述
id	String	映射ID。
<b>links</b>	Object	映射的资源链接信息。
<b>rules</b>	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-720 mapping.links

参数	参数类型	描述
self	String	资源链接地址。

表 5-721 mappings.rules

参数	参数类型	描述
<b>local</b>	Array of objects	表示联邦用户在本系统中的用户信息。user: 联邦用户在本系统中的用户名称。group: 联邦用户在本系统中所属用户组。
<b>remote</b>	Array of objects	表示联邦用户在IdP中的用户信息。使用SAML协议时, 由断言属性及运算符组成的表达式, 取值由断言决定。使用OIDC协议时, 取值由ID token 决定。

表 5-722 mappings.rules.local

参数	参数类型	描述
<b>user</b>	user object	联邦用户在本系统中的用户名称
<b>group</b>	group object	联邦用户在本系统中所属用户组

表 5-723 mappings.rules.local.user

名称	类型	描述
name	String	联邦用户在本系统中的用户名称

表 5-724 mappings.rules.local.group

名称	类型	描述
name	String	联邦用户在本系统中所属用户组

表 5-725 mapping.rules.remote

参数	参数类型	描述
type	String	表示IdP断言 ( SAML协议 ) 或ID token ( OIDC协议 ) 中的属性。

参数	参数类型	描述
any_one_of	Array of strings	输入属性值中包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。在同一个remote数组元素中，any_one_of与not_any_of互斥，两者至多填写一个，不能同时填写。
not_any_of	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 请求示例

注册映射。

```
PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/{id}
{
 "mapping": {
 "rules": [
 {
 "local": [
 {
 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
 "name": "LocalGroup"
 }
 }
],
 "remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
 }
]
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "mapping": {
 "rules": [
 {
 "local": [
 {
```

```

 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
 "name": "LocalGroup"
 }
 }
],
"remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
}
],
"id": "ACME",
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/ACME"
}
}
}

```

## 返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
409	资源冲突。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无



### 5.13.3.4 更新映射

#### 功能介绍

该接口可以用于[管理员](#)更新映射。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PATCH /v3/OS-FEDERATION/mappings/{id}

表 5-726 路径参数

参数	是否必选	参数类型	描述
id	是	String	待更新的映射ID。

#### 请求参数

表 5-727 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-728 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">mapping</a>	是	Object	映射信息。

表 5-729 mapping

参数	是否必选	参数类型	描述
<b>rules</b>	是	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-730 mapping.rules

参数	是否必选	参数类型	描述
<b>local</b>	是	Array of RulesLocal objects	表示联邦用户在本系统中的用户信息。 user:联邦用户在本系统中的用户名称。 group:联邦用户在本系统中所属用户组。
<b>remote</b>	是	Array of objects	表示联邦用户在IdP中的用户信息。使用SAML协议时，由断言属性及运算符组成的表达式，取值由断言决定。使用OIDC协议时，取值由ID token决定。

表 5-731 mappings.rules.local

参数	是否必选	参数类型	描述
<b>user</b>	否	user object	联邦用户在本系统中的用户名称
<b>group</b>	否	group object	联邦用户在本系统中所属用户组

表 5-732 mappings.rules.local.user

名称	是否必选	类型	描述
name	是	String	联邦用户在本系统中的用户名称

表 5-733 mappings.rules.local.group

名称	是否必选	类型	描述
name	是	String	联邦用户在本系统中所属用户组

表 5-734 mapping.rules.remote

参数	是否必选	参数类型	描述
type	是	String	表示IdP断言中的属性。
any_one_of	否	Array of strings	输入属性值中包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。在同一个remote数组元素中，any_one_of与not_any_of互斥，两者至多填写一个，不能同时填写。
not_any_of	否	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 响应参数

表 5-735 响应 Body 参数

参数	参数类型	描述
<b>mapping</b>	Object	映射信息。

表 5-736 mapping

参数	参数类型	描述
id	String	映射ID。
<b>links</b>	Object	映射的资源链接信息。
<b>rules</b>	Array of objects	将联邦用户映射为本地用户的规则列表。

表 5-737 mapping.links

参数	参数类型	描述
self	String	资源链接地址。

表 5-738 mappings.rules

参数	参数类型	描述
<b>local</b>	Array of objects	表示联邦用户在本系统中的用户信息。user: 联邦用户在本系统中的用户名称。group: 联邦用户在本系统中所属用户组。
<b>remote</b>	Array of objects	表示联邦用户在IdP中的用户信息。使用SAML协议时, 由断言属性及运算符组成的表达式, 取值由断言决定。使用OIDC协议时, 取值由ID token 决定。

表 5-739 mappings.rules.local

参数	参数类型	描述
<b>user</b>	user object	联邦用户在本系统中的用户名称
<b>group</b>	group object	联邦用户在本系统中所属用户组

表 5-740 mappings.rules.local.user

名称	类型	描述
name	String	联邦用户在本系统中的用户名称

表 5-741 mappings.rules.local.group

名称	类型	描述
name	String	联邦用户在本系统中所属用户组

表 5-742 mapping.rules.remote

参数	参数类型	描述
type	String	表示IdP断言 ( SAML协议 ) 或ID token ( OIDC协议 ) 中的属性。
any_one_of	Array of strings	输入属性值中包含指定值才生效, 并返回布尔值, 返回值不能用于local块中的占位符。在同一个remote数组元素中, any_one_of与not_any_of 互斥, 两者至多填写一个, 不能同时填写。

参数	参数类型	描述
not_any_of	Array of strings	输入属性值中不包含指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。not_any_of与any_one_of互斥，两者至多填写一个，不能同时填写。

## 请求示例

更新映射。

```
PATCH https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/{id}
{
 "mapping": {
 "rules": [
 {
 "local": [
 {
 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
 "name": "LocalGroup"
 }
 }
],
 "remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
 }
]
 }
}
```

## 响应示例

**状态码为 200 时:**

请求成功。

```
{
 "mapping": {
 "rules": [
 {
 "local": [
 {
 "user": {
 "name": "LocalUser"
 }
 },
 {
 "group": {
```

```
 "name": "LocalGroup"
 }
],
 "remote": [
 {
 "type": "UserName"
 },
 {
 "type": "orgPersonType",
 "not_any_of": [
 "Contractor",
 "Guest"
]
 }
]
 }
},
"id": "ACME",
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/ACME"
}
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
409	资源冲突。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.3.5 删除映射

#### 功能介绍

该接口可以用于[管理员](#)删除映射。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

DELETE /v3/OS-FEDERATION/mappings/{id}

表 5-743 路径参数

参数	是否必选	参数类型	描述
id	是	String	待删除的映射ID。

## 请求参数

表 5-744 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

无

## 请求示例

删除映射。

```
DELETE https://iam.myhuaweicloud.com/v3/OS-FEDERATION/mappings/{id}
```

## 响应示例

无

## 返回值

返回值	描述
204	删除成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

## 5.13.4 协议

### 5.13.4.1 查询协议列表

#### 功能介绍

该接口可以用于查询协议列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols

表 5-745 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商ID。



## 请求参数

表 5-746 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-747 响应 Body 参数

参数	参数类型	描述
<a href="#">links</a>	Object	资源链接信息。
<a href="#">protocols</a>	Array of objects	协议信息列表。

表 5-748 links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

表 5-749 protocols

参数	参数类型	描述
id	String	协议ID。
mapping_id	String	映射ID。
<a href="#">links</a>	Object	协议的资源链接信息。

表 5-750 protocols.links

参数	参数类型	描述
identity_provider	String	身份提供商的资源链接地址。
self	String	资源链接地址。

## 请求示例

查询协议列表。

GET https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/protocols",
 "previous": null,
 "next": null
 },
 "protocols": [
 {
 "mapping_id": "ACME",
 "id": "saml",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml",
 "identity_provider": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME"
 }
 }
]
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。

返回值	描述
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.4.2 查询协议详情

#### 功能介绍

该接口可以用于查询协议详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}

表 5-751 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商ID。
protocol_id	是	String	待查询的协议ID。

#### 请求参数

表 5-752 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-753 响应 Body 参数

参数	参数类型	描述
<b>protocol</b>	Object	协议信息。

表 5-754 protocol

参数	参数类型	描述
id	String	协议ID。
mapping_id	String	映射ID。
<b>links</b>	Object	协议的资源链接信息。

表 5-755 protocol.links

参数	参数类型	描述
identity_provider	String	身份提供商的资源链接地址。
self	String	资源链接地址。

## 请求示例

查询协议详情。

GET https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "protocol": {
 "mapping_id": "ACME",
 "id": "saml",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml",
 "identity_provider": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME"
 }
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.4.3 注册协议

#### 功能介绍

该接口可以用于[管理员](#)在[创建身份提供商](#)后，将协议关联到某一身份提供商。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

PUT /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}

表 5-756 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	待注册的协议ID。该字段内容为“saml”或“oidc”。

## 请求参数

表 5-757 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-758 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">protocol</a>	是	Object	协议信息。

表 5-759 protocol

参数	是否必选	参数类型	描述
mapping_id	否	String	映射ID。身份提供商类型为 iam_user_sso时，不需要绑定映射ID，无需传入此字段；否则此字段必填。

## 响应参数

表 5-760 响应 Body 参数

参数	参数类型	描述
<a href="#">protocol</a>	Object	协议信息。

表 5-761 protocol

参数	参数类型	描述
id	String	协议ID。该字段内容为“saml”或“oidc”。
mapping_id	String	映射ID。
<a href="#">links</a>	Object	协议的资源链接信息。

表 5-762 protocol.links

参数	参数类型	描述
identity_provider	String	身份提供商的资源链接地址。
self	String	资源链接地址。

## 请求示例

注册协议。

```
PUT https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
{
 "protocol": {
 "mapping_id": "ACME"
 }
}
```

## 响应示例

状态码为 201 时:

请求成功。

```
{
 "protocol": {
 "mapping_id": "ACME",
 "id": "saml",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml",
 "identity_provider": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME"
 }
 }
}
```

## 返回值

返回值	描述
201	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.4.4 更新协议

## 功能介绍

该接口可以用于[管理员](#)更新协议。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

PATCH /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}

表 5-763 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	待更新的协议ID。

## 请求参数

表 5-764 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-765 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">protocol</a>	是	Object	协议信息。



表 5-766 protocol

参数	是否必选	参数类型	描述
mapping_id	否	String	映射ID。身份提供商类型为 iam_user_sso 时，不需要绑定映射ID，无需传入此字段；否则此字段必填。

## 响应参数

表 5-767 响应 Body 参数

参数	参数类型	描述
<b>protocol</b>	Object	协议信息。

表 5-768 protocol

参数	参数类型	描述
id	String	协议ID。
mapping_id	String	映射ID。
<b>links</b>	Object	协议的资源链接信息。

表 5-769 protocol.links

参数	参数类型	描述
identity_provider	String	身份提供商的资源链接地址。
self	String	资源链接地址。

## 请求示例

更新协议。

```
PATCH https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
{
 "protocol": {
 "mapping_id": "ACME"
 }
}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "protocol": {
 "mapping_id": "ACME",
 "id": "saml",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/
saml",
 "identity_provider": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/ACME"
 }
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
409	资源冲突。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.4.5 删除协议

#### 功能介绍

该接口可以用于[管理员](#)删除协议。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

DELETE /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}

表 5-770 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	待删除的协议ID。

## 请求参数

表 5-771 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

无

## 请求示例

删除协议。

```
DELETE https://iam.myhuaweicloud.com/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
```

## 响应示例

无

## 返回值

返回值	描述
204	删除成功。
400	参数无效。
401	认证失败。

返回值	描述
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

## 5.13.5 Metadata

### 5.13.5.1 查询 Metadata 文件

#### 功能介绍

该接口可以用于[管理员](#)查询身份提供商导入到IAM中的Metadata文件。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3-ext/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}/metadata

表 5-772 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	协议ID。

## 请求参数

表 5-773 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

## 响应参数

表 5-774 响应 Body 参数

参数	参数类型	描述
id	String	Metadata的ID。
idp_id	String	身份提供商名称。
entity_id	String	Metadata文件中的entityID字段。
protocol_id	String	协议ID。
domain_id	String	用户所属账号ID。
xaccount_type	String	账号来源，默认为空。
update_time	String	导入或更新Metadata文件的时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DD HH:mm:ss。
data	String	Metadata文件的内容。

## 请求示例

查询Metadata文件。

```
GET https://iam.myhuaweicloud.com/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "domain_id": "d78cbac186b744899480f25bd022f468",
 "update_time": "2020-02-12T13:26:25.0",
```

```
"data": "<md:EntityDescript...",
"idp_id": "ACME",
"protocol_id": "saml",
"id": "11354739a6c940bc899fd9070ed1036d",
"entity_id": "https://idp.test.com/idp/shibboleth",
"xaccount_type": ""
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
500	内部服务错误。

## 错误码

无

### 5.13.5.2 查询 Keystone 的 Metadata 文件

#### 功能介绍

该接口可以用于查询keystone的Metadata文件。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /v3-ext/auth/OS-FEDERATION/SSO/metadata

#### 请求参数

表 5-775 请求 Header 参数

参数	是否必选	参数类型	描述
unsigned	否	Boolean	是否按SAML2.0规范对元数据做签名，默认为false。

## 响应参数

无

## 请求示例

查询Keystone的Metadata文件。

