

开天企业工作台

## API 参考

文档版本 01  
发布日期 2023-08-29



版权所有 © 华为云计算技术有限公司 2023。保留一切权利。

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

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限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，华为云计算技术有限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。

---

# 目录

---

<b>1 使用前必读</b>	<b>1</b>
1.1 概述	1
1.2 调用说明	1
1.3 终端节点	1
1.4 基本概念	1
<b>2 API 概览</b>	<b>3</b>
<b>3 如何调用 API</b>	<b>4</b>
3.1 构造请求	4
3.2 认证鉴权	6
3.3 返回结果	7
<b>4 API ( 圆桌 )</b>	<b>10</b>
4.1 统一认证接口定义	10
4.1.1 统一认证注销 token	10
4.1.2 统一认证获取 access_token	11
4.1.3 统一认证获取 userinfo	13
<b>5 应用示例</b>	<b>15</b>
5.1 获取 access_token	15
5.2 获取用户信息	15
<b>6 权限和授权项</b>	<b>17</b>
6.1 权限及授权项说明	17
<b>7 附录</b>	<b>19</b>
7.1 状态码	19
7.2 错误码	22
<b>8 修订记录</b>	<b>23</b>

# 1 使用前必读

## 1.1 概述

开天企业工作台聚焦于企业办公应用，其包含了企业工作台和圆桌两个子产品。

企业工作台（MacroVerse SmartStage for Enterprises, MSSE）是企业一站式数字化工作台，是企业应用的统一门户，为企业提供了用户、组织的统一管理，应用的统一管理和授权及应用间的单点登录，解决企业内应用管理和用户不统一的问题，提升企业的办公效率。

圆桌（RoundTable）是一个智能化云办公平台，致力于打造企业数字化的业务即IT融合平台，降低企业流程应用开发门槛，提升企业员工办公效率。包含了业务流构建平台、个人工作台、模板市场等功能。

您可以使用本文档提供的API进行相关操作，如创建、修改、删除等。支持的全部操作请参见[API概览](#)。

在调用API之前，请确保已经充分了解产品的相关概念，详细信息请参见《[产品介绍](#)》。

## 1.2 调用说明

开天企业工作台提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见[3 如何调用API](#)。

## 1.3 终端节点

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

## 1.4 基本概念

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

安全，建议您不要直接使用账号进行日常管理工作，而是创建用户并使用它们进行日常管理工作。

- 用户

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

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

- 区域（Region）

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

详情请参见[区域和可用区](#)。

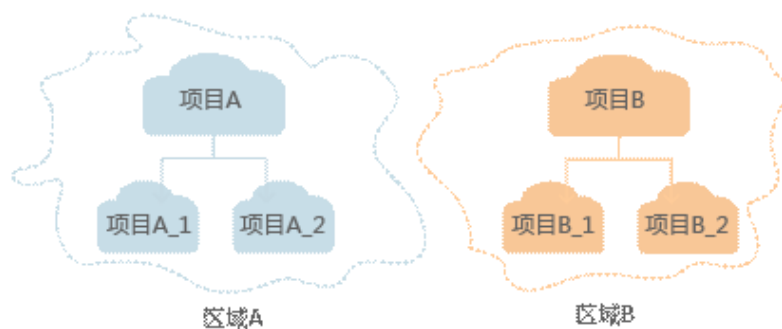
- 可用区（AZ，Availability Zone）

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

- 项目

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

图 1-1 项目隔离模型



同样在[我的凭证](#)下，您可以查看项目ID。

- 企业项目

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

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

# 2 API 概览

## 圆桌统一认证相关接口

圆桌提供了基于OAuth2.0协议实现的统一认证接口，多系统间可通过这些接口实现单点登录，如表2-1所示。

表 2-1 统一认证接口

API	说明
<a href="#">统一认证注销token</a>	注销当前的access_token及用户会话。
<a href="#">统一认证获取access_token</a>	根据code获取认证鉴权使用的access_token。
<a href="#">统一认证获取userinfo</a>	根据access_token获取用户信息。

# 3 如何调用 API

## 3.1 构造请求

本节介绍REST API请求的组成，并以圆桌[统一认证获取access\\_token](#)接口说明如何调用API，以及使用该API获取可用的access\_token。

