统一身份认证服务

API 参考

文档版本 01

发布日期 2022-08-15

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 使用前必读

1.1 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份管理服务，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云服务的访问。

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。

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**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询所有服务的终端节点。

1.4 约束与限制

您创建的IAM资源的数量与配额有关系，如果您想查看服务配额、扩大配额，具体请参见：《IAM用户指南》中的“约束与限制”章节。

IAM所有的API都可以使用全局区域的Endpoint调用；除了全局区域外，使用其他区域的Endpoint可以调用部分API，如**下表**所示。这些API不仅可以使用其他区域的

Endpoint调用，还可以使用全局区域进行调用，除了这些API之外，IAM其他的API仅能使用全局区域的Endpoint调用。

说明

使用IAM其他区域的域名获取的token和临时ak/sk，不能跨region使用，即在A区域生成的token或者ak/sk仅能调用A区域的服务接口。

表 1-1 全局以及其他区域的 API 接口

分类	API URI	接口
Token管理	POST /v3/auth/tokens	**获取用户Token** **获取委托Token** **获取联邦认证scoped token**
	GET /v3/auth/tokens	**校验Token的有效性**
访问密钥管理	POST /v3.0/OS-CREDENTIAL/securitytokens	**获取临时AK/SK**
服务和终端节点	GET /v3/services{?type}	**查询服务列表**
	GET /v3/endpoints{? interface, service_id}	**查询终端节点列表**
版本信息管理	GET /	**查询Keystone API的版本信息**
	GET /v3	**查询Keystone API的3.0版本信息**
项目管理	GET /v3/auth/projects	**查询用户可以访问的项目列表**
租户管理	GET /v3/auth/domains	**查询用户可以访问的租户列表**
联邦身份认证管理	GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/auth	**获取联邦认证unscoped token(SP initiated)**
	POST /v3.0/OS-FEDERATION/tokens	**IdP initiated方式**
	GET /v3/OS-FEDERATION/projects	**查询联邦用户可以访问的项目列表**
	GET /v3/OS-FEDERATION/domains	**查询联邦用户可以访问的租户列表**
	GET /v3-ext/auth/OS-FEDERATION/SSO/metadata	**查询Keystone的Metadata文件**

1.5 基本概念

使用IAM API涉及的常用概念

- 账号

  用户注册时的账号，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。

- 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）

  区域指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。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。

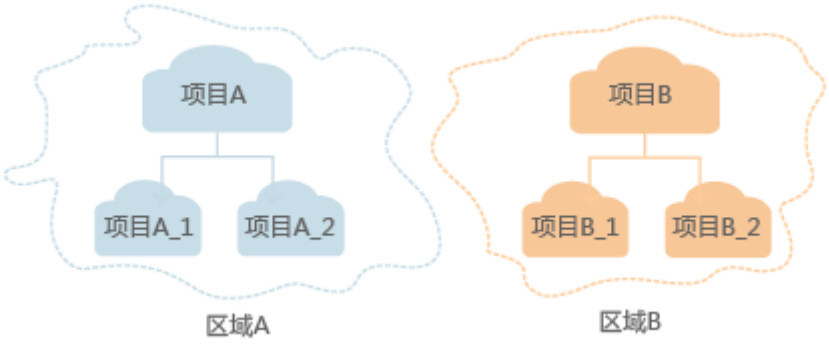
- 可用区（AZ，Availability Zone）

  可用区是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

- 项目

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

图 1-1 项目隔离模型



2 API 概览

Token 管理

接口	说明
获取用户Token	该接口通过用户名/密码的方式进行认证，用来获取用户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	该接口用来校验Token的有效性，如果有效则返回Token的详细信息。
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。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200。
删除用户Token	该接口用来删除token，即无视token的过期时间直接使指定的Token失效。

访问密钥管理

接口	说明
获取临时AK/SK	该接口可以用于获取临时访问密钥（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。

接口	说明
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。
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信息	该接口可以用于查询指定条件下的项目列表。
查询用户的项目列表	该接口可以用于查询指定用户的项目列表。
查询用户可以访问的项目列表	该接口可以用于查询用户可以访问的项目列表。
创建项目	该接口可以用于创建项目。
修改项目	该接口可以用于修改指定项目信息。
查询指定项目的信息	该接口可以用于查询指定项目详情。
设置指定项目的状态	该接口可以用于设置指定项目状态。项目状态包括：正常、冻结。
查询指定项目信息及状态	该接口可以用于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。

租户管理

接口	说明
查询用户可以访问的租户列表	该接口用于查询用户可以用访问的租户列表。

接口	说明
查询租户密码强度策略	该接口用于查询租户密码强度策略，包括密码强度策略的正则表达式以及描述。
按照条件查询租户密码强度策略	该接口用于按照条件查询租户密码强度策略，可以查询密码强度策略的正则表达式或者描述。
查询租户配额	该接口用于按照条件查询租户配额，可以查询的配额类型有：user、group、idp、agency、policy。

用户管理

接口	说明
查询用户列表	该接口可以用于查询用户列表。
查询用户详情	该接口用于查询指定用户的详细信息。
查询用户详情（推荐）	该接口可以用于管理员查询IAM用户详情，或IAM用户查询自己的详情。
查询用户所属用户组	该接口用于查询指定用户所属的用户组信息。
查询用户组所包含的用户	该接口可以用于管理员查询用户组中所包含的IAM用户。
创建用户	该接口用于在某一租户下创建用户。
修改密码	该接口用于用户修改自己密码。
修改用户信息	该接口用于修改租户下对应的用户信息。
修改用户信息（包含邮箱和手机号码）	该接口用于修改IAM用户信息，使用对象：IAM用户。
管理员修改IAM用户信息（包含邮箱和手机号码)	该接口可以用于修改IAM用户信息,使用对象：管理员 。
删除用户	该接口可以用于管理员删除指定IAM用户。
删除用户组中用户	该接口提供删除用户组中用户的功能。

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。

接口	说明
添加用户到用户组	该接口可以用于管理员添加IAM用户到用户组。
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。

权限管理

接口	说明
查询角色列表	该接口可以用于管理员查询权限列表。
查询角色的详细信息	该接口可以用于管理员查询权限详情。
查询租户中用户组的权限	该接口提供查询租户下用户组的权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。
查询项目对应的用户组的权限	该接口提供查询某个项目对应的指定用户组的权限，权限通过角色（Role）来表达，一个Role代表成一组action。
为租户所属用户组授权	该接口提供给租户所属用户组增加权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。
为项目对应的用户组授权	该接口提供项目对应用户组增加权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。
删除项目对应的用户组的权限	该接口提供删除项目对应用户组权限的功能。
删除租户所属用户组的权限	该接口提供删除某租户所属指定用户组权限的功能。
查询租户中用户组是否包含权限	该接口提供检查某租户中指定用户组是否包含特定权限的功能。
查询项目对应的用户组是否包含权限	该接口提供查询项目对应用户组是否包含权限的功能
为用户组授予所有项目权限	该接口提供授予用户组的项目权限。
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。
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。
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。

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
创建委托	该接口提供创建委托关系的功能。
查询指定条件下的委托列表信息	该接口用来获取指定条件下的委托列表信息。
获取指定委托的详细信息	该接口用来获取指定委托的详细信息。
修改委托	该接口提供修改委托的信息，包括租户的trust_domain_id、description、trust_domain_name字段。
删除委托	该接口可以用于删除委托。
通过项目给委托赋予权限	该接口用来通过项目给委托赋予权限。
检查委托在项目上是否有指定权限	该接口用来检查委托在项目上是否有指定权限。
查询委托在项目上具有的权限列表	该接口用来查询委托在项目上具有的权限列表。
通过项目删除委托的权限	该接口用来通过项目信息删除委托的权限。
通过租户给委托赋予权限	该接口用来通过租户信息给委托赋予权限。
检查委托在租户上是否有指定权限	该接口用来检查委托在租户上是否具有指定权限。
查询委托在租户上具有的权限列表	该接口用来查询委托在租户上具有的权限列表。

接口	说明
通过租户删除委托的权限	该接口用来通过租户信息删除委托的权限。
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。

安全设置

接口	说明
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。
查询账号密码策略	该接口可以用于查询账号密码策略。
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。
查询账号登录策略	该接口可以用于查询账号登录策略。
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。
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。

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。
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	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创建身份提供商。
更新SAML身份提供商	该接口可以用于管理员更新身份提供商。
删除身份提供商	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	该接口可以用于查询映射信息。
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	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。

接口	说明
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。
查询联邦用户可以访问的租户列表	该接口用于查询联邦用户可以访问的租户列表。

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**获取用户Token**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

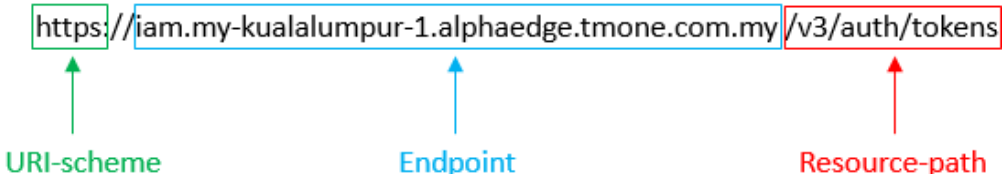
参数	说明
URI-scheme	传输请求的协议，当前所有API均采用**HTTPS**协议。
Endpoint	承载REST服务端点的服务器域名或IP，不同服务在不同区域，Endpoint不同，可以从地点和终端节点处获取。 例如IAM服务在“**my-kualalumpur-1**”区域的Endpoint为“**iam.my-kualalumpur-1.alphaedge.tmone.com.my**”。
resource-path	资源路径，即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
query-string	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IAM在“my-kualalumpur-1”区域的Token，则需使用“my-kualalumpur-1”区域的Endpoint（iam.my-

kualalumpur-1.alphaedge.tmone.com.my），并在**获取用户Token**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

图 3-1 URI 示意图



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**获取用户Token**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/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**获取用户Token**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

  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**认证鉴权**的“AK/SK认证”。

对于**获取用户Token**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.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
```

请求消息体（可选）

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，如"application/json;charset=utf8"。

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**获取用户Token**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，***xxxxxxxxxxxxxxxxxx***为project的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domainname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：**获取用户Token**。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json

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

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**获取用户Token**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。
- 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**获取用户Token**接口获取，调用本服务API需要全局级别的Token，即调用**获取用户Token**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。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

AK/SK 认证

说明

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

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

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

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

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

3.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于**获取用户Token**接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于**获取用户Token**接口，返回如**图1**所示的消息头，其中“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。

图 3-2 获取用户 Token 响应消息头

响应消息体

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

对于**获取用户Token**接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "az-01",
.....
```

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 API

4.1 Token 管理

4.1.1 获取用户 Token

功能介绍

该接口通过用户名/密码的方式进行认证，用来获取用户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。

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将立即失效，请重新获取。

- 账号或IAM用户修改密码、访问密钥，该账号或IAM用户Token将立即失效。
- 删除/停用IAM用户，该IAM用户Token将立即失效。
- IAM用户权限发生变化，该IAM用户Token将立即失效。如IAM用户加入或移出用户组、用户所在用户组权限变更等。

URI

POST /v3/auth/tokens

请求

- Request Header参数说明

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

- Request Body参数说明

参数	是否必选	类型	说明

identity	是	Json Object	认证参数，包含：methods，password。
			"identity": {
			"methods": ["password"],
			"password": {

methods	是	String Array	认证方法，该字段内容为“password”。如果用户开启了虚拟MFA设备的登录保护功能时，该字段内容为[“password”,"totp"]。

password	是	Json Object	认证信息，示例：
			"password": {
			"user": {
			"name": "*user A*",
			"password": "**********",
			"domain": {
			"name": "*domain A*"
			● user.name：用户名称，根据获取token的主体填写，可以在我的凭证中获取。
			● password：用户的登录密码。
			● domain.name：用户所属的账号名称，可以在我的凭证中获取。

参数	是否必选	类型	说明

totp	否	Json Object	认证信息，仅在您开启了虚拟MFA方式的登录保护功能时，该参数需要填写。
			user.id和user.name二选一即可
			示例1：
			"totp": {
			"user": {
			"id": "b95b78b67fa045b38104c12fb...",
			"passcode": "******"
			● user.id：用户ID，可以在我的凭证中获取。
			● passcode：虚拟MFA验证码，在MFA应用程序中获取动态验证码。
			示例2：
			"totp": {
			"user": {
			"name": "user A",
			"passcode": "******"
			● user.name：用户名
			● passcode：虚拟MFA验证码，在MFA应用程序中获取动态验证码。

scope	否	Json Object	token的使用范围，取值为project或domain，二选一即可。
			● 示例1：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。project支持id和name，二选一即可。
			"scope": {
			"project": {
			"id": "0b95b78b67fa045b38104c12fb..."
			}
			}
			● 示例2：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。domain支持id和name，二选一即可。
			"scope": {
			"domain": {
			"name": " domain A"
			}
			}

- 请求样例
  获取用户名为“user A”，登录密码为“**********”，所属账号名为“domain A”，作用范围为“domain”的token。

```
{
  "auth": {
    "identity": {
      "methods": ["password"],
      "password": {
        "user": {
          "name": "user A",
          "password": "**********",
          "domain": {
            "name": "domain A"
          }
        }
      }
    },
    "scope": {
      "domain": {
        "name": "domain A"
      }
    }
  }
}
```

响应

- Response Header参数说明

参数	是否必选	类型	描述
X-Subject-Token	是	String	获取到的token。

- Token格式说明

参数	是否必选	类型	描述
methods	是	Json Array	获取token的方式。
expires_at	是	String	token到期时间。
issued_at	是	String	token产生时间。

参数	是否必选	类型	描述

user	是	Json Object	示例：
			"user": {
			"name": "user A",
			"id": "b95b78b67fa045b38104...",
			"password_expires_at":"2016-11-06T15:32:17.000000",
			"domain": {
			"name": "domain A",
			"id": "fdec73ffea524aa1b373e40..."
			}
			}
			● user.name：用户名称。
			● user.id：用户ID。
			● domain.name：用户的所属账号的名称。
			● domain.id：用户的所属账户的ID。
			● password_expires_at：密码过期时间（UTC时间），“null”表示密码不过期。

domain	否	Json Object	如果请求体中scope参数设置为domain，则返回该字段。 示例： "domain": { "name" : "domain A" "id" : "fdec73ffea524aa1b373e40..." ● domain.name：用户的所属的账户名称。 ● domain.id：用户的所属账户的ID。

参数	是否必选	类型	描述

project	否	Json Object	如果请求体中scope参数设置为project，则返回该字段。
			示例：
			"project": {
			"name": "project A",
			"id": "34c77f3eaf84c00aaf54...",
			"domain": {
			"name": "domain A",
			"id": "fdec73ffea524aa1b373e40..."
			}
			}
			● project.name：project名称。
			● project.id：project的ID。
			● domain.name：project的账户名称。
			● domain.id：project的账户的ID。

catalog	是	Json Array	endpoints相关信息。
			示例：
			"catalog": [{
			"type": "identity",
			"id": "1331e5cff2a74d76b03da1225910e...",
			"name": "iam",
			"endpoints": [{
			"url": "*https://sample.domain.com*/v3",
			"region": "*",
			"region_id": "*",
			"interface": "public",
			"id": "089d4a381d574308a703122d3ae73..."
			}]
			}]
			● type：该接口所属的服务。
			● id：服务的id。
			● name：服务的名称。
			● endpoints：终端节点。
			● url：调用该接口的url。
			● region：服务的所属区域。
			● region_id：服务的所属区域id。
			● interface：接口状态，public表示为公开。
			● id：接口的id。

参数	是否必选	类型	描述

roles	是	Json Object	Token的权限信息。
			示例：
			"roles" : [{
			"name" : "role1",
			"id" : "roleid1"
			}, {
			"name" : "role2",
			"id" : "roleid2"
			}
			]

- 响应样例

  获取用户名为“user A”，登录密码为“**********”，所属账号名为“domain A”，作用范围为“domain”的token。

```
Response Header中存储信息为：
X-Subject-Token:MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALBglghkgBZQMEAgEwgXXXXX...

Response Body中存储信息为：
{
  "token" : {
    "methods" : ["password"],
    "expires_at" : "2015-11-09T01:42:57.527363Z",
    "issued_at" : "2015-11-09T00:42:57.527404Z",
    "user" : {
      "domain" : {
      "id" : "ded485def148s4e7d2se41d5se...",
      "name" : "domain A"
      },
      "id" : "ee4dfb6e5540447cb37419051...",
      "name" : "user A",
      "password_expires_at":"2016-11-06T15:32:17.000000",
    },
    "domain" : {
       "name" : "domain A",
       "id" : "dod4ed5e8d4e8d2e8e8d5d2d..."
    },
    "catalog": [{
        "type": "identity",
        "id": "1331e5cff2a74d76b03da12259...",
        "name": "iam",
        "endpoints": [{
            "url": "https://sample.domain.com/v3",
            "region": "*",
            "region_id": "*",
           "interface": "public",
            "id": "089d4a381d574308a703122d3a..."
      }]
    }],
    "roles" : [{
      "name" : "role1",
      "id" : "roleid1"
      }, {
      "name" : "role2",
      "id" : "roleid2"
      }
  ]
  }
}
```

状态码

状态码	说明
201	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
500	内部服务错误。可能是格式错误。
503	服务不可用。

4.1.2 获取委托 Token

功能介绍

该接口用来获取委托Token，例如：A账号与B账号创建了委托关系，A账号为委托方，B账号为被委托方，则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，需要通过**获取用户Token**获取自己的Token。

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。

URI

POST /v3/auth/tokens

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	被委托方用户B具有Agent Operator权限的token。

- Request Body参数说明

参数	是否为必选	类型	说明

identity	是	Json Object	认证参数，包含：methods，assume_role。
			"identity": {
			"methods": ["assume_role"],
			"assume_role": {

methods	是	String Array	token的获取方式，该字段内容为“assume_role”。
domain_name或domain_id	是	String	委托方用户A的账号名称或者ID，domain_name和domain_id二选一。
xrole_name	是	String	委托方用户A创建的委托的名称。

scope	否	Json Object	token的使用范围，取值为project或domain，二选一即可。
			● 示例1：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。
			"scope": {
			"project": {
			"id": "0b95b78b67fa045b38104c12fb..."
			}
			}
			● 示例2：取值为domain时，表示获取的Token可以访问委托方账号中授权的所有资源，domain支持id和name，二选一即可。
			"scope": {
			"domain": {
			"id": "6b8eb224c76842e3ac2..."
			}
			}

- 请求样例
  获取委托方账号名为“domain A”，委托名称为“agencytest”的委托token。

```
{
    "auth":{
        "identity":{
            "methods":[
                "assume_role"
            ],
            "assume_role":{
                "domain_name":"domain A",
                "xrole_name":"agencytest"
                }
        },
        "scope":{
            "domain":{
                "name":"domain A"
            }
        }
    }
}
```

响应

- Response Header参数说明

参数	是否必选	类型	描述
X-Subject-Token	是	String	获取的委托token。

- Token格式说明

参数	是否必选	类型	描述
methods	是	Json Array	获取token的方式。
expires_at	是	String	token到期时间。
issued_at	是	String	token产生时间。

user	是	Json Object	委托方用户的详细信息，示例：
			"user": {
			"name": "*user A*",
			"id": "*userid*",
			"password_expires_at":"2016-11-06T15:32:17.000000",
			"domain": {
			"name": "*domain A*",
			"id": "*domainid*"
			}
			}
			● user.name：委托方的用户名称。
			● user.id：委托方的用户ID。
			● domain.name：委托方用户的所属的账户名称。
			● domain.id：委托方用户的所属账户的ID。
			● password_expires_at：可选，密码过期时间（UTC时间），“null”表示密码不过期。

domain	否	Json Object	如果请求体中scope参数设置为domain，则返回该字段。
			示例：
			"domain": {
			"name" : "*domain A*",
			"id" : "*domainid*"
			}
			● domain.name：委托方用户的所属账户的名称。
			● domain.id：委托方用户的所属账户的ID。

参数	是否必选	类型	描述

project	否	Json Object	如果请求体中scope参数设置为project，则返回该字段。
			示例：
			"project": {
			"name": "*projectname*",
			"id": "*projectid*"
			}
			● project.name：project名称。
			● project.id：project的ID。

catalog	否	Json Array	endpoints相关信息。
			示例：
			"catalog": [{
			"type": "identity",
			"id":
			"1331e5cff2a74d76b03da1225910e31d",
			"name": "iam",
			"endpoints": [{
			"url": "*https://sample.domain.com/*
			v3",
			"region": "*",
			"region_id": "*",
			"interface": "public",
			"id":
			"089d4a381d574308a703122d3ae738e9"
			}]
			}]

roles	是	Json Object	Token的权限信息。
			示例：
			"roles" : [{
			"name" : "role1",
			"id" : "roleid1"
			}, {
			"name" : "role2",
			"id" : "roleid2"
			}
			]

assumed_by	是	Json Object	被委托方用户的详细信息。
			示例：
			"assumed_by": {
			"user": {
			"domain": {
			"name": "domain B",
			"id":
			"bfdd55e02a014894b5a2693f31..."
			},
			"name": "user B",
			"id": "ff5ea657f1dd45c4b8f398cab..."
			}
			}
			● domain.name：被委托方用户的所属账户的名称。
			● user.name：被委托方用户的用户名称。

- 响应样例

```
Response Header中存储信息为：
X-Subject-Token:MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALBglghkgBZQMEAgEwgXXXXX...

X-Frame-Options: SAMEORIGIN

Response Body中存储信息为：
{
  "token": {
    "methods": [
      "assume_role"
    ],
    "issued_at": "2017-05-18T11:44:05.232000Z",
    "expires_at": "2017-05-19T11:44:05.232000Z",
    "user": {
      "id": "93e12ecdad6f4abd84968741da...",
      "name": "user A/agencytest",
      "password_expires_at":"2016-11-06T15:32:17.000000",
      "domain": {
        "id": "ce925c42c25943bebba10ea64a...",
        "name": "domain A"
      }
    },
    "domain": {
      "id": "ce925c42c25943bebba10ea64a...",
      "name": "domain A"
    },
    "roles": [
      {
        "id": "c11c61319f08404eaf94f8030b9...",
        "name": "role1"
      },
      {
        "id": "d52dde35ijg62fex2ijhdc785sc3...",
        "name": "role2"
      },
      {
        "id": "d862dwd32dwhu854rdcs447ed1d7..."
        "name": "op_gated_tasssg6"
      }
    ],
    "assumed_by": {
      "user": {
        "domain": {
          "name": "domain B",
          "id": "c1a78a82d81c4a19b03bfe82d3ad..."
        },
        "id": "cdeb158dda854cc3bab77d8926ff...",
        "name": "User B"
      }
    }
  }
}
```

状态码

状态码	说明
201	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。

状态码	说明
404	找不到资源。
500	内部服务错误。
503	服务不可用。

4.1.3 校验 Token 的有效性

功能介绍

该接口用来校验Token的有效性，如果有效则返回Token的详细信息。

URI

GET /v3/auth/tokens

请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	• 校验自己的Token有效性，使用自己的token即可，该token不需要具备特殊权限。 • 校验本账号中其他用户的token有效性，需要具有Security Administrator权限的token。
X-Subject-Token	是	String	待校验的token。