```
GET https://iam.myhuaweicloud.com/v3-ext/auth/OS-FEDERATION/SSO/metadata
```

## 响应示例

状态码为 200 时:

请求成功。

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor ID="Mc106d5b14b70a4945fa270d8b52d0ed" entityID="https://
iam.myhuaweicloud.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 <ds:SignedInfo>
 <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
 <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
 <ds:Reference URI="#Mc106d5b14b70a4945fa270d8b52d0ed">
 <ds:Transforms>
 <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
 <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
 </ds:Transforms>
 <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
 <ds:DigestValue>GmS+Nvta/AvNy4fE7dFID5D+P1U=</ds:DigestValue>
 </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue>ljRL...</ds:SignatureValue>
 </ds:Signature>
 <ds:KeyInfo>
 <ds:X509Data>
 <ds:X509Certificate>MIIC...</ds:X509Certificate>
 </ds:X509Data>
 </ds:KeyInfo>
</md:EntityDescriptor>
<md:SPSSODescriptor WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
 <md:KeyDescriptor use="signing">
 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 <ds:X509Data>
 <ds:X509Certificate>MIIC...</ds:X509Certificate>
 </ds:X509Data>
 </ds:KeyInfo>
 </md:KeyDescriptor>
 <md:KeyDescriptor use="encryption">
 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 <ds:X509Data>
 <ds:X509Certificate>MIIC...</ds:X509Certificate>
 </ds:X509Data>
 </ds:KeyInfo>
 </md:KeyDescriptor>
 <md:NameIDFormat
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</
md:NameIDFormat>
 <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://iam.myhuaweicloud.com/v3-ext/auth/OS-FEDERATION/SSO/SAML2/POST" index="0"
isDefault="true" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" />
 <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
Location="https://iam.myhuaweicloud.com/v3-ext/auth/OS-FEDERATION/SSO/SAML2/ECP" index="1"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" />
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

## 返回值

返回值	描述
200	请求成功。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.5.3 导入 Metadata 文件

#### 功能介绍

该接口可以用于[管理员](#)导入Metadata文件。

账号在使用联邦认证功能前，需要先将Metadata文件导入到IAM中。Metadata文件是SAML 2.0协议约定的接口文件，包含访问接口地址和证书信息，请找企业管理员获取企业IdP的Metadata文件。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3-ext/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}/metadata

表 5-776 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	协议ID。



## 请求参数

表 5-777 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	访问令牌，承载用户的身份、权限等信息。 token所需权限请参见 <a href="#">授权项</a> 。

表 5-778 请求 Body 参数

参数	是否必选	参数类型	描述
domain_id	是	String	用户所属账号ID。
xaccount_type	是	String	该字段为标识租户来源字段，默认为空。
metadata	是	String	该字段为用户IdP服务器的Metadata文件的内容。

## 响应参数

表 5-779 响应 Body 参数

参数	参数类型	描述
message	String	导入结果信息。

## 请求示例

导入Metadata文件。

```
POST https://iam.myhuaweicloud.com/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata
{
 "xaccount_type": "",
 "domain_id": "d78cbac186b744899480f25bd...",
 "metadata": "<md:EntityDescript..."
}
```

## 响应示例

状态码为 201 时:

导入成功。

```
{
 "message": "Import metadata successful"
}
```

## 返回值

返回值	描述
201	导入成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
500	内部服务错误。

## 错误码

无

## 5.13.6 Token

### 5.13.6.1 获取联邦认证 unscoped token(IdP initiated)

#### 功能介绍

该接口可以用于通过IdP initiated的联邦认证方式获取unscoped token。

Unscoped token不能用来鉴权，若联邦用户需要使用token进行鉴权，请参考[获取联邦认证scoped token](#)获取scoped token。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 📖 说明

- 该接口支持在命令行侧调用，需要客户端使用IdP initiated的联邦认证方式获取SAMLResponse，并采用浏览器提交表单数据的方式，获取unscoped token。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

POST /v3.0/OS-FEDERATION/tokens

## 请求参数

表 5-780 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	客户端必须使用浏览器提交表单数据的方式向服务端传SAMLResponse参数，故该字段需取值如下：application/x-www-form-urlencoded
X-Idp-Id	是	String	身份提供商ID。

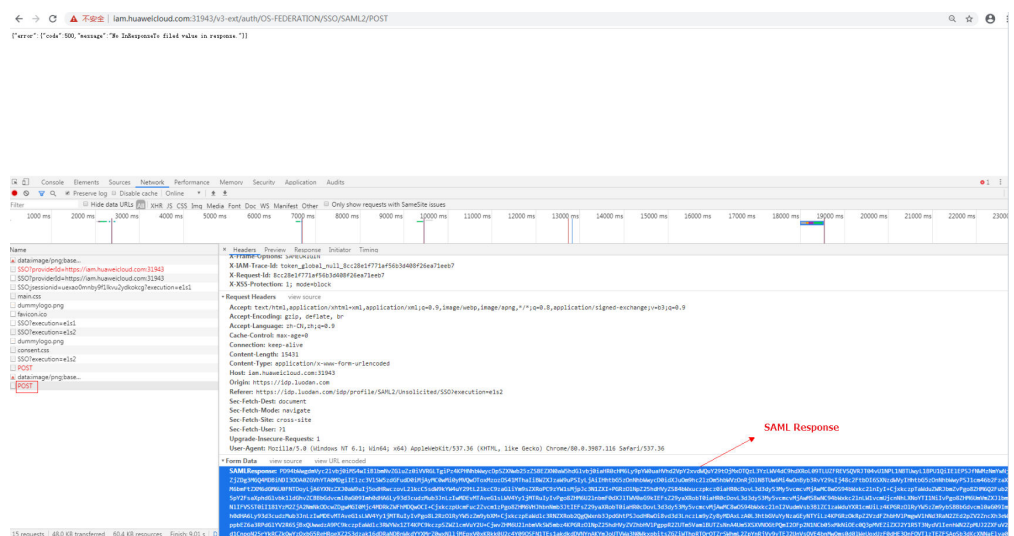
表 5-781 请求 formData 参数

参数	是否必选	参数类型	描述
SAMLResponse	是	String	在IdP认证成功后返回的响应体。

### SAMLResponse获取方式：

1. 在浏览器的地址栏输入并跳转链接：<https://idp.example.org/idp/profile/SAML2/Unsolicited/SSO?providerId=iam.example.com>。
2. idp.example.org：IDPmetadata中的entityID；  
iam.example.com：SPmetadata中获取的entityID。
3. 该链接可打开身份提供商登录页面，根据需要输入映射规则中的用户名（支持免密登录），单击登录，跳入认证页面后按F12，单击认证页面的accept。从下图所示的POST中获取SAMLResponse。

图 5-6 获取 SAMLResponse



## 响应参数

表 5-782 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的unscoped token。

表 5-783 响应 Body 参数

参数	参数类型	描述
<b>token</b>	Object	联邦认证的unscoped token信息。

表 5-784 token

参数	参数类型	描述
issued_at	String	token产生时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
expires_at	String	token到期时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
methods	Array of strings	获取token的方式。
<b>user</b>	Object	获取token的用户信息。

表 5-785 token.user

参数	参数类型	描述
<b>domain</b>	Object	用户所属账号信息。
id	String	用户ID。
name	String	用户名称。
<b>OS-FEDERATION</b>	Object	联邦身份认证信息。

表 5-786 token.user.domain

参数	参数类型	描述
name	String	用户所属账号名。
id	String	用户所属账号ID。

表 5-787 token.user.OS-FEDERATION

参数	参数类型	描述
<b>groups</b>	Array of objects	用户组信息列表。
<b>identity_provider</b>	Object	身份提供商信息。
<b>protocol</b>	Object	协议信息。

表 5-788 token.user.OS-FEDERATION.groups

参数	参数类型	描述
id	String	用户组ID。
name	String	用户组名称。

表 5-789 token.user.OS-FEDERATION.identity\_provider

参数	参数类型	描述
id	String	身份提供商ID。

表 5-790 token.user.OS-FEDERATION.protocol

参数	参数类型	描述
id	String	协议ID。

## 请求示例

获取联邦认证unscoped token(IdP initiated)。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-FEDERATION/tokens
SAMLResponse=PD94b...
```

## 响应示例

### 状态码为 201 时:

创建成功。

响应Header参数:

X-Subject-Token:MIlatAYJKoZlhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
 "token": {
 "expires_at": "2020-02-13T14:21:34.042000Z",
 "methods": [
 "mapped"
],
 "issued_at": "2020-02-12T14:21:34.042000Z",
 "user": {
 "OS-FEDERATION": {
 "identity_provider": {
 "id": "ACME"
 },
 "protocol": {
 "id": "saml"
 },
 "groups": [
 {
 "id": "06aa22601502cec4a23ac0084a74038f",
 "name": "admin"
 }
]
 },
 "domain": {
 "name": "IAMDomain",
 "id": "06ba0970a097acc0f36c0086bb6cfe0"
 },
 "name": "FederationUser",
 "id": "LdUTYSC7zmJVlic3yaCbLBDxPAdDxLg"
 }
 }
}
```

## 返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.6.2 获取联邦认证 scoped token

#### 功能介绍

该接口可以用于通过联邦认证方式获取scoped token。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3/auth/tokens

#### 请求参数

表 5-791 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	否	String	该字段内容填为“application/json;charset=utf8”。

表 5-792 请求 Body 参数

参数	是否必选	参数类型	描述
<b>auth</b>	是	Object	认证信息。

表 5-793 auth

参数	是否必选	参数类型	描述
<b>identity</b>	是	Object	认证参数。
<b>scope</b>	是	Object	token的使用范围，取值为project或domain，二选一即可。

表 5-794 auth.identity

参数	是否必选	参数类型	描述
methods	是	Array of strings	认证方法，该字段内容为“token”。
<b>token</b>	是	Object	联邦unscoped token的信息。

表 5-795 auth.identity.token

参数	是否必选	参数类型	描述
id	是	String	联邦unscoped token的ID。

表 5-796 auth.scope

参数	是否必选	参数类型	描述
<b>domain</b>	否	Object	取值为domain时，表示获取的token可以跨区域使用，domain支持id和name，二选一即可。
<b>project</b>	否	Object	取值为project时，表示获取的token仅能访问指定project下的资源，project支持id和name，二选一即可。

表 5-797 auth.scope.domain

参数	是否必选	参数类型	描述
id	否	String	账号ID，id与name二选一即可。
name	否	String	账号名，id与name二选一即可。

表 5-798 auth.scope.project

参数	是否必选	参数类型	描述
<b>domain</b>	否	Object	项目所属账号，使用name时必填。
id	否	String	项目ID，id与name二选一即可。



参数	是否必选	参数类型	描述
name	否	String	项目名, id与name二选一即可。

表 5-799 auth.scope.project.domain

参数	是否必选	参数类型	描述
id	否	String	账号ID, id与name二选一即可。
name	否	String	账号名, id与name二选一即可。

## 响应参数

表 5-800 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的scoped token。

表 5-801 响应 Body 参数

参数	参数类型	描述
<b>token</b>	Object	联邦认证的scoped token信息。

表 5-802 token

参数	参数类型	描述
methods	Array of strings	获取token的方式。
expires_at	String	token过期时间。 <b>说明</b> UTC时间, 格式为YYYY-MM-DDTHH:mm:ss.ssssssZ, 日期和时间戳格式参照ISO-8601, 如: 2023-06-28T08:56:33.710000Z。
<b>catalog</b>	Array of objects	服务目录信息。
<b>domain</b>	Object	获取token的用户所属的账号信息。如果获取token时请求体中scope参数设置为domain, 则返回该字段。

参数	参数类型	描述
<b>project</b>	Object	获取token的用户所属账号的项目信息。如果获取token时请求体中scope参数设置为project，则返回该字段。
<b>roles</b>	Array of objects	token的权限信息。
<b>user</b>	Object	获取token的用户信息。
issued_at	String	token下发时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。

表 5-803 token.catalog

参数	参数类型	描述
type	String	该接口所属服务。
id	String	服务ID。
name	String	服务名称。
<b>endpoints</b>	Array of objects	终端节点。

表 5-804 token.catalog.endpoints

参数	参数类型	描述
url	String	终端节点的URL。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
id	String	终端节点ID。

表 5-805 token.domain

参数	参数类型	描述
name	String	账号名。

参数	参数类型	描述
id	String	账号ID。

表 5-806 token.project

参数	参数类型	描述
name	String	项目名。
id	String	项目ID。
<b>domain</b>	Object	项目所属账号信息。

表 5-807 token.project.domain

参数	参数类型	描述
name	String	账号名。
id	String	账号ID。

表 5-808 token.roles

参数	参数类型	描述
name	String	权限名称。
id	String	权限ID。默认显示为0，非真实权限ID。

表 5-809 token.user

参数	参数类型	描述
<b>domain</b>	Object	用户所属账号信息。
<b>OS-FEDERATION</b>	Object	联邦身份认证信息。
id	String	用户ID。
name	String	用户名。
password_expires_at	String	密码过期时间，“ ”表示密码不过期。 <b>说明</b> UTC时间，格式为 YYYY-MM-DDTHH:mm:ss.sssssZ，日期和时间戳格式参照 <a href="#">ISO-8601</a> ，如：2023-06-28T08:56:33.710000Z。

表 5-810 token.user.domain

参数	参数类型	描述
name	String	用户所属账号名称。
id	String	用户所属账号ID。

表 5-811 token.user.OS-FEDERATION

参数	参数类型	描述
<b>groups</b>	Array of objects	用户组信息列表。
<b>identity_provider</b>	Object	身份提供商信息。
<b>protocol</b>	Object	协议信息。

表 5-812 token.user.OS-FEDERATION.groups

参数	参数类型	描述
id	String	用户组ID。
name	String	用户组名称。

表 5-813 token.user.OS-FEDERATION.identity\_provider

参数	参数类型	描述
id	String	身份提供商ID。

表 5-814 token.user.OS-FEDERATION.protocol

参数	参数类型	描述
id	String	协议ID。

## 请求示例

获取联邦认证Scoped token。

```
POST https://iam.myhuaweicloud.com/v3/auth/tokens
{
 "auth": {
 "identity": {
```

```
 "methods": [
 "token"
],
 "token": {
 "id": "MIIlatAYJKoZlIhvcNAQcCollapTCCGqECAQExDTALB..."
 }
 },
 "scope": {
 "domain": {
 "id": "063bb260a480cecc0f36c0086bb6c..."
 }
 }
}
```

## 响应示例

### 状态码为 201 时:

创建成功。

响应Header参数:

X-Subject-Token:MIIlatAYJKoZlIhvcNAQcCollapTCCGqECAQExDTALB...

响应Body参数:

```
{
 "token": {
 "expires_at": "2020-02-13T14:21:34.042000Z",
 "methods": [
 "token"
],
 "catalog": [
 {
 "endpoints": [
 {
 "id": "d2983f677ce14f1e81cbb6a9345a107a",
 "interface": "public",
 "region": "*",
 "region_id": "*",
 "url": "https://iam.ap-southeast-1.myhuaweicloud.com/v3"
 }
],
 "id": "fd631b3426cb40f0919091d5861d8fea",
 "name": "keystone",
 "type": "identity"
 }
],
 "domain": {
 "id": "06aa2260a480cecc0f36c0086bb6cfe0",
 "name": "IAMDomain"
 },
 "roles": [
 {
 "id": "0",
 "name": "te_admin"
 },
 {
 "id": "0",
 "name": "secu_admin"
 }
],
 "issued_at": "2020-02-12T14:21:34.042000Z",
 "user": {
 "OS-FEDERATION": {
 "groups": [
 {
 "id": "06aa2260bb00cecc3f3ac0084a74038f",
 "name": "admin"
 }
],
 }
 }
 },
}
```

```
 "identity_provider": {
 "id": "ACME"
 },
 "protocol": {
 "id": "saml"
 }
 },
 "domain": {
 "id": "06aa2260a480cecc0f36c0086bb6cfe0",
 "name": "IAMDomain"
 },
 "id": "LdQTDSC7zmJVlic3yaCbLBXDxPAdDxLg",
 "name": "FederationUser",
 "password_expires_at": ""
} }
}
```

## 返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
500	内部服务错误。
503	服务不可用。

## 错误码

无

### 5.13.6.3 获取联邦认证 token(OpenID Connect ID token 方式)

#### 功能介绍

该接口可以用于通过OpenID Connect ID token方式获取联邦认证token。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3.0/OS-AUTH/id-token/tokens

## 请求参数

表 5-815 请求 Header 参数

参数	是否必选	参数类型	描述
X-Idp-Id	是	String	身份提供商ID。

表 5-816 请求 Body 参数

参数	是否必选	参数类型	描述
<b>auth</b>	是	object	请求auth参数详情。

表 5-817 GetIdTokenAuthParams

参数	是否必选	参数类型	描述
<b>id_token</b>	是	object	请求id token参数详情。
<b>scope</b>	否	object	请求scope参数详情，限制获取token的权限范围。不传此字段，获取unscoped toke。

表 5-818 GetIdTokenIdTokenBody

参数	是否必选	参数类型	描述
id	是	String	id_token的值。id_token由企业IdP构建，携带联邦用户身份信息。请参考企业IdP文档了解获取id_token的方法。

表 5-819 GetIdTokenIdScopeBody

参数	是否必选	参数类型	描述
<b>domain</b>	否	object	domain scope详情，与project二选一。
<b>project</b>	否	object	project scope详情，与domain二选一。

表 5-820 GetIdTokenScopeDomainOrProjectBody

参数	是否必选	参数类型	描述
id	否	String	domain id或者project id, 与name字段至少存在一个。
name	否	String	domain name或者project name, 与id字段至少存在一个。

## 响应参数

状态码为 201 时:

表 5-821 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的Token。

表 5-822 响应 Body 参数

参数	参数类型	描述
<b>token</b>	object	获取的token详情。

表 5-823 token

参数	参数类型	描述
expires_at	String	过期时间。 <b>说明</b> UTC时间, 格式为YYYY-MM-DDTHH:mm:ss.ssssssZ, 日期和时间戳格式参照 <a href="#">ISO-8601</a> , 如: 2023-06-28T08:56:33.710000Z。
methods	Array of strings	获取token的方式, 联邦用户默认为mapped。
issued_at	String	生成时间。 <b>说明</b> UTC时间, 格式为YYYY-MM-DDTHH:mm:ss.ssssssZ, 日期和时间戳格式参照 <a href="#">ISO-8601</a> , 如: 2023-06-28T08:56:33.710000Z。
<b>user</b>	object	用户详情。
<b>domain</b>	object	租户详情。



参数	参数类型	描述
<b>project</b>	object	项目详情，仅请求scope为project时，返回此对象。
<b>roles</b>	Array of objects	角色/策略详情。
<b>catalog</b>	Array of objects	catalog详情。

表 5-824 token.user

参数	参数类型	描述
<b>OS-FEDERATION</b>	object	联邦用户user详情。
<b>domain</b>	object	租户详情。
id	String	用户id。
name	String	用户名。

表 5-825 token.user.OS-FEDERATION

参数	参数类型	描述
<b>identity_provider</b>	object	身份提供商详情。
<b>protocol</b>	object	协议详情。
<b>groups</b>	Array of objects	用户组详情。

表 5-826 token.user.OS-FEDERATION.identity\_provider

参数	参数类型	描述
id	String	身份提供商id。

表 5-827 token.user.OS-FEDERATION.protocol

参数	参数类型	描述
id	String	协议id。

表 5-828 token.user.OS-FEDERATION.groups

参数	参数类型	描述
id	String	用户组id。
name	String	用户组名。

表 5-829 token.user.domain

参数	参数类型	描述
id	String	租户id。
name	String	租户名。

表 5-830 token.domain

参数	参数类型	描述
id	String	租户id。
name	String	租户名。

表 5-831 token.project

参数	参数类型	描述
<b>domain</b>	object	租户详情。
id	String	项目id。
name	String	项目名。

表 5-832 token.project.domain

参数	参数类型	描述
id	String	租户id。
name	String	租户名。

表 5-833 roles

参数	参数类型	描述
id	String	权限id。

参数	参数类型	描述
name	String	权限名。

表 5-834 token.catalog

参数	参数类型	描述
<b>endpoints</b>	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-835 token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

表 5-836 CatalogInfo

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。
url	String	终端节点的URL。

## 请求示例

- 获取联邦认证project scoped token

POST /v3.0/OS-AUTH/id-token/tokens

```
{
 "auth": {
 "id_token": {
 "id": "eyJhbGciOiJSU..."
 },
 "scope": {
 "project": {
 "id": "46419baef4324...",
 "name": "ap-southeast-1"
 }
 }
 }
}
```

- 获取联邦认证domain scoped token

POST /v3.0/OS-AUTH/id-token/tokens

```
{
 "auth": {
 "id_token": {
 "id": "eyJhbGciOiJSU..."
 },
 "scope": {
 "domain": {
 "id": "063bb260a480...",
 "name": "IAMDomain"
 }
 }
 }
}
```

- 获取unscoped token

POST /v3.0/OS-AUTH/id-token/tokens

```
{
 "auth": {
 "id_token": {
 "id": "eyJhbGciOiJSU..."
 }
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

```
{
 "token": {
 "expires_at": "2018-03-13T03:00:01.168000Z",
 "methods": ["mapped"],
 "issued_at": "2018-03-12T03:00:01.168000Z",
 "user": {
 "OS-FEDERATION": {
 "identity_provider": {
 "id": "idptest"
 },
 "protocol": {
 "id": "oidc"
 }
 }
 }
 }
}
```

```

 },
 "groups": [{
 "name": "admin",
 "id": "45a8c8f..."
 }]
 },
 "domain": {
 "id": "063bb260a480...",
 "name": "IAMDomain"
 },
 "name": "FederationUser",
 "id": "suvmgvUZc4PaCOEc..."
}
}
}

```

#### 状态码为 400 时:

参数无效。

```

{
 "error_msg": "Request body is invalid.",
 "error_code": "IAM.0011"
}

```

#### 状态码为 401 时:

认证失败。

```

{
 "error_msg": "The request you have made requires authentication.",
 "error_code": "IAM.0001"
}

```

#### 状态码为 403 时:

没有操作权限。

```

{
 "error_msg": "Policy doesn't allow %(actions)s to be performed.",
 "error_code": "IAM.0003"
}

```

#### 状态码为 404 时:

未找到相应的资源。

```

{
 "error_msg": "Could not find %(target)s: %(target_id)s.",
 "error_code": "IAM.0004"
}

```

#### 状态码为 500 时:

系统内部异常。

```

{
 "error_msg": "An unexpected error prevented the server from fulfilling your request.",
 "error_code": "IAM.0006"
}

```

## 状态码

状态码	描述
201	创建成功。

状态码	描述
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
500	系统内部异常。

## 错误码

请参见[错误码](#)。

### 5.13.6.4 获取联邦认证 unscoped token(OpenID Connect ID token 方式)

#### 功能介绍

该接口可以用于通过OpenID Connect ID token方式获取联邦认证unscoped token。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3/OS-FEDERATION/identity\_providers/{idp\_id}/protocols/{protocol\_id}/auth

表 5-837 路径参数

参数	是否必选	参数类型	描述
idp_id	是	String	身份提供商名称。
protocol_id	是	String	协议id。

## 请求参数

表 5-838 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	OpenID Connect身份提供商的ID Token，格式为Bearer {ID Token}。

## 响应参数

状态码为 201 时:

表 5-839 响应 Header 参数

参数	参数类型	描述
X-Subject-Token	String	签名后的Token。

表 5-840 响应 Body 参数

参数	参数类型	描述
<b>token</b>	object	获取的token详情。

表 5-841 token

参数	参数类型	描述
expires_at	String	过期时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
methods	Array of strings	token获取方式，联邦认证默认为mapped。
issued_at	String	生成时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照ISO-8601，如：2023-06-28T08:56:33.710000Z。
<b>user</b>	object	用户详情。

参数	参数类型	描述
<b>roles</b>	Array of objects	角色/策略详情。
<b>catalog</b>	Array of objects	catalog详情。

表 5-842 token.user

参数	参数类型	描述
<b>OS-FEDERATION</b>	object	联邦用户user详情。
<b>domain</b>	object	租户详情。
id	String	用户id。
name	String	用户名。

表 5-843 token.user.OS-FEDERATION

参数	参数类型	描述
<b>identity_provider</b>	object	身份提供商详情。
<b>protocol</b>	object	协议详情。
<b>groups</b>	Array of objects	用户组详情。

表 5-844 token.user.OS-FEDERATION.identity\_provider

参数	参数类型	描述
id	String	身份提供商id。

表 5-845 token.user.OS-FEDERATION.identity\_provider

参数	参数类型	描述
id	String	协议id。



表 5-846 token.user.OS-FEDERATION.groups

参数	参数类型	描述
id	String	用户组id。
name	String	用户组名。

表 5-847 token.domain

参数	参数类型	描述
id	String	租户id。
name	String	租户名。

表 5-848 token.roles

参数	参数类型	描述
id	String	权限id。
name	String	权限名。

表 5-849 token.catalog

参数	参数类型	描述
<b>endpoints</b>	Array of objects	终端节点。
id	String	服务ID。
name	String	服务名称。
type	String	该接口所属服务。

表 5-850 token.catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	接口类型，描述接口在该终端节点的可见性。值为“public”，表示该接口为公开接口。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域ID。

参数	参数类型	描述
url	String	终端节点的URL。

## 请求示例

获取联邦认证unscoped token(OpenID Connect ID token方式)。

```
POST https://{address}/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/auth
```

## 响应示例

**状态码为 201 时:**

创建成功。

```
{
 "token": {
 "expires_at": "2018-03-13T03:00:01.168000Z",
 "methods": ["mapped"],
 "issued_at": "2018-03-12T03:00:01.168000Z",
 "user": {
 "OS-FEDERATION": {
 "identity_provider": {
 "id": "idptest"
 },
 "protocol": {
 "id": "oidc"
 },
 "groups": [{
 "name": "admin",
 "id": "45a8c8f..."
 }]
 }
 },
 "domain": {
 "id": "063bb260a480...",
 "name": "IAMDomain"
 },
 "name": "FederationUser",
 "id": "suvmgvUZc4PaCOEc..."
 }
}
```

**状态码为 400 时:**

参数无效。

```
{
 "error": {
 "code": 400,
 "message": "Request parameter 'idp id' is invalid.",
 "title": "Bad Request"
 }
}
```

**状态码为 401 时:**

认证失败。

```
{
 "error": {
 "code": 401,
 "message": "The request you have made requires authentication.",
 }
}
```

```
"title": "Unauthorized"
}
```

#### 状态码为 403 时:

没有操作权限。

```
{
 "error": {
 "code": 403,
 "message": "You are not authorized to perform the requested action.",
 "title": "Forbidden"
 }
}
```

#### 状态码为 404 时:

未找到相应资源。

```
{
 "error": {
 "code": 404,
 "message": "Could not find %(target)s: %(target_id)s.",
 "title": "Not Found"
 }
}
```

#### 状态码为 500 时:

系统内部异常。

```
{
 "error": {
 "code": 500,
 "message": "An unexpected error prevented the server from fulfilling your request.",
 "title": "Internal Server Error"
 }
}
```

## 状态码

状态码	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应资源。
500	系统内部异常。

## 错误码

请参见[错误码](#)。

## 5.13.7 查询联邦用户可以访问的账号列表

### 功能介绍

该接口用于查询联邦用户可以访问的账号列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 说明

- 推荐使用[查询IAM用户可以访问的账号详情](#)，该接口可以返回相同的响应格式。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/OS-FEDERATION/domains

### 请求参数

表 5-851 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	联邦认证的unscoped token。

### 响应参数

表 5-852 响应 Body 参数

参数	参数类型	描述
<a href="#">domains</a>	Array of objects	账号信息列表。
<a href="#">links</a>	Object	资源链接信息。

表 5-853 domains

参数	参数类型	描述
enabled	Boolean	是否启用账号，true为启用，false为停用，默认为true。
id	String	账号ID。

参数	参数类型	描述
name	String	账号名。
<b>links</b>	Object	账号的资源链接信息。
description	String	账号的描述信息。