### 请求 URI

请求URI由如下部分组成。

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

尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

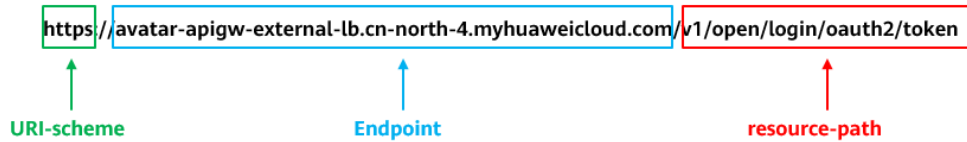
表 3-1 URI 中的参数说明

参数	描述
URI-scheme	表示用于传输请求的协议，当前所有API均采用HTTPS协议。
Endpoint	指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从 <a href="#">地区和终端节点</a> 中获取。例如在“华北-北京四”区域圆桌的Endpoint为“roundtable.macoverse.huaweicloud.com”，圆桌apig的Endpoint为“avatar-apigw-external-lb.cn-north-4.myhuaweicloud.com”。
resource-path	资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取access_token”API的resource-path为“v1/open/login/oauth2/token”。
query-string	查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需使用的Endpoint ( avatar-apigw-external-lb.cn-north-4.myhuaweicloud.com )，并在URI部分找到resource-path ( /v1/open/login/oauth2/token )，拼接起来如下所示。

```
https://avatar-apigw-external-lb.cn-north-4.myhuaweicloud.com/v1/open/login/oauth2/token
```

图 3-1 URI 示意图



### 说明

为查看方便，在每个具体API的URI部分，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。

表 3-2 HTTP 方法

方法	说明
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。

## 请求消息头

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

如下公共消息头需要添加到请求中。



表 3-3 公共请求消息头

名称	描述	是否必选	示例
Content-Type	消息体的类型（格式），默认取值为“application/json”，有其他取值时会在具体接口中专门说明。	是	application/json
X-Auth-Token	用户Token，也就是调用 <a href="#">获取用户Token</a> 接口的响应值，该接口是唯一不需要认证的接口。	否 使用Token认证时该字段必选。	-

## 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。

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。

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，*domainname* 为用户所属的账号名称，*\*\*\*\*\** 为用户登录密码，*xxxxxxxxxx* 为 project 的名称，如 cn-north-1，您可以从 [地区和终端节点](#) 中获取。

### 说明

scope 参数定义了 Token 的作用域，下面示例中获取的 Token 仅能访问 project 下的资源。您还可以设置 Token 作用域为某个账号下所有资源或账号的某个 project 下的资源。

```
POST https://avatar-apigw-external-lb.cn-north-4.myhuaweicloud.com/v1/open/login/oauth2/token
Content-Type: application/x-www-form-urlencoded
Accept: application/json
```

```
Form-Data:
client_id={ClientId}&client_secret={SECRET}&code=akaZnezUrvT7KY4haEAo_KPiubG97fjZXuenXvTkMiL_UF7
JdWAg514j4r1-PYsxhoypJjIFVx6WE7nisqzvhCsfSQQORO8DjQunZu8nLnqO3EDE7LvBbVpjU-
dTSo&grant_type=authorization_code
```

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。这里的 code 是统一认证页面登录后返回的 code、clientId 和 clientSecret 则是您的应用在圆桌中注册的应用 id 和 secret

## 3.2 认证鉴权

调用接口支持 Token 认证鉴权。

## Token 认证

### 📖 说明

Token的有效期为30分钟，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

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

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

Token可通过调用**获取用户Token**接口获取，调用本服务API需要项目级别的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project，如下所示。

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

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Token。例如Token值为“ABCDEFJ...”，则调用接口时将“X-Auth-Token: ABCDEFJ...”加到请求消息头即可，如下所示。

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

您还可以通过这个视频教程了解如何使用Token认证：<https://bbs.huaweicloud.com/videos/101333>。

## 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iam\_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iam\_token接口，返回如图3-2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

```
connection → keep-alive
content-type → application/json
date → Tue, 12 Feb 2019 06:52:13 GMT
server → Web Server
strict-transport-security → max-age=31536000; includeSubdomains;
transfer-encoding → chunked
via → proxy A
x-content-type-options → nosniff
x-download-options → noopen
x-frame-options → SAMEORIGIN
x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5
x-subject-token
→ MIiYXQVJKoZiIhvcNAQcCoIITJCCGEoCAQExDTALBglghkgBZQMEAgEwggharBgkqhkiG9w0BBwGggghacBIIWmHsidG9rZW4iOansiZXhwaXJlc19hdCI6IiwMTktMDItMTNUMC
fj3Kjs6YgKnpVNRbW2eZ5eb78S2OkqjACgkqO1wi4IJGzrpd18LGXK5txdfq4lqHCYb8P4NaY0NYejcAgzJVeFYtLWT1GSO0zxKZmlQHj82H8qHdgIZO9fuEbl5dMhdavj+33wEI
xHRCe9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASX1IjipPEGA270g1FruooL6jqgIFKNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpXk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3Hrozv0vN--n5d6Nbxg==
x-xss-protection → 1; mode=block;
```