- 查询参数说明

参数	是否必选	类型	说明
nocatalog	否	String	如果设置该参数，返回的响应体中将不显示catalog信息。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H "X-Subject-Token:$token" -X GET https://sample.domain.com/v3/auth/tokens
```

响应

- Response Header参数说明

参数	是否必选	类型	说明
X-Subject-Token	是	String	校验的token。

- Response body参数说明

参数	是否必选	类型	描述
token	是	Object	token信息列表。

- token格式说明

参数	是否必选	类型	描述
methods	是	Array	获取token的方式，例如：“password”。
expires_at	是	String	token到期时间。
issued_at	是	String	token产生时间。

user	是	Object	示例：
			"user": {
			"name": "*username*",
			"id": "*userid*",
			
			"password_expires_at":"2016-11-06T15:32:17.000000",
			"domain": {
			"name": "*domainname*",
			"id": "*domainid*"
			}
			}
			● user.name：用户名称。
			● user.id：用户ID。
			● domain.name：用户的账号名称。
			● domain.id：用户的账号的ID。
			● password_expires_at：可选，密码过期时间（UTC时间），“null”表示密码不过期。

domain	否	Object	根据获取token的请求里的scope，判断是否返回该字段。
			示例：
			"domain": {
			"name" : "domainame",
			"id" : "domainid"
			}
			● domain.name：账号名称。
			● domain.id：账号的ID。

参数	是否必选	类型	描述

project	否	Object	根据获取token的请求里的scope，判断是否返回该字段。
			示例：
			"project": {
			"name": "*projectname*",
			"id": "*projectid*",
			}
			● project.name：project名称。
			● project.id：project的ID。

catalog	否	Json Array	endpoints相关信息。
			示例：
			"catalog": [{
			"type": "identity",
			"id":
			"1331e5cff2a74d76b03da1225910e31d",
			"name": "iam",
			"endpoints": [{
			"url": "*https://sample.domain.com/*v3",
			"region": "*",
			"region_id": "*",
			"interface": "public",
			"id":
			"089d4a381d574308a703122d3ae738e9"
			}]
			}]
			● type：该接口所属的服务。
			● id：服务的id。
			● name：服务的名称。
			● endpoints：终端节点。
			● url：调用该接口的url。
			● region：服务的所属区域。
			● region_id：服务的所属区域id。
			● interface：接口状态，public表示为公开。
			● id：接口的id。

roles	是	Array	Token的权限信息。
			示例：
			"roles" : [{
			"name" : "role1",
			"id" : "roleid1"
			}, {
			"name" : "role2",
			"id" : "roleid2"
			}
			]

- Response样例

```
{
 "token" : {
  "methods" : ["password"],
  "expires_at" : "2015-11-09T01:42:57.527363Z",
  "issued_at" : "2015-11-09T00:42:57.527404Z",
  "user" : {
    "domain" : {
    "id" : "default",
    "name" : "Default"
    },
    "id" : "ee4dfb6e5540447cb3741905149XXX...",
    "password_expires_at":"2016-11-06T15:32:17.000000",
    "name" : "admin"
  },
  "domain" : {
     "name" : "Default",
     "id" : "default"
  },
  "roles" : [{
     "name" : "role1",
     "id" : "roleid1"
     }, {
     "name" : "role2",
     "id" : "roleid2"
     }
 ]
 }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
503	服务不可用。

4.1.4 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200。

URI

HEAD /v3/auth/tokens

请求参数

表 4-1 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	• 校验自己的Token有效性，使用自己的token即可，该token不需要具备特殊权限。 • 校验本账号中其他用户的token有效性，需要具有Security Administrator权限的token。
X-Subject-Token	是	String	待校验的token。

响应参数

无

请求示例

```
curl -i -k -H "X-Auth-Token:$token" -H "X-Subject-Token:$token" -X HEAD https://sample.domain.com/v3/auth/tokens
```

响应示例

无

状态码

状态码	描述
200	请求成功。
401	认证失败。
404	找不到资源。
500	系统异常。

4.1.5 删除用户 Token

功能介绍

该接口用来删除token，即无视token的过期时间直接使指定的Token失效。

URI

DELETE /v3/auth/tokens

请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	获取的token。 ● 用户删除自己的Token时，使用用户自己的token即可，该token不需要具备特殊权限。 ● 删除本账号中其他用户的token时，需要具有Security Administrator权限的token。
X-Subject-Token	是	String	待删除的token。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H "X-Subject-Token:$token" -X DELETE https://sample.domain.com/v3/auth/tokens
```

响应

无

状态码

状态码	说明
204	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
503	服务不可用。

4.2 访问密钥管理

4.2.1 获取临时 AK/SK

功能介绍

通过已经获取的用户token、委托token和联邦token，可以获取临时的AK/SK、securitytoken（离线AK/SK）。临时AK/SK即给用户颁发的具有临时权限的令牌，遵循权限最小化原则，可应用于临时访问OBS等。

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

请求消息

- Request Header参数说明
  - 使用委托token，即methods为assume_role时

参数	是否必选	类型	描述
X-Auth-Token	是	String	具有Agent Operator权限的token。
Content-Type	是	String	该字段填为“application/json;charset=utf8”。

  - 使用普通token（用户token、联邦token），即methods为token时

参数	是否必选	类型	描述
Content-Type	是	String	该字段填为“application/json;charset=utf8””。
X-Auth-Token	否	String	用户token或者联邦token，该值与请求体中token的id二选一，X-Auth-Token优先。

- Request Body参数说明
  - 使用委托token，即methods为assume_role时

参数	必选/可选	类型	描述
methods	必选	String Array	该字段内容为“assume_role”。
agency_name	必选	String	委托方用户创建的委托的名称。
domain_name或domain_id	必选	String	委托用户的所属账号的名称。
duration_seconds	可选	Int	AK/SK和securitytoken的有效期，时间单位为秒。取值范围：15min ~ 24h，默认为15min

参数	必选/可选	类型	描述

scope	可选	Object	AK/SK和securitytoken。该值若不填，生成的securitytoken不包括scope信息。推荐不填。该值若填写，取值为project或domain，二选一即可。
			● 示例1：取值为project时，表示获取的AK/SK和securitytoken仅能访问指定project下的资源，project支持id和name，二选一即可。
			"scope": {
			"project": {
			"id": "0b95b78b67fa045b38104c12fb...."
			}
			}
			● 示例2：取值为domain时，表示获取的AK/SK和securitytoken可以访问指定账号下所有资源，domain支持id和name，二选一即可。
			"scope": {
			"domain": {
			"name": " domain A"
			}
			}

- 使用普通token（用户token、联邦token），即methods为token时

参数	必选/可选	类型	描述
methods	必选	String Array	该字段内容为“token”。
token	可选	Json Object	用于获取临时AK/SK的普通token或者联邦token，该对象中的id与请求头部中的X-Auth-Token二选一，X-Auth-Token优先。
duration_seconds	可选	Int	AK/SK和securitytoken的有效期，时间单位为秒。取值范围：15min ~ 24h ，默认为15min。

- 请求示例
  - methods为assume_role方式进行请求

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

```
            "methods": [
                "assume_role"
            ],
            "assume_role": {
                "domain_id": "411edb4b634144f587ffc88f9bbdxxx",
                "xrole_name": "testagency",
                "duration_seconds": 3600
            }
        }
    }
}
```

– methods为tokens方式进行请求

```
{
    "auth": {
        "identity": {
            "methods": [
                "token"
            ],
            "token": {
                "id":
"MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALBglghkgBZQMEAgEwgXXXXX...",
                "duration_seconds": 900
            }
        }
    }
}
```

响应

- Response Body参数说明

参数	必选/可选	类型	描述
credential	必选	Object	认证信息

- credential内容说明

参数	必选/可选	类型	描述
expires_at	必选	String	过期时间
access	必选	String	AK
secret	必选	String	SK
securitytoken	必选	String	用于后续换SK或Token使用

- 响应示例

```
{
  "credential": {
    "access": "NQC51NFINJS1JXX...",
    "secret": "EY74MByPZ46kTRJL9ay5DskqXX...",
    "expires_at": "2017-04-17T07:55:18.575000Z",
    "securitytoken": "gAAAAABY9GbWUaGtoa9DPj7_dE4qUSnAXXX..."
  }
}
```

状态码

状态码	说明
201	请求成功
400	请求失败
401	认证失败
403	鉴权失败
500	系统异常

4.2.2 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）访问系统时的身份凭证，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。

该接口可以使用全局区域的Endpoint和其他区域的Endpoint调用。

URI

POST /v3.0/OS-CREDENTIAL/credentials

请求参数

表 4-2 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段填为“application/json;charset=utf8”。
X-Auth-Token	是	String	管理员给IAM用户创建永久访问密钥：拥有Security Administrator权限的token。 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 4-3 请求 Body 参数

参数	是否必选	参数类型	描述
credential	是	Object	认证信息。

表 4-4 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。
description	否	String	访问密钥描述信息。

响应参数

表 4-5 响应 Body 参数

参数	参数类型	描述
credential	Object	认证结果信息。

表 4-6 credential

参数	参数类型	描述
create_time	String	创建访问密钥时间。
access	String	创建的AK。
secret	String	创建的SK。
status	String	访问密钥状态。
user_id	String	IAM用户ID。
description	String	访问密钥描述信息。

请求示例

```
POST https://sample.domain.com/v3.0/OS-CREDENTIAL/credentials
{
    "credential": {
        "description": "IAMDescription",
        "user_id": "07609fb9358010e21f7bc003751c7c32"
    }
}
```

响应示例

状态码为 201 时:

创建成功。

```
{
    "credential": {
        "access": "P83EVBZJMXCYTMUII...",
        "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"
    }
}
```

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

4.2.3 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。

URI

GET /v3.0/OS-CREDENTIAL/credentials

表 4-7 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 4-8 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	管理员查询IAM用户的所有永久访问密钥：填写拥有Security Administrator权限的token。 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）。

响应参数

表 4-9 响应 Body 参数

参数	参数类型	描述
credentials	Array of objects	认证结果信息列表。

表 4-10 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。
create_time	String	访问密钥创建时间。
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://sample.domain.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://sample.domain.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

4.2.4 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。

URI

GET /v3.0/OS-CREDENTIAL/credentials/{access_key}

表 4-11 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 4-12 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	管理员查询IAM用户的指定永久访问密钥：拥有Security Administrator权限的token。 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 4-13 响应 Body 参数

参数	参数类型	描述
credential	Object	认证结果信息。

表 4-14 credential

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。
create_time	String	访问密钥创建时间。
last_use_time	String	访问密钥的上次使用时间。
description	String	访问密钥描述信息。

请求示例

```
GET https://sample.domain.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": "LOSZM4YRVLKOY9E8...",
        "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。
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

4.2.5 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。

URI

PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}

表 4-15 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 4-16 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	管理员修改IAM用户的指定永久访问密钥：拥有Security Administrator权限的token。 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 4-17 请求 Body 参数

参数	是否必选	参数类型	描述
credential	是	Object	认证信息。

表 4-18 credential

参数	是否必选	参数类型	描述
status	否	String	访问密钥状态。取值为：“active”（启用）或者 “inactive”（停用）。 取值范围： • active • inactive
description	否	String	访问密钥描述信息。

响应参数

表 4-19 响应 Body 参数

参数	参数类型	描述
credential	Object	认证信息。

表 4-20 credential

参数	参数类型	描述
user_id	String	IAM用户ID。
access	String	修改的AK。
status	String	访问密钥状态。
create_time	String	访问密钥创建时间。
description	String	访问密钥描述信息。

请求示例

```
PUT https://sample.domain.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": "LOSZM4YRVLKOY9...",
        "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。
500	内部服务错误。

错误码

无

4.2.6 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。

URI

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

表 4-21 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 4-22 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	管理员删除IAM用户的指定永久访问密钥：拥有Security Administrator权限的token。 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

```
DELETE https://sample.domain.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

4.3 区域管理

4.3.1 查询区域列表

功能介绍

该接口用于查询区域列表。

URI

GET /v3/regions

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。如果token中没有私有region信息，则查询结果不返回私有region。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/regions
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	Dict	区域的资源链接。
regions	是	List	区域列表。

- regions格式说明

参数	是否必选	类型	说明
description	是	String	区域描述。
parent_region_id	是	String	区域的父区域ID。
id	是	String	区域id。
locales	是	Dict	区域名。
type	否	String	区域类型。
links	是	Dict	区域的资源链接。

- 响应样例（响应成功）

```
{
    "regions": [
        {
            "parent_region_id": null,
            "description": "",
            "links": {
                "self": "None/v3/regions/1500365963661574434"
            },
            "type": "private",
            "id": "1500365963661574434",
            "locales": {

                "en-us": "region_name2"
            }
        },
        {
            "parent_region_id": null,
            "description": "",
            "links": {
                "self": "https://sample.domain.com/v3/regions/500017826026667755"
            },
            "type": "private",
            "id": "500017826026667755",
            "locales": {

                "en-us": "region_name2"
            }
        },
        {
            "parent_region_id": null,
            "description": "",
            "links": {
                "self": "https://sample.domain.com/v3/regions/region_name"
            },
            "type": "public",
            "id": "test2",
            "locales": {

                "en-us": "region_name2"
            }
        },
        {
            "parent_region_id": null,
            "links": {
                "self": "https://sample.domain.com/v3/regions/test1112244"
            },
            "id": "test1112244",
            "locales": {

                "en-us": "testregion1"
            },
            "description": ""
        }
    ],
    "links": {
        "self": "https://sample.domain.com/v3/regions",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。

状态码	说明
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.3.2 查询区域详情

功能介绍

该接口用于查询区域详情。

URI

- URI格式
  GET /v3/regions/{region_id}
- 参数说明

参数	是否必选	类型	说明
region_id	是	String	指定区域ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例
  curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/regions/test-pusb999999991

响应

响应样例

```
{
    "region": {
        "parent_region_id": null,
        "description": "",
        "links": {
            "self": "https://sample.domain.com/v3/regions/test-pusb999999991"
        },
        "type": "public",
        "id": "test-pusb999999991",
        "locales": {
            "en-us": "region_name"
        }
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.4 项目管理

4.4.1 查询指定条件下的项目信息

功能介绍

该接口用于查询指定条件下的项目信息。

URI

- URI格式

  GET /v3/projects{?domain_id,name,enabled,parent_id,is_domain,page,per_page}

- 参数说明

参数	是否必选	类型	说明
domain_id	否	String	用户所属企业账户的ID。
name	否	String	项目名称。
parent_id	否	String	项目的父项目ID。
enabled	否	Boolean	项目是否启用。
is_domain	否	Boolean	是否为租户。
page	否	Integer	查询第几页的数据，查询值最小为1。
per_page	否	Integer	每页的数据个数，取值范围为[1,5000]。

说明

需要分页查询时，必须保证查询参数中同时存在page和per_page。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	目标租户已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -X "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/projects?domain_id=5c9f5525d9d24c5bbf91e74d86772029&name=region_name
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
projects	是	List	项目列表。
links	是	Object	项目的资源链接。

- projects格式说明

参数	是否必选	类型	说明
is_domain	是	Boolean	是否为租户。

参数	是否必选	类型	说明
description	是	String	项目的描述。
links	是	Object	项目的资源链接。
enabled	是	Boolean	项目是否可用。
id	是	String	项目ID。
parent_id	是	String	project的父ID。
domain_id	是	String	项目所在企业账户的ID。
name	是	String	项目名称。

- 响应样例

```
{
  "links": {
    "self": "https://sample.domain.com/v3/projects?
domain_id=c9f5525d9d24c5bbf91e74d86772029&name=region_name",
    "previous": null,
    "next": null
  },
  "projects": [
    {
      "is_domain": false,
      "description": "",
      "links": {
        "self": "https://sample.domain.com/v3/projects/e86737682ab64b2490c48f08bcc41914"
      },
      "enabled": true,
      "id": "e86737682ab64b2490c48f08bcc41914",
      "parent_id": "c9f5525d9d24c5bbf91e74d86772029",
      "domain_id": "c9f5525d9d24c5bbf91e74d86772029",
      "name": "region_name"
    }
  ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
500	内部服务错误。
503	服务不可用。

4.4.2 查询用户的项目列表

功能介绍

该接口用于查询指定用户的项目列表。

URI

- URI格式

  GET /v3/users/{user_id}/projects

- 参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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，或用户自身的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/users/43cbe5e77aaf4665bbb962062dc1fc9d/projects
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
projects	是	Array	project列表。
links	是	Object	项目的资源链接。

- project格式说明

参数	是否必选	类型	说明
description	是	String	project描述。
id	是	String	project ID。

参数	是否必选	类型	说明
domain_id	是	String	project所在domain的ID。
name	是	String	project名称。
links	是	Object	项目的资源链接。
is_domain	是	Boolean	是否为domain。
enabled	是	Boolean	project是否可用。
parent_id	是	String	project的父ID。

- 响应样例

```
{
  "links": {
    "self": "https://sample.domain.com/v3/auth/projects",
    "previous": null,
    "next": null
  },
  "projects": [
    {
      "is_domain": false,
      "description": "",
      "links": {
        "self": "https://sample.domain.com/v3/projects/9041929bcc6e4bfe85add4e7b96ffdd7"
      },
      "enabled": true,
      "id": "9041929bcc6e4bfe85add4e7b96ffdd7",
      "parent_id": "398998b5392f4150ad48fe456d6de4f1",
      "domain_id": "398998b5392f4150ad48fe456d6de4f1",
      "name": "region_name"
    },
    {
      "is_domain": false,
      "description": "",
      "links": {
        "self": "https://sample.domain.com/v3/projects/ee65ca70d3cf43aaa1ea6492ce15f289"
      },
      "enabled": true,
      "id": "ee65ca70d3cf43aaa1ea6492ce15f289",
      "parent_id": "398998b5392f4150ad48fe456d6de4f1",
      "domain_id": "398998b5392f4150ad48fe456d6de4f1",
      "name": "MOS" MOS为OBS默认项目的名称
    }
  ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。

状态码	说明
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。

4.4.3 查询用户可以访问的项目列表

功能介绍

该接口用于查询用户可以访问的项目列表。

URI

GET /v3/auth/projects

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的需要查询的用户的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET /v3/auth/projects
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
projects	是	JSONArray	项目列表。
links	是	Object	项目的资源链接。

- project格式说明

参数	是否必选	类型	说明
description	是	String	project描述。
id	是	String	project的ID。
domain_id	是	String	project所在domain ID。
name	是	String	project名称。
links	是	Object	project的资源链接。
is_domain	是	Boolean	是否为domain。
enabled	是	Boolean	project是否可用。
parent_id	是	String	project的父ID。

- 响应样例

```
{
 "links": {
  "self": "https://sample.domain.com/v3/auth/projects",
  "previous": null,
  "next": null
 },
 "projects": [
  {
   "is_domain": false,
   "description": "",
   "links": {
    "self": "https://sample.domain.com/v3/projects/9041929bcc6e4bfe85add4e7b96ffdd7"
   },
   "enabled": true,
   "id": "9041929bcc6e4bfe85add4e7b96ffdd7",
   "parent_id": "398998b5392f4150ad48fe456d6de4f1",
   "domain_id": "398998b5392f4150ad48fe456d6de4f1",
   "name": "region"
  },
  {
   "is_domain": false,
   "description": "",
   "links": {
    "self": "https://sample.domain.com/v3/projects/ee65ca70d3cf43aaa1ea6492ce15f289"
   },
   "enabled": true,
   "id": "ee65ca70d3cf43aaa1ea6492ce15f289",
   "parent_id": "398998b5392f4150ad48fe456d6de4f1",
   "domain_id": "398998b5392f4150ad48fe456d6de4f1",
   "name": "{project_name}"
  }
 ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。

状态码	说明
403	鉴权失败。
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。

4.4.4 创建项目

功能介绍

该接口提供创建项目功能。

URI

POST /v3/projects

请求

- Request Header参数说明

参数	是否为必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的具有Security Administrator权限的token。

- Request Body参数说明

属性	是否为必选	类型	说明
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。 示例：*{region_id}*_test1。
parent_id	是	String	项目所属的父项目ID。
domain_id	否	String	项目所在租户的ID。
description	否	String	项目描述，长度小于等于255。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X POST -d '{"project":{"domain_id":"acf2ffabba974fae8f30378ffde2c...","name":"region_test1"}}' https://sample.domain.com/v3/projects
```

响应

响应样例

```
{
    "project": {
        "is_domain": false,
        "description": "",
        "links": {
            "self": "https://sample.domain.com/v3/projects/3de1461665f045ef91ba1efe8121b979"
        },
        "enabled": true,
        "id": "3de1461665f045ef91ba1efe8121b979",
        "parent_id": "d1294857fdf64251994892b344f53e88",
        "domain_id": "d1294857fdf64251994892b344f53e88",
        "name": "region_test1"
    }
}
```

状态码

状态码	说明
201	请求成功。
400	参数无效。
401	认证失败。
403	鉴权失败。
409	项目名重复。

4.4.5 修改项目

功能介绍

该接口提供修改项目信息的功能。

URI

- URI格式

  PATCH /v3/projects/{project_id}

- URI参数说明

参数	是否为必选	类型	说明
project_id	是	String	项目的ID。

请求

- Request Header参数说明

参数	是否为必选	类型	说明
Content-Type	是	String	文本类型及编码方式。 该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的具有Security Administrator权限的token。

- Request Body参数说明

属性	是否为必选	类型	说明
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。 示例：{region}_test2
description	否	String	项目描述，长度小于等于255。

- 请求示例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PATCH -d
'{"project":{"name":"region_test2","description":"test_project_desc"}}' https://sample.domain.com/v3/
projects/23da5961c8214f5caf701c27d9703959
```

响应消息

响应示例

```
{
    "project": {
        "is_domain": false,
        "description": "test_project_desc",
        "links": {
            "self": "https://sample.domain.com/v3/projects/23da5961c8214f5caf701c27d9703959"
        },
        "enabled": true,
        "id": "23da5961c8214f5caf701c27d9703959",
        "parent_id": "d1294857fdf64251994892b344f53e88",
        "domain_id": "d1294857fdf64251994892b344f53e88",
        "name": "region_test2"
    }
}
```

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。
409	项目名称重复。

4.4.6 查询指定项目的信息

功能介绍

该接口提供根据Project ID获取Project的详细信息。

URI

- URI格式

  GET /v3/projects/{project_id}

- URI参数说明

参数	是否必选	类型	描述
project_id	是	String	指定的项目ID。

请求

- Request Header参数说明

参数	是否必选	类型	描述
X-Auth-Token	是	String	已认证的token。
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

- 请求示例

  获取project_id=619d3e78f61b4be68bc5aa0b59edcf7b的project信息

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/projects/619d3e78f61b4be68bc5aa0b59edcf7b
```

响应

响应示例

```
{
  "project": {
    "is_domain": false,
    "description": "",
    "links": {
      "self": "https://sample.domain.com/v3/projects/2e93d63d8d2249f5a4ac5e2c78586a6e"
    },
    "enabled": true,
    "id": "2e93d63d8d2249f5a4ac5e2c78586a6e",
    "parent_id": "44c0781c83484eb9a4a5d4d233522cea",
    "domain_id": "44c0781c83484eb9a4a5d4d233522cea",
    "name": "MOS" MOS为OBS默认项目的名称
  }
}
```

状态码

状态码	说明
200	请求成功
400	请求错误。
401	认证失败。
403	鉴权失败。
404	资源不存在。
500	内部服务错误。

4.4.7 设置指定项目的状态

功能介绍

该接口用于设置指定项目的状态，项目的状态包括正常、冻结。

URI

- URI格式
  PUT /v3-ext/projects/{project_id}
- URI参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的具有Security Administrator权限的token。

- Request Body参数说明

属性	是否为必选	类型	说明
status	是	String	项目的状态信息，范围['suspended', 'normal']。

说明

- status值为'suspended'时，会将project设置为冻结状态；
- status值为'normal'时，会将project设置为正常（解冻）状态。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -X "X-Auth-Token:$token" -X PUT -d '{"project": {"status":"suspended"}}'https://sample.domain.com/v3-ext/projects/5c9f5525d9d24c5bbf91e74d86772029
```

响应

无响应体。

状态码

状态码	说明
204	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
500	内部服务错误。
503	服务不可用。

4.4.8 查询指定项目信息及状态

功能介绍

该接口用于查询指定项目的详细信息，包含项目的状态。

URI

- URI格式

  GET /v3-ext/projects/{project_id}

- URI参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的具有Security Administrator权限的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -X "X-Auth-Token:$token" -X GET https://sample.domain.com/v3-ext/projects/5c9f5525d9d24c5bbf91e74d86772029
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
project	是	Object	项目信息。

- project格式说明

参数	是否必选	类型	说明
description	是	String	项目描述。
id	是	String	项目ID。
domain_id	是	String	项目所在domain的ID。
name	是	String	项目名称。
is_domain	是	Boolean	是否为domain。
enabled	是	Boolean	项目是否可用。
parent_id	是	String	项目的父ID。
status	是	String	项目的状态。
suspended_time	否	String	项目的冻结时间。

- 响应样例