表 5-854 domains.links

参数	参数类型	描述
self	String	资源链接地址。

表 5-855 links

参数	参数类型	描述
self	String	资源链接地址。

## 请求示例

查询联邦用户可以访问的账号列表。

GET <https://iam.myhuaweicloud.com/v3/OS-FEDERATION/domains>

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "domains": [
 {
 "description": "",
 "enabled": true,
 "id": "d78cbac186b744899480f25bd022f468",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/domains/d78cbac186b744899480f25bd022f468"
 },
 "name": "IAMDomain"
 }
],
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/domains"
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无

## 5.13.8 查询联邦用户可以访问的项目列表

### 功能介绍

该接口可以用于查询联邦用户可以访问的项目列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 说明

- 推荐使用[查询IAM用户可以访问的项目列表](#)，该接口可以返回相同的响应格式。

## URI

GET /v3/OS-FEDERATION/projects

## 请求参数

表 5-856 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	联邦认证的unscoped token信息。

## 响应参数

表 5-857 响应 Body 参数

参数	参数类型	描述
<a href="#">links</a>	Object	资源链接信息。
<a href="#">projects</a>	Array of objects	项目信息列表。

表 5-858 links

参数	参数类型	描述
self	String	资源链接地址。

表 5-859 projects

参数	参数类型	描述
is_domain	Boolean	false.
description	String	项目描述信息。
<a href="#">links</a>	Object	项目的资源链接。
enabled	Boolean	项目是否可用。
id	String	项目ID。
parent_id	String	如果查询自己创建的项目，则此处返回所属区域的项目ID。 如果查询的是系统内置项目，如ap-southeast-1，则此处返回账号ID。
domain_id	String	项目所属账号ID。
name	String	项目名称。

表 5-860 projects.links

参数	参数类型	描述
self	String	资源链接地址。

## 请求示例

GET <https://iam.myhuaweicloud.com/v3/OS-FEDERATION/projects>

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "projects": [
 {
 "domain_id": "d78cbac186b744899480f25...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f2...",
 "name": "af-south-1",
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/06f1cbbaf280106b2f14c00313a9d065"
 },
 "id": "06f1cbbaf280106b2f14c00313a9...",
 "enabled": true
 },
 {
 "domain_id": "d78cbac186b744899480f25bd02...",
 "is_domain": false,
 "parent_id": "d78cbac186b744899480f25bd0...",
 "name": "ap-southeast-1",
 "description": "",
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/projects/065a7c66da0010992ff7c0031e..."
 },
 "id": "065a7c66da0010992ff7c0031e5...",
 "enabled": true
 }
],
 "links": {
 "self": "https://iam.myhuaweicloud.com/v3/OS-FEDERATION/projects"
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
405	未找到相应的资源。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

## 错误码

无



## 5.14 自定义身份代理

### 5.14.1 获取自定义身份代理登录票据

#### 功能介绍

该接口用于获取自定义身份代理登录票据logintoken。logintoken是系统颁发给自定义身份代理用户的登录票据，承载用户的身份、session等信息。调用自定义身份代理URL登录云服务控制台时，可以使用本接口获取的logintoken进行认证。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 说明

自定义身份代理登录票据logintoken默认有效期为10分钟，可设置范围为10分钟~12小时。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

POST /v3.0/OS-AUTH/securitytoken/logintokens

#### 请求参数

表 5-861 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

表 5-862 请求 Body 参数

参数	是否必选	参数类型	描述
<a href="#">auth</a>	是	Object	认证信息。

表 5-863 auth

参数	是否必选	参数类型	描述
<a href="#">securitytoken</a>	是	Object	认证参数。

表 5-864 auth.securitytoken

参数	是否必选	参数类型	描述
access	是	String	AK。
secret	是	String	SK。
id	是	String	<p>即临时安全凭证securitytoken。</p> <p>支持使用自定义身份代理用户或普通用户获取的securitytoken换取logintoken，详情请参见：<a href="#">通过token获取临时访问密钥和securitytoken</a>。</p> <p>支持委托的方式，但获取securitytoken时，请求体中必须填写session_user.name参数，详情请参见：<a href="#">通过委托获取临时访问密钥和securitytoken</a>。</p>
duration_seconds	否	Integer	<p>自定义身份代理登录票据logintoken的有效时间，时间单位为秒。默认10分钟，即600秒，取值范围10分钟~12小时。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>如果传入的值不在取值范围（10分钟~12小时）内，则取默认值10分钟。</li> <li>logintoken有效时间为临时安全凭证securitytoken剩余有效时间与duration_seconds传参的最小值。</li> <li>为避免duration_seconds传参无效，建议设置临时安全凭证securitytoken具有较长的有效期（15分钟~24小时），且duration_seconds传参小于临时安全凭证securitytoken剩余有效时间。</li> <li>当临时安全凭证securitytoken剩余有效时间小于10分钟时，logintoken的有效时间将取默认值10分钟。</li> </ul>

## 响应参数

表 5-865 响应 Header 参数

参数	参数类型	描述
X-Subject-LoginToken	String	签名后的logintoken。

表 5-866 响应 Body 参数

参数	参数类型	描述
<b>logintoken</b>	Object	自定义身份代理登录票据信息。

表 5-867 logintoken

参数	参数类型	描述
domain_id	String	账号ID。
expires_at	String	logintoken的过期时间。
method	String	认证方法。当认证用户为华为云用户时，该字段内容为“token”，当认证用户为自定义身份代理用户时，该字段内容为“federation_proxy”。
user_id	String	用户ID。
user_name	String	用户名。
session_id	String	会话ID。
session_user_id	String	自定义身份代理用户ID。 <b>说明</b> 通过 <a href="#">委托获取临时访问密钥和securitytoken</a> 且请求体中填写session_user.name参数时，会返回该字段。该字段的值即为session_user.name所填写的值。
session_name	String	自定义身份代理用户名。 <b>说明</b> 通过 <a href="#">委托获取临时访问密钥和securitytoken</a> 且请求体中填写session_user.name参数时，会返回该字段。该字段的值即为session_user.name所填写的值。
<b>assumed_by</b>	Object	被委托方用户信息。 <b>说明</b> 通过 <a href="#">委托获取临时访问密钥和securitytoken</a> 且请求体中填写session_user.name参数时，会返回该字段。

表 5-868 logintoken.assumed\_by

参数	参数类型	描述
<a href="#">user</a>	Object	被委托方用户信息。

表 5-869 logintoken.assumed\_by.user

参数	参数类型	描述
<a href="#">domain</a>	Object	被委托方用户所属账号信息。
name	String	被委托方用户名。
password_expires_at	String	被委托方用户的密码过期时间。 <b>说明</b> UTC时间，格式为YYYY-MM-DDTHH:mm:ss.ssssssZ，日期和时间戳格式参照 <a href="#">ISO-8601</a> ，如： 2023-06-28T08:56:33.710000Z。
id	String	被委托方用户ID。

表 5-870 logintoken.assumed\_by.user.domain

参数	参数类型	描述
name	String	被委托方用户所属账号名称。
id	String	被委托方用户所属账号ID。

## 请求示例

获取自定义身份代理登录票据。

```
POST https://iam.myhuaweicloud.com/v3.0/OS-AUTH/securitytoken/logintokens
{
 "auth": {
 "securitytoken": {
 "access": "LUJHNN4WB569PGAP...",
 "secret": "7qtrm2cku0XubixiVkB0cvMfpnu7H2mLN...",
 "id": "gQpjb1ub3J0a...",
 "duration_seconds": "600"
 }
 }
}
```

## 响应示例

状态码为 201 时:

创建成功。

示例1：通过token获取临时访问密钥和securitytoken。

示例2：通过委托获取临时访问密钥和securitytoken且请求体中填写 session\_user.name参数。

● 示例 1

```

响应Header参数:
X-Subject-LoginToken:MIlatAYJKoZlIhvcNAQcCollapTCCGqECAQExDTALB...
响应Body参数:
{
 "logintoken": {
 "domain_id": "05262121fb00d5c30fbec013bc1...",
 "expires_at": "2020-01-20T08:18:36.447000Z",
 "method": "token",
 "user_id": "0526213b8a80d38a1f31c013ed...",
 "user_name": "IAMUser",
 "session_user_id": "093f75808b8089ba1f6dc000c7cac...",
 "session_id": "40b328b6683a41b9bf8e7185e..."
 }
}

```

● 示例 2

```

响应Header参数:
X-Subject-LoginToken:MIlatAYJKoZlIhvcNAQcCollapTCCGqECAQExDTALB...
响应Body参数:
{
 "logintoken": {
 "domain_id": "05262121fb00d5c30fbec01...",
 "expires_at": "2020-01-23T03:27:26.728000Z",
 "method": "federation_proxy",
 "user_id": "07826f367b80d2474ff9c013a...",
 "user_name": "IAMDomainA/IAMAgency",
 "session_id": "0012c8e6adda4ce787e90585d...",
 "session_user_id": "093f75808b8089ba1f6dc000c7cac...",
 "session_name": "SessionUserName",
 "assumed_by": {
 "user": {
 "domain": {
 "name": "IAMDomainB",
 "id": "0659ef9c9c80d4560f14c009ac..."
 },
 "name": "IAMUserB",
 "password_expires_at": "2020-02-16T02:44:57.000000Z",
 "id": "0659ef9d4d00d3b81f26c009fe..."
 }
 }
 }
}

```

## 返回值

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。

返回值	描述
503	服务不可用。

## 错误码

无

## 5.15 版本信息管理

### 5.15.1 查询 Keystone API 的版本信息

#### 功能介绍

该接口用于查询Keystone API的版本信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

#### URI

GET /

#### 请求参数

无

#### 响应参数

表 5-871 响应 Body 参数

参数	参数类型	描述
<a href="#">versions</a>	Object	Keystone API的版本信息。

表 5-872 versions

参数	参数类型	描述
<a href="#">values</a>	Array of objects	Keystone API的版本信息列表。

表 5-873 versions.values

参数	参数类型	描述
status	String	版本状态。
updated	String	最后更新时间。
<b>links</b>	Array of objects	版本的资源链接信息
id	String	版本号，如v3.6。
<b>media-types</b>	Array of objects	支持的消息格式。

表 5-874 versions.values.links

参数	参数类型	描述
rel	String	链接类型。self: 自助链接包含了版本链接的资源。bookmark: 书签链接提供了一个永久资源的永久链接。alternate: 备用链接包含了资源的替换表示形式。
href	String	资源链接地址。

表 5-875 versions.values.media-types

参数	参数类型	描述
type	String	媒体类型。
base	String	基础类型。

## 请求示例

查询Keystone API的版本信息。

GET https://iam.myhuaweicloud.com/

## 响应示例

状态码为 300 时:

查询成功。( Multiple Choices )

```
{
 "versions": {
 "values": [
 {
 "media-types": [
 {
```

```
 "type": "application/vnd.openstack.identity-v3+json",
 "base": "application/json"
 },
],
 "links": [
 {
 "rel": "self",
 "href": "https://iam.myhuaweicloud.com/v3/"
 }
],
 "id": "v3.6",
 "updated": "2016-04-04T00:00:00Z",
 "status": "stable"
}]
}
```

## 返回值

返回值	描述
300	查询成功。( Multiple Choices )
400	参数无效。
404	未找到相应的资源。
503	服务不可用。

## 错误码

无

## 5.15.2 查询 Keystone API 的 3.0 版本信息

### 功能介绍

该接口用于查询Keystone API的3.0版本的信息。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3

### 请求参数

无



## 响应参数

表 5-876 响应 Body 参数

参数	参数类型	描述
<b>version</b>	Object	Keystone API的3.0版本信息。

表 5-877 version

参数	参数类型	描述
status	String	版本状态。
updated	String	最后更新时间。
<b>links</b>	Array of objects	版本的资源链接信息。
id	String	版本号，如v3.6。
<b>media-types</b>	Array of objects	支持的消息格式。

表 5-878 version.links

参数	参数类型	描述
rel	String	链接类型。self: 自助链接包含了版本链接的资源。bookmark: 书签链接提供了一个永久资源的永久链接。alternate: 备用链接包含了资源的替换表示形式。
href	String	资源链接地址。

表 5-879 version.media-types

参数	参数类型	描述
type	String	媒体类型。
base	String	基础类型。

## 请求示例

查询Keystone API的3.0版本信息。

GET <https://iam.myhuaweicloud.com/v3>

## 响应示例

### 状态码为 200 时:

请求成功。

```
{
 "version": {
 "media-types": [
 {
 "type": "application/vnd.openstack.identity-v3+json",
 "base": "application/json"
 }
],
 "links": [
 {
 "rel": "self",
 "href": "https://iam.myhuaweicloud.com/v3/"
 }
],
 "id": "v3.6",
 "updated": "2016-04-04T00:00:00Z",
 "status": "stable"
 }
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
404	未找到相应的资源。
503	服务不可用。

## 错误码

无

## 5.16 服务和终端节点

### 5.16.1 查询服务列表

#### 功能介绍

该接口可以用于查询服务列表。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

#### 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/services

表 5-880 Query 参数

参数	是否必选	参数类型	描述
type	否	String	服务类型。

## 请求参数

表 5-881 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token（无需特殊权限）。

## 响应参数

表 5-882 响应 Body 参数

参数	参数类型	描述
<b>links</b>	Object	服务的资源链接信息。
<b>services</b>	Array of objects	服务信息列表。

表 5-883 links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

表 5-884 services

参数	参数类型	描述
name	String	服务名。
description	String	服务描述信息，未注册服务描述信息时，不返回此字段。
<b>links</b>	Object	服务的资源链接。
id	String	服务ID。
type	String	服务类型。
enabled	Boolean	服务是否可用。

表 5-885 services.links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

## 请求示例

查询服务列表。

```
GET https://iam.myhuaweicloud.com/v3/services
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/services"
 },
 "services": [
 {
 "name": "keystone",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/services/1842ae22353d45a39a1eb89c22f0fe50"
 },
 "id": "1842ae22353d45a39a1eb89c22f0fe50",
 "type": "identity",
 "enabled": true
 }
]
}
```

