统一身份认证

API 参考

文档版本 04

发布日期 2022-07-30

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

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

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**

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。

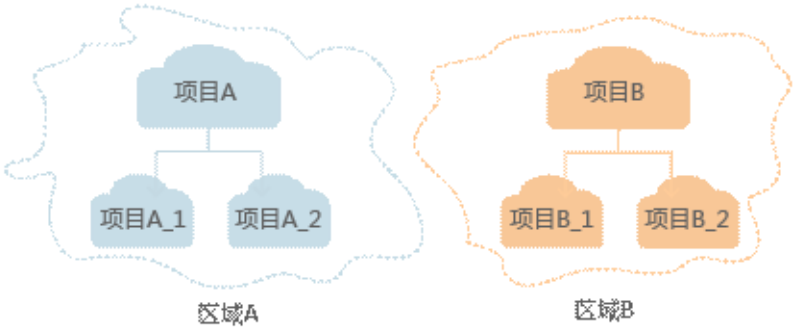
- 可用区（AZ，Availability Zone）

  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。

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。

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**地区和终端节点**处获取。 例如IAM服务在“**ae-ad-1**”区域的Endpoint为“**iam.ae-ad-1.myhuaweicloud.com**”。
resource-path	资源路径，即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
query-string	查询参数，可选，查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“ae-ad-1”区域的Token，则需使用“ae-ad-1”区域的Endpoint（iam.ae-ad-1.myhuaweicloud.com），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.ae-ad-1.myhuaweicloud.com/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.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
```

请求消息头

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

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。X-Auth-Token是调用**获取用户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.ae-ad-1.myhuaweicloud.com/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，***domianname***为用户所属的账号名称，如果是账号本身获取token，***username***和***domianname***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.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json

{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domianname"
                    }
                }
            }
        },
        "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.ae-ad-1.myhuaweicloud.com/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。

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。
			示例：
			"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。

参数	是否必选	类型	说明

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。

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。

4.2 项目管理

4.2.1 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。
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。

5 权限和授权项

权限及授权项说明

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。

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	账号管理员不能被删除。	账号管理员不能被删除。	不允许此操作。
400	1108	新密码不能与原密码相同。	新密码不能与原密码相同。	请修改新密码。
400	1109	用户名已存在。	用户名已存在。	请修改用户名。
400	1110	邮箱已存在。	邮箱已存在。	请修改邮箱。
400	1111	手机号已存在。	手机号已存在。	请修改手机号。
400	1113	xuser_id、xuser_type已存在。	xuser_id、xuser_type已存在。	请修改xuser_id和xuser_type。
400	1115	IAM用户数量达到最大限制。	IAM用户数量达到最大限制。	请修改用户配额或联系技术支持。
400	1117	用户描述校验失败。	用户描述校验失败。	请修改用户描述。
400	1118	密码是弱密码。	密码是弱密码。	重新选择密码。

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 128 characters.	策略display_name不能超过128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。	请输入正确的账号密码。
401	IAM.0063	Access token authentication failed.	accesstoken认证失败。	请联系技术支持。
401	IAM.0064	The access token does not have permissions for the request.	IAM用户没有权限请求。	请确认该IAM用户的权限信息。
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reigon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

日期	修订记录
2022-07-30	第四次正式发布。 刷新API列表。
2021-11-30	第三次正式发布。 新增5.13-企业项目管理章节。
2021-02-25	第二次正式发布。 6.2-授权项列表增加IAM项目、企业项目。
2020-10-30	第一次正式发布。