```
{
  "project": {
    "is_domain": false,
    "description": "",
    "enabled": true,
    "id": "ee65ca70d3cf43aaa1ea6492ce15f289",
    "parent_id": "9041929bcc6e4bfe85add4e7b96ffdd7",
    "domain_id": "398998b5392f4150ad48fe456d6de4f1",
    "name": "{region_id}_test1",
    "status": "suspended",
    "suspended_time": "2017-08-17T02:50:23.000000"
  }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
500	内部服务错误。
503	服务不可用。

4.4.9 查询项目配额

功能介绍

该接口可以用于查询项目配额。

URI

- URI格式
  GET /v3.0/OS-QUOTA/projects/{project_id}
- 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	待查询的项目ID。

请求参数

表 4-23 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	此token可以如下任意一个： • 拥有Security Administrator权限的token。 • IAM用户的Token（Token的scope需为待查询项目project）。

响应参数

表 4-24 响应 Body 参数

参数	参数类型	描述
quotas	object	账号配额信息。

表 4-25 quotas

参数	参数类型	描述
resources	Array of objects	资源信息

表 4-26 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。

请求示例

```
GET https://sample.domain.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。

4.5 租户管理

4.5.1 查询用户可以访问的租户列表

功能介绍

该接口用于查询用户可以用访问的租户列表。

URI

GET /v3/auth/domains

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token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/auth/domains
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
domains	是	JSONArray	租户列表。
links	是	JSONObject	租户的资源链接。

- domain格式说明

参数	是否必选	类型	说明
enabled	是	Boolean	是否启用租户，true为启用，false为停用，默认为true。
id	是	String	租户ID。
name	是	String	租户名称。
links	是	JSONObject	租户资源的链接。
description	否	String	租户描述。

- 响应样例

```
{
    "domains": [{
        "description": "desc of domain",
        "enabled": true,
        "id": "37ef61",
        "links": {
            "self": "https://sample.domain.com/v3/domains/37ef61"
        },
        "name": "my domain"
    }],
    "links": {
        "self": "https://sample.domain.com/v3/auth/domains",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
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。

4.5.2 查询租户密码强度策略

功能介绍

该接口用于查询租户密码强度策略，包括密码强度策略的正则表达式以及描述。

URI

- URI格式
  GET /v3/domains/{domain_id}/config/security_compliance
- 参数说明

参数	是否必选	类型	说明
domain_id	是	String	需要查询的租户domain的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的用户自身的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/domains/{domain_id}/config/security_compliance
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
security_compliance	是	JSON	租户密码强度策略。
password_regex	是	String	密码强度策略的正则表达式。
password_regex_description	是	String	密码强度策略的描述。

- 响应样例

```
{
  "config": {
    "security_compliance": {
      "password_regex": "^(?=.*\\d)(?=.*[a-zA-Z]).{7,}$",
      "password_regex_description": "Passwords must contain at least 1 letter, 1 digit, and be a minimum length of 7 characters."
    }
  }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.5.3 按照条件查询租户密码强度策略

功能介绍

该接口用于按照条件查询租户密码强度策略，可以查询密码强度策略的正则表达式或者描述。

URI

- URI格式
  GET /v3/domains/{domain_id}/config/security_compliance/{option}
- 参数说明

参数	是否必选	类型	说明
domain_id	是	String	需要查询的租户domain的ID。
option	是	String	查询条件，password_regex或者password_regex_description。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的用户自身的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/domains/{domain_id}/config/security_compliance/password_regex
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
config	是	JSON	租户密码强度策略。

- config格式说明

参数	是否必选	类型	说明
password_regex	否	String	密码强度策略的正则表达式。(当option为password_regex时)。

参数	是否必选	类型	说明
password_regex_description	否	String	密码强度策略的描述。(当option为password_regex_description时)。

- 响应样例

```
当option为password_regex时：
{
  "config": {
    "password_regex": "^(?=.*\\d)(?=.*[a-zA-Z]).{7,}$"
  }
}
当option为password_regex_description时：
{
  "config": {
    "password_regex_description": "Passwords must contain at least 1 letter, 1 digit, and be a minimum length of 7 characters."
  }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.5.4 查询租户配额

功能介绍

该接口用于按照条件查询租户配额，可以查询的配额类型有：user、group、idp、agency、policy。

URI

- URI格式

  GET /v3.0/OS-QUOTA/domains/{domain_id}

- 参数说明

参数	是否必选	类型	说明
domain_id	是	String	需要查询的租户domain的ID。
type	否	String	查询租户配额的类型，支持user, group, idp, agency, policy五种类型。

请求

- Request Header参数说明

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

- 请求样例

```
GET https://sample.domain.com/v3.0/OS-QUOTA/domains/{domain_id}?type=group
```

响应

表 4-27 响应 Body 参数

参数	参数类型	描述
quotas	Object	账号配额信息。

表 4-28 quotas

参数	参数类型	描述
resources	Array of objects	资源信息。

表 4-29 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。

- 响应样例

```
当type为group时：
{
    "quotas": {
        "resources": [
            {
                "max": 200,
                "min": 10,
                "quota": 20,
                "type": "group",
                "used": 6
            }
        ]
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
500	内部服务错误。
503	服务不可用。

4.6 用户管理

4.6.1 查询用户列表

功能介绍

该接口用于查询用户列表。

URI

- URI格式

  GET /v3/users

- 参数说明

参数	是否必选	类型	说明
domain_id	否	String	用户所属的domain的ID。
enabled	否	String	是否启用用户，true为启用，false为停用，默认为true。
name	否	String	用户名。
password_expires_at	否	String	密码过期时间，格式为：password_expires_at={operator}:{timestamp}。 示例： password_expires_at=lt:2016-12-08T22:02:00Z ● operator取值范围：lt，lte，gt，gte，eq，neq – lt：过期时间小于timestamp – lte：过期时间小于等于timestamp – gt：过期时间大于timestamp – gte：过期时间大于等于timestamp – eq：过期时间等于timestamp – neq：过期时间不等于timestamp ● timestamp格式为YYYY-MM-DDTHH:mm:ssZ

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/users
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
users	是	JSONArray	用户列表。
links	是	JSONObject	用户资源的链接。

- user格式说明

参数	是否必选	类型	说明
description	是	String	用户的描述。
domain_id	是	String	用户所属租户的ID。
enabled	是	Boolean	用户是否启用，true表示启用，false表示停用，默认为true。
id	是	String	用户的ID。
links	是	JSONObject	用户资源的链接。
name	是	String	用户的名称。
password_expires_at	是	String	密码过期时间（UTC时间），“null”表示密码不过期。
pwd_status	否	Boolean	密码状态，true：需要修改密码，false：正常。
default_project_id	否	String	用户登录控制台后默认跳转的项目ID。
last_project_id	否	String	用户退出系统前，在控制台最后访问的项目的ID。
email	否	String	IAM用户邮箱。

- 响应样例

```
{
   "users": [{
      "name": "username",
      "links": {
         "self": "https://sample.domain.com/v3/users/6d8b04e3bf99445b8f76300xxx"
      },
      "description": "1234",
      "domain_id": "88b16b6440684467b8825d7xxx",
      "enabled": false,
      "id": "6d8b04e3bf99445b8f763009xxx",
      "email" : ""
      "default_project_id": "263fd9",
      "password_expires_at": "2016-12-07T00:00:00.000000Z",
      "pwd_status": true,

      "last_project_id": ""
   }],
```

```
    "links": {
        "self": "https://sample.domain.com/v3/users?
domain_id=88b16b6440684467b882xxx154d8&enabled=false",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.2 查询用户详情

功能介绍

该接口用于查询指定用户的详细信息。

URI

- URI格式
  GET /v3/users/{user_id}
- 参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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，或用户自身的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/users/43cbe5e77aaf4665bbb962062dc1fxxx
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
user	是	JSONObject	user对象。

- user格式说明

参数	是否必选	类型	说明
description	是	String	用户的描述。
domain_id	是	String	用户所属租户的ID。
enabled	是	Boolean	用户是否启用，true表示启用，false表示停用，默认为true。
id	是	String	用户的ID。
links	是	JSONObject	用户资源的链接。
name	是	String	用户的名称。
password_expires_at	是	String	密码过期时间（UTC时间），“null”表示密码不过期。
pwd_status	否	Boolean	密码状态，true：需要修改密码，false：正常。
pwd_strength	否	String	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。
default_project_id	否	String	用户登录控制台后默认跳转的项目ID。
last_project_id	否	String	用户退出系统前，在控制台最后访问的项目的ID。

- 响应样例

```
{
    "users": [{
        "name": "username",
        "links": {
            "self": "https://sample.domain.com/v3/users/6d8b04e3bf99445b8f76300xxx"
        },
        "description": "1234",
        "domain_id": "88b16b6440684467b8825d7xxx",
        "enabled": false,
        "id": "6d8b04e3bf99445b8f763009xxx",
        "password_expires_at": "2016-12-07T00:00:00.000000Z",
        "pwd_status": true,
        "pwd_strength": "high",
        "last_project_id": ""
    }],
    "links": {
        "self": "https://sample.domain.com/v3/users?
domain_id=88b16b6440684467b882xxx154d8&enabled=false",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.3 查询用户详情（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。

URI

GET /v3.0/OS-USER/users/{user_id}

表 4-30 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。

请求参数

表 4-31 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	管理员查询IAM用户详情：拥有Security Administrator权限的token。 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 4-32 响应 Body 参数

参数	参数类型	描述
user	Object	IAM用户信息。

表 4-33 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。

参数	参数类型	描述
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。
update_time	String	IAM用户更新时间。
create_time	String	IAM用户创建时间。
last_login_time	String	IAM用户最后登录时间。
pwd_strength	String	IAM用户密码强度。结果为Low/Middle/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。
description	String	IAM用户描述信息。

表 4-34 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。
next	String	后一邻接资源链接地址。

请求示例

```
GET https://sample.domain.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",
    "last_login_time" : null,
    "areacode" : "",
    "enabled" : true,
    "domain_id" : "086ba757f90089cf0fe5c000dbe7f...",
    "xuser_id" : "",
    "pwd_status" : false,
    "update_time" : null,
    "phone" : "-",
    "name" : "autotest1",
```

```
  "links" : {
    "next" : null,
    "previous" : null,
    "self" : "https://sample.domain.com/v3.0/OS-USER/users/093f75808b8089ba1f6dc000c7cac..."
  },
  "id" : "093f75808b8089ba1f6dc000c7cac...",
  "xuser_type" : "",
  "email" : "",
 }
}
```

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。

4.6.4 查询用户所属用户组

功能介绍

该接口用于查询指定用户所属的用户组信息。

URI

- URI格式

  GET /v3/users/{user_id}/groups
- 参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

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

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，或已认证的用户自身的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/users/43cbe5e77aaf4665bbb962062dc1fc9d/groups
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
groups	是	JSONArray	用户组列表。
links	是	JSONObject	用户组的资源链接。

- group格式说明

参数	是否必选	类型	说明
description	是	String	用户组描述。
id	是	String	用户组ID。
domain_id	是	String	用户组所在domain的ID。
name	是	String	用户组名称。
links	是	JSONObject	用户组的资源链接。
create_time	是	Long	用户组创建时间。

- 响应样例

```
{
    "links": {
        "self": "https://sample.domain.com/v3/users/f7cb4876e5174c0885433e280e831c43/groups",
        "previous": null,
        "next": null
    },
    "groups": [{
        "description": "User group that has the permission for all system operations",
        "links": {
            "self": "https://sample.domain.com/v3/groups/e21c7a1e415c4604927948dc24750716"
        },
        "id": "e21c7a1e415c4604927948dc24750716",
        "create_time": 1472888495993,
        "domain_id": "88b16b6440684467b8825d7d96e154d8",
        "name": "admin"
    }]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.5 查询用户组所包含的用户

功能介绍

该接口提供查询用户组中所包含的用户的功能。

URI

- URI格式
  GET /v3/groups/{group_id}/users
- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。

- 查询参数说明

属性	是否必选	类型	说明
domain_id	否	String	用户组所属domain的ID。
name	否	String	用户的名称，长度小于等于64字符。
enabled	否	String	用户是否启用。true是启用，false是停用。

属性	是否必选	类型	说明
password_expires_at	否	String	密码过期时间，格式为：password_expires_at={operator}:{timestamp}。 示例： password_expires_at=lt:2016-12-08T22:02:00Z • operator取值范围：lt，lte，gt，gte，eq，neq – lt：过期时间小于timestamp – lte：过期时间小于等于timestamp – gt：过期时间大于timestamp – gte：过期时间大于等于timestamp – eq：过期时间等于timestamp – neq：过期时间不等于timestamp • timestamp格式为YYYY-MM-DDTHH:mm:ssZ

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”
X-Auth-Token	是	String	已认证的具有Security Administrator权限的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/groups/00007111583e457389b0d4252643181b/users
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	JSONObject	用户组内用户的资源链接。

参数	是否必选	类型	说明
users	是	JSONArray	用户组内用户的列表。

- user格式说明

参数	是否必选	类型	说明
description	是	String	用户的描述。
domain_id	是	String	用户所属租户的ID。
enabled	是	Boolean	用户是否启用，true表示启用，false表示停用，默认为true。
id	是	String	用户的ID。
links	是	JSONObject	用户资源的链接。
name	是	String	用户的名称。
password_expires_at	是	String	密码过期时间（UTC时间），“null”表示密码不过期。
pwd_status	否	Boolean	密码状态，true：需要修改密码，false：正常。
default_project_id	否	String	用户登录控制台后默认跳转的项目ID。
last_project_id	否	String	用户退出系统前，在控制台最后访问的项目的ID。
email	否	String	IAM用户邮箱。

- 响应样例

```
{
    "users": [{
        "name": "username",
        "links": {
            "self": "https://sample.domain.com/v3/users/6d8b04e3bf99445b8f76300xxx"
        },
        "description": "1234",
        "domain_id": "88b16b6440684467b8825d7xxx",
        "enabled": false,
        "id": "6d8b04e3bf99445b8f763009xxx",
        "email" : ""
        "default_project_id": "263fd9",
        "password_expires_at": "2016-12-07T00:00:00.000000Z",
        "pwd_status": true,

        "last_project_id": ""
    }],
    "links": {
        "self": "https://sample.domain.com/v3/users?
domain_id=88b16b6440684467b882xxx154d8&enabled=false",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.6.6 创建用户

功能介绍

该接口用于在某一租户下创建用户。

URI

POST /v3/users

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

表 4-35 user 格式说明

参数	是否必选	参数类型	描述
user	是	Object	用户信息。

表 4-36 user

参数	是否必选	类型	说明
name	是	String	用户名，长度5~32之间，首位不能为数字，特殊字符只能包含“下划线_、中划线-、和空格”。
domain_id	否	String	用户所在domain的ID。
enabled	否	Boolean	是否启用用户。 true为启用，false为停用，默认为true。
password	否	String	用户密码。 ● 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； ● 不能与用户名以及用户名的倒序； ● 不能包含手机号和邮箱； ● 必须满足账户设置中密码策略的要求；
default_project_id	否	String	用户默认的project ID。
description	否	String	用户的描述信息。

- 请求样例

1.按照以下模板创建临时文件${filename}.json。${filename}是临时文件名，用户可以自定义。

```
{
    "user": {
        "default_project_id": "acf2ffabba974fae8f30378ffde2cfa6",
        "domain_id": "88b16b6440684467b8825d7d96e154d8",
        "enabled": true,
        "name": "jamesdoe",
        "password": "********"
    }
}
```

2.在${filename}.json文件同目录下，执行如下curl命令。

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X POST -d @${filename}.json https://sample.domain.com/v3/users
```

3.在${filename}.json文件同目录下，执行如下命令删除临时文件${filename}.json。

```
rm ${filename}.json
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
user	是	JSONObject	user对象。

- user格式说明

参数	是否必选	类型	说明
enabled	是	Boolean	是否启用用户。 true为启用，false为停用，默认为true。
id	是	String	用户ID。
domain_id	是	String	用户所在domain的ID。
name	是	String	用户名称。
links	是	JSONObject	用户的资源链接。
default_project_id	否	String	用户默认的project ID。
password_expires_at	是	String	密码过期时间（UTC时间），“null”表示密码不过期。

- 响应样例

```
{
    "user": {
        "name": "jamesdoe",
        "links": {
            "self": "https://sample.domain.com/v3/users/614d1d2fb86940faab8f350bf1b9dbac"
        },
        "domain_id": "88b16b6440684467b8825d7d96e154d8",
        "enabled": true,
        "id": "614d1d2fb86940faab8f350bf1b9dbac",
        "default_project_id": "acf2ffabba974fae8f30378ffde2cfa6",
        "password_expires_at": null
    }
}
```

状态码

状态码	说明
201	创建成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

状态码	说明
503	服务不可用。

4.6.7 修改密码

功能介绍

该接口用于用户修改自己密码。

URI

- URI格式
  POST /v3/users/{user_id}/password
- URI参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- Request Body参数说明

参数	是否必选	类型	说明
original_password	是	String	用户的原密码。

参数	是否必选	类型	说明
password	是	String	用户的新密码。 ● 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； ● 不能与用户名以及用户名的倒序； ● 不能包含手机号和邮箱； ● 必须满足账户设置中密码策略的要求；

- 请求样例

```
1.按照以下模板创建临时文件${filename}.json。${filename}是临时文件名，用户可以自定义。
{
    "user": {
        "password": "********",
        "original_password": "********"
    }
}
2.在${filename}.json文件同目录下，执行如下curl命令。
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X POST -d @${filename}.json https://sample.domain.com/v3/users/2c1c6c54e59141b889c99e6fada5f19f/password
3.在${filename}.json文件同目录下，执行如下命令删除临时文件${filename}.json。
rm ${filename}.json
```

响应

无响应体。

状态码

状态码	说明
204	修改成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.8 修改用户信息

功能介绍

该接口用于修改租户下对应的用户信息。

URI

- URI格式
  PATCH /v3/users/{user_id}
- URI参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
name	否	String	用户名，长度5~32之间，首位不能为数字，特殊字符只能包含“下划线_、中划线-、和空格”。
domain_id	否	String	用户所在domain的ID。
enabled	否	Boolean	是否启用用户，true为启用，false为停用，默认为true。

参数	是否必选	类型	说明
password	否	String	用户的新密码。 ● 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； ● 不能与用户名以及用户名的倒序； ● 不能包含手机号和邮箱； ● 必须满足账户设置中密码策略的要求；
default_project_id	否	String	用户默认的project ID。
description	否	String	用户的描述信息。

- 请求样例

1.按照以下模板创建临时文件${filename}.json。${filename}是临时文件名，用户可以自定义。

```
{
    "user": {
        "name": "james1234",
        "default_project_id": "88b16b6440684467b8825d7d96e154d8",
        "enabled": false,
        "password": "********"
    }
}
```

2.在${filename}.json文件同目录下，执行如下curl命令。

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X POST -d @${filename}.json https://sample.domain.com/v3/users/2c1c6c54e59141b889c99e6fada5f19f
```

3.在${filename}.json文件同目录下，执行如下命令删除临时文件${filename}.json。

```
rm ${filename}.json
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
user	是	JSONObject	user对象。

- user格式说明

参数	是否必选	类型	说明
enabled	是	Boolean	是否启用用户。true为启用，false为停用，默认为true。
id	是	String	用户ID。
domain_id	是	String	用户所在domain的ID。

参数	是否必选	类型	说明
name	是	String	用户名称。
links	是	JSONObject	用户的资源链接。
description	是	String	用户的描述信息。
default_project_id	否	String	用户默认的project ID。
password_expires_at	是	String	密码过期时间（UTC时间），“null”表示密码不过期。

- 响应样例

```
{
    "user": {
        "name": "james1234",
        "links": {
            "self": "https://sample.domain.com/v3/users/6d8b04e3bf99445b8f76300903e5bf32"
        },
        "description": {
        },
        "domain_id": "88b16b6440684467b8825d7d96e154d8",
        "enabled": false,
        "id": "6d8b04e3bf99445b8f76300903e5bf32",
        "default_project_id": "88b16b6440684467b8825d7d96e154d8",
        "password_expires_at": "2016-12-07T00:00:00.000000Z"
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.9 修改用户信息（包含邮箱和手机号码）

功能介绍

该接口用于修改IAM用户信息，使用对象：IAM用户。

URI

PUT /v3.0/OS-USER/users/{user_id}/info

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	用户自己的token。

- Request Body参数说明

表 4-37 请求 Body 参数

参数	是否必选	参数类型	描述
user	是	Object	IAM用户信息。

表 4-38 user

参数	是否必选	类型	说明
email	否	String	邮箱，符合邮箱格式，长度小于等于255位。
phone	否	String	手机号，纯数字，长度小于等于32位。 如需修改手机号码，国家码为必选参数。
areacode	否	String	国家码。 如需修改手机号码，此项为必选。

- 请求样例
  - 按照以下模板创建临时文件${filename}.json。${filename}是临时文件名，用户可以自定义。

```
{
   "user": {
      "areacode": "0001",
      "phone": "1234567890",
      "email": "abcdefg@123.com"
   }
}
```

- 在${filename}.json文件同目录下，执行如下curl命令。

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PUT -d @${filename}.json https://sample.domain.com/v3.0/OS-USER/users/0638848aa7801dbe1f01c01e92b95df7/info
```

- 在${filename}.json文件同目录下，执行如下命令删除临时文件${filename}.json。

```
rm ${filename}.json
```

响应

无响应

状态码

状态码	说明
204	修改成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.6.10 管理员修改 IAM 用户信息（包含邮箱和手机号码)

功能介绍

该接口可以用于修改IAM用户信息,使用对象：管理员 。

URI

PUT /v3.0/OS-USER/users/{user_id}

表 4-39 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。

请求参数

表 4-40 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 4-41 请求 Body 参数

参数	是否必选	参数类型	描述
user	是	Object	IAM用户信息。

表 4-42 user

参数	是否必选	参数类型	描述
name	否	String	新用户名，长度5~32之间，首位不能为数字，特殊字符只能包含“下划线_、中划线-、和空格”。
password	否	String	IAM用户新密码。 • 系统默认密码最小长度为6位字符，在6-32位之间支持用户自定义密码长度。 • 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。 • 必须满足账户设置中密码策略的要求。 • 新密码不能与当前密码相同。

参数	是否必选	参数类型	描述
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用户首次登录是否需要修改密码。true为需要修改密码，false为不需要修改密码，默认为true。
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。 **说明** 外部系统指与系统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，无法在系统获取，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，必须与xuser_type同时存在。 **说明** 外部系统指与系统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，无法在系统获取，请咨询企业管理员。
access_mode	否	String	IAM用户访问方式。 ● default：默认访问模式，编程访问和管理控制台访问。 ● programmatic：编程访问。 ● console：管理控制台访问。
description	否	String	IAM用户新描述信息。

响应参数

表 4-43 响应 Body 参数

参数	参数类型	描述
user	Object	IAM用户信息。

表 4-44 user

参数	参数类型	描述
pwd_status	Boolean	首次登录是否重置密码。
xuser_id	String	IAM用户在外部系统中的ID。 **说明** 外部系统指与系统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，无法在系统获取，请咨询企业管理员。
xuser_type	String	IAM用户在外部系统中的类型。 **说明** 外部系统指与系统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，无法在系统获取，请咨询企业管理员。
description	String	IAM用户的新描述信息。
name	String	IAM用户新用户名，长度5~32之间，首位不能为数字，特殊字符只能包含下划线“_”、中划线“-”和空格。
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。
pwd_status	Boolean	IAM用户首次登录是否需要修改密码。true为需要修改密码，false为不需要修改密码，默认为true。
areacode	String	国家码。
email	String	IAM用户新邮箱。
id	String	IAM用户ID。
links	Object	IAM用户的资源链接信息。
password_expires_at	String	密码过期时间（UTC时间），“null”表示密码不过期。

表 4-45 user.links

参数	参数类型	描述
self	String	资源链接地址。

请求示例