```
"name": "iam",
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/services/6cf6e23e00dd49beb13313b024aec598"
},
"id": "6cf6e23e00dd49beb13313b024aec598",
"type": "identity",
"enabled": true
}
]
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
501	接口没有实现。
503	服务不可用。

## 错误码

无

## 5.16.2 查询服务详情

### 功能介绍

该接口可以用于查询服务详情。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/services/{service\_id}

表 5-886 路径参数

参数	是否必选	参数类型	描述
service_id	是	String	待查询的服务ID。

## 请求参数

表 5-887 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token（无需特殊权限）。

## 响应参数

表 5-888 响应 Body 参数

参数	参数类型	描述
<a href="#">service</a>	Object	服务信息。

表 5-889 service

参数	参数类型	描述
name	String	服务名。
description	String	服务描述信息，未注册服务描述信息时，不返回此字段。
<a href="#">links</a>	Object	服务的资源链接。
id	String	服务ID。
type	String	服务类型。
enabled	Boolean	服务是否可用。

表 5-890 service.links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

## 请求示例

查询服务详情。

GET https://iam.myhuaweicloud.com/v3/services/{service\_id}

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "service": {
 "name": "iam",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/services/6cf6e23e00dd49beb13313b024aec598"
 }
 },
 "id": "6cf6e23e00dd49beb13313b024aec598",
 "type": "identity",
 "enabled": true
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
501	接口没有实现。
503	服务不可用。

## 错误码

无

## 5.16.3 查询服务目录

### 功能介绍

该接口可以用于查询请求头中X-Auth-Token对应的服务目录。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

### 调试

您可以在[API Explorer](#)中调试该接口。

### URI

GET /v3/auth/catalog

### 请求参数

表 5-891 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token。（无需特殊权限，但token的scope需为project。）

### 响应参数

表 5-892 响应 Body 参数

参数	参数类型	描述
<a href="#">catalog</a>	Array of objects	服务目录信息列表。
<a href="#">links</a>	Object	资源链接信息。



表 5-893 catalog

参数	参数类型	描述
<b>endpoints</b>	Array of objects	终端节点信息。
id	String	服务ID。
name	String	服务名。
type	String	服务类型。

表 5-894 catalog.endpoints

参数	参数类型	描述
id	String	终端节点ID。
interface	String	终端节点平面，public表示为公开。
region	String	终端节点所属区域。
region_id	String	终端节点所属区域的ID。
url	String	终端节点的地址。

表 5-895 links

参数	参数类型	描述
self	String	资源链接地址。

## 请求示例

查询服务目录。

```
GET https://iam.myhuaweicloud.com/v3/auth/catalog
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "catalog": [
 {
 "endpoints": [
 {
 "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
 "interface": "public",
 "region": "*",
 "region_id": "*",
 "url": "https://iam.myhuaweicloud.com/v3.0"
 }
]
 }
]
}
```

```

 }
],
 "id": "100a6a3477f1495286579b819d399e36",
 "name": "iam",
 "type": "iam"
},
{
 "endpoints": [
 {
 "id": "6c91faa9890f40b397542561e3d87444",
 "interface": "public",
 "region": "*",
 "region_id": "*",
 "url": "https://cbc.sample.domain.com/v1.0"
 }
],
 "id": "ad7396ee0eea4281a180c4230641b72f",
 "name": "bss-intlv1",
 "type": "bss-intlv1"
}
],
"links": {
 "self": "https://iam.myhuaweicloud.com/v3/auth/catalog"
}
}

```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
501	接口没有实现。
503	服务不可用。

## 错误码

无

## 5.16.4 查询终端节点列表

### 功能介绍

该接口可以用于查询终端节点列表。终端节点用来提供服务访问入口。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/endpoints

表 5-896 Query 参数

参数	是否必选	参数类型	描述
interface	否	String	终端节点平面。
service_id	否	String	服务ID。

## 请求参数

表 5-897 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token（无需特殊权限）。

## 响应参数

表 5-898 响应 Body 参数

参数	参数类型	描述
<b>endpoints</b>	Array of objects	资源链接地址。
<b>links</b>	Object	终端节点信息列表。

表 5-899 endpoints

参数	参数类型	描述
service_id	String	终端节点所属服务的ID。
region_id	String	终端节点所属区域的ID。
<b>links</b>	Object	终端节点的资源链接信息。

参数	参数类型	描述
id	String	终端节点ID。
interface	String	终端节点平面。
region	String	终端节点所属区域。
url	String	终端节点的地址。
enabled	Boolean	终端节点是否可用。

表 5-900 endpoints.links

参数	参数类型	描述
self	String	资源链接地址。
next	String	后一邻接资源链接地址，不存在时为null。
previous	String	前一邻接资源链接地址，不存在时为null。

表 5-901 links

参数	参数类型	描述
self	String	资源链接地址。
previous	String	前一邻接资源链接地址，不存在时为null。
next	String	后一邻接资源链接地址，不存在时为null。

## 请求示例

查询终端节点列表。

```
GET https://iam.myhuaweicloud.com/v3/endpoints
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "endpoints": [
 {
 "service_id": "3e93d3eb20b34bfbbdccc81a79c1c3045",
 "region_id": "ap-southeast-1",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/endpoints/0046cca357c94165b7a10ec2c01bdf60"
 }
 }
]
}
```

```
"id": "0046cca357c94165b7a10ec2c01bdf60",
"interface": "public",
"region": "ap-southeast-1",
"url": "https://ims.sample.domain.com",
"enabled": true
},
{
 "service_id": "5186586acd38461d84b3dbf9f02e33ae",
 "region_id": "ap-southeast-1",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/endpoints/00d546d4823e452491407284ab26612c"
 },
 "id": "00d546d4823e452491407284ab26612c",
 "interface": "public",
 "region": "ap-southeast-1",
 "url": "https://ges.sample.domain.com/v1.0/${tenant_id}s",
 "enabled": true
}
},
"links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/endpoints"
}
}
```

## 返回值

返回值	描述
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
501	接口没有实现。
503	服务不可用。

## 错误码

无

## 5.16.5 查询终端节点详情

### 功能介绍

该接口可以用于查询终端节点详情。终端节点用来提供服务访问入口。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。IAM的Endpoint请参见：[地区和终端节点](#)。

## 调试

您可以在[API Explorer](#)中调试该接口。

## URI

GET /v3/endpoints/{endpoint\_id}

表 5-902 路径参数

参数	是否必选	参数类型	描述
endpoint_id	是	String	待查询的终端节点ID。

## 请求参数

表 5-903 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	IAM用户的token（无需特殊权限）。

## 响应参数

表 5-904 响应 Body 参数

参数	参数类型	描述
<a href="#">endpoint</a>	Object	终端节点信息。

表 5-905 endpoint

参数	参数类型	描述
service_id	String	终端节点所属服务的ID。
region_id	String	终端节点所属区域的ID。
<a href="#">links</a>	Object	终端节点的资源链接信息。

参数	参数类型	描述
id	String	终端节点ID。
interface	String	终端节点平面。
region	String	终端节点所属区域。
url	String	终端节点的地址。
enabled	Boolean	终端节点是否可用。

表 5-906 endpoint.links

参数	参数类型	描述
self	String	资源链接地址。
next	String	后一邻接资源链接地址，不存在时为null。
previous	String	前一邻接资源链接地址，不存在时为null。

## 请求示例

查询终端节点详情。

```
GET https://iam.myhuaweicloud.com/v3/endpoints/{endpoint_id}
```

## 响应示例

状态码为 200 时:

请求成功。

```
{
 "endpoint": {
 "service_id": "3e93d3eb20b34bfbbdcc81a79c1c3045",
 "region_id": "ap-southeast-1",
 "links": {
 "next": null,
 "previous": null,
 "self": "https://iam.myhuaweicloud.com/v3/endpoints/0046cca357c94165b7a10ec2c01bdf60"
 },
 "id": "0046cca357c94165b7a10ec2c01bdf60",
 "interface": "public",
 "region": "ap-southeast-1",
 "url": "https://ims.sample.domain.com",
 "enabled": true
 }
}
```

## 返回值

返回值	描述
200	请求成功。

返回值	描述
400	参数无效。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
405	不允许的方法。
413	请求体过大。
501	接口没有实现。
503	服务不可用。

## 错误码

无



# 6 历史 API

## 6.1 查询企业项目关联的用户组

### 功能介绍

该接口用于查询指定ID的企业项目所关联的用户组。

#### 说明

根据产品迭代计划，该接口将逐步下线，推荐您使用[查询企业项目关联的用户组](#)。

### URI

- URI格式  
GET /v3.0/OS-PAP/enterprise-projects/{enterprise\_project\_id}/groups
- URI参数说明

属性	是否必选	类型	说明
enterprise_project_id	是	String	待查询的企业项目的ID。

### 请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	已认证的拥有Security Administrator权限的token。
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://iam.myhuaweicloud.com/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0ee5d/groups
```

## 响应

- Reponse Body参数说明

参数	是否必选	类型	说明
groups	是	Array	企业项目关联的用户组详情。

- groups格式说明

参数	是否必选	类型	说明
group_id	是	String	关联用户组的ID。
group_name	是	String	关联用户组的名称。
group_desc	是	String	关联用户组的描述。
user_num	是	Int	关联用户组中的用户数。
policy_num	是	Int	关联用户组的策略数。
created_at	是	Int	关联用户组创建的时间（Unix时间：毫秒）。

- 响应样例：查询的企业项目关联了用户组。

```
{
 "groups": [
 {
 "group_id": "758b99fa1fa24ec4a297d44e092bd...",
 "group_name": "Test",
 "group_desc": "Test",
 "user_num": 4,
 "policy_num": 1,
 "created_at": 1549088526...
 }
]
}
```

- 查询的企业项目没有关联任何用户组，返回的响应体中“groups”的内容为空。

```
{
 "groups": []
}
```

## 状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	鉴权失败。

状态码	说明
404	找不到资源。

## 6.2 查询企业项目已关联用户组的权限

### 功能介绍

该接口用于查询指定ID的企业项目所关联用户组的权限，适用于待查询的企业项目已关联了用户组。

该接口可以使用全局区域的域名调用，全局区域的域名为iam.myhuaweicloud.com。

#### 说明

根据产品迭代计划，该接口将逐步下线，推荐您使用[查询企业项目关联用户组的权限](#)。

### URI

- URI格式  
GET /v3.0/OS-PAP/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles
- URI参数说明

属性	是否必选	类型	说明
enterprise_project_id	是	String	待查询的企业项目的ID。
group_id	是	String	企业项目已关联的用户组的ID。

### 请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	已认证的拥有Security Administrator权限的token。
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://iam.myhuaweicloud.com/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles
```

## 响应

- Reponse Body参数说明

参数	是否必选	类型	说明
roles	是	JSONArray	权限的详细信息或者列表。

- role格式说明

参数	是否必选	类型	说明
display_name	是	String	权限在界面中的名称。
description	是	String	权限的英文描述。
description_cn	是	String	权限的中文描述。
domain_id	是	String	<ul style="list-style-type: none"> <li>• 用户组绑定的是自定义策略，该参数为创建该自定义策略用户的租户ID。</li> <li>• 用户组绑定的是系统策略，该参数为空：null。</li> </ul>
flag	否	String	fine_grained，标识系统内置的细粒度权限Role
catalog	是	String	权限所属目录。 <ul style="list-style-type: none"> <li>• 用户组绑定的是自定义策略时，权限所属目录为“CUSTOMED”。</li> <li>• 用户组绑定的是系统预置策略时，权限所属目录为云服务名称，例如：ECS。</li> </ul>
policy	是	Dict	权限的详情。请参见： <a href="#">policy格式说明</a> 。
id	是	String	权限的ID。
type	是	String	权限的显示位置，其中： <ul style="list-style-type: none"> <li>• AX表示在全局项目中显示</li> <li>• XA表示在除全局项目外的其他项目中显示</li> </ul> <b>说明</b> 权限的显示位置只能为AX或者XA，不能在全局项目和其他项目都显示（AA），或者在全局项目和其他项目中都不显示（XX）。
name	是	String	权限在系统内部的名称。

- policy格式说明

参数	是否必选	类型	说明
Version	是	String	策略的版本号。
Statement	是	JSONArray	策略授权语句，限制8个。包括了基本元素：作用（Effect）和权限集（Action）。

- Statement格式说明

参数	是否必选	类型	说明
Effect	是	String	允许（Allow）和拒绝（Deny），当策略中既有Allow又有Deny的授权语句时，遵循Deny优先的原则。
Action	是	StringArray	权限集，对资源的具体操作权限，不能超过100个。 格式为： 服务名:资源类型:操作，例如： vpc:ports:create。 “服务名”为产品名称，例如ecs、evs和vpc等，服务名仅支持小写。 “资源类型”和“操作”没有大小写要求，支持通配符号*，用户不需要罗列全部授权项，通过配置通配符号*可以方便快捷地实现授权。

- 响应样例（响应成功）

```
{
 "roles": [
 {
 "display_name": "Customed ECS Viewer",
 "description": "The read-only permissions to all ECS resources, which can be used for statistics and survey.",
 "domain_id": "9698542758bc422088c0c3eabf...",
 "catalog": "CUSTOMED",
 "policy": {
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "ecs:*get*",
 "ecs:*list*",
 "ecs:blockDevice:use",
 "ecs:serverGroups:manage",
 "ecs:serverVolumes:use",
 "evs:*get*",
 "evs:*list*",
 "vpc:*get*",
 "vpc:*list*",
 "ims:*get*",
]
 }
]
 }
 }
]
}
```

```

 "ims*:list*"
],
 "Effect": "Allow"
 }
]
},
"id": "24e7a89bffe443979760c4e9715c1...",
"type": "XA",
"name": "custom_9698542758bc422088c0c3eabfc30d1..."
}
]
}

```

- Error Reponse Body参数说明

参数	是否必选	类型	说明
error	是	Dict	响应错误。
message	是	String	错误详情。
code	是	Int	状态码。
title	是	String	错误类别。