```
PUT https://sample.domain.com/v3.0/OS-USER/users/{user_id}
{
    "user": {
        "email": "IAMEmail@123.com",
        "areacode": "0086",
        "phone": "12345678910",
        "enabled": true,
        "name": "IAMUser",
        "password": "IAMPassword@",
        "pwd_status": false,
        "xuser_type": "",
        "xuser_id": "",
        "description": "IAMDescription"
    }
}
```

响应示例

状态码为 200 时:

请求成功。

```
{
    "user": {
        "description": "IAMDescription",
        "areacode": "0086",
        "enabled": true,
        "pwd_status": false,
        "xuser_id": "",
        "domain_id": "d78cbac186b744899480f25bd0...",
        "phone": "12345678910",
        "name": "IAMUser",
        "links": {
            "self": "https://sample.domain.com/3.0/OS-USER/users/076934ff9f0010cd1f0bc003..."
        },
        "id": "076934ff9f0010cd1f0bc0031019...",
        "xuser_type": "",
        "email": "IAMEmail@123.com"
    }
}
```

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。
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

状态码	错误码	错误信息
400	1100	缺失必选参数。
400	1101	用户名校验失败。
400	1102	邮箱校验失败。
400	1103	密码校验失败。
400	1104	手机号校验失败。
400	1105	xuser_type必须与xdomain_type相同。
400	1106	国家码、手机号必须同时存在。
400	1107	账号管理员不能被删除。
400	1108	新密码不能与原密码相同。
400	1109	用户名已存在。
400	1110	邮箱已存在。
400	1111	手机号已存在。
400	1113	xuser_id、xuser_type已存在。
400	1115	IAM用户数量达到最大限制。
400	1117	用户描述校验失败。

4.6.11 删除用户

功能介绍

该接口用于删除指定用户。

URI

- URI格式
  DELETE /v3/users/{user_id}
- URI参数说明

参数	是否必选	类型	说明
user_id	是	String	用户ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/users/2c1c6c54e59141b889c99e6fada5f19f
```

响应

无响应体。

状态码

状态码	说明
204	删除成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
405	不允许的方法。

状态码	说明
413	请求体过大。
500	内部服务错误。
503	服务不可用。

4.6.12 删除用户组中用户

功能介绍

该接口提供删除用户组中用户的功能。

URI

- URI格式
  DELETE /v3/groups/{group_id}/users/{user_id}
- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。
user_id	是	String	用户的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/groups/00007111583e457389b0d4252643181b/users/edb66d2b656c43d0b67fb143d670bb3a
```

响应

无响应体。

状态码

状态码	说明
204	请求成功。
400	请求错误
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.7 用户组管理

4.7.1 查询用户组列表

功能介绍

该接口提供查询用户组信息的功能。

URI

- URI格式
  GET /v3/groups{?domain_id,name}
- 查询参数说明

属性	是否必选	类型	说明
domain_id	否	String	用户组所在domain的ID。
name	否	String	用户组的名称，长度小于等于64字符。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例
  curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://sample.domain.com/v3/groups?domain_id=ac7197fd67a24dc5850972854729a762&name=group123

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	JSONObject	用户组的资源链接。
groups	是	JSONArray	用户组列表。

- group参数说明

参数	是否必选	类型	说明
description	是	String	用户组的描述。
domain_id	是	String	用户组所属domain的ID。
id	是	String	用户组的ID。
links	是	JSONObject	用户组的资源链接。
name	是	String	用户组的名称。
create_time	是	Long	用户组创建的时间。

- 响应样例

```
{
    "links": {
        "self": "https://sample.domain.com/v3/groups?
domain_id=ac7197fd67a24dc5850972854729a762&name=group123",
        "previous": null,
        "next": null
    },
    "groups": [{
        "description": "",
        "links": {
            "self": "https://sample.domain.com/v3/groups/ff74abaeabe34c278a4b7693c7f0dff7"
        },
        "id": "ff74abaeabe34c278a4b7693c7f0dff7",
        "create_time": 1482566254983,
        "domain_id": "ac7197fd67a24dc5850972854729a762",
        "name": "group123"
    }]
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。

4.7.2 查询用户组详情

功能介绍

该接口提供查询用户组详细信息的功能。

URI

- URI格式
  GET /v3/groups/{group_id}
- 查询参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://sample.domain.com/v3/groups/ab9f261180d746ef8624beb5ae39b5aa
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
group	是	JSONObject	用户组的响应体。
description	是	String	用户组的描述。
domain_id	是	String	用户组所属domain的ID。
id	是	String	用户组的ID。
links	是	JSONObject	用户组的链接。
name	是	String	用户组的名称。
create_time	是	Long	用户组创建时间。

- 响应样例

```
{
   "group":{
      "domain_id":"d54061ebcb5145dd814f8eb3fe9b7ac0",
      "description":"Contract developers",
      "id":"ab9f261180d746ef8624beb5ae39b5aa",
      "links":{
         "self":"https://sample.domain.com/v3/groups/ab9f261180d746ef8624beb5ae39b5aa"
      },
      "name":"abcdef",
      "create_time": 1494943784468
   }
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.7.3 创建用户组

功能介绍

该接口提供创建用户组的功能。

URI

POST /v3/groups

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
description	否	String	用户组的描述，长度小于等于255字符。

参数	是否必选	类型	说明
domain_id	否	String	用户组所属domain的ID。
name	是	String	用户组的名称，长度小于等于64字符。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X POST -d'{"group": {"description": "Contract developers","domain_id": "d54061ebcb5145dd814f8eb3fe9b7ac0","name": "jixiang2"}}' https://sample.domain.com/v3/groups
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
description	是	String	用户组的描述。
domain_id	是	String	用户组所属domain的ID。
id	是	String	用户组的ID。
links	是	JSONObject	用户组的链接。
name	是	String	用户组的名称。

- 响应样例

```
{
    "group":{
        "domain_id":"d54061ebcb5145dd814f8eb3fe9b7ac0",
        "description":"Contract developers",
        "id":"ab9f261180d746ef8624beb5ae39b5aa",
        "links":{
            "self":"https://sample.domain.com/v3/groups/ab9f261180d746ef8624beb5ae39b5aa"
        },
        "name":"abcdef"
    }
}
```

状态码

状态码	说明
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。

4.7.4 添加用户到用户组

功能介绍

该接口提供为用户组添加用户的功能。

URI

- URI格式
  PUT /v3/groups/{group_id}/users/{user_id}
- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。
user_id	是	String	用户的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PUT https://sample.domain.com/v3/groups/00007111583e457389b0d4252643181b/users/edb66d2b656c43d0b67fb143d670bb3a
```

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	没有操作权限。
404	找不到资源。

4.7.5 更新用户组

功能介绍

该接口提供更新用户组信息的功能。

URI

- URI格式

  PATCH /v3/groups/{group_id}

- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
group	是	Object	group请求体。
description	否	String	用户组的描述，长度小于等于255字符。
domain_id	否	String	用户组所属domain的ID。
name	否	String	用户组的名称，长度小于等于64字符。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PATCH -d'{"group": {"description": "Contract developers 2016"}}' https://sample.domain.com/v3/groups/aaec2abd4eba430fbf61541ffde76650
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
group	是	Dict	用户组的响应体。
description	是	String	用户组描述。
domain_id	是	String	用户组所属domain的ID。
id	是	String	用户组的ID。
links	是	Dict	用户组的资源链接。
name	是	String	用户组的名称。

- 响应样例

```
{
  "group": {
    "domain_id": "d54061ebcb5145dd814f8eb3fe9b7ac0",
    "description": "Contract developers 2016",
    "id": "aaec2abd4eba430fbf61541ffde76650",
    "links": {
      "self": "https://sample.domain.com/v3/groups/aaec2abd4eba430fbf61541ffde76650"
    },
    "name": "jixiang1"
  }
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。
409	资源冲突。
501	接口没有实现。

4.7.6 删除用户组

功能介绍

该接口提供删除用户组的功能。

URI

- URI格式

  DELETE /v3/groups/{group_id}

- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/groups/aaec2abd4eba430fbf61541ffde76650
```

响应

无响应体。

状态码

状态码	说明
204	删除成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.7.7 查询用户是否在用户组中

功能介绍

该接口查询某用户是否属于某用户组的功能。

URI

- URI格式

  HEAD /v3/groups/{group_id}/users/{user_id}

- URI参数说明

属性	是否必选	类型	说明
group_id	是	String	用户组的ID。
user_id	是	String	用户的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X HEAD https://sample.domain.com/v3/groups/00007111583e457389b0d4252643181b/users/edb66d2b656c43d0b67fb143d670bb3a
```

响应

无响应体。

状态码

状态码	说明
204	用户在用户组中。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源或用户不在用户组中。

4.8 权限管理

4.8.1 查询角色列表

功能介绍

该接口提供查询角色列表功能，包括角色中的权限策略，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

GET /v3/roles

表 4-46 Query 参数

参数	是否必选	参数类型	描述
domain_id	否	String	账号ID。 **说明** • 如果填写此参数，则返回账号下所有自定义策略。 • 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）。
name	否	String	系统内部权限名。（非控制台权限展示名“display_name”）

请求参数

表 4-47 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。

响应参数

表 4-48 响应 Body 参数

参数	参数类型	描述
links	Object	资源链接信息。
roles	Array of objects	权限信息列表。
total_number	Integer	返回权限的总数。

表 4-49 links

参数	参数类型	描述
self	String	资源链接。
previous	String	上一个临接资源链接。
next	String	下一个临接资源链接。

表 4-50 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。
links	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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • AA表示在domain和project层均显示。 • XX表示在domain和project层均不显示。 • 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）。
policy	Object	权限的具体内容。
updated_time	String	权限更新时间。
created_time	String	权限创建时间。

表 4-51 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。
next	String	后一邻接资源链接地址。

表 4-52 roles.policy

参数	参数类型	描述
Depends	Array of objects	该权限所依赖的权限。
Statement	Array of objects	授权语句，描述权限的具体内容。
Version	String	权限版本号。 **说明** • 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。 • 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。

表 4-53 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 4-54 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，不超过100个。 **说明** • 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。 • 当自定义策略为委托自定义策略时，该字段值为： *"Action": ["iam:agencies:assume"]*。
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。 取值范围： • Allow • Deny
Condition	Object	限制条件。不超过10个。
Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。 • 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"]}*。

表 4-55 roles.policy.Statement.Condition.operator

参数	参数类型	描述
attribute	Array of strings	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。 该参数类型为自定义字符串数组。

请求示例

```
GET https://sample.domain.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://sample.domain.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"
      } ]
    }
  }, {
    "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://sample.domain.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://sample.domain.com/v3/roles"
  },
  "total_number" : 300
}
```


状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。

状态码	说明
403	没有操作权限。

4.8.2 查询角色的详细信息

功能介绍

该接口提供查询角色详细信息功能，包括角色中的权限策略，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  GET /v3/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
role_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://sample.domain.com/v3/roles/19bb93eec4ca4f08aefdc02da76d8f3c
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
role	是	Dict	role的详细信息。

- role格式说明

参数	是否必选	类型	说明
domain_id	是	String	role所属domain的ID。
id	是	String	role的ID。

参数	是否必选	类型	说明
links	是	Dict	role的资源链接。
name	是	String	role的名称。
type	是	String	role的显示模式，其中： ● AX表示在domain层显示； ● XA表示在project层显示； ● AA表示在domain和project层均显示； ● XX表示在domain和project层均不显示。
display_name	否	String	role所展示的名称。
catalog	否	String	role所在的目录。
policy	否	Dict	role的具体策略。
description	否	String	role的描述。

- 响应样例

```
{
  "role": {
    "display_name": "Tanent Guest",
    "description": "Tanent Guest",
    "links": {
      "self": "https://sample.domain.com/v3/roles/19bb93eec4ca4f08aefdc02da76d8f3c"
    },
    "domain_id": null,
    "catalog": "BASE",
    "policy": {
      "Version": "1.0",
      "Statement": [
        {
          "Action": [
            "::Get",
            "::List"
          ],
          "Effect": "Allow"
        },
        {
          "Action": [
            "identity:*"
          ],
          "Effect": "Deny"
        }
      ]
    },
    "id": "19bb93eec4ca4f08aefdc02da76d8f3c",
    "type": "AA",
    "name": "readonly"
  }
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.8.3 查询租户中用户组的权限

功能介绍

该接口提供查询租户下用户组的权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

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

- URI参数说明

属性	是否必选	类型	说明
domain_id	是	String	待查询的账号ID。
group_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://sample.domain.com/v3/domains/d54061ebcb5145dd814f8eb3fe9b7ac0/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	Dict	Domain中指定用户组的role的资源链接。
roles	是	Array	Domain中指定用户组的role。

- role参数说明

参数	是否必选	类型	说明
id	是	String	Domain中指定用户组的role的ID。
links	是	Dict	role的资源链接。
name	是	String	role的名称。
domain_id	是	String	role所属domain的ID。
type	是	String	role的显示模式，其中： ● AX表示在domain层显示； ● XA表示在project层显示； ● AA表示在domain和project层均显示； ● XX表示在domain和project层均不显示。
display_name	否	String	role所展示的名称。
catalog	否	String	role所在的目录。
policy	否	Dict	role的具体策略。
description	否	String	role的描述。

- 响应样例

```
{
  "links": {
    "self": "https://sample.domain.com/v3/domains/d54061ebcb5145dd814f8eb3fe9b7ac0/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles",
    "previous": null,
    "next": null
  },
  "roles": [
    {
      "display_name": "Security Administrator",
      "description": "Security Administrator",
      "links": {
        "self": "https://sample.domain.com/v3/roles/005cf92cfd364105afaa5df2eec25012"
      },
      "domain_id": null,
      "name": "secu_admin",
      "type": "AX",
      "catalog": "BASE",
      "policy": {
        "Version": "1.0",
```

```
      "Statement": [
        {
          "Action": [
            "identity:*"
          ],
          "Effect": "Allow"
        }
      ]
    },
    "id": "005cf92cfd364105afaa5df2eec25012"
  },
  {
    "display_name": "Agent Operator",
    "description": "Agent Operator",
    "links": {
      "self": "https://sample.domain.com/v3/roles/d160d30477c642a486ad10e3b4d9820f"
    },
    "domain_id": null,
    "name": "te_agency",
    "type": "AX",
    "catalog": "IAM",
    "policy": {
      "Version": "1.0",
      "Statement": [
        {
          "Action": [
            "identity:assume role"
          ],
          "Effect": "Allow"
        }
      ]
    },
    "id": "d160d30477c642a486ad10e3b4d9820f"
  }
 ]
}
```


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。
404	找不到资源。

4.8.4 查询项目对应的用户组的权限

功能介绍

该接口提供查询某个项目对应的指定用户组的权限，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式
  GET /v3/projects/{project_id}/groups/{group_id}/roles
- URI参数说明

属性	是否必选	类型	说明
project_id	是	String	项目的ID。
group_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://sample.domain.com/v3/projects/073bbf60da374853841cf6624c94de4b/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	Dict	role的资源链接。
roles	是	Array	role列表。

- role参数说明

参数	是否必选	类型	说明
id	是	String	role的ID。
links	是	Dict	role的资源链接。
name	是	String	role的名称。
domain_id	是	String	role所属domain的ID。

参数	是否必选	类型	说明
type	是	String	role的显示模式，其中： ● AX表示在domain层显示； ● XA表示在project层显示； ● AA表示在domain和project层均显示； ● XX表示在domain和project层均不显示。
display_name	否	String	role所展示的名称。
catalog	否	String	role所在的目录。
policy	否	Dict	role的具体策略。
description	否	String	role的描述。

- 响应样例

```
{
    "links": {
        "self": " https://sample.domain.com/v3/projects/3a4cd4d559d8492bbe7bd355643f9763/groups/728da352c017480f80b5a96beb15f0e6/roles",
        "previous": null,
        "next": null
    },
    "roles": [
        {
            "catalog": "BASE",
            "display_name": "Guest",
            "name": "readonly",
            "links": {
                "self": " https://sample.domain.com/v3/roles/13d132b7856945788f6df7eb3ed5c35e"
            },
            "policy": {
                "Version": "1.0",
                "Statement": [
                    {
                        "Action": [
                            "*:*:Get*",
                            "*:*:List*"
                        ],
                        "Effect": "Allow"
                    },
                    {
                        "Action": [
                            "identity:*"
                        ],
                        "Effect": "Deny"
                    }
                ]
            },
            "domain_id": null,
            "type": "AA",
            "id": "13d132b7856945788f6df7eb3ed5c35e",
            "description": "Guest"
        },
        {
            "catalog": "BASE",
            "display_name": "Tenant Administrator",
            "name": "te_admin",
```

```
        "links": {
            "self": " https://sample.domain.com/v3/roles/1def304b73f14e8eb8d1eb9bf8337ae6"
        },
        "policy": {
            "Version": "1.0",
            "Statement": [
                {
                    "Action": [
                        "*"
                    ],
                    "Effect": "Allow"
                },
                {
                    "Action": [
                        "identity:*"
                    ],
                    "Effect": "Deny"
                }
            ]
        },
        "domain_id": null,
        "type": "AA",
        "id": "1def304b73f14e8eb8d1eb9bf8337ae6",
        "description": "Tenant Administrator"
    }
  ]
}
```

状态码

状态码	说明
200	请求成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
404	找不到资源。

4.8.5 为租户所属用户组授权

功能介绍

该接口提供给租户所属用户组增加权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
- URI参数说明

属性	是否必选	类型	说明
domain_id	是	String	用户组所属domain的ID。获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
group_id	是	String	用户组的ID。获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
role_id	是	String	role的ID。获取方式请参见：**获取权限ID**。 **说明** 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

- 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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https://sample.domain.com/v3/domains/d54061ebcb5145dd814f8eb3fe9b7ac0/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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。
409	资源冲突。

4.8.6 为项目对应的用户组授权

功能介绍

该接口提供项目对应用户组增加权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
project_id	是	String	项目的ID。获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。 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。 **说明** 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**查询指定条件下的项目信息**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。
group_id	是	String	用户组的ID。获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
role_id	是	String	role的ID。获取方式请参见：**获取权限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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https://sample.domain.com/v3/projects/073bbf60da374853841cf6624c94de4b/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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	没有操作权限。
404	找不到资源。
409	资源冲突。

4.8.7 删除项目对应的用户组的权限

功能介绍

该接口提供删除项目对应用户组权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
project_id	是	String	项目的ID。
group_id	是	String	用户组的ID。
role_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X  DELETE https://sample.domain.com/v3/projects/073bbf60da374853841cf6624c94de4b/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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。

4.8.8 删除租户所属用户组的权限

功能介绍

该接口提供删除某租户所属指定用户组权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
domain_id	是	String	用户组所属domain的ID。
group_id	是	String	用户组的ID。
role_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https://sample.domain.com/v3/domains/d54061ebcb5145dd814f8eb3fe9b7ac0/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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	没有操作权限。
404	找不到资源。

4.8.9 查询租户中用户组是否包含权限

功能介绍

该接口提供检查某租户中指定用户组是否包含特定权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
domain_id	是	String	用户组所属domain的ID。
group_id	是	String	用户组的ID。
role_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X HEAD https://10.22.44.158:31943/v3/domains/d54061ebcb5145dd814f8eb3fe9b7ac0/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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。

4.8.10 查询项目对应的用户组是否包含权限

功能介绍

该接口提供查询项目对应用户组是否包含权限的功能，权限通过角色（Role）来表达，一个Role代表成一组action。

URI

- URI格式

  HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

- URI参数说明

属性	是否必选	类型	说明
project_id	是	String	项目的ID。
group_id	是	String	用户组的ID。
role_id	是	String	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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X HEAD https://sample.domain.com/v3/projects/073bbf60da374853841cf6624c94de4b/groups/47d79cabc2cf4c35b13493d919a5bb3d/roles/e62d9ba0d6a544cd878d9e8a4663f6e2
```

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	没有操作权限。
404	找不到资源。

4.8.11 为用户组授予所有项目权限

功能介绍

该接口提供授予用户组的所有项目权限。

URI

- URI格式

  PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

- URI参数说明

属性	是否必选	类型	说明
domain_id	是	String	用户组所属domain的ID。
group_id	是	String	用户组的ID。
role_id	是	String	用户角色的ID。

请求

- Request Header参数说明

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

参数	是否必选	类型	说明
X-Auth-Token	是	String	当前租户下具有secu_admin权限的用户token（如果角色指定domainid，则domainid必须是本租户）,op_service或op_auth的权限的token。

- 请求样例
  curl -i -k -H "X-Auth-Token:$token" -X PUT https://sample.domain.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

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。

4.8.12 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。

URI

DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

表 4-56 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。
group_id	是	String	用户组ID。
role_id	是	String	权限ID。

请求参数

表 4-57 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-token	是	String	拥有本账号Security Administrator权限的token或者op_auth权限的token。

响应参数

无

请求示例

```
DELETE https://sample.domain.com/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

响应示例

无

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	找不到资源。
500	内部服务错误。

4.8.13 查询用户组是否拥有所有项目指定权限

功能介绍

该接口可以用于查询用户组是否拥有所有项目指定权限。

URI

HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

表 4-58 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ID，获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
group_id	是	String	用户组ID，获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
role_id	是	String	权限ID，获取方式请参见：**获取权限ID**。

请求参数

表 4-59 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:///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**。

4.8.14 查询用户组的所有项目权限列表

功能介绍

该接口可以用于查询用户组所有项目服务权限列表。

URI

GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects

表 4-60 路径参数

参数	是否必选	参数类型	描述
domain_id	是	String	ID，获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。
group_id	是	String	用户组ID，获取方式请参见：**获取用户、账号、用户组、项目、委托的名称和ID**。

请求参数

表 4-61 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 4-62 响应 Body 参数

参数	参数类型	描述
links	object	资源链接信息。
roles	Array of objects	权限信息列表。

参数	参数类型	描述
total_number	Integer	在查询参数存在domain_id时，返回自定义策略总数。

表 4-63 RoleResult

参数	参数类型	描述
domain_id	String	权限所属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。
links	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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • AA表示在domain和project层均显示。 • XX表示在domain和project层均不显示。 • 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）。
policy	object	权限的具体内容。
updated_time	String	权限更新时间。 **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。
created_time	String	权限创建时间。 **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。

表 4-64 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。
next	String	后一邻接资源链接地址。

表 4-65 RolePolicy

参数	参数类型	描述
Depends	Array of objects	该权限所依赖的权限。
Statement	Array of objects	授权语句，描述权限的具体内容。
Version	String	权限版本号。 **说明** • 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。 • 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。

表 4-66 PolicyDepends

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 4-67 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，不超过100个。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** • 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。 • 当自定义策略为委托自定义策略时，该字段值为：*"Action": ["iam:agencies:assume"]*。
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。 枚举值： • Allow • Deny
Condition	Object	限制条件。不超过10个。了解更多相关参数，请参考：。 **说明** 以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。 `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。 • 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"]}*。

请求示例

查询用户组的所有项目权限列表。

```
GET https:///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" : [ {
    "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:///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"
      } ]
    }
  }, {
    "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:///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:///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**。

4.9 自定义策略管理

4.9.1 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。

URI

GET /v3.0/OS-ROLE/roles

表 4-68 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 4-69 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 4-70 响应 Body 参数

参数	参数类型	描述
links	Object	资源链接信息。
roles	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 4-71 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。
next	String	后一邻接资源链接地址。

表 4-72 roles

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。
created_time	String	自定义策略创建时间。
description_cn	String	自定义策略的中文描述信息。
catalog	String	自定义策略所在目录。

参数	参数类型	描述
name	String	自定义策略名。
description	String	自定义策略的描述信息。
links	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。
type	String	自定义策略的显示模式。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
policy	Object	自定义策略的具体内容。

表 4-73 roles.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-74 roles.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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	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 4-75 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，不超过100个。 **说明** • 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。 • 当自定义策略为委托自定义策略时，该字段值为： *"Action": ["iam:agencies:assume"]*。
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。不超过10个。
Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。 • 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"]}*。

表 4-76 roles.policy.Statement.Condition

参数	参数类型	描述
operator	Object	运算符。具体运算符如 “Bool”、“StringEquals”等。 该参数类型为自定义对象。

表 4-77 roles.policy.Statement.Condition.operator

参数	参数类型	描述
attribute	Array of strings	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。 该参数类型为自定义字符串数组。

请求示例

```
GET https://sample.domain.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://sample.domain.com/v3/roles/93879fd90f1046f69e6e0b31c94d2..."
    },
    "id" : "93879fd90f1046f69e6e0b31c94d2...",
    "display_name" : "IAMCloudServicePolicy",
    "type" : "AX",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Condition" : {
          "StringStartWith" : {
            "g:ProjectName" : [ "AZ-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://sample.domain.com/v3/roles/f67224e84dc849ab954ce29fb4f47..."
    },
    "id" : "f67224e84dc849ab954ce29fb4f473...",
    "display_name" : "IAMAgencyPolicy",
    "type" : "AX",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Action" : [ "iam:agencies:assume" ],
        "Resource" : {
          "uri" : [ "/iam/agencies/07805acaba800fdd4fbdc00b8f888..." ]
        },
        "Effect" : "Allow"
      } ]
    }
  } ],
  "links" : {
    "next" : null,
    "previous" : null,
    "self" : "https://sample.domain.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。
401	认证失败。
403	没有操作权限。
500	内部服务错误。

错误码

无

4.9.2 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。

URI

GET /v3.0/OS-ROLE/roles/{role_id}

表 4-78 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：**自定义策略ID**。

请求参数

表 4-79 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。

响应参数

表 4-80 响应 Body 参数

参数	参数类型	描述
role	Object	自定义策略信息。

表 4-81 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。
created_time	String	自定义策略创建时间。
description_cn	String	自定义策略的中文描述信息。
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。
links	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。
type	String	自定义策略的显示模式。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
policy	Object	自定义策略的具体内容。

表 4-82 role.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-83 role.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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	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 4-84 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，不超过100个。 **说明** • 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。 • 当自定义策略为委托自定义策略时，该字段值为：*"Action": ["iam:agencies:assume"]*。
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。 取值范围： • Allow • Deny
Condition	Object	限制条件。不超过10个。
Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。 • 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"]}*。

表 4-85 role.policy.Statement.Condition

参数	参数类型	描述
operator	Object	运算符。具体运算符如 “Bool”、“StringEquals”等。 ● 该参数类型为自定义对象。

表 4-86 role.policy.Statement.Condition.operator

参数	参数类型	描述
attribute	Array of strings	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。 ● 该参数类型为自定义字符串数组。

请求示例

```
GET https://sample.domain.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://sample.domain.com/v3/roles/a24a71dcc41f4da989c2a1c900b52d1a"
        },
        "id": "a24a71dcc41f4da989c2a1c900b52d1a",
        "display_name": "IAMCloudServicePolicy",
        "type": "AX",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Condition": {
                        "StringStartWith": {
                            "g:ProjectName": [
                                "example-west-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

4.9.3 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。

URI

POST /v3.0/OS-ROLE/roles

请求参数

表 4-87 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 4-88 请求 Body 参数

参数	是否必选	参数类型	描述
role	是	Object	自定义策略信息。

表 4-89 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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
policy	是	Object	自定义策略的具体内容。

表 4-90 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”。 **说明** • 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。 • 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 4-91 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，不超过100个。 **说明** • 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： • Allow • Deny

Condition	否	Object	限制条件。不超过10个。
			说明
			以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。
			`"Condition": {`
			`"StringEquals": {`
			`"obs:prefix": [`
			`"public"`
			`]`
			`}`
			`}`

Resource	否	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • 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 4-92 响应 Body 参数

参数	参数类型	描述
role	Object	自定义策略信息。

表 4-93 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。
links	Object	自定义策略的资源链接信息。
policy	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。
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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
created_time	String	自定义策略创建时间。
references	String	自定义策略的引用次数。

表 4-94 role.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-95 role.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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。

参数	参数类型	描述
Statement	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 4-96 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，不超过100个。 **说明** • 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	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： • Allow • Deny

Condition	Map<String,Map<String,Array<String>>>	限制条件。不超过10个。
		说明
		以请求示例中的Condition为例：条件键（obs:prefix）和字符串（public）需相等（StringEquals）。
		"Condition": {
		"StringEquals": {
		"obs:prefix": [
		"public"
		]
		}
		}

Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。

请求示例

```
POST https://sample.domain.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": [
                            "example-west-1"
                        ]
                    }
                },
            }
        ]
    }
  }
}
```

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://sample.domain.com/v3/roles/93879fd90f1046f69e6e0b31c94d2..."
    },
    "policy": {
        "Version": "1.1",
        "Statement": [
            {
                "Action": [
                    "obs:bucket:GetBucketAcl"
                ],
                "Resource": [
                    "obs:*:*:bucket:*"
                ],
                "Effect": "Allow",
                "Condition": {
                    "StringStartWith": {
                        "g:ProjectName": [
                            "example-west-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

4.9.4 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。

URI

POST /v3.0/OS-ROLE/roles

请求参数

表 4-97 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 4-98 请求 Body 参数

参数	是否必选	参数类型	描述
role	是	Object	自定义策略信息。

表 4-99 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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
policy	是	Object	自定义策略的具体内容。

表 4-100 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”。 **说明** • 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。 • 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 4-101 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。 **说明** • 当自定义策略为委托自定义策略时，该字段值为： *"Action": ["iam:agencies:assume"]*。 取值范围： • iam:agencies:assume
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： • Allow • Deny
Resource	否	Object	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： `"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}`

表 4-102 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： `"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]`

响应参数

表 4-103 响应 Body 参数

参数	参数类型	描述
role	Object	自定义策略信息。

表 4-104 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。
links	Object	自定义策略的资源链接信息。
policy	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。
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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
created_time	String	自定义策略创建时间。
references	String	自定义策略的引用次数。

表 4-105 role.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-106 role.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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。

参数	参数类型	描述
Statement	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 4-107 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。 **说明** • 当自定义策略为委托自定义策略时，该字段值为：*"Action": ["iam:agencies:assume"]*。
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。 取值范围： • Allow • Deny
Resource	Object	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： "Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}

表 4-108 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： "uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]

请求示例

```
POST https://sample.domain.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://sample.domain.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

4.9.5 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。

URI

PATCH /v3.0/OS-ROLE/roles/{role_id}

表 4-109 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：自定义策略ID。

请求参数

表 4-110 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 4-111 请求 Body 参数

参数	是否必选	参数类型	描述
role	是	Object	自定义策略信息。

表 4-112 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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
policy	是	Object	自定义策略的具体内容。

表 4-113 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”。 **说明** • 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。 • 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 4-114 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，不超过100个。 **说明** • 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： • Allow • Deny
Condition	否	Object	限制条件。不超过10个。
Resource	否	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。

表 4-115 role.policy.Statement.Condition

参数	是否必选	参数类型	描述
<operator>	否	Object	运算符。具体运算符如 “Bool”、“StringEquals”等。 • 该参数类型为自定义对象。

表 4-116 role.policy.Statement.Condition.<operator>

参数	是否必选	参数类型	描述
<attribute>	否	Array of strings	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。 ● 该参数类型为自定义字符串数组。

响应参数

表 4-117 响应 Body 参数

参数	参数类型	描述
role	Object	自定义策略信息。

表 4-118 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。
links	Object	自定义策略的资源链接信息。
policy	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。
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。 **说明** ● AX表示在domain层显示。 ● XA表示在project层显示。 ● 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）。
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。
created_time	String	自定义策略创建时间。

参数	参数类型	描述
references	String	自定义策略的引用次数。

表 4-119 role.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-120 role.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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	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 4-121 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，不超过100个。 **说明** • 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	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： • Allow • Deny
Condition	Object	限制条件。不超过10个。

参数	参数类型	描述
Resource	Array of strings	资源。数组长度不超过10，每个字符串长度不超过128，规则如下： **说明** • 可填 * 的五段式：::::，例："obs:::bucket:*"。 • region字段为*或用户可访问的region。service必须存在且resource属于对应service。

表 4-122 role.policy.Statement.Condition

参数	参数类型	描述
operator	Object	运算符。具体运算符如 “Bool”、“StringEquals”等。 • 该参数类型为自定义对象。

表 4-123 role.policy.Statement.Condition.operator

参数	参数类型	描述
attribute	Array of strings	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。 • 该参数类型为自定义字符串数组。

请求示例

```
PATCH https://sample.domain.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": [
                                "example-west-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://sample.domain.com/v3/roles/93879fd90f1046f69e6e0b31c94d2615"
    },
    "policy": {
      "Version": "1.1",
      "Statement": [
        {
          "Action": [
            "obs:bucket:GetBucketAcl"
          ],
          "Resource": [
            "obs:*:*:bucket:*"
          ],
          "Effect": "Allow",
          "Condition": {
            "StringStartWith": {
              "g:ProjectName": [
                "example-west-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。
404	未找到相应的资源。
500	内部服务错误。

错误码

无

4.9.6 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。

URI

PATCH /v3.0/OS-ROLE/roles/{role_id}

表 4-124 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：**自定义策略ID**。

请求参数

表 4-125 请求 Header 参数

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

表 4-126 请求 Body 参数

参数	是否必选	参数类型	描述
role	是	Object	自定义策略信息。

表 4-127 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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
policy	是	Object	自定义策略的具体内容。

表 4-128 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”。 **说明** • 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。 • 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 4-129 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。 **说明** • 当自定义策略为委托自定义策略时，该字段值为： *"Action": ["iam:agencies:assume"]*。 取值范围： • iam:agencies:assume
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： • Allow • Deny
Resource	否	Object	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： `"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}`

表 4-130 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： `"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]`

响应参数

表 4-131 响应 Body 参数

参数	参数类型	描述
role	Object	自定义策略信息。

表 4-132 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。
links	Object	自定义策略的资源链接信息。
policy	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。
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。 **说明** • AX表示在domain层显示。 • XA表示在project层显示。 • 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）。
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。
created_time	String	自定义策略创建时间。
references	String	自定义策略的引用次数。

表 4-133 role.links

参数	参数类型	描述
self	String	资源链接地址。

表 4-134 role.policy

参数	参数类型	描述
Version	String	权限版本号。 **说明** • 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。 • 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。

参数	参数类型	描述
Statement	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 4-135 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。 **说明** • 当自定义策略为委托自定义策略时，该字段值为：*"Action": ["iam:agencies:assume"]*。
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。 取值范围： • Allow • Deny
Resource	Object	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： "Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}

表 4-136 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： "uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]

请求示例

```
PATCH https://sample.domain.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://sample.domain.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

4.9.7 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。

URI

DELETE /v3.0/OS-ROLE/roles/{role_id}

表 4-137 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：**自定义策略ID**。

请求参数

表 4-138 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。

响应参数

无

请求示例

```
DELETE https://sample.domain.com/v3.0/OS-ROLE/roles/{role_id}
```

响应示例

无

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

4.10 委托管理

4.10.1 创建委托

功能介绍

该接口提供创建委托关系的功能。

URI

POST /v3.0/OS-AGENCY/agencies

请求消息

- Request Header参数说明

参数	必选/可选	类型	描述
Content-Type	必选	String	application/json;charset=utf8
X-Auth-Token	必选	String	已认证的拥有Security Administrator权限的token。

- Request Body参数说明

参数	是否为必选	类型	说明
name	是	String	委托的名称，长度不大于64位。
domain_id	是	String	当前租户的ID。

参数	是否为必选	类型	说明
trust_domain_id	至少一个	String	委托租户的ID。
trust_domain_name		String	委托租户的名称。
description	否	String	委托的描述，长度不大于255位。
duration	否	String	委托的期限，默认为null，表示委托不过期；取值为FOREVER，表示委托的期限为永久；取值为ONEDAY，表示委托的期限为一天。

说明

请求体中的trust_domain_id和trust_domain_name至少有一个存在，两者都存在的话，以trust_domain_name优先。

- 请求示例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X POST -d'{"agency" : {"name" : "exampleagency","domain_id" : "0ae9c6993a2e47bb8c4c7a9bb8278d61","trust_domain_id" : "35d7706cedbc49a18df0783d00269c20","trust_domain_name" : "exampledomain","description" : "testsfdas"}}' https:///v3.0/OS-AGENCY/agencies
```

响应消息

- Response Body参数说明

参数	必选/可选	类型	描述
agency	是	JSONObject	委托对象。

- agency格式说明

参数	必选/可选	类型	描述
id	是	String	委托的ID。
name	是	String	委托的名称。
domain_id	是	String	当前租户的ID。
trust_domain_id	是	String	委托租户的ID。
description	是	String	委托的描述。
duration	是	String	委托的期限。
expire_time	是	String	委托的到期时间。

参数	必选/可选	类型	描述
create_time	是	String	委托的创建时间。

- 响应示例（请求成功）

```
{
  "agency" : {
    "description" : "testsfdas",
    "trust_domain_id" : "35d7706cedbc49a18df0783d00269c20",
    "id" : "c1a06ec7387f430c8122d6f336c66dcf",
    "duration" : null,
    "create_time" : "2017-01-06T05:56:09.738212",
    "expire_time" : null,
    "domain_id" : "0ae9c6993a2e47bb8c4c7a9bb8278d61",
    "name" : "exampleagency"
   }
}
```

- 响应样例（请求失败）

```
{
   "error": {
      "message": "'name' is a required property",
      "code": 400,
      "title": "Bad Request"
   }
}
```

状态码

状态码	说明
201	请求成功。
400	参数错误。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
409	委托已经存在。
500	内部服务错误。

4.10.2 查询指定条件下的委托列表信息

功能介绍

该接口用来获取指定条件下的委托列表信息。

URI

- URI格式

  GET /v3.0/OS-AGENCY/agencies{?domain_id,name,trust_domain_id}
- 查询参数说明

参数	是否为必选	类型	说明
domain_id	是	String	当前租户的ID。
name	否	String	委托的名称。
trust_domain_id	否	String	被委托方租户的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https:///v3.0/OS-AGENCY/agencies?domain_id=0ae9c6993a2e47bb8c4c7a9bb8278d61
```

响应消息

- Response Body参数说明

参数	必选/可选	类型	描述
agencies	是	JSONArray	委托列表。

- agency格式说明

参数	必选/可选	类型	描述
id	是	String	委托的ID。
name	是	String	委托的名称。
domain_id	是	String	当前租户的ID。
trust_domain_id	是	String	委托租户的ID。
trust_domain_name	是	String	委托租户的名称。
description	是	String	委托的描述。
duration	是	String	委托的期限。默认为null，表示不过期。
expire_time	是	String	委托的到期时间。

参数	必选/可选	类型	描述
create_time	是	String	委托的创建时间。

- 响应示例（请求成功）

```
{
  "agencies": [
    {
      "trust_domain_name": "exampledomain",
      "description": " testsfdas ",
      "trust_domain_id": "b3f266d0c08544a0859740de8b84e850",
      "id": "afca8ddf2e92469a8fd26a635da5206f",
      "duration": null,
      "create_time": "2017-01-04T09:09:15.000000",
      "expire_time": null,
      "domain_id": "0ae9c6993a2e47bb8c4c7a9bb8278d61",
      "name": "exampleagency"
    }
  ]
}
```

- 响应样例（请求失败）

```
{
  "error": {
    "message": "You are not authorized to perform the requested action: identity:list_agencies",
    "code": 403,
    "title": "Forbidden"
  }
}
```

状态码

状态码	说明
200	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.3 获取指定委托的详细信息

功能介绍

该接口用来获取指定委托的详细信息。

URI

- URI格式

  GET /v3.0/OS-AGENCY/agencies/{agency_id}

- URI参数说明

参数	是否为必选	类型	说明
agency_id	是	String	委托的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https:///v3.0/OS-AGENCY/agencies/2809756f748a46e2b92d58d309f67291
```

响应消息

- Response Body参数说明

参数	必选/可选	类型	描述
agency	是	JSONObject	委托对象。

- agency格式说明

参数	必选/可选	类型	描述
id	是	String	委托的ID。
name	是	String	委托的名称。
domain_id	是	String	当前租户的ID。
trust_domain_id	是	String	委托租户的ID。
trust_domain_name	是	String	委托租户的名称。
description	是	String	委托的描述。
duration	是	String	委托的期限。默认为null，表示不过期。
expire_time	是	String	委托的到期时间。
create_time	是	String	委托的创建时间。

- 响应示例（请求成功）

```
{
 "agency" : {
    "description" : " testsfdas ",
    "trust_domain_id" : "3ebe1024db46485cb02ef08d3c348477",
    "trust_domain_name" : "exampledomain",
    "id" : "c1a06ec7387f430c8122d6f336c66dcf",
    "duration": "FOREVER",
    "create_time" : "2017-01-06T05:56:09.738212",
    "expire_time" : null,
    "domain_id" : "0ae9c6993a2e47bb8c4c7a9bb8278d61",
    "name" : "exampleagency"
   }
}
```

- 响应样例（请求失败）

```
{
   "error": {
      "message": "Could not find agency: 2809756f748a46e2b92d58d309f67291",
      "code": 404,
      "title": "Not Found"
   }
}
```

状态码

状态码	说明
200	请求成功。
401	认证失败。
403	鉴权失败。
404	不存在对应的委托。
500	内部服务错误。

4.10.4 修改委托

功能介绍

该接口提供修改委托的信息，包括租户的trust_domain_id、description、trust_domain_name字段。

URI

- URI格式

  PUT /v3.0/OS-AGENCY/agencies/{agency_id}

- URI参数说明

参数	是否为必选	类型	说明
agency_id	是	String	委托的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- Request Body参数说明

属性	是否为必选	类型	说明
trust_domain_id	否	String	委托租户的ID，且委托租户必须已存在。
trust_domain_name	否	String	委托租户的名称，且委托租户必须已存在。
description	否	String	委托的描述。

说明

请求体中的trust_domain_id和trust_domain_name两者二选一，即有一个存在即可，两者都存在的话，以trust_domain_name为主。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT -d '{"agency" : {"trust_domain_id" : "35d7706cedbc49a18df0783d00269c20","trust_domain_name" : "exampledomain","description" : "111111"}}' https:///v3.0/OS-AGENCY/agencies/2809756f748a46e2b92d58d309f67291
```

响应消息

- Response Body参数说明

参数	必选/可选	类型	描述
agency	是	JSONObject	委托对象。

- agency格式说明

参数	必选/可选	类型	描述
id	是	String	委托的ID。
name	是	String	委托的名称。
domain_id	是	String	当前租户的ID。

参数	必选/可选	类型	描述
trust_domain_id	是	String	委托租户的ID。
description	是	String	委托的描述。
duration	是	String	委托的期限。默认为null，表示不过期。
expire_time	是	String	委托的到期时间。
create_time	是	String	委托的创建时间。

- 响应示例（请求成功）

```
{
  "agency" : {
     "description" : " testsfdas ",
     "trust_domain_id" : "3ebe1024db46485cb02ef08d3c348477",
     "id" : "c1a06ec7387f430c8122d6f336c66dcf",
     "duration" : null,
     "create_time" : "2017-01-06T05:56:09.738212",
     "expire_time" : null,
     "domain_id" : "0ae9c6993a2e47bb8c4c7a9bb8278d61",
     "name" : "exampleagency"
    }
}
```

- 响应样例（请求失败）

```
{
  "error": {
    "message": "TrustDomainNotFound",
    "code": 404,
    "title": "Not Found"
  }
}
```

状态码

状态码	说明
200	请求成功。
400	参数错误。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.5 删除委托

功能介绍

该接口用来删除委托。

说明

当前操作将使委托方无法访问资源，请谨慎操作。

URI

- URI格式

  DELETE /v3.0/OS-AGENCY/agencies/{agency_id}

- URI参数说明

参数	是否为必选	类型	说明
agency_id	是	String	委托的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https:///v3.0/OS-AGENCY/agencies/2809756f748a46e2b92d58d309f67291
```

响应消息

- 响应样例（请求失败）

```
{
    "error": {
        "message": "Could not find agency: 2809756f748a46e2b92d58d309f67291",
        "code": 404,
        "title": "Not Found"
    }
}
```

状态码

状态码	说明
204	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.6 通过项目给委托赋予权限

功能介绍

该接口用来通过项目给委托赋予权限。

URI

- URI格式

  PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
project_id	是	String	当前租户下的项目ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

说明

请求体中角色ID对应的角色名称有黑名单控制，不能是secu_admin、te_agency。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https:///v3.0/OS-AGENCY/projects/0945241c5ebc4660bac540d48f2a2c14/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 无响应：表示响应成功
- 响应样例（请求失败）

```
{
  "error" : {
    "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
```

```
    "code" : 404,
    "title" : "Not Found"
  }
}
```

状态码

状态码	说明
204	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.7 检查委托在项目上是否有指定权限

功能介绍

该接口用来检查委托在项目上是否有指定权限。

URI

- URI格式

  HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
project_id	是	String	当前租户下的项目ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X HEAD
https:///v3.0/OS-AGENCY/projects/0945241c5ebc4660bac540d48f2a2c14/agencies/
37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 响应样例（请求失败）

```
{
  "error" : {
     "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
     "code" : 404,
     "title" : "Not Found"
   }
}
```

状态码

状态码	说明
204	请求成功且，具有指定权限。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.8 查询委托在项目上具有的权限列表

功能介绍

该接口用来查询委托在项目上具有的权限列表。

URI

- URI格式

  GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles

- URI参数说明

参数	是否为必选	类型	说明
project_id	是	String	当前租户下的项目ID。
agency_id	是	String	委托的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https:///v3.0/OS-AGENCY/projects/0945241c5ebc4660bac540d48f2a2c14/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles
```

响应消息

- Response Body参数说明

参数	是否为必选	类型	说明
roles	是	Array	role的列表。

- role格式说明

参数	是否为必选	类型	说明
id	是	String	role的ID。
name	是	String	role的名称。
domain_id	是	String	role所属的租户的ID。
type	是	String	role的显示模式，其中： ● AX表示在domain层显示 ● XA表示在project层显示 ● AA表示在domain和project层均显示 ● XX表示在domain和project层均不显示
display_name	是	String	role所展示名称。
catalog	是	String	role所在的目录。
policy	是	Dict	role的具体策略。
description	是	String	role的描述。

- 响应样例（请求成功）

```
{
  "roles": [
    {
      "catalog": "BASE",
      "display_name": "Tenant Guest",
      "name": "readonly",
```

```
    "policy": {
      "Version": "1.0",
      "Statement": [
        {
          "Action": [
            "::Get",
            "::List"
          ],
          "Effect": "Allow"
        },
        {
          "Action": [
            "identity:*"
          ],
          "Effect": "Deny"
        }
      ]
    },
    "domain_id": null,
    "type": "AA",
    "id": "b32d99a7778d4fd9aa5bc616c3dc4e5f",
    "description": "Tenant Guest"
  }
 ]
}
```


- 响应样例（请求失败）


```
{
 "error": {
  "message": "You are not authorized to perform the requested action: identity:list_domain_grants",
  "code": 403,
  "title": "Forbidden"
 }
}
```


状态码

状态码	说明
200	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.9 通过项目删除委托的权限

功能介绍

该接口用来通过项目信息删除委托的权限。

URI

- URI格式

  DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
project_id	是	String	当前租户下的项目ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https:///v3.0/OS-AGENCY/projects/0945241c5ebc4660bac540d48f2a2c14/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 响应样例（请求失败）

```
{
  "error" : {
     "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
     "code" : 404,
     "title" : "Not Found"
    }
}
```

状态码

状态码	说明
204	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.10 通过租户给委托赋予权限

功能介绍

该接口用来通过租户信息给委托赋予权限。

URI

- URI格式

  PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
domain_id	是	String	当前租户的ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