- 响应样例（响应失败）

```

{
 "error": {
 "message": "Authentication failed",
 "code": 401,
 "title": "Unauthorized"
 }
}

```

## 状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	鉴权失败。
500	内部服务错误。

## 6.3 基于用户组为企业项目授权

### 功能介绍

该接口用于给指定ID的企业项目授权，建立企业项目、用户组和权限的绑定关系。

该接口可以使用全局区域的域名调用，全局区域的域名为iam.myhuaweicloud.com。

 说明

根据产品迭代计划，该接口将逐步下线，推荐您使用[基于用户组为企业项目授权](#)。

## URI

- URI格式  
PUT /v3.0/OS-PAP/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles/{role\_id}
- URI参数说明

属性	是否必选	类型	说明
enterprise_project_id	是	String	企业项目的ID。
group_id	是	String	待授权用户组的ID。
role_id	是	String	权限的ID。只能给用户组授予细粒度权限策略（包括系统策略和自定义策略），细粒度策略即策略版本号为1.1的策略。

## 请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	已认证的拥有Security Administrator权限的token。
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https://iam.myhuaweicloud.com/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles/013ad036ee4c4d108327f02cbb479...
```

## 响应

无响应体。

## 状态码

状态码	说明
204	请求成功。
400	参数无效。
401	认证失败。

状态码	说明
403	鉴权失败。
404	找不到资源。
500	内部服务错误。

## 6.4 删除企业项目关联的用户组权限

### 功能介绍

该接口提供删除某个企业项目关联的用户组权限。

该接口可以使用全局区域的域名调用，全局区域的域名为iam.myhuaweicloud.com。

#### 说明

根据产品迭代计划，该接口将逐步下线，推荐您使用[删除企业项目关联用户组的权限](#)。

### URI

- URI格式  
DELETE /v3.0/OS-PAP/enterprise-projects/{enterprise\_project\_id}/groups/{group\_id}/roles/{role\_id}
- URI参数说明

属性	是否必选	类型	说明
enterprise_project_id	是	String	企业项目的ID。
group_id	是	String	用户组的ID。
role_id	是	String	关联的role的ID。

### 请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	已认证的拥有Security Administrator权限的token。
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

- 请求样例