说明

请求体中角色id对应的角色名称有黑名单控制，不能是secu_admin、te_agency的名称。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https:///v3.0/OS-AGENCY/domains/b32d99a7778d4fd9aa5bc616c3dc4e5f/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 无响应：表示响应成功
- 响应样例（请求失败）

```
{
  "error" : {
     "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
     "code" : 404,
     "title" : "Not Found"
   }
}
```

状态码

状态码	说明
204	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.11 检查委托在租户上是否有指定权限

功能介绍

该接口用来检查委托在租户上是否具有指定权限。

URI

- URI格式

  HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
domain_id	是	String	当前租户的ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X HEAD https:///v3.0/OS-AGENCY/domains/b32d99a7778d4fd9aa5bc616c3dc4e5f/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 响应样例（请求失败）

```
{
  "error" : {
     "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
     "code" : 404,
     "title" : "Not Found"
    }
}
```

状态码

状态码	说明
204	请求成功，具有指定权限。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.12 查询委托在租户上具有的权限列表

功能介绍

该接口用来查询委托在租户上具有的权限列表。

URI

- URI格式

  GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles
- URI参数说明

参数	是否为必选	类型	说明
domain_id	是	String	当前租户的ID。
agency_id	是	String	委托的ID。

请求消息

- Request Header参数说明

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

参数	是否为必选	类型	说明
X-Auth-Token	是	String	已认证的拥有Security Administrator权限的token。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https:///v3.0/OS-AGENCY/domains/b32d99a7778d4fd9aa5bc616c3dc4e5f/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles
```

响应消息

- Response Body参数说明

参数	是否为必选	类型	说明
roles	是	Array	role的列表。

- role格式说明

参数	是否为必选	类型	说明
catalog	否	String	role所在的目录。
display_name	否	String	role所展示名称。
name	是	String	role的名称。
policy	否	Dict	role的具体策略。
domain_id	是	String	role所属的租户的ID。
type	是	String	role的显示模式，其中： ● AX表示在domain层显示 ● XA表示在project层显示 ● AA表示在domain和project层均显示 ● XX表示在domain和project层均不显示
id	是	String	role的ID。
description	否	String	role的描述。

- 响应样例（请求成功）

```
{
  "roles": [
    {
      "catalog": "BASE",
      "display_name": "Tenant Guest",
      "name": "readonly",
      "policy": {
```

```
      "Version": "1.0",
      "Statement": [
        {
          "Action": [
            "::Get",
            "::List"
          ],
          "Effect": "Allow"
        },
        {
          "Action": [
            "identity:*"
          ],
          "Effect": "Deny"
        }
      ]
    },
    "domain_id": null,
    "type": "AA",
    "id": "b32d99a7778d4fd9aa5bc616c3dc4e5f",
    "description": "Tenant Guest"
  }
 ]
}
```


- 响应样例（请求失败）


```
{
 "error": {
  "message": "You are not authorized to perform the requested action: identity:list_domain_grants",
  "code": 403,
  "title": "Forbidden"
 }
}
```


状态码

状态码	说明
200	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.13 通过租户删除委托的权限

功能介绍

该接口用来通过租户信息删除委托的权限。

URI

- URI格式

  DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

- URI参数说明

参数	是否为必选	类型	说明
domain_id	是	String	当前租户的ID。
agency_id	是	String	委托的ID。
role_id	是	String	角色对应的ID。

请求消息

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https:///v3.0/OS-AGENCY/domains/b32d99a7778d4fd9aa5bc616c3dc4e5f/agencies/37f90258b820472bbc8a0f4f0bfd720d/roles/0f3a2d418ed747fa8be46e92757be9ff
```

响应消息

- 响应样例（请求失败）

```
{
  "error" : {
     "message" : "Could not find role: 0f3a2d418ed747fa8be46e92757be9ddff",
     "code" : 404,
     "title" : "Not Found"
    }
}
```

状态码

状态码	说明
204	请求成功。
401	认证失败。
403	鉴权失败。
404	未找到相应的资源。
500	内部服务错误。

4.10.14 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。

URI

GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects

表 4-139 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托ID。
domain_id	是	String	委托方账号ID。

请求参数

表 4-140 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

表 4-141 响应 Body 参数

参数	参数类型	描述
roles	Array of objects	权限信息列表。
links	object	资源链接信息。

表 4-142 roles

参数	参数类型	描述
id	String	权限ID。

参数	参数类型	描述
links	object	权限的资源链接信息。
name	String	权限名。

表 4-143 links

参数	参数类型	描述
self	String	资源链接地址。

请求示例

```
GET https://sample.domain.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://sample.domain.com/v3/roles/04570dfe267c45a3940e1ae9de868..."
                  },
        "id" : "04570dfe267c45a3940e1ae9de868..."
      },
     {
        "name" : "test1_admin",
        "links" : {
                     "self" : "https://sample.domain.com/v3/roles/1bf20f1adba94747a6e02e1be3810..."
                   },
        "id" : "1bf20f1adba94747a6e02e1be3810..."
      }
     ],
  "links" : {
         "self" : "https://sample.domain.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。

状态码	描述
500	内部服务错误。

4.10.15 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。

URI

PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

表 4-144 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托ID。
domain_id	是	String	委托方的账号ID。
role_id	是	String	权限ID。

请求参数

表 4-145 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

```
PUT https://sample.domain.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。

4.10.16 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。

URI

HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

表 4-146 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托ID。
domain_id	是	String	委托方的账号ID。
role_id	是	String	权限ID。

请求参数

表 4-147 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

```
HEAD https://sample.domain.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。

4.10.17 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。

URI

DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

表 4-148 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托ID。
domain_id	是	String	委托方的账号ID。
role_id	是	String	权限ID。

请求参数

表 4-149 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

```
DELETE https://sample.domain.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。

4.11 安全设置

4.11.1 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。

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy

表 4-150 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。

请求参数

表 4-151 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

表 4-152 响应 Body 参数

参数	参数类型	描述
protect_policy	object	操作保护策略。

表 4-153 protect_policy

参数	参数类型	描述
operation_protection	Boolean	是否开启操作保护，开启为"true"，未开启为"false"。

请求示例

```
GET https://sample.domain.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。

4.11.2 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。

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy

表 4-154 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。

请求参数

表 4-155 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 4-156 请求 Body 参数

参数	是否必选	参数类型	描述
protect_policy	是	object	操作保护策略。

表 4-157 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"，未开启为"false"。

响应参数

表 4-158 响应 Body 参数

参数	参数类型	描述
protect_policy	object	操作保护策略。

表 4-159 protect_policy

参数	参数类型	描述
operation_protection	Boolean	是否开启操作保护，开启为"true"，未开启为"false"。

请求示例

```
PUT https://sample.domain.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" : {
    "operation_protection" : false
  }
}
```

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。

4.11.3 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。

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy

表 4-160 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。

请求参数

表 4-161 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

表 4-162 响应 Body 参数

参数	参数类型	描述
password_policy	object	密码策略。

表 4-163 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	密码是否可以是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）。

请求示例

```
GET https://sample.domain.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
  }
}
```

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。

4.11.4 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。

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy

表 4-164 路径参数

参数	是否必选	参数类型	描述
domain_id	是	String	账号ID。

请求参数

表 4-165 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 4-166 请求 Body 参数

参数	是否必选	参数类型	描述
password_policy	是	object	密码策略。

表 4-167 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]。

参数	是否必选	参数类型	描述
minimum_password_length	否	Integer	密码最小字符数，取值范围[6,32]。
number_of_recent_passwords_disallowed	否	Integer	密码不能与历史密码重复次数，取值范围[0,10]。
password_not_username_or_invert	否	Boolean	密码是否可以是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。

响应参数

表 4-168 响应 Body 参数

参数	参数类型	描述
password_policy	object	密码策略。

表 4-169 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	密码是否可以是用户名或用户名的反序。

参数	参数类型	描述
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）。

请求示例

```
PUT https://sample.domain.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password_policy

{
  "password_policy" : {
    "minimum_password_length" : 6,
    "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
  }
}
```

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
  }
}
```

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。

4.11.5 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。

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy

表 4-170 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。

请求参数

表 4-171 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

表 4-172 响应 Body 参数

参数	参数类型	描述
login_policy	object	登录策略。

表 4-173 login_policy

参数	参数类型	描述
account_validity_period	Integer	登录停用信息（天），取值范围[0,240]。账号在该值设置的有效期内未使用，则被停用。设置为0时，关闭该策略。
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

```
GET https://sample.domain.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。

4.11.6 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。

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy

表 4-174 路径参数

参数	是否必选	参数类型	描述
domain_id	是	String	账号ID。

请求参数

表 4-175 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 4-176 请求 Body 参数

参数	是否必选	参数类型	描述
login_policy	是	object	登录策略。

表 4-177 login_policy

参数	是否必选	参数类型	描述
account_validity_period	否	Integer	登录停用信息（天），取值范围[0,240]。账号在该值设置的有效期内未使用，则被停用。设置为0时，关闭该策略。
custom_info_for_login	否	String	登录提示信息。
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 4-178 响应 Body 参数

参数	参数类型	描述
login_policy	object	登录策略。

表 4-179 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	限定时间内登录失败次数。

参数	参数类型	描述
period_with_login_failures	Integer	限定时间长度（分钟）。
session_timeout	Integer	登录会话失效时间。
show_recent_login_info	Boolean	是否显示最近一次的登录信息。

请求示例

```
PUT https://sample.domain.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。

4.11.7 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。

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy

表 4-180 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。

请求参数

表 4-181 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

表 4-182 响应 Body 参数

参数	参数类型	描述
console_acl_policy	object	控制台访问控制策略。

表 4-183 console_acl_policy

参数	参数类型	描述
allow_address_netmasks	Array of objects	允许访问的IP地址或网段。
allow_ip_ranges	Array of objects	允许访问的IP地址区间。

表 4-184 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 4-185 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

```
GET https://sample.domain.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。

4.11.8 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。

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy

表 4-186 路径参数

参数	是否必选	参数类型	描述
domain_id	是	String	账号ID。

请求参数

表 4-187 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 4-188 请求 Body 参数

参数	是否必选	参数类型	描述
console_acl_policy	是	object	控制台访问控制策略。

表 4-189 console_acl_policy

参数	是否必选	参数类型	描述
allow_address_netmasks	是	Array of objects	允许访问的IP地址或网段。
allow_ip_ranges	是	Array of objects	允许访问的IP地址区间。

表 4-190 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 4-191 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 4-192 响应 Body 参数

参数	参数类型	描述
console_acl_policy	object	Console访问控制策略。

表 4-193 console_acl_policy

参数	参数类型	描述
allow_address_netmasks	Array of objects	允许访问的IP地址或网段。

参数	参数类型	描述
allow_ip_ranges	Array of objects	允许访问的IP地址区间。

表 4-194 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 4-195 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

```
PUT https://sample.domain.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",
      "description" : "1"
    }, {
      "ip_range" : "0.0.0.0-255.255.255.253",
      "description" : "12"
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "3"
    }, {
      "address_netmask" : "192.168.0.2/23",
      "description" : "4"
    } ]
  }
}
```

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 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。

4.11.9 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。

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy

表 4-196 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。

请求参数

表 4-197 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

表 4-198 响应 Body 参数

参数	参数类型	描述
api_acl_policy	object	接口访问控制策略。

表 4-199 api_acl_policy

参数	参数类型	描述
allow_address_netmasks	Array of objects	允许访问的IP地址或网段。
allow_ip_ranges	Array of objects	允许访问的IP地址区间。

表 4-200 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。

参数	参数类型	描述
description	String	描述信息。

表 4-201 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

```
GET https://sample.domain.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。

4.11.10 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。

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy

表 4-202 路径参数

参数	是否必选	参数类型	描述
domain_id	是	String	账号ID。

请求参数

表 4-203 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 4-204 请求 Body 参数

参数	是否必选	参数类型	描述
api_acl_policy	是	object	接口访问控制策略。

表 4-205 api_acl_policy

参数	是否必选	参数类型	描述
allow_address_netmasks	是	Array of objects	允许访问的IP地址或网段。
allow_ip_ranges	是	Array of objects	允许访问的IP地址区间。

表 4-206 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 4-207 allow_ip_ranges

参数	是否必选	参数类型	描述
description	否	String	描述信息。

参数	是否必选	参数类型	描述
ip_range	是	String	IP地址区间，例如:0.0.0.0-255.255.255.255。

响应参数

表 4-208 响应 Body 参数

参数	参数类型	描述
api_acl_policy	object	接口访问控制策略。

表 4-209 api_acl_policy

参数	参数类型	描述
allow_address_netmasks	objects	允许访问的IP地址或网段。
allow_ip_ranges	objects	允许访问的IP地址区间。

表 4-210 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 4-211 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

```
PUT https://sample.domain.com/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy
```

```
{
  "api_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "1"
    }, {
      "ip_range" : "0.0.0.0-255.255.255.253",
      "description" : "12"
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "3"
    }, {
      "address_netmask" : "192.168.0.2/23",
      "description" : "4"
    } ]
  }
}
```

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 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。

4.11.11 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。

URI

GET /v3.0/OS-MFA/virtual-mfa-devices

请求参数

表 4-212 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

表 4-213 响应 Body 参数

参数	参数类型	描述
virtual_mfa_devices	Array of objects	虚拟MFA设备信息列表。

表 4-214 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

```
GET https://sample.domain.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/mfa/16b26081f43d4c628c4bb88cf32e9..."
         },
        {
           "user_id" : "47026081f43d4c628c4bb88cf32e9...",
           "serial_number" : "iam/mfa/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。

4.11.12 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。

URI

GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device

表 4-215 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。

请求参数

表 4-216 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	管理员查询IAM用户的MFA绑定信息：拥有Security Administrator权限的token。 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 4-217 响应 Body 参数

参数	参数类型	描述
virtual_mfa_device	object	虚拟MFA设备信息。

表 4-218 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

```
GET https://sample.domain.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/mfa/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。
404	未找到相应的资源。
500	内部服务错误。

4.11.13 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。

URI

GET /v3.0/OS-USER/login-protects

请求参数

表 4-219 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

表 4-220 响应 Body 参数

参数	参数类型	描述
login_protects	Array of objects	登录保护状态信息列表。 **说明** 只返回配置过登录保护的用户状态信息。

表 4-221 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。 • email：邮件验证码 • vmfa：虚拟MFA • SMS：手机验证码

请求示例

```
GET https://sample.domain.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"
          }
        {
          "user_id" : "08c16cb6c58010691f81c0028dd94...",
          "enabled" : false,
          "verification_method" : "none"
          }
```

```
    ]
}
```

说明

对于从未配置过登录保护的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。

4.11.14 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。

URI

GET /v3.0/OS-USER/users/{user_id}/login-protect

表 4-222 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。

请求参数

表 4-223 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	管理员查询IAM用户的登录保护状态信息：拥有Security Administrator权限的token。 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 4-224 响应 Body 参数

参数	参数类型	描述
login_protect	object	登录状态保护信息。

表 4-225 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

```
GET https://sample.domain.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

对于从未配置过登录保护的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。
500	内部服务错误。

4.11.15 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。

URI

PUT /v3.0/OS-USER/users/{user_id}/login-protect

表 4-226 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。

请求参数

表 4-227 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 4-228 请求 Body 参数

参数	是否必选	参数类型	描述
login_protect	是	object	登录保护状态信息。

表 4-229 Login_project

参数	是否必选	参数类型	描述
enabled	是	Boolean	IAM用户是否开启登录保护，开启为"true"，未开启为"false"。
verification_method	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 4-230 响应 Body 参数

参数	参数类型	描述
login_protect	object	登录保护状态信息。

表 4-231 login_protect

参数	参数类型	描述
user_id	String	待修改登录保护信息的IAM用户ID。
enabled	Boolean	IAM用户是否开启登录保护，开启为"true"，不开启为"false"。
verification_method	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

```
PUT https://sample.domain.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	找不到资源。
500	系统错误。

4.11.16 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。

URI

PUT /v3.0/OS-MFA/mfa-devices/bind

请求参数

表 4-232 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 4-233 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

```
PUT https://sample.domain.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

无

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。

4.11.17 解绑 MFA 设备

功能介绍

该接口可以用于管理员解绑IAM用户的MFA设备，或IAM用户为自己解绑MFA设备。

URI

PUT /v3.0/OS-MFA/mfa-devices/unbind

请求参数

表 4-234 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	• 管理员为IAM用户解绑MFA设备：拥有Security Administrator权限的token。 • 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）。

表 4-235 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	• 管理员为IAM用户解绑MFA设备：填写任意值，不进行校验。 • IAM用户为自己解绑MFA设备：填写虚拟MFA验证码并校验。
serial_number	是	String	MFA设备序列号。

响应参数

无

请求示例

```
PUT  https://sample.domain.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

无

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。

4.11.18 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。

URI

POST /v3.0/OS-MFA/virtual-mfa-devices

请求参数

表 4-236 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM用户为自己创建MFA设备。请求Body中user_id所对应IAM用户的token（无需特殊权限）。

表 4-237 请求 Body 参数

参数	是否必选	参数类型	描述
virtual_mfa_device	是	object	创建的MFA设备信息。

表 4-238 virtual_mfa_device

参数	是否必选	参数类型	描述
name	是	String	设备名称。 最小长度：1 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 4-239 响应 Body 参数

参数	参数类型	描述
virtual_mfa_device	object	创建的MFA设备信息。

表 4-240 virtual_mfa_device

参数	参数类型	描述
serial_number	String	MFA设备序列号。
base32_string_seed	String	密钥信息，用于第三方生成图片验证码。

请求示例

```
POST https://sample.domain.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。
403	请求未授权。
409	保存请求资源时发生冲突。
500	系统错误。

4.11.19 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。

URI

DELETE /v3.0/OS-MFA/virtual-mfa-devices

表 4-241 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，即管理员自己的用户ID。
serial_number	是	String	MFA设备序列号。

请求参数

表 4-242 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

```
DELETE https://sample.domain.com/v3.0/OS-MFA/virtual-mfa-devices?
user_id=09f6bd85fc801de41f0cc00ce9172...&serial_number=iam:09f6bd6a96801de40f01c00c85691...:mfa/
{device_name}
```

响应示例

无

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。

4.12 联邦身份认证管理

4.12.1 通过联邦认证获取 token

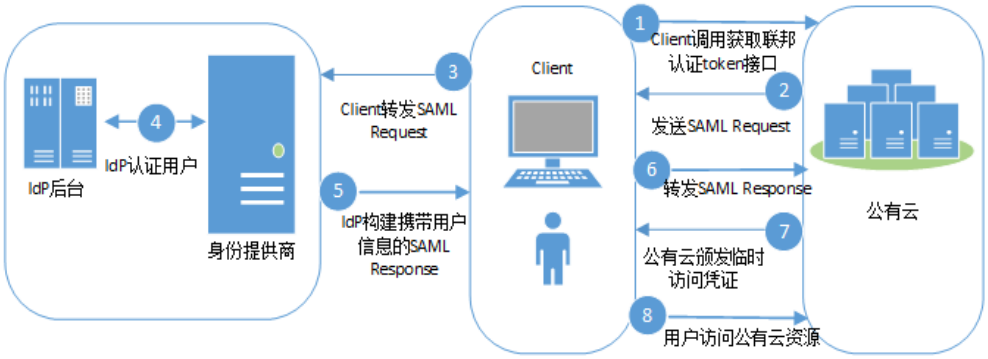
4.12.1.1 SP initiated 方式

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 4-1 流程图（SP initiated 方式）



步骤说明

1. Client调用云平台提供的“通过SP initiated方式获取联邦token”接口。
2. 云平台根据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给云平台。
7. 云平台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云平台资源。

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，可能会收到中间人攻击。

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4-243所示。

示例如下：

export OS_IDENTITY_API_VERSION=3

export OS_AUTH_TYPE=v3samlpassword

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 4-243 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*”。 ● 端口号：固定值为“443”。 ● 接口版本：固定值为“v3”。
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 Provider认证时使用的用户名。
OS_PASSWORD	用户在Identity Provider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文件放置在对应路径下。

```
<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 enpoints
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: MIIDbQYJKoZIhvcNAQcCoIIDXXX...
```

X-Subject-Token为获取到联邦认证token。

----结束

4.12.1.2 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。

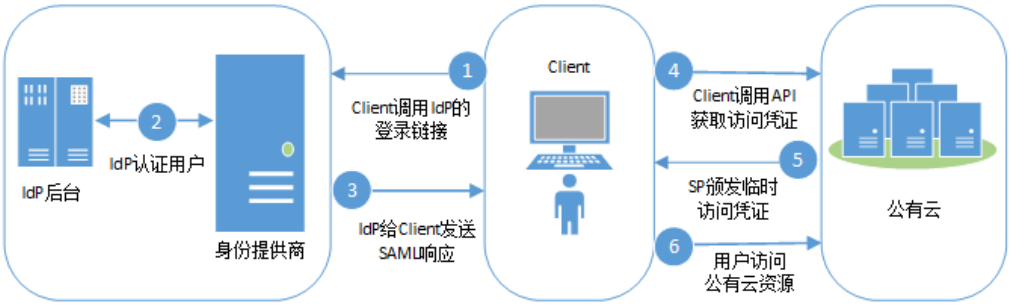
前提条件

- 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 4-2 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云平台的地址，即云平台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，调用云平台提供的“通过IdP initiated方式获取联邦token”接口。
5. 云平台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云平台资源。

客户端实现

步骤1 配置企业IdP的登录连接。

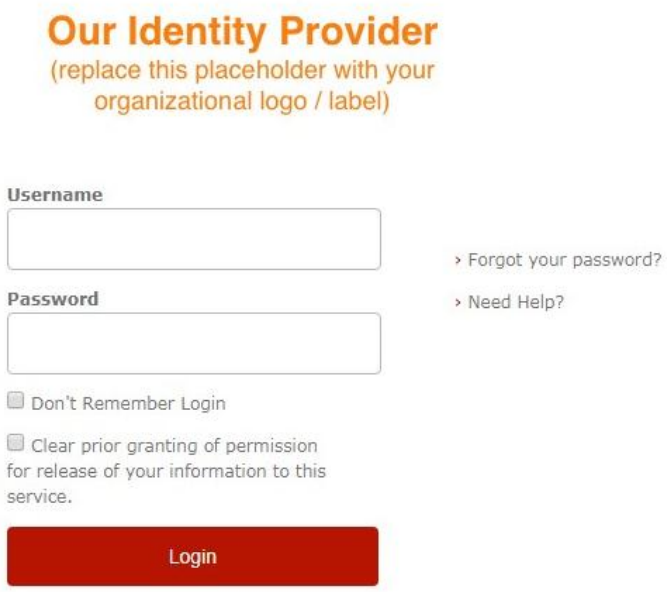
表 4-244 常用 IdP 产品的登录 URL

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

IdP	URL中标记SP的参数	登录URL示例
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 4-3 登录页面



Client4ShibbolethIdP脚本实现：

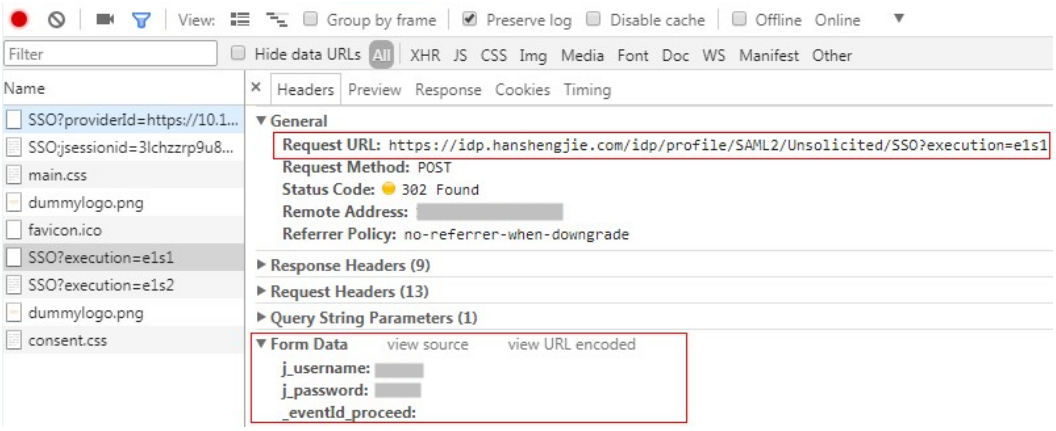
```
import sys
import requests
import getpass
import re
from bs4 import BeautifulSoup
from urlparse import urlparse