```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https://iam.myhuaweicloud.com/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles/013ad036ee4c4d108327f02cbb479...
```

## 响应

无响应体。

## 状态码

状态码	说明
204	请求成功。
400	参数无效。
401	认证失败。
403	鉴权失败
404	找不到资源。
500	内部服务错误。

# 7 权限及授权项

## 7.1 权限及授权项说明

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

### 说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

账号具备所有接口的调用权限，如果使用账号下的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，用户要调用接口来查询云服务器列表，那么这个IAM用户被授予的策略中必须包含允许“ecs:servers:list”的授权项，该接口才能调用成功。

## 支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在**自定义策略**中的Action中写入授权项，可以实现授权项对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如

果在企业管理中授权，则该自定义策略不生效。关于IAM项目与企业项目的区别，详情请参见：[IAM项目与企业项目的区别](#)。

**说明**

- “√”表示支持，“×”表示暂不支持，“-”表示不涉及。
- IAM为全局服务，不涉及基于项目授权。
- 目前，存在部分权限仅支持授权项（Action），暂未支持API，如[虚拟MFA管理](#)。

## 7.2 授权项

### Token 管理

权限	对应API接口	授权项 ( Action )	IAM 项目 (Project)	企业项目 (Enterprise Project)
获取委托Token	<a href="#">POST /v3/auth/tokens</a>	iam:tokens:assume	-	-

### 访问密钥管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询所有永久访问密钥	<a href="#">GET /v3.0/OS-CREDENTIAL/credentials</a>	iam:credentials:listCredentials	-	-
查询指定永久访问密钥	<a href="#">GET /v3.0/OS-CREDENTIAL/credentials/{access_key}</a>	iam:credentials:getCredential	-	-
创建永久访问密钥	<a href="#">POST /v3.0/OS-CREDENTIAL/credentials</a>	iam:credentials:createCredential	-	-
修改指定永久访问密钥	<a href="#">PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}</a>	iam:credentials:updateCredential	-	-
删除指定永久访问密钥	<a href="#">DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}</a>	iam:credentials:deleteCredential	-	-

## 虚拟 MFA 管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
绑定MFA设备	<a href="#">PUT /v3.0/OS-MFA/mfa-devices/bind</a>	iam:mfa:bindMFADevice	-	-
解绑MFA设备	<a href="#">PUT /v3.0/OS-MFA/mfa-devices/unbind</a>	iam:mfa:unbindMFADevice	-	-
创建虚拟MFA设备密钥	<a href="#">POST /v3.0/OS-MFA/virtual-mfa-devices</a>	iam:mfa:createVirtualMFADevice	-	-
删除MFA设备	<a href="#">DELETE /v3.0/OS-MFA/virtual-mfa-devices</a>	iam:mfa:deleteVirtualMFADevice	-	-

## 项目管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询项目列表	<a href="#">GET /v3/projects</a>	iam:projects:listProjects	-	-
创建项目	<a href="#">POST /v3/projects</a>	iam:projects:createProject	-	-
修改项目信息	<a href="#">PATCH /v3/projects/{project_id}</a>	iam:projects:updateProject	-	-
设置项目状态	<a href="#">PUT /v3-ext/projects/{project_id}</a>	iam:projects:updateProject	-	-
查询指定IAM用户的项目列表	<a href="#">GET /v3/users/{user_id}/projects</a>	iam:projects:listProjectsForUser	-	-
删除指定项目	×	iam:projects:deleteProject	-	-
查询指定项目的配额	<a href="#">GET /v3.0/OS-QUOTA/projects/{project_id}</a>	iam:quotas:listQuotasForProject	-	-

## 账号管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询账号配额	<a href="#">GET /v3.0/OS-QUOTA/domains/{domain_id}</a>	iam:quotas:list Quotas	-	-

## IAM 用户管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
管理员查询IAM 用户列表	<a href="#">GET /v3/users</a>	iam:users:listUsers	-	-
管理员创建IAM 用户	<a href="#">POST /v3/users</a>	iam:users:create User	-	-
管理员修改IAM 用户信息	<a href="#">PATCH /v3/users/{user_id}</a>	iam:users:updateUser	-	-
管理员删除IAM 用户	<a href="#">DELETE /v3/users/{user_id}</a>	iam:users:delete User	-	-
管理员创建IAM 用户（推荐）	<a href="#">POST /v3.0/OS-USER/users</a>	iam:users:create User	-	-
查询用户详情 (包含邮箱和手机号码)	<a href="#">GET /v3.0/OS-USER/users/{user_id}</a>	iam:users:getUser	-	-
查询IAM用户详情	<a href="#">GET /v3/users/{user_id}</a>	iam:users:getUser	-	-
管理员重置IAM 用户密码	×	iam:users:reset UserPassword	-	-
设置登录保护	×	iam:users:setUserLoginProtect	-	-
查询指定项目上有权限的用户列表	×	iam:users:listUsersForProject	-	-
查询IAM用户的MFA绑定信息列表	<a href="#">GET /v3.0/OS-MFA/virtual-mfa-devices</a>	iam:mfa:listVirtualMFADevices	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询指定IAM用户的MFA绑定信息	<a href="#">GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device</a>	iam:mfa:getVirtualMFADevice	-	-
查询IAM用户的登录保护状态信息列表	<a href="#">GET /v3.0/OS-USER/login-protects</a>	iam:users:listUserLoginProtects	-	-
查询指定IAM用户的登录保护状态信息	<a href="#">GET /v3.0/OS-USER/users/{user_id}/login-protect</a>	iam:users:getUserLoginProtect	-	-

## 用户组管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询IAM用户所属用户组	<a href="#">GET /v3/users/{user_id}/groups</a>	iam:groups:listGroupsForUser	-	-
管理员查询用户组所包含的IAM用户	<a href="#">GET /v3/groups/{group_id}/users</a>	iam:users:listUsersForGroup	-	-
查询用户组列表	<a href="#">GET /v3/groups</a>	iam:groups:listGroups	-	-
查询用户组详情	<a href="#">GET /v3/groups/{group_id}</a>	iam:groups:getGroup	-	-
创建用户组	<a href="#">POST /v3/groups</a>	iam:groups:createGroup	-	-
更新用户组	<a href="#">PATCH /v3/groups/{group_id}</a>	iam:groups:updateGroup	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
删除用户组	<a href="#">DELETE /v3/groups/{group_id}</a>	iam:groups:deleteGroup iam:permissions:removeUserFromGroup iam:permissions:revokeRoleFromGroup iam:permissions:revokeRoleFromGroupOnProject iam:permissions:revokeRoleFromGroupOnDomain	-	-
查询用户是否在用户组中	<a href="#">HEAD /v3/groups/{group_id}/users/{user_id}</a>	iam:permissions:checkUserInGroup	-	-
添加IAM用户到用户组	<a href="#">PUT /v3/groups/{group_id}/users/{user_id}</a>	iam:permissions:addUserToGroup	-	-
移除用户组中的IAM用户	<a href="#">DELETE /v3/groups/{group_id}/users/{user_id}</a>	iam:permissions:removeUserFromGroup	-	-

## 权限管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询权限列表	<a href="#">GET /v3/roles</a>	iam:roles:listRoles	-	-
查询权限详情	<a href="#">GET /v3/roles/{role_id}</a>	iam:roles:getRole	-	-
查询租户授权信息	<a href="#">GET /v3.0/OS-PERMISSION/role-assignments</a>	iam:permissions:listRoleAssignments	√	√

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询全局服务中的用户组权限	<a href="#">GET /v3/domains/{domain_id}/groups/{group_id}/roles</a>	iam:permissions: listRolesForGroupOnDomain	-	-
查询项目服务中的用户组权限	<a href="#">GET /v3/projects/{project_id}/groups/{group_id}/roles</a>	iam:permissions: listRolesForGroupOnProject	-	-
为用户组授予全局服务权限	<a href="#">PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: grantRoleToGroupOnDomain	-	-
为用户组授予项目服务权限	<a href="#">PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: grantRoleToGroupOnProject	-	-
移除用户组的项目服务权限	<a href="#">DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: revokeRoleFromGroupOnProject	-	-
移除用户组的全局服务权限	<a href="#">DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: revokeRoleFromGroupOnDomain	-	-
查询用户组是否拥有全局服务权限	<a href="#">HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: checkRoleForGroupOnDomain	-	-
查询用户组是否拥有项目服务权限	<a href="#">HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}</a>	iam:permissions: checkRoleForGroupOnProject	-	-
为用户组授予所有项目服务权限	<a href="#">PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects</a>	iam:permissions: grantRoleToGroup	-	-
查询用户在指定项目上拥有的权限	x	iam:permissions: listRolesForUserOnProject	-	-



权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询用户组的所有权限	x	iam:permissions:listRolesForGroup	-	-
查询用户组是否拥有指定权限	x	iam:permissions:checkRoleForGroup	-	-
移除用户组的指定权限	x	iam:permissions:revokeRoleFromGroup	-	-
查询账号授权记录	x	iam:permissions:listRoleAssignments	-	-

## 自定义策略管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询自定义策略列表	<a href="#">GET /v3.0/OS-ROLE/roles</a>	iam:roles:listRoles	-	-
查询自定义策略详情	<a href="#">GET /v3.0/OS-ROLE/roles/{role_id}</a>	iam:roles:getRole	-	-
创建云服务自定义策略	<a href="#">POST /v3.0/OS-ROLE/roles</a>	iam:roles:createRole	-	-
修改云服务自定义策略	<a href="#">PATCH /v3.0/OS-ROLE/roles/{role_id}</a>	iam:roles:updateRole	-	-
删除自定义策略	<a href="#">DELETE /v3.0/OS-ROLE/roles/{role_id}</a>	iam:roles:deleteRole	-	-

## 委托管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
创建委托	<a href="#">POST /v3.0/OS-AGENCY/agencies</a>	iam:agencies:createAgency	-	-
查询指定条件下的委托列表	<a href="#">GET /v3.0/OS-AGENCY/agencies</a>	iam:agencies:listAgencies	-	-
查询委托详情	<a href="#">GET /v3.0/OS-AGENCY/agencies/{agency_id}</a>	iam:agencies:getAgency	-	-
修改委托	<a href="#">PUT /v3.0/OS-AGENCY/agencies/{agency_id}</a>	iam:agencies:updateAgency	-	-
删除委托	<a href="#">DELETE /v3.0/OS-AGENCY/agencies/{agency_id}</a>	iam:agencies:deleteAgency	-	-
为委托授予项目服务权限	<a href="#">PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}</a>	iam:permissions:grantRoleToAgencyOnProject	-	-
查询委托是否拥有项目服务权限	<a href="#">HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}</a>	iam:permissions:checkRoleForAgencyOnProject	-	-
查询项目服务中的委托权限	<a href="#">GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles</a>	iam:permissions:listRolesForAgencyOnProject	-	-
移除委托的项目服务权限	<a href="#">DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}</a>	iam:permissions:revokeRoleFromAgencyOnProject	-	-
为委托授予全局服务权限	<a href="#">PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}</a>	iam:permissions:grantRoleToAgencyOnDomain	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询委托是否拥有全局服务权限	HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:checkRoleForAgencyOnDomain	-	-
查询全局服务中的委托权限	GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:permissions:listRolesForAgencyOnDomain	-	-
移除委托的全局服务权限	DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:revokeRoleFromAgencyOnDomain	-	-
查询委托的所有权限	GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:permissions:listRolesForAgency	-	-
查询委托是否拥有指定权限	HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:checkRoleForAgency	-	-
为委托授予指定权限	PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:grantRoleToAgency	-	-
移除委托的指定权限	DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:revokeRoleFromAgency	-	-

## 企业项目管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询企业项目关联的用户组	<b>GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups</b>	iam:permissions:listGroupsOnEnterpriseProject	-	√
查询企业项目已关联用户组的权限	<b>GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles</b>	iam:permissions:listRolesForGroupOnEnterpriseProject	-	√
基于用户组为企业项目授权	<b>PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}</b>	iam:permissions:grantRoleToGroupOnEnterpriseProject	-	√
删除企业项目关联的用户组权限	<b>DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}</b>	iam:permissions:revokeRoleFromGroupOnEnterpriseProject	-	√
查询用户组关联的企业项目	<b>GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects</b>	iam:permissions:listEnterpriseProjectsForGroup	-	√
查询用户直接关联的企业项目	<b>GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects</b>	iam:permissions:listEnterpriseProjectsForUser	-	√
查询企业项目直接关联用户	<b>GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users</b>	iam:permissions:listUsersForEnterpriseProject	-	√
查询企业项目直接关联用户的角色	<b>GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles</b>	iam:permissions:listRolesForUserOnEnterpriseProject	-	√

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
基于用户为企业项目授权	<a href="#">PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}</a>	iam:permissions:grantRoleToUserOnEnterpriseProject	-	√
删除企业项目直接关联用户的权限	<a href="#">DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}</a>	iam:permissions:revokeRoleFromUserOnEnterpriseProject	-	√

## 安全设置

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
修改账号操作保护策略	<a href="#">PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy</a>	iam:securitypolicies:updateProtectPolicy	-	-
查询账号操作保护策略	<a href="#">GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy</a>	iam:securitypolicies:getProtectPolicy	-	-
修改账号密码策略	<a href="#">PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy</a>	iam:securitypolicies:updatePasswordPolicy	-	-
查询账号密码策略	<a href="#">GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy</a>	iam:securitypolicies:getPasswordPolicy	-	-
修改账号登录策略	<a href="#">PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy</a>	iam:securitypolicies:updateLoginPolicy	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询账号登录策略	<a href="#">GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy</a>	iam:securitypolicies:getLoginPolicy	-	-
修改账号控制台访问策略	<a href="#">PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy</a>	iam:securitypolicies:updateConsoleAclPolicy	-	-
查询账号控制台访问策略	<a href="#">GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy</a>	iam:securitypolicies:getConsoleAclPolicy	-	-
修改账号接口访问策略	<a href="#">PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy</a>	iam:securitypolicies:updateApiAclPolicy	-	-
查询账号接口访问策略	<a href="#">GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy</a>	iam:securitypolicies:getApiAclPolicy	-	-

## 联邦身份认证管理

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
查询身份提供商列表	<a href="#">GET /v3/OS-FEDERATION/identity_providers</a>	iam:identityProviders:listIdentityProviders	-	-
查询身份提供商详情	<a href="#">GET /v3/OS-FEDERATION/identity_providers/{id}</a>	iam:identityProviders:getIdentityProvider	-	-
创建SAML身份提供商	<a href="#">PUT /v3/OS-FEDERATION/identity_providers/{id}</a>	iam:identityProviders:createIdentityProvider	-	-
修改SAML身份提供商配置	<a href="#">PATCH /v3/OS-FEDERATION/identity_providers/{id}</a>	iam:identityProviders:updateIdentityProvider	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
删除SAML身份提供商	<a href="#">DELETE /v3/OS-FEDERATION/identity_providers/{id}</a>	iam:identityProviders:deleteIdentityProvider	-	-
创建OIDC身份提供商	<a href="#">POST /v3.0/OS-FEDERATION/identity_providers/{idp_id}/openid-connect-config</a>	iam:identityProviders:createOpenIDConnectConfig	-	-
修改OIDC身份提供商配置	<a href="#">PUT /v3.0/OS-FEDERATION/identity_providers/{idp_id}/openid-connect-config</a>	iam:identityProviders:updateOpenIDConnectConfig	-	-
查询OIDC身份提供商	<a href="#">GET /v3.0/OS-FEDERATION/identity_providers/{idp_id}/openid-connect-config</a>	iam:identityProviders:getOpenIDConnectConfig	-	-
查询映射列表	<a href="#">GET /v3/OS-FEDERATION/mappings</a>	iam:identityProviders:listMappings	-	-
查询映射详情	<a href="#">GET /v3/OS-FEDERATION/mappings/{id}</a>	iam:identityProviders:getMapping	-	-
注册映射	<a href="#">PUT /v3/OS-FEDERATION/mappings/{id}</a>	iam:identityProviders:createMapping	-	-
更新映射	<a href="#">PATCH /v3/OS-FEDERATION/mappings/{id}</a>	iam:identityProviders:updateMapping	-	-
删除映射	<a href="#">DELETE /v3/OS-FEDERATION/mappings/{id}</a>	iam:identityProviders:deleteMapping	-	-
查询协议列表	<a href="#">GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols</a>	iam:identityProviders:listProtocols	-	-
查询协议详情	<a href="#">GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}</a>	iam:identityProviders:getProtocol	-	-

权限	对应API接口	授权项	IAM 项目 (Project)	企业项目 (Enterprise Project)
注册协议	<a href="#">PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}</a>	iam:identityProviders:createProtocol	-	-
更新协议	<a href="#">PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}</a>	iam:identityProviders:updateProtocol	-	-
删除协议	<a href="#">DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}</a>	iam:identityProviders:deleteProtocol	-	-
查询Metadata文件	<a href="#">GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata</a>	iam:identityProviders:getIDPMetadata	-	-
导入Metadata文件	<a href="#">POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata</a>	iam:identityProviders:createIDPMetadata	-	-



# 8 附录

## 8.1 状态码

表 8-1 状态码

状态码	编码	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	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，请确认用户名和密码是否正确。
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	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。

## 8.2 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。

状态码	错误码	错误信息	描述	处理措施
400	1100	缺失必选参数。	缺失必选参数。	请检查请求参数。

状态码	错误码	错误信息	描述	处理措施
400	1101	用户名校验失败。	用户名校验失败。	请检查用户名。
400	1102	邮箱校验失败。	邮箱校验失败。	请检查邮箱。