# 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 4-4 认证信息（1）



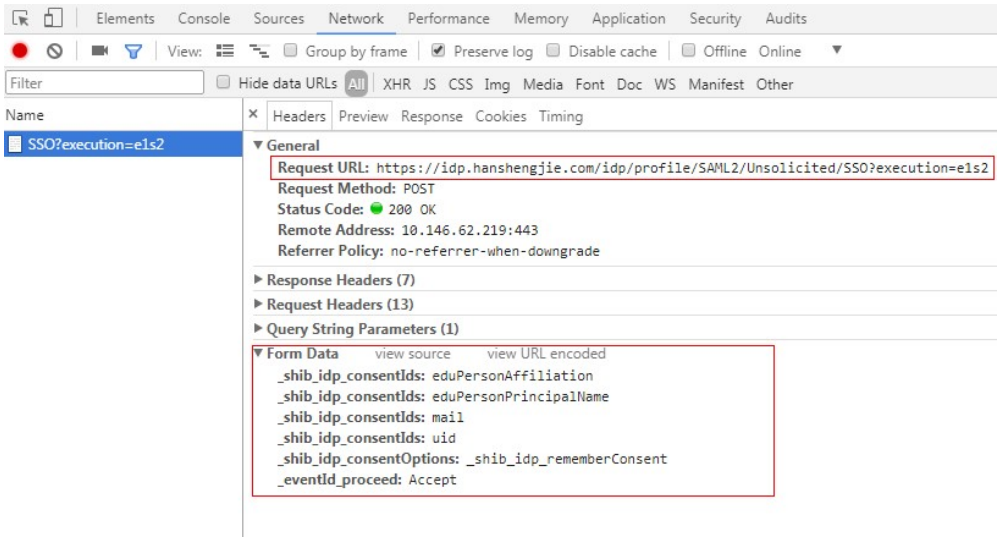
Client4ShibbolethIdP脚本实现：

```
# 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 4-5 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_consentIds = []
for inputtag in formsoup.find_all(re.compile('input')):
    name = inputtag.get("name")
    value = inputtag.get("value")
    if name == "_shib_idp_consentIds":
        _shib_idp_consentIds.append(value)
payload["_shib_idp_consentIds"] = _shib_idp_consentIds
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://iam.example.com/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。

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://iam.example.com/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

4.12.2 身份提供商

4.12.2.1 查询身份提供商列表

功能介绍

该接口用于查询身份提供商列表信息。

URI

GET /v3/OS-FEDERATION/identity_providers

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/identity_providers
```


响应

- Response Body参数说明

参数	是否必选	类型	说明
identity_providers	是	Array	身份提供商列表。
links	是	Object	身份提供商的资源链接。

- identity_providers格式说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。
description	是	String	身份提供商的描述信息。
enabled	是	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	是	Array	身份提供商的联邦用户ID列表。
links	是	Object	身份提供商的资源链接。

- 响应样例

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

            "links": {
                "protocols": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME-
contractors/protocols",
                "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME-contractors"
            }
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://sample.domain.com/v3/OS-FEDERATION/identity_providers"
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.2.2 查询身份提供商

功能介绍

该接口用于查询身份提供商信息。

URI

- URI格式
  GET /v3/OS-FEDERATION/identity_providers/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。
description	是	String	身份提供商的描述信息。
enabled	是	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。
remote_ids	是	Array	身份提供商的联邦用户ID列表。
links	是	Object	身份提供商的资源链接。

- 响应样例

```
{
    "identity_provider": {
        "description": "Stores ACME identities",
        "enabled": false,
        "id": "ACME",

        "remote_ids": [],
        "links": {
            "protocols": "https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/
protocols",
            "self": "https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME"
        }
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.2.3 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。

URI

- URI格式
  PUT /v3/OS-FEDERATION/identity_providers/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

表 4-245 请求 Body 参数

参数	是否必选	参数类型	描述
identity_provider	是	Object	身份提供商信息。

表 4-246 identity_provider

参数	是否必选	参数类型	描述
sso_type	否	string	身份提供商类型。当前支持如下两种： • virtual_user_sso：联邦登录跳转后映射为虚拟用户。 • 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，请确保您已创建IAM用户。 默认配置为virtual_user_sso类型。
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。

- 请求样例

```
PUT https://sample.domain.com/v3/OS-FEDERATION/identity_providers/{id}
{
    "identity_provider": {
        "description": "Stores ACME identities.",
        "enabled": true
    }
}
```

响应

- Response Body参数说明

表 4-247 响应 Body 参数

参数	参数类型	描述
identity_provider	Object	身份提供商信息。

表 4-248 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。
enabled	Boolean	身份提供商是否启用，true为启用，false为停用，默认为false。

参数	参数类型	描述
remote_ids	Array of strings	身份提供商的联邦用户ID列表。
links	Object	身份提供商的资源链接信息。

表 4-249 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。

- 响应样例

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

        "remote_ids": [],
        "links": {
            "protocols": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols",
            "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME"
        }
    }
}
```

状态码

状态码	说明
201	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
405	不允许的方法。
409	身份提供商ID重复。
413	请求体过大。
500	内部服务错误。
503	服务不可用。

4.12.2.4 更新 SAML 身份提供商

功能介绍

该接口用于更新基于SAML协议的身份提供商信息。

URI

- URI格式

  PATCH /v3/OS-FEDERATION/identity_providers/{id}

- 参数说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

表 4-250 请求 Body 参数

参数	是否必选	参数类型	描述
identity_provider	是	Object	身份提供商信息。

表 4-251 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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PATCH -d'{"identity_provider":{"enabled":false}}' https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME
```

响应

- Response Body参数说明

表 4-252 响应 Body 参数

参数	参数类型	描述
identity_provider	Object	身份提供商信息。

表 4-253 identity_provider

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。
links	Object	身份提供商的资源链接信息。

表 4-254 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。

- 响应样例

```
{
    "identity_provider": {
        "description": "Stores ACME identities",
        "enabled": false,
        "id": "ACME",

        "remote_ids": [],
        "links": {
            "protocols": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols",
            "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME"
        }
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.2.5 删除身份提供商

功能介绍

该接口用于删除身份提供商信息，包括基于SAML协议和OIDC协议的身份提供商。

URI

- URI格式

  DELETE /v3/OS-FEDERATION/identity_providers/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	身份提供商的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例
  curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME

响应

无响应体。

状态码

状态码	说明
204	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.3 映射

4.12.3.1 查询映射列表

功能介绍

该接口用于查询映射列表信息。

URI

GET /v3/OS-FEDERATION/mappings

请求

- Request Header参数说明

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

参数	是否必选	类型	说明
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/mappings
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
mappings	是	Array	映射列表。
links	是	Object	映射的资源链接。

- mappings参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。
links	是	Object	映射的资源链接。

- 响应样例

```
{
    "links": {
        "next": null,
        "previous": null,
        "self": "https://example.com/v3/OS-FEDERATION/mappings"
    },
    "mappings": [
        {
            "id": "ACME",
            "links": {
                "self": "https://example.com/v3/OS-FEDERATION/mappings/ACME"
            },
            "rules": [
                {
                    "local": [
                        {
                            "user": {
                                "name": "{0}"
                            }
                        },
                        {
                            "group": {
                                "id": "0cd5e9"
                            }
                        }
                    ],
                    "remote": [
                        {
                            "type": "UserName"
                        },
                        {
                            "type": "orgPersonType",
                            "any_one_of": [
                                "Contractor",
                                "SubContractor"
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
405	不允许的方法。
413	请求体过大。
500	内部服务错误。

状态码	说明
503	服务不可用。

4.12.3.2 查询映射

功能介绍

该接口用于查询映射信息。

URI

- URI格式
  GET /v3/OS-FEDERATION/mappings/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/mappings/ACME
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。
links	是	Object	映射的资源链接。

- 响应样例

```
{
    "mapping": {
        "id": "ACME",
        "links": {
            "self": "https://example.com/v3/OS-FEDERATION/mappings/ACME"
        },
        "rules": [
            {
                "local": [
                    {
                        "user": {
                            "name": "{0}"
                        }
                    },
                    {
                        "group": {
                            "name": "0cd5e9"
                        }
                    }
                ],
                "remote": [
                    {
                        "type": "UserName"
                    },
                    {
                        "type": "orgPersonType",
                        "not_any_of": [
                            "Contractor",
                            "Guest"
                        ]
                    }
                ]
            }
        ]
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.3.3 注册映射

功能介绍

该接口用于注册一个映射。

URI

- URI格式
  PUT /v3/OS-FEDERATION/mappings/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PUT -d'{"mapping":{"rules":[{"local":[{"user":{"name":"{0}"}},{"group":{"name":"0cd5e9"}}],"remote":[{"type":"UserName"},{"type":"orgPersonType","not_any_of":["Contractor","Guest"]}]}]}}' https://sample.domain.com/v3/OS-FEDERATION/mappings/ACME
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。
links	是	Object	映射的资源链接。

- 响应样例

```
{
    "mapping": {
        "id": "ACME",
        "links": {
            "self": "https://example.com/v3/OS-FEDERATION/mappings/ACME"
        },
        "rules": [
            {
                "local": [
                    {
                        "user": {
                            "name": "{0}"
                        }
                    },
                    {
                        "group": {
                            "name": "0cd5e9"
                        }
                    }
                ],
                "remote": [
                    {
                        "type": "UserName"
                    },
                    {
                        "type": "orgPersonType",
                        "not_any_of": [
                            "Contractor",
                            "Guest"
                        ]
                    }
                ]
            }
        ]
    }
}
```

状态码

状态码	说明
201	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.3.4 更新映射

功能介绍

该接口用于更新映射信息。

URI

- URI格式
  PATCH /v3/OS-FEDERATION/mappings/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PATCH -d'{"mapping":{"rules":[{"local":[{"user":{"name":"{0}"}},{"group":{"name":"0cd5e9"}}],"remote":[{"type":"UserName"},{"type":"orgPersonType","any_one_of":
```

```
["Contractor","SubContractor"]}]}}}' https://sample.domain.com/v3/OS-FEDERATION/mappings/ACME
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

参数	是否必选	类型	说明
rules	是	Object	将联邦用户映射为本地用户的规则列表。 以使用SAML协议为例： "rules": [{ "local": [{ "user": { "name": "{0}" } }, { "group": { "name": "0cd5e9" } }], "remote": [{ "type": "UserName" }, { "type": "orgPersonType", "not_any_of": ["Contractor", "Guest"] }] }] local：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。{0}表示remote中用户信息的第一个属性。 ● group：联邦用户在本系统中所属用户组。 remote：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。 ● "type": "UserName"表示IdP断言中的属性。 ● "type": "orgPersonType"表示IdP断言中的属性。 ● "not_any_of"：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。
links	是	Object	映射的资源链接。

- 响应样例

```
{
    "mapping": {
        "id": "ACME",
        "links": {
            "self": "https://example.com/v3/OS-FEDERATION/mappings/ACME"
        },
        "rules": [
            {
                "local": [
                    {
                        "user": {
                            "name": "{0}"
                        }
                    },
                    {
                        "group": {
                            "name": "0cd5e9"
                        }
                    }
                ],
                "remote": [
                    {
                        "type": "UserName"
                    },
                    {
                        "type": "orgPersonType",
                        "any_one_of": [
                            "Contractor",
                            "SubContractor"
                        ]
                    }
                ]
            }
        ]
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.3.5 删除映射

功能介绍

该接口用于删除映射信息。

URI

- URI格式
  DELETE /v3/OS-FEDERATION/mappings/{id}
- 参数说明

参数	是否必选	类型	说明
id	是	String	映射的ID。

请求

- Request Header参数说明

参数	是否为必选	类型	说明
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。

- 请求样例
  curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/OS-FEDERATION/mappings/ACME

响应

无响应体。

状态码

状态码	说明
204	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
405	不允许的方法。
413	请求体过大。

状态码	说明
500	内部服务错误。
503	服务不可用。

4.12.4 协议

4.12.4.1 查询协议列表

功能介绍

该接口用于查询协议列表信息。

URI

- URI格式
  GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols
- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例
  curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/

响应

- Response Body参数说明

参数	是否必选	类型	说明
protocols	是	List of objects	Protocol的列表。

参数	是否必选	类型	说明
links	是	Object	Protocol的资源链接。

- protocols参数说明

参数	是否必选	类型	说明
id	是	String	Protocol的ID。
mapping_id	是	String	映射的ID。
links	是	Object	Protocol的资源链接。

- 响应样例

```
{
    "links": {
        "next": null,
        "previous": null,
        "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols"
    },
    "protocols": [
        {
            "id": "saml",
            "links": {
                "identity_provider": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME",
                "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml"
            },
            "mapping_id": "ACME"
        }
    ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.4.2 查询协议

功能介绍

该接口用于查询协议信息。

URI

- URI格式
  GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol _id	是	String	Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	Protocol的ID。
mapping_id	是	String	映射的ID。
links	是	Object	Protocol的资源链接。

- 响应样例

```
{
    "protocol": {
        "id": "saml",
        "links": {
            "identity_provider": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME",
            "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml"
        },
        "mapping_id": "ACME"
```

```
  }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.4.3 注册协议

功能介绍

该接口用于注册一个协议，就是将规则关联到某一身份提供商。

URI

- URI格式
  PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol _id	是	String	Protocol的ID。

请求

- Request Header参数说明

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

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。

- Request Body参数说明

参数	是否必选	类型	说明
mapping_id	是	String	映射的ID。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PUT -d'{"protocol":{"mapping_id":"ACME"}}' https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	Protocol的ID。
mapping_id	是	String	映射的ID。
links	是	Object	Protocol的资源链接。

- 响应样例

```
{
    "protocol": {
        "id": "saml",
        "links": {
            "identity_provider": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME",
            "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml"
        },
        "mapping_id": "ACME"
    }
}
```

状态码

状态码	说明
201	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
405	不允许的方法。
413	请求体过大。

状态码	说明
500	内部服务错误。
503	服务不可用。

4.12.4.4 更新协议

功能介绍

该接口用于更新协议信息。

URI

- URI格式

  PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol _id	是	String	Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
mapping_id	是	String	映射的ID。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X PATCH -d'{"protocol":{"mapping_id":"ACME"}}' https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	Protocol的ID。
mapping_id	是	String	映射的ID。
links	是	Object	Protocol的资源链接。

- 响应样例

```
{
    "protocol": {
        "id": "saml",
        "links": {
            "identity_provider": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME",
            "self": "https://example.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml"
        },
        "mapping_id": "ACME"
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.4.5 删除协议

功能介绍

该接口用于删除协议信息。

URI

- URI格式

  DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol _id	是	String	Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X DELETE https://sample.domain.com/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml
```

响应

无响应体。

状态码

状态码	说明
204	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.12.5 Metadata

4.12.5.1 查询 Metadata 文件

功能介绍

该接口用于查询身份提供商导入到IAM中的Metadata文件内容。

URI

- URI格式

  GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol _id	是	String	Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3-ext/OS-FEDERATION/identity_providers/ACME/protocols/saml/metadata
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
id	是	String	Metadata的ID。
idp_id	是	String	身份提供商的ID。
entity_id	是	String	Metadata文件中的entityID字段。

参数	是否必选	类型	说明
protocol_id	是	String	Protocol的ID。
domain_id	是	String	用户所属domain的ID。
xaccount_type	是	String	租户来源，默认为空。
update_time	是	String	导入或更新Metadata文件的时间。
data	是	String	Metadata文件的内容。

- 响应样例

```
{
"id": "40c174f35ff94e31b8257ad4991bce8b",
"idp_id": "ACME",
"entity_id": "https://idp.test.com/idp/shibboleth",
"protocol_id": "saml",
"domain_id": "ed7a77d365304f458f7d0a7909c6d889",
"xaccount_type": "",
"update_time": "2016-10-26T09:26:23.000000",
"data": "$data"}
```

状态码

状态码	说明
200	获取成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
500	内部服务错误。

4.12.5.2 查询 Keystone 的 Metadata 文件

功能介绍

该接口用于查询keystone的Metadata文件。

URI

GET /v3-ext/auth/OS-FEDERATION/SSO/metadata

请求

- Request Header参数说明

参数	是否必选	类型	说明
unsigned	否	Boolean	是否按SAML2.0规范，对元数据做签名，默认为“false”。

- 请求样例
  GET /v3-ext/auth/OS-FEDERATION/SSO/metadata

响应

响应样例

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="43ebac773925f6849b196a3c803baba5" entityID="https://www.example.com">
<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/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#43ebac773925f6849b196a3c803baba5">
<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>yuQJc6OI3xilt6X4cOEUBnVV2Vs=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>...</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>...</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<md:SPSSODescriptor AuthnRequestsSigned="true" 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>...</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>...</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 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://www.example.com/v3-ext/
auth/OS-FEDERATION/SSO/SAML2/POST" index="0" isDefault="true"/>
<md:AssertionConsumerService xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Location="https://www.example.com/v3-ext/auth/OS-
FEDERATION/SSO/SAML2/ECP" index="1"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

状态码

状态码	说明
200	请求成功。
500	内部服务错误。
503	服务不可用。

4.12.5.3 导入 Metadata 文件

功能介绍

租户使用联邦认证功能时，需要先将Metadata文件导入IAM中，该接口用于导入租户的Metadata文件。

URI

- URI格式

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

- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	已经创建的身份提供商的ID。
protocol _id	是	String	已经创建的Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
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。

- Request Body参数说明

参数	是否必选	类型	说明
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。

参数	是否必选	类型	说明
domain_id	是	String	用户所属domain的ID。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X POST -d '{"xaccount_type":"","domain_id":"ed7a77d365304f458f7d0a7909c6d889","metadata":"$metadataContent"}' https://sample.domain.com/v3-ext/OS-FEDERATION/identity_providers/ACME/protocols/saml/metadata
```

响应

响应样例

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

状态码

状态码	说明
201	导入成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
500	内部服务错误。

4.12.6 token

4.12.6.1 获取联邦认证 unscoped token(SP initiated)

功能介绍

该接口用于通过SP 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。

URI

- URI格式

  GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/auth

- 参数说明

参数	是否必选	类型	说明
idp_id	是	String	身份提供商的ID。
protocol_id	是	String	Protocol的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Accept	否	string	• 通过页面单点认证（WebSSO）方式获取token时，不需要该参数。 • 通过增强客户端代理（ECP）方式获取token时，该字段需取值如下： application/vnd.paos+xml
PAOS	否	string	• 通过页面单点认证（WebSSO）方式获取token时，不需要该参数。 • 增强客户端代理（ECP）获取token时，该字段需取值如下： urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp

说明

1. 该接口支持通过页面单点认证（WebSSO）和增强客户端代理（ECP）两种方式获取token。通过不同的请求header区分，具体使用请参考Request Header参数说明。
2. 不建议直接调用该接口，请使用openstackclient获取token。

- 请求样例

```
GET /v3/OS-FEDERATION/identity_providers/idptest/protocols/saml/auth
```

响应

- Response Body参数说明

名称	参数	类型	说明
X-Subject-Token	header	string	签名后的unscoped token。
token	body	Object	联邦认证的unscoped token，包含methods和用户信息。

- 响应样例

```
{
    "token": {
        "issued_at": "2017-05-23T06:54:51.763000Z",
```

```
        "expires_at": "2017-05-24T06:54:51.763000Z",
        "methods": [
            "mapped"
        ],
        "user": {
            "domain": {
                "id": "e31ac82d778b4d128cb6fed37fd72cdb",
                "name": "exampledomain"
            },
            "id": "RMQTgtjjSNGDcKy7oUmI3AZg7GgsWG0Z",
            "name": "exampleuser",
            "OS-FEDERATION": {
                "identity_provider": {
                    "id": "exampleuser"
                },
                "protocol": {
                    "id": "saml"
                },
                "groups": [
                    {
                        "id": "b40189e26ea44f959877621b4b298db5"
                    }
                ]
            }
        }
    }
}
```


状态码

状态码	说明
200	请求成功，需进一步获取用户信息。
201	请求成功，返回token。
302	请求未携带Identity Provider用户信息时，跳转到Identity Provider认证页面。
400	请求错误。
401	认证失败。
403	鉴权失败。
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。

4.12.6.2 获取联邦认证 unscoped token(IdP initiated)

功能介绍

该接口用于通过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。

URI

POST /v3.0/OS-FEDERATION/tokens

请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Idp-Id	是	String	身份提供商的ID。
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

- Request Body参数说明

参数	是否必选	类型	说明
SAMLResponse	是	String	在IdP认证成功后返回的响应体。

说明

该接口只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。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'x-Idp-Id:test_local_idp' -H 'Content-Type:application/x-www-form-urlencoded' -X POST -d 'SAMLResponse=PD94bWwgdmVyc2lvbj0iMS4wIiBl4WXZ1OGNmYmRzWk1ZeWlLKy96anpEbm1rT2FrVVBrUmlSWEpLYUt5NzJtUmtoRFBCNjgwVQpzalU3R2hKNHE4ZG48L3hlbmM6Q2lwaGVyVmFsdWU%2BPC94ZW5jOkNpcGhlckRhdGE%2BPC94ZW5jOkVuY3J5cHRlZERhdGE%2BPC9zYW1sMjpFbmNyeXB0ZWRBc3NlcnRpb24%2BPC9zYW1sMnA6UmVzcG9uc2U%2B' https://sample.domain.com/v3.0/OS-FEDERATION/tokens
```

响应

- Response Body参数说明

名称	参数	类型	说明
X-Subject-Token	header	string	签名后的unscoped token。
token	body	Object	联邦认证的unscoped token，包含methods和用户信息。

- 响应样例

```
{
    "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": "test_local_idp"
            },
            "protocol": {
                "id": "saml"
            },
            "groups": [{
                "name": "admin",
                "id": "45a8c8f1894444e9a016af065e152b91"
            }]
        },
        "domain": {
            "name": "hansheng",
            "id": "c0e20cc993a24ad4aa3251661ef37c87"
        },
        "name": "FederationUser",
        "id": "QNSzD0bycqUXE4hiRNfyFcWfoOs8z6gT"
    }
  }
}
```


状态码

状态码	说明
201	请求成功，返回token。
400	请求错误。
401	认证失败。
403	鉴权失败。
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。

4.12.6.3 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。

URI

POST /v3/auth/tokens

请求参数

表 4-255 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 4-256 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 4-257 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。

表 4-258 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	是	Object	联邦unscoped token的信息。

表 4-259 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 4-260 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可以跨区域使用，domain支持id和name，二选一即可。
project	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 4-261 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 4-262 auth.scope.project

参数	是否必选	参数类型	描述
domain	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。
name	否	String	项目名，id与name二选一即可。

表 4-263 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 4-264 响应 Header 参数

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

表 4-265 响应 Body 参数

参数	参数类型	描述
token	Object	联邦认证的scoped token信息。

表 4-266 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。
catalog	Array of objects	服务目录信息。
domain	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。
project	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。
roles	Array of objects	token的权限信息。
user	Object	获取token的用户信息。
issued_at	String	token下发时间。

表 4-267 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。

参数	参数类型	描述
endpoints	Array of objects	终端节点。

表 4-268 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 4-269 token.domain

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

表 4-270 token.project

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

表 4-271 token.project.domain

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

表 4-272 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 4-273 token.user

参数	参数类型	描述
domain	Object	用户所属账号信息。
OS-FEDERATION	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（UTC时间），“”表示密码不过期。

表 4-274 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 4-275 token.user.OS-FEDERATION

参数	参数类型	描述
groups	Array of objects	用户组信息列表。
identity_provider	Object	身份提供商信息。
protocol	Object	协议信息。

表 4-276 token.user.OS-FEDERATION.groups

参数	参数类型	描述
id	String	用户组ID。

参数	参数类型	描述
name	String	用户组名称。

表 4-277 token.user.OS-FEDERATION.identity_provider

参数	参数类型	描述
id	String	身份提供商ID。

表 4-278 token.user.OS-FEDERATION.protocol

参数	参数类型	描述
id	String	协议ID。

请求示例

```
POST https://sample.domain.com/v3/auth/tokens
{
    "auth": {
        "identity": {
            "methods": [
                "token"
            ],
            "token": {
                "id": "MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB..."
            }
        },
        "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:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
响应Body参数:
{
    "token": {
        "expires_at": "2020-02-13T14:21:34.042000Z",
        "methods": [
            "token"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "id": "d2983f677ce14f1e81cbb6a9345a1...",
```

```
                    "interface": "public",
                    "region": "*",
                    "region_id": "*",
                    "url": "https://sample.domain.com/v3"
                }
            ],
            "id": "fd631b3426cb40f0919091d5861d8...",
            "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": "LdQTDSC7zmJVIic3yaCbLBXDxPAdDxLg",
        "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。

返回值	描述
500	内部服务错误。
503	服务不可用。

错误码

无

4.12.7 租户

4.12.7.1 查询联邦用户可以访问的租户列表

功能介绍

该接口用于查询联邦用户可以访问的租户列表。

URI

GET /v3/OS-FEDERATION/domains

请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	Unscope token，请参考**获取联邦认证unscoped token(SP initiated)**。

- 请求样例

```
GET /v3/OS-FEDERATION/domains
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
domains	是	array	租户列表。
links	是	Object	租户的资源链接。

- 响应样例

```
{
  "domains": [
    {
      "links": {
        "self": "https://sample.domain.com/v3/domains/e31ac82d778b4d128cb6fed37fd72cdb"
      },
```

```
    "description": null,
    "name": "exampledomain",
    "enabled": true,
    "id": "e31ac82d778b4d128cb6fed37fd72cdb"
  }
 ],
 "links": {
  "self": "https://sample.domain.com/v3/OS-FEDERATION/domains",
  "previous": null,
  "next": null
 }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
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。

4.12.8 项目

4.12.8.1 查询联邦用户可以访问的项目列表

功能介绍

该接口用于查询联邦用户可以访问的项目列表，需要项目列表来获取联邦scoped token。

URI

GET /v3/OS-FEDERATION/projects

请求

- Request Header参数说明

参数	是否必选	类型	说明
X-Auth-Token	是	String	Unscoped token，请参考**获取联邦认证unscoped token(SP initiated)**获取token。

- 请求样例
  GET /v3/OS-FEDERATION/projects

响应

- Response Body参数说明

参数	是否必选	类型	说明
projects	是	array	项目列表。
links	是	Object	项目的资源链接。

- 响应样例

```
{
  "links": {
    "self": "https://sample.domain.com/v3/OS-FEDERATION/projects",
    "previous": null,
    "next": null
  },
  "projects": [
    {
      "is_domain": false,
      "description": "",
      "links": {
        "self": "https://sample.domain.com/v3/projects/05cf683c351e43518618d9fa96a5efa9"
      },
      "enabled": true,
      "id": "05cf683c351e43518618d9fa96a5efa9",
      "parent_id": "e31ac82d778b4d128cb6fed37fd72cdb",
      "domain_id": "e31ac82d778b4d128cb6fed37fd72cdb",
      "name": "region_name"
    },
    {
      "is_domain": false,
      "description": "",
      "links": {
        "self": "https://sample.domain.com/v3/projects/32b56f108f87418e8219317beb0fff3c"
      },
      "enabled": true,
      "id": "32b56f108f87418e8219317beb0fff3c",
      "parent_id": "e31ac82d778b4d128cb6fed37fd72cdb",
      "domain_id": "e31ac82d778b4d128cb6fed37fd72cdb",
      "name": "MOS" MOS为OBS默认项目的名称
    }
  ]
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
405	不允许的方法。

状态码	说明
413	请求体过大。
500	内部服务错误。
503	服务不可用。

4.13 版本信息管理

4.13.1 查询 Keystone API 的版本信息

功能介绍

该接口用于获取Keystone API的版本信息。

URI

GET /

请求

请求样例

```
curl -i -k -X GET https://sample.domain.com/
```

响应

- 响应参数说明

参数	是否必选	类型	描述
versions	是	Object	Keystone API的版本信息。
values	是	Array	Keystone API的版本列表。

- values格式说明

参数	是否必选	类型	说明
status	是	String	版本状态。
updated	是	String	版本最后更新时间。
media-types	是	Array	版本支持的消息格式。
id	是	String	版本号，如v3.0。
links	是	Array	版本的资源链接。

- 响应样例（响应成功）

```
{
   "versions": {
      "values": [
         {
            "media-types": [
               {
                  "type": "application/vnd.openstack.identity-v3+json",
                  "base": "application/json"
               }
            ],
            "links": [
               {
                  "rel": "self",
                  "href": "https://sample.domain.com/v3/"
               }
            ],
            "id": "v3.6",
            "updated": "2016-04-04T00:00:00Z",
            "status": "stable"
         }
      ]
   }
}
```

状态码

状态码	说明
300	请求成功。
400	请求错误。
404	找不到资源。
503	服务不可用。

4.13.2 查询 Keystone API 的 3.0 版本信息

功能介绍

该接口用于获取Keystone API的3.0版本的信息。

URI

GET /v3

请求

请求样例

```
curl -i -k -X GET https://sample.domain.com/v3
```

响应

- 响应参数说明

参数	是否必选	类型	描述
version	是	Object	Keystone API的版本信息。

- version格式说明

参数	是否必选	类型	说明
status	是	String	版本状态。
updated	是	String	版本最后更新时间。
media-types	是	Array	版本支持的消息格式。
id	是	String	版本号，如v3.0。
links	是	Array	版本的资源链接。

- 响应样例（响应成功）

```
{
    "version": {
        "status": "stable",
        "updated": "2016-04-04T00:00:00Z",
        "media-types": [
            {
                "base": "application/json",
                "type": "application/vnd.openstack.identity-v3+json"
            }
        ],
        "id": "v3.6",
        "links": [
            {
                "href": "https://sample.domain.com/v3/",
                "rel": "self"
            }
        ]
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
404	找不到资源。
503	服务不可用。

4.14 服务和终端节点

4.14.1 查询服务列表

功能介绍

该接口用于查询服务列表。

URI

- URI格式
  GET /v3/services{?type}
- 参数说明

参数	是否必选	类型	说明
type	否	String	服务类型。 可能取值为compute，ec2，identity，image，network，或volume。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/services?type=compute
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	Dict	服务的资源链接。
services	是	List	服务列表。

- services格式说明

参数	是否必选	类型	说明
description	否	String	服务描述。
enabled	是	Boolean	服务是否可用。

参数	是否必选	类型	说明
id	是	String	服务ID。
name	否	String	服务名。
type	是	String	服务类型。
links	是	Dict	服务的资源链接。

- 响应样例（响应成功）

```
{
    "services": [
        {
            "name": "compute5",
            "links": {
                "self": "https://sample.domain.com/v3/services/053d21d488d1463c818132d9d08fb617"
            },
            "enabled": true,
            "type": "compute",
            "id": "053d21d488d1463c818132d9d08fb617",
            "description": "Compute service 5"
        },
        {
            "name": "compute3",
            "links": {
                "self": "https://sample.domain.com/v3/services/c2474183dca7453bbd73123a0b78feae"
            },
            "enabled": true,
            "type": "compute",
            "id": "c2474183dca7453bbd73123a0b78feae",
            "description": "Compute service 3"
        },
        {
            "name": "compute2",
            "links": {
                "self": "https://sample.domain.com/v3/services/c7166694ebdd4616bd927737f7b12ca2"
            },
            "enabled": true,
            "type": "compute",
            "id": "c7166694ebdd4616bd927737f7b12ca2",
            "description": "Compute service 2"
        }
    ],
    "links": {
        "self": "https://sample.domain.com/v3/services?type=compute",
        "previous": null,
        "next": null
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。

状态码	说明
404	找不到资源。
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。

4.14.2 查询服务详情

功能介绍

该接口用于查询服务详情。

URI

- URI格式
  GET /v3/services/{service_id}
- 参数说明

参数	是否必选	类型	说明
service_id	是	String	服务的ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例
  curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/services/5a4ed456d228428c800ed2b67b4363a7

响应

响应样例（响应成功）

```
{
    "service": {
        "enabled": true,
        "type": "compute",
        "name": "nova",
        "links": {
```

```
            "self": "sample.domain.com/v3/services/5a4ed456d228428c800ed2b67b4363a7"
        },
        "id": "5a4ed456d228428c800ed2b67b4363a7"
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.14.3 查询终端节点列表

功能介绍

该接口用于查询终端节点列表，提供服务访问入口。

URI

- URI格式
  GET /v3/endpoints{?interface, service_id}
- 参数说明

参数	是否必选	类型	说明
interface	否	String	终端节点平面。 可能取值为：public，internal或admin。 • public： 用户可在公共网络接口上看到。 • internal：用户可在内部网络接口上看到。 • admin：管理员可以在安全的网络接口上看到。
service_id	否	String	服务ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/endpoints?interface=public&service_id=43cbe5e77aaf4665bbb962062dc1fc9d
```

响应

- Response Body参数说明

参数	是否必选	类型	说明
links	是	dict	终端节点的资源链接。
endpoints	是	list	终端节点列表。

- endpoints格式说明

参数	是否必选	类型	说明
id	是	String	终端节点ID。
url	是	String	终端节点的地址。
region	是	String	终端节点的区域。
region_id	是	String	终端节点的区域ID。
enabled	是	Boolean	终端节点是否可用。
interface	是	String	终端节点的平面。
service_id	是	String	终端节点所属服务的ID。
links	是	dict	终端节点的资源链接。

- 响应样例（请求成功）

```
{
    "endpoints": [
        {
            "region_id": null,
            "links": {
                "self": "https://sample.domain.com/v3/endpoints/162277d696f54cf592f19b569f85d158"
            },
            "url": "https://sample.domain.com/v3",
            "region": null,
```

```
            "enabled": true,
            "interface": "public",
            "service_id": "053d21d488d1463c818132d9d08fb617",
            "id": "162277d696f54cf592f19b569f85d158"
        }
    ],
    "links": {
        "self": "https://sample.domain.com/v3/endpoints?
service_id=053d21d488d1463c818132d9d08fb617&interface=public",
        "previous": null,
        "next": null
    }
}
```


状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.14.4 查询终端节点详情

功能介绍

该接口用于查询终端节点详情。

URI

- URI格式
  GET /v3/endpoints/{endpoint_id}
- 参数说明

参数	是否必选	类型	说明
endpoint_id	是	String	终端节点ID。

请求

- Request Header参数说明

参数	是否必选	类型	说明
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-Auth-Token	是	String	已认证的token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'Content-Type:application/json;charset=utf8' -H "X-Auth-Token:$token" -X GET https://sample.domain.com/v3/endpoints/62ea3602f8ee42b1825956473f5295a8
```

响应

响应样例（请求成功）

```
{
    "endpoint": {
        "region_id": "region_id",
        "links": {
            "self": "https://sample.domain.com/v3/endpoints/62ea3602f8ee42b1825956473f5295a8"
        },
        "url": "https://sample.domain.com/v2/",
        "region": "region_name",
        "enabled": true,
        "interface": "public",
        "service_id": "5a4ed456d228428c800ed2b67b4363a7",
        "id": "62ea3602f8ee42b1825956473f5295a8"
    }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。
403	鉴权失败。
404	找不到资源。
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。

4.14.5 查询服务目录

功能介绍

该接口用于查询请求中携带的X-Auth-Token对应的服务目录。

URI

GET /v3/auth/catalog

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project scoped token。

- 请求样例

```
curl -i -k -H 'Accept:application/json' -H 'X-Auth-Token:$token' -H 'Content-Type:application/
json;charset=utf8' -X GET https://sample.domain.com/v3/auth/catalog
```

响应

响应样例（请求成功）

```
{
  "catalog": [
    {
      "endpoints": [
        {
          "region_id": null,
          "url": "https://sample.domain.com/v2/c972a59e958e407e89b0c6d8e522df3b",
          "region": null,
          "interface": "public",
          "id": "04f0ee42038447f0a9c7b407028fd7b9"
        }
      ],
      "type": "compute",
      "id": "eb884e9f64b44dd0ac73cdc55d817286",
      "name": "nova"
    }
  ],
  "links": {
    "self": "https://sample.domain.com/v3/auth/catalog"
  }
}
```

状态码

状态码	说明
200	请求成功。
400	请求错误。
401	认证失败。

状态码	说明
403	鉴权失败。
404	找不到资源。
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。

5 权限和授权项

5.1 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，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。

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：自定义策略中授权项定义的内容即为权限
- 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与企业管理的区别。

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。

5.2 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	POST /v3/auth/tokens	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	GET /v3.0/OS-CREDENTIAL/credentials	iam:credentials:listCredentials	-	-
查询指定永久访问密钥	GET /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam:credentials:getCredential	-	-
创建永久访问密钥	POST /v3.0/OS-CREDENTIAL/credentials	iam:credentials:createCredential	-	-
修改指定永久访问密钥	PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam:credentials:updateCredential	-	-
删除指定永久访问密钥	DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}	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)
解绑MFA设备	×	iam:mfa:unbindMFADevice	-	-
绑定MFA设备	×	iam:mfa:bindMFADevice	-	-
创建MFA设备	×	iam:mfa:createVirtualMFADevice	-	-
删除MFA设备	×	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)
创建项目	POST /v3/projects	iam:projects:createProject	-	-
修改项目	PATCH /v3/projects/{project_id}	iam:projects:updateProject	-	-
设置指定项目的状态	PUT /v3-ext/projects/{project_id}	iam:projects:updateProject	-	-
查询用户的项目列表	GET /v3/users/{user_id}/projects	iam:projects:listProjectsForUser	-	-
删除项目	×	iam:projects:deleteProject	-	-

租户管理

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询租户配额	GET /v3.0/OS-QUOTA/domains/{domain_id}	iam:quotas:listQuotas	-	-

用户管理

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询用户列表	GET /v3/users	iam:users:listUsers	-	-
查询用户详情	GET /v3/users/{user_id}	iam:users:getUser	-	-
查询用户详情(推荐)	GET /v3.0/OS-USER/users/{user_id}	iam:users:getUser	-	-
查询用户所属用户组	GET /v3/users/{user_id}/groups	iam:groups:listGroupsForUser	-	-
查询用户组所包含的用户	GET /v3/groups/{group_id}/users	iam:users:listUsersForGroup	-	-
创建用户	POST /v3/users	iam:users:createUser	-	-
修改密码	POST /v3/users/{user_id}/password	iam:users:updateUserPassword	-	-
修改用户信息	PATCH /v3/users/{user_id}	iam:users:updateUser	-	-
删除用户	DELETE /v3/users/{user_id}	iam:users:deleteUser	-	-
管理员重置IAM用户密码	×	iam:users:resetUserPassword	-	-
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	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
删除用户组中用户	DELETE /v3/groups/{group_id}/users/{user_id}	iam:permissions:removeUserFromGroup	-	-
查询IAM用户的MFA绑定信息列表	GET /v3.0/OS-MFA/virtual-mfa-devices	iam:mfa:listVirtualMFADevices	-	-
查询指定IAM用户的MFA绑定信息	GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device	iam:mfa:getVirtualMFADevice	-	-
查询IAM用户的登录保护状态信息列表	GET /v3.0/OS-USER/login-protects	iam:users:listUserLoginProtects	-	-
查询指定IAM用户的登录保护状态信息	GET /v3.0/OS-USER/users/{user_id}/login-protect	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)
管理员查询用户组所包含的IAM用户	GET /v3/groups/{group_id}/users	iam:users:listUsersForGroup	-	-
查询用户组列表	GET /v3/groups{?domain_id,name}	iam:groups:listGroups	-	-
查询用户组详情	GET /v3/groups/{group_id}	iam:groups:getGroup	-	-
创建用户组	POST /v3/groups	iam:groups:createGroup	-	-
添加用户到用户组	PUT /v3/groups/{group_id}/users/{user_id}	iam:permissions:addUserToGroup	-	-
更新用户组	PATCH /v3/groups/{group_id}	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	DELETE /v3/groups/{group_id}	• 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	HEAD /v3/groups/{group_id}/users/{user_id}	iam:permissions:checkUserInGroup	-	-

权限管理

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询角色列表	GET /v3/roles	iam:roles:listRoles	-	-
查询角色的详细信息	GET /v3/roles/{role_id}	iam:roles:getRole	-	-
查询租户中用户组的权限	GET /v3/domains/{domain_id}/groups/{group_id}/roles	iam:permissions:listRolesForGroupOnDomain	-	-
查询项目对应的用户组的权限	GET /v3/projects/{project_id}/groups/{group_id}/roles	iam:permissions:listRolesForGroupOnProject	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
为租户所属用户组授权	PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:permissions:grantRoleToGroupOnDomain	-	-
为项目对应的用户组授权	PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:permissions:grantRoleToGroupOnProject	-	-
删除项目对应的用户组的权限	DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:permissions:revokeRoleFromGroupOnProject	-	-
删除租户所属用户组的权限	DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:permissions:revokeRoleFromGroupOnDomain	-	-
查询租户中用户组是否包含权限	HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:permissions:checkRoleForGroupOnDomain	-	-
查询项目对应的用户组是否包含权限	HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:permissions:checkRoleForGroupOnProject	-	-
为用户组授予指定权限	PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id} PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:permissions:grantRoleToGroup	-	-
查询用户在指定项目上拥有的权限	×	iam:permissions:listRolesForUserOnProject	-	-
查询用户组的所有权限	×	iam:permissions:listRolesForGroup	-	-
查询用户组是否拥有指定权限	×	iam:permissions:checkRoleForGroup	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
移除用户组的指定权限	×	iam:permissions:revokeRoleFromGroup	-	-
查询租户配额	GET /v3.0/OS-QUOTA/domains/{domain_id}?type={user, group, idp, agency, policy}	iam:quotas:listQuotas	-	-

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	GET /v3.0/OS-ROLE/roles	iam:roles:listRoles	-	-
查询自定义策略详情	GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:getRole	-	-
创建云服务自定义策略	POST /v3.0/OS-ROLE/roles	iam:roles:createRole	-	-
修改云服务自定义策略	PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:updateRole	-	-
删除自定义策略	DELETE /v3.0/OS-ROLE/roles/{role_id}	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	POST /v3.0/OS-AGENCY/agencies	iam:agencies:createAgency	-	-
查询指定条件下的委托列表	GET /v3.0/OS-AGENCY/agencies	iam:agencies:listAgencies	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
获取指定委托的详细信息	GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:getAgency	-	-
修改委托	PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:updateAgency	-	-
删除委托	DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:deleteAgency	-	-
通过项目给委托赋予权限	PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:grantRoleToAgencyOnProject	-	-
检查委托在项目上是否有指定权限	HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:checkRoleForAgencyOnProject	-	-
查询委托在项目上具有的权限列表	GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:permissions:listRolesForAgencyOnProject	-	-
通过项目删除委托的权限	DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:revokeRoleFromAgencyOnProject	-	-
通过租户给委托赋予权限	PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:grantRoleToAgencyOnDomain	-	-
检查委托在租户上是否有指定权限	HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:checkRoleForAgencyOnDomain	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询委托在租户上具有的权限列表	GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:permissions:listRolesForAgencyOnDomain	-	-
通过租户删除委托的权限	DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:permissions:revokeRoleFromAgencyOnDomain	-	-
查询委托下的所有项目服务权限列表	GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:permissions:listRolesForAgency	-	-
为委托授予所有项目服务权限	PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:grantRoleToAgency	-	-
检查委托下是否具有所有项目服务权限	HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:checkRoleForAgency	-	-
移除委托下的所有项目服务权限	DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:permissions:revokeRoleFromAgency	-	-

安全设置

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询账号操作保护策略	GET v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securitypolicies:getProtectPolicy	-	-
查询账号密码策略	GET v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securitypolicies:getPasswordPolicy	-	-
查询账号登录策略	GET v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securitypolicies:getLoginPolicy	-	-
查询账号控制台访问策略	GET v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securitypolicies:getConsoleAclPolicy	-	-
查询账号接口访问策略	GET v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	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	GET /v3/OS-FEDERATION/identity_providers	iam:identityProviders:listIdentityProviders	-	-
查询身份提供商	GET /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:getIdentityProvider	-	-
创建身份提供商	PUT /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:createIdentityProvider	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
更新身份提供商	PATCH /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:updateIdentityProvider	-	-
删除身份提供商	DELETE /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:deleteIdentityProvider	-	-
查询映射列表	GET /v3/OS-FEDERATION/mappings	iam:identityProviders:listMappings	-	-
查询映射详情	GET /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:getMapping	-	-
注册映射	PUT /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:createMapping	-	-
更新映射	PATCH /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:updateMapping	-	-
删除映射	DELETE /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:deleteMapping	-	-
查询协议列表	GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols	iam:identityProviders:listProtocols	-	-
查询协议	GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-	-
注册协议	PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:createProtocol	-	-
更新协议	PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:updateProtocol	-	-

权限	对应API接口	授权项	IAM项目(Project)	企业项目(Enterprise Project)
删除协议	DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:deleteProtocol	-	-
查询Metadata文件	GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:getIDPMetadata	-	-
导入Metadata文件	POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:createIDPMetadata	-	-

6 附录

6.1 状态码

表 6-1 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。

状态码	编码	说明
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。
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。

状态码	编码	说明
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。
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	UnprocessableEntity	请求格式正确，但是由于含有语义错误，无法响应。
429	TooManyRequests	表明请求超出了客户端访问频率的限制或者服务端接收到多于它能处理的请求。建议客户端读取相应的Retry-After首部，然后等待该首部指出的时间后再重试。
500	InternalServerError	表明服务端能被请求访问到，但是不能理解用户的请求。
501	Not Implemented	服务器不支持请求的功能，无法完成请求。
502	Bad Gateway	充当网关或代理的服务器，从远端服务器接收到了一个无效的请求。
503	ServiceUnavailable	被请求的服务无效。 建议直接修改该请求，不要重试该请求。
504	ServerTimeout	请求在给定的时间内无法完成。客户端仅在为请求指定超时（Timeout）参数时会得到该响应。
505	HTTP Version not supported	服务器不支持请求的HTTP协议的版本，无法完成处理。

6.2 错误码

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。
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	管理员不能被删除。	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。

状态码	错误码	错误信息	描述	处理措施
400	IAM.0007	Request parameter %(key)s is invalid.	请求参数校验失败。	请检查请求参数。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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字段的的值是否正确。
400	IAM.1017	Invalid name.	非法的name字段。	检查name字段的的值是否正确。
400	IAM.1018	Invalid description.	非法的description字段。	检查description字段的的值是否正确。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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verion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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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condtion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。

状态码	错误码	错误信息	描述	处理措施
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范。	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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

状态码	错误码	错误信息	描述	处理措施
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。
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。

6.3 获取用户、账号、用户组、项目、委托的名称和 ID

获取用户名、用户 ID、账号名、账号 ID、项目名称、项目 ID

在调用接口时，部分URI中需要填入用户名、用户ID、账号名、账号ID、项目名称、项目ID，在“我的凭证”页面可以获取这些信息。

步骤1 登录控制台。

步骤2 单击右上角已登录的用户名，选择“我的凭证”。

步骤3 在“我的凭证”界面，可以查看用户名、用户ID、账号名、账号ID、项目名称、项目ID。

----结束

获取用户组名称和 ID

步骤1 登录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

获取委托的名称和 ID

步骤1 登录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

表 A-1 修订记录

发布时间	修改记录
2022-08-15	第一次正式发布。