400	1103	密码校验失败。	密码校验失败。	请检查密码。
400	1104	手机号校验失败。	手机号校验失败。	请检查手机号。
400	1105	xuser_type必须与xdomain_type相同。	xuser_type必须与xdomain_type相同。	请确认xuser_type与xdomain_type是否相同。
400	1106	国家码、手机号必须同时存在。	国家码、手机号必须同时存在。	请检查国家码和手机号是否同时存在。
400	1107	账号管理员不能被删除。	账号管理员不能被删除。	不允许此操作。
400	1108	新密码不能与原密码相同。	新密码不能与原密码相同。	请修改新密码。
400	1109	用户名已存在。	用户名已存在。	请修改用户名。
400	1110	邮箱已存在。	邮箱已存在。	请修改邮箱。
400	1111	手机号已存在。	手机号已存在。	请修改手机号。
400	1113	xuser_id、xuser_type已存在。	xuser_id、xuser_type已存在。	请修改xuser_id和xuser_type。
400	1115	IAM用户数量达到最大限制。	IAM用户数量达到最大限制。	请修改用户配额或联系技术支持。
400	1117	用户描述校验失败。	用户描述校验失败。	请修改用户描述。
400	1118	密码是弱密码。	密码是弱密码。	重新选择密码。
400	IAM.0007	Request parameter % (key)s is invalid.	请求参数校验失败。	请检查请求参数。

状态码	错误码	错误信息	描述	处理措施
400	IAM.0008	Please scan the QR code first.	请先扫描二维码。	请先扫描二维码。
400	IAM.0009	X-Subject-Token is invalid in the request.	请求中的X-Subject-Token 校验失败。	请检查请求参数。
400	IAM.0010	The QR code has already been scanned by another user.	此二维码已经被其他人扫描。	无需处理。
400	IAM.0011	Request body is invalid.	请求体校验失败。	请检查请求体。
400	IAM.0072	'%(key)s' is a required property.	请求校验异常。举例：%(key)s为必填属性	请联系技术支持。
400	IAM.0073	Invalid input for field '%(key)s'. The value is '%(value)s'.	输入字段无效。	请联系技术支持。
400	IAM.0077	Invalid policy type.	策略类型错误。	请联系技术支持。
400	IAM.1000	The role must be a JSONObject.	缺少role对象。	检查请求体中是否有role对象。
400	IAM.1001	The display_name must be a string and cannot be left blank or contain spaces.	策略 display_name 为空或包含空格。	检查display_name字段的值是否正确。
400	IAM.1002	The length [input length] of the display name exceeds 64 characters.	策略 display_name 不能超过64个字符。	检查display_name字段的长度。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1003	The display_name contains invalid characters.	策略 display_name 包含非法字符。	检查display_name字段的值是否正确。
400	IAM.1004	The type must be a string and cannot be left blank or contain spaces.	type为空。	检查type字段的值是否正确。
400	IAM.1005	Invalid type [input type].	非法的type字段。	检查type字段的值是否正确。
400	IAM.1006	The custom policy does not need a catalog.	自定义策略不需要catalog。	删除catalog字段。
400	IAM.1007	The custom policy does not need a flag.	自定义策略不需要flag。	删除flag字段。
400	IAM.1008	The custom policy does not need a name.	自定义策略不需要name。	删除name字段。
400	IAM.1009	The type of a custom policy must be 'AX' or 'XA'.	自定义策略的type只能为'AX'或'XA'。	根据需求修改type字段为'AX'或'XA'。
400	IAM.1010	The catalog must be a string.	catalog字段必须为字符串。	检查catalog字段的值是否正确。
400	IAM.1011	The length [input length] of the catalog exceeds 64 characters.	catalog字段不能超过64个字符。	检查catalog字段的长度。
400	IAM.1012	Invalid catalog.	非法的catalog字段。	检查catalog字段的值是否正确。
400	IAM.1013	The flag must be a string.	flag字段必须为字符串。	检查flag字段的值是否正确。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1014	The value of the flag must be 'fine_grained'.	flag字段的值应为 "fine_grained" 。	将flag字段的值修改为 "fine_grained"。
400	IAM.1015	The name must be a string and cannot be left blank or contain spaces.	name字段不能为空。	系统角色的name字段必须填写。
400	IAM.1016	The length of the name [input name] cannot exceed 64 characters.	name字段长度不能超过64字符。	检查name字段的值是否正确。
400	IAM.1017	Invalid name.	非法的name字段。	检查name字段的值是否正确。
400	IAM.1018	Invalid description.	非法的description字段。	检查description字段的值是否正确。
400	IAM.1019	Invalid description_cn .	非法的description_cn字段。	检查description_cn字段的值是否正确。
400	IAM.1020	The policy must be a JSONObject.	缺少policy对象。	检查请求体中是否有policy对象。
400	IAM.1021	The size [input policySize] of the policy exceeds 6,144 characters.	policy对象大小超过6144字符。	检查policy对象的长度。
400	IAM.1022	The length [input id length] of the ID exceeds 128 characters.	id字段大小超过128字符。	检查id字段的长度。
400	IAM.1023	Invalid ID '[input id]'.	策略id字段无效。	检查id字段的值是否正确。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1024	The version of a fine-grained policy must be '1.1'.	细粒度策略的version不为1.1。	细粒度策略version字段的值应改为1.1。
400	IAM.1025	Fine-grained policies do not need depends.	细粒度策略不需要depends字段。	删除depends字段。
400	IAM.1026	The version of an RBAC policy must be '1.0' or '1.1'.	RBAC的version只能为1.0和1.1。	version字段的值改为1.0或1.1。
400	IAM.1027	The Statement/ Rules must be a JSONArray.	statement字段不为JSONArray。	检查是否存在statement，类型为json数组。
400	IAM.1028	The number of statements [input statement size] must be greater than 0 and less than or equal to 8.	statement字段长度不为1-8。	至少应填写一个statement，删除超过8个的statement。
400	IAM.1029	The value of Effect must be 'allow' or 'deny'.	effect字段只能为allow或deny。	effect字段填写allow或deny。
400	IAM.1030	The Action or NotAction must be a JSONArray.	action或notAction字段不合法。	检查action对象的值是否正确。
400	IAM.1031	The Action and NotAction cannot be set at the same time in a statement.	action和notAction字段不能同时存在。	删除action或notAction字段。
400	IAM.1032	The OCP NotAction cannot be 'allow'.	OCP的notAction不能为allow。	OCP策略如果使用notAction则只能为deny。



状态码	错误码	错误信息	描述	处理措施
400	IAM.1033	The number of actions [input action size] exceeds 100.	action的数量超过100。	检查action的数量，不能超过100。
400	IAM.1034	The length [input urn length] of an action URN exceeds 128 characters.	action长度超过128。	检查每条action的长度，不能超过128字符。
400	IAM.1035	Action URN '[input urn]' contains invalid characters.	action包含非法字符。	检查action的值是否正确。
400	IAM.1036	Action '[input action]' has not been registered.	action未被注册。	通过注册中心的接口先注册action。
400	IAM.1037	The number of resource URIs [input Resource uri size ] must be greater than 0 and less than or equal to 20.	resource数量只能为1-20。	检查resource的数量。
400	IAM.1038	Resource URI '[input resource uri]' is invalid. Old resources only support agencies.	非法的资源URI。	检查每条资源URI的值是否正确。
400	IAM.1039	Old policies do not support conditions.	旧格式策略不支持condition。	删除condition或使用新格式策略。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1040	The number of resources [input Resource size] must be greater than 0 and less than or equal to 10.	资源URI数量只能为1-10。	检查每个resource对象的URI数量。
400	IAM.1041	The resource URI cannot be left blank or contain spaces.	资源URI为空。	检查每条资源URI的值是否正确。
400	IAM.1042	The length [input uri length] of a resource URI exceeds 1,500 characters.	资源URI超过1500字符。	检查每条资源URI的长度。
400	IAM.1043	A region must be specified.	缺少资源region。	资源URI中填写region。
400	IAM.1044	Region '[input resource region ]' of resource '[input resource]' is invalid.	Region字段不合法。	检查region字段的值是否正确。
400	IAM.1045	Resource URI '[input resource uri]' or service '[input resource split]' is invalid.	资源URI中服务名无效。	检查云服务名是否正确或先注册云服务。
400	IAM.1046	Resource URI '[input resource]' or resource type '[input resource split]' is invalid.	资源URI中类型无效。	检查资源类型是否正确或先注册资源类型。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1047	Resource URI '[input resource uri]' contains invalid characters.	资源URI不合法。	检查资源URI的值是否正确。
400	IAM.1048	Resource URI '[input resource uri]' is too long or contains invalid characters.	资源URI包含非法字符。	检查id值是否包含非法字符。
400	IAM.1049	The Resource must be a JSONObject or JSONArray.	缺少resource对象。	检查resource对象是否为json数组。
400	IAM.1050	The number of conditions [input condition size] must be greater than 0 and less than or equal to 10.	条件数量只能为1-10。	至少填写一个条件，或删除多余的条件。
400	IAM.1051	The values of Operator '[input operator]' cannot be null.	操作符为空。	填写正确的操作符。
400	IAM.1052	Invalid Attribute '[input attribute ]'.	非法的属性字段。	检查属性的值是否正确。
400	IAM.1053	Attribute '[input attribute]' must be a JSONArray.	attribute不为json数组。	检查attribute对象是否为json数组。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1054	The number [input attribute size ] of attributes '[input attribute]' for operator '[input operator]' must be greater than 0 and less than or equal to 10.	每个操作符对应的属性数量只能为1-10。	检查每个操作符下的attribute数量是否正确。
400	IAM.1055	Attribute '[input attribute ]' does not match operator '[input operator]'.	属性与操作符不匹配。	检查attribute和操作符类型是否匹配。
400	IAM.1056	The length [condition length] of attribute '[input attribute]' for operator '[input operator]' must be greater than 0 and less than or equal to 1024 characters.	condition长度只能为1-1024。	检查condition对象的总长度。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1057	Value [input condition] of attribute [input attributes] for operator [input operator] contains invalid characters.	condition包含非法字符。	检查condition中是否包括非法字符。
400	IAM.1058	The number of depends [input policyDepends size] exceeds 20.	depends数量超过20。	删除多余的depends值。
400	IAM.1059	Invalid key '{}'.	策略包含非法的Key。	修改或删除策略请求体中非法的key。
400	IAM.1060	The value of key '{}' must be a string.	该字段必须为字符串。	display_name和name字段改为字符串类型。
400	IAM.1061	Invalid TOTP passcode.	非法的认证密钥。	请确认请求或联系技术支持。
400	IAM.1062	Login protection has been bound to mfa, the unbinding operation cannot be performed.	登录保护已经绑定MFA认证，解绑操作不能执行。	请确认请求或联系技术支持。
400	IAM.1101	The request body size %s is invalid.	请求体的大小不合规。	请检查请求体是否为空或过大（大于32KB）。
400	IAM.1102	The %s in the request body is invalid.	请求体中的某个值错误。	请参照接口资料检查请求体中的属性值。
400	IAM.1103	The %s is required in the request body.	请求体中的必选值缺失。	请参照接口资料检查请求体。

状态码	错误码	错误信息	描述	处理措施
400	IAM.1104	The access key %s is in the blacklist.	请求的AK已在黑名单中。	请确认AK是否存在。
400	IAM.1105	The access key %s has expired.	请求的AK已经过期。	请重新创建访问密钥。
400	IAM.1106	The user %s with access key %s cannot be found.	找不到AK所属用户信息。	请确认AK所属用户或委托是否存在。
400	IAM.1107	The access key %s is inactive.	请求的AK已被禁用。	重新启用AK。
400	IAM.1108	The securitytoken has expired.	临时访问密钥已过期。	请重新获取临时访问密钥。
400	IAM.1109	The project information cannot be found.	找不到project信息。	请检查请求体或者token中的project是否存在，如不能解决请联系技术支持。
401	IAM.0001	The request you have made requires authentication.	请求认证失败。	请补充或确认请求认证信息。
401	IAM.0061	Account locked.	用户被锁定。	请等待自动解锁。
401	IAM.0062	Incorrect password.	用户密码错误。	请输入正确的账号密码。
401	IAM.0063	Access token authentication failed.	accesstoken认证失败。	请联系技术支持。
401	IAM.0064	The access token does not have permissions for the request.	IAM用户没有权限请求。	请确认该IAM用户的权限信息。

状态码	错误码	错误信息	描述	处理措施
401	IAM.0065	HUAWEI IDs registered in European countries cannot log in to HUAWEI CLOUD.	欧洲站点不允许登录。	请输入华为云支持的账号。
401	IAM.0066	The token has expired.	token已过期。	传入有效期内的token。
401	IAM.0067	Invalid token.	错误的token。	传入正确的token。
403	IAM.0002	You are not authorized to perform the requested action.	请求未授权。	请确认是否授权成功。
403	IAM.0003	Policy doesn't allow % (actions)s to be performed.	策略未授权此操作。	请确认策略是否授权此操作。
403	IAM.0080	The user %s with access key %s is disabled.	AK所属用户被禁用。	联系用户所属租户的安全管理员。
403	IAM.0081	This user only supports console access, not programmatic access.	用户仅支持控制台访问，不支持程序访问。	联系用户所属租户的安全管理员修改用户访问模式。
403	IAM.0082	The user %s is disabled.	用户被禁用。	请联系用户所属租户安全管理员。
403	IAM.0083	You do not have permission to access the private region %s.	你没有私有region的访问权限。	请使用其他region或者联系私有region管理员。
404	IAM.0004	Could not find % (target)s: % (target_id)s.	无法找到请求资源。	请确认请求或联系技术支持。

状态码	错误码	错误信息	描述	处理措施
409	IAM.0005	Conflict occurred when attempting to store % (type)s - % (details)s.	保存请求资源时发生冲突。	请确认请求或联系技术支持。
410	IAM.0020	Original auth failover to other regions, please auth downgrade	源区域Auth服务故障转移至其他区域，系统将自动进行认证降级。	系统将自动进行认证降级。
429	IAM.0012	The throttling threshold has been reached. Threshold: %d times per %d seconds	已达到限流阈值。	请确认请求或联系技术支持。
500	IAM.0006	An unexpected error prevented the server from fulfilling your request.	系统错误。	请联系技术支持。

## 8.3 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 8-1 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 8-2 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。

----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。

----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。

----结束

# A 修订记录

发布时间	修改记录
2022-06-20	第四十九次正式发布。 新增章节： <a href="#">查询租户授权信息</a>
2021-11-15	第四十八次正式发布。 新增如下章节： <ul style="list-style-type: none"> <li>● <a href="#">查询企业项目直接关联用户</a></li> <li>● <a href="#">查询企业项目直接关联用户的权限</a></li> <li>● <a href="#">基于用户为企业项目授权</a></li> <li>● <a href="#">删除企业项目直接关联用户的权限</a></li> </ul>
2021-05-15	第四十七次正式发布。 本次变更说明如下： 新增章节： <a href="#">企业项目管理</a>
2021-02-01	第四十六次正式发布。 以下章节新增参数“access_mode”。 <a href="#">查询IAM用户详情（推荐）</a> <a href="#">管理员创建IAM用户（推荐）</a> <a href="#">管理员修改IAM用户信息（推荐）</a>
2021-01-30	第四十五次正式发布。 <a href="#">获取自定义身份代理登录票据</a> 新增请求参数“duration_seconds”。
2021-01-21	第四十四次正式发布。 以下章节增加请求参数“page”、“per_page”，增加响应参数“total_number” <a href="#">查询权限列表</a> <a href="#">查询自定义策略列表</a>

发布时间	修改记录
2020-11-09	第四十三次正式发布。 优化如下章节： <a href="#">查询IAM用户详情（推荐）</a> 新增如下章节： <a href="#">修改IAM用户的登录保护状态信息</a> <a href="#">绑定MFA设备</a> <a href="#">解绑MFA设备</a> <a href="#">创建MFA设备</a> <a href="#">删除MFA设备</a> <a href="#">查询用户组的所有项目权限列表</a> <a href="#">查询用户组是否拥有所有项目指定权限</a> <a href="#">移除用户组的所有项目服务权限</a>
2020-11-05	第四十二次正式发布。 新增如下章节： <a href="#">创建OpenID Connect身份提供商配置</a> <a href="#">修改OpenID Connect身份提供商配置</a> <a href="#">查询OpenID Connect身份提供商配置</a> <a href="#">获取联邦认证token(OpenID Connect ID token方式)</a> <a href="#">获取联邦认证unscoped token(OpenID Connect ID token方式)</a>
2020-08-27	第四十一次正式发布。 优化章节： <a href="#">授权项</a>
2020-08-18	第四十次正式发布。 本次变更说明如下： 优化如下章节： <a href="#">查询IAM用户详情（推荐）</a> 新增如下章节： <a href="#">查询项目配额</a> <a href="#">查询账号配额</a> <a href="#">查询IAM用户的MFA绑定信息列表</a> <a href="#">查询指定IAM用户的MFA绑定信息</a> <a href="#">查询IAM用户的登录保护状态信息列表</a> <a href="#">查询指定IAM用户的登录保护状态信息</a> <a href="#">查询委托下的所有项目服务权限列表</a> <a href="#">为委托授予所有项目服务权限</a> <a href="#">检查委托下是否具有所有项目服务权限</a> <a href="#">移除委托下的所有项目服务权限</a> <a href="#">安全设置</a>

发布时间	修改记录
2020-07-15	第三十九次正式发布。 本次变更说明如下： 优化章节： <a href="#">授权项</a>
2020-07-03	第三十八次正式发布。 本次变更说明如下： 优化章节： <a href="#">授权项</a>
2020-06-19	第三十七次正式发布。 本次变更说明如下： 新增章节： <a href="#">错误码</a>
2020-06-16	第三十六次正式发布。 本次变更说明如下： 优化章节： <a href="#">授权项</a>
2020-06-08	第三十五次正式发布。 本次变更说明如下： 新增API Explorer跳转链接。
2020-05-30	第三十四次正式发布。 本次变更说明如下： 新增如下章节： <a href="#">企业管理华为云上多租户的联邦认证对IAM用户的权限进行安全审计</a>
2020-05-21	第三十三次正式发布。 本次变更说明如下： 新增章节： <a href="#">密钥定期自动化轮换</a> 。

发布时间	修改记录
2020-02-24	<p>第三十二次正式发布。</p> <p>本次变更说明如下：</p> <ul style="list-style-type: none"> <li>• 以下章节新增参数“policy”：  <a href="#">获取委托的临时访问密钥和securitytoken</a>  <a href="#">获取用户的临时访问密钥和securitytoken</a></li> <li>• 优化以下章节：  <a href="#">Token管理</a>  <a href="#">访问密钥管理</a>  <a href="#">区域管理</a>  <a href="#">项目管理</a>  <a href="#">账号管理</a>  <a href="#">IAM用户管理</a>  <a href="#">用户组管理</a>  <a href="#">权限管理</a>  <a href="#">自定义策略管理</a>  <a href="#">委托管理</a>  <a href="#">联邦身份认证管理</a>  <a href="#">自定义身份代理</a>  <a href="#">版本信息管理</a>  <a href="#">服务和终端节点</a></li> </ul>
2020-01-20	<p>第十次正式发布。</p> <p>本次变更说明如下：</p> <p>新增如下章节：</p> <p><a href="#">为用户组授予所有项目服务权限授权项</a></p>
2019-11-01	<p>第九次正式发布。</p> <p>本次变更说明如下：</p> <p>新增如下章节：</p> <p><a href="#">查询IAM用户详情（推荐）</a>  <a href="#">修改IAM用户信息（推荐）</a>  <a href="#">管理员修改IAM用户信息（推荐）</a></p>
2019-09-29	<p>第八次正式发布。</p> <p>本次变更说明如下：</p> <p>新增如下章节：</p> <p><a href="#">自定义身份代理</a></p>

发布时间	修改记录
2019-09-23	<p>第七次正式发布。</p> <p>本次变更说明如下： 新增以下章节：</p> <ul style="list-style-type: none"> <li>● <a href="#">如何调用API</a></li> <li>● <a href="#">创建永久访问密钥</a></li> <li>● <a href="#">查询所有永久访问密钥</a></li> <li>● <a href="#">查询指定永久访问密钥</a></li> <li>● <a href="#">修改指定永久访问密钥</a></li> <li>● <a href="#">删除指定永久访问密钥</a></li> <li>● <a href="#">查询账号密码强度策略</a></li> <li>● <a href="#">按条件查询账号密码强度策略</a></li> <li>● <a href="#">自定义策略管理</a></li> </ul> <p><a href="#">获取账号、IAM用户、项目、用户组、区域、委托的名称和ID</a>中新增通过调用API获取项目ID。</p>
2018-08-14	<p>第五次正式发布。</p> <p>本次变更说明如下： 优化目录结构，方便用户查阅文档。</p>
2018-06-29	<p>第四次正式发布。</p> <p>本次变更说明如下：</p> <ul style="list-style-type: none"> <li>● 将“相关参数信息获取”内容从“API说明”章节移到“环境准备”章节。</li> <li>● <a href="#">管理员查询IAM用户列表、查询IAM用户详情、查询IAM用户是否在用户组中、管理员创建IAM用户和管理员修改IAM用户信息</a>响应体中新增“password_expires_at”（密码过期时间）字段</li> </ul>
2018-03-23	<p>第三次正式发布。</p> <p>本次变更说明如下：</p> <ul style="list-style-type: none"> <li>● 新增<a href="#">获取联邦认证unscoped token(IdP initiated)</a>章节。</li> <li>● 新增<a href="#">查询服务目录</a>章节。</li> </ul>
2018-02-28	<p>第二次正式发布。</p> <p>新增<a href="#">获取用户的临时访问密钥和securitytoken</a>章节。</p>
2017-11-30	<p>第一次正式发布。</p>