## 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[统一认证获取access\\_token](#)接口，返回如下消息体。

```
{
  "access_token":
  "eyJraWQiOiJzE0Y2EzZi1LZTM3LTRhYWItYWY5ZS1kMjIyZS5NDZkZDIiLCJhbGciOiJSUzI1NiJ9.eyJzdWUiOiIxMjMwNDAwMDAxNyIsImF1ZCI6ImFpLXNoZW5nc2ktY2xpZW50LWkiwibmJmIjojNjkyNzc0MTUyLCJzY29wZSI6
  WyJwcm9maWxll0sImVzcyI6Imh0dHA6XC9clzEwLjI0Ny4xMzMuNTg6ODAwMyIsImV4cCI6IjE5MjM0MTUyMjc3NTk1MiwiYWV0IjojNjkyNzc0MTUyLCJhdXRob3JpdGllcyI6ImBFUk1JU1NJT05fQUxMin0.fqWdl18V0tUNeR6QXdrJj8ZaQ
  5cG_JXx1ZYaMfJhOQfclS_L1qYdOz44T88KbWvVf-gzbY0zAiNAYomgkK6eGwFmc38Gfkgg-
  T9AtIqE_4yQIN-1nHIDT2irn_CLhCPVH2Zpl-GtVUbWHstK-
  lISsrznbV9QLByS45JgBzcXtl8Nb0v2AehqPpDXxClR0F_PUG58ldLKZtC6MFN_AcFfcWE9V_h6P8B9x3aUKJnOJA
  hx9Hmt52DbWeeZBTPq6VD1dqffORrP28d6nwac0bgLmfJUB9Y0S9otSoWFBryE-
  vY1TXtd1nYBfcKkGXlsWyepocfvE4aJdJikd95Rr9tl_kR50z7KqC9_nmtMt2v9UpN100W5lY9GRkhrwaMziKEe0v9
  mkjAROIiX5N5JuQQ4If3Nx_BGJL-OEy6tQiqdOE0dGxDz9KtWSVlp_UIY9eb8GCQszXZa9-
  jYJhPPpgixLA5ZEWh_KUHKctZ7877VMDLrFI-D964XqNkXTUk",
  "refresh_token": "Y1DyijFg6KaBi-q0xgiqNQM5QrhoGOI-
  lgTpihU5xl18eiuSP95kSHz_YBCB7pL_wlj9-6Cun97JLxvv9GfSTzMhxvdFGmsvb3EbphPu-
  zKqVMWrbmPbw5ghXiFPcuav",
  "scope": "profile",
  "token_type": "Bearer",
  "expires_in": 1800
}
```

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。

```
{
  "code": 61010202,
```

```
"data": "invalid_grant",  
"message": "无效的code"  
}
```

其中，code表示错误码，message表示错误描述信息。

# 4 API (圆桌)

## 4.1 统一认证接口定义

### 4.1.1 统一认证注销 token

#### 功能介绍

统一认证注销token。

#### URI

GET /v1/open/login/oauth2/logout

#### 请求参数

表 4-1 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	获取的access_token。

#### 响应参数

状态码： 200

表 4-2 响应 Body 参数

参数	参数类型	描述
code	Integer	返回状态。
data	String	返回数据。

参数	参数类型	描述
message	String	信息。

### 请求示例

无

### 响应示例

```
{  
  "code": 200,  
  "data": "200 OK",  
  "message": "OK"  
}
```

### 状态码

状态码	描述
200	注销成功。

### 错误码

请参见[错误码](#)。

## 4.1.2 统一认证获取 access\_token

### 功能介绍

统一认证获取access\_token。

### URI

POST /v1/open/login/oauth2/token

### 请求参数

表 4-3 FormData 参数

参数	是否必选	参数类型	描述
client_id	是	String	应用唯一标识。
client_secret	是	String	应用密钥。
grant_type	是	String	固定填authorization_code。
code	是	String	登录凭据code。

## 响应参数

状态码：200

表 4-4 响应 Body 参数

参数	参数类型	描述
access_token	String	access token。
refresh_token	String	refresh token。
scope	String	token 作用域。
expires_in	Integer	过期时间。

## 请求示例

无

## 响应示例

```
{
  "access_token":
  "eyJraWQioiJzJE0Y2EzZi1lZTM3LTRhYWItYWY5ZS1kMjJiYzY5NDZkZDliLCJhbGciOiJSUzI1Ni9.eyJzdWliOiIxMzcxOTU0PTI9BTEwifQ.bs2W-X0mYIFdVhqDeYaqCpl9bX4IG82no7PEYRIKJCKVNS59fkVgm8dqWBACensQTMxerYgJSvLEcXNIFldP3GgtlcDqRBTtYLF-d-tJquesU_z3q0uOP4AmZlahpnJBuVYPp-gEpljm-3BVC2bT7L8o0_3QSqN0U_kq0GGOHVrcKvTwjkl5wsShQ_RvMopqxCEO7EsA1yFVck9m2qyFTw9hxbPyH6d7Jfd0dmBebxHJs8GQ2Kxk1Z87yfN08Y6T7xKhtrKjBjN9Wz7QEzkB0KDntCBnhjanim8cPKnVoCcC3FX0Td5xrEhBoPT1an0bSlpW-HSy1_UbwRj4ld91aZcDPAjt9poc9QxK91V431x3REgdNXbJEU2U80z050LasBFM0SnB4V8ZowupJfUpXbTd5XPQTiUVt1aDGGGoQctO9wfmEhycQZz_xmdysyqrKwETP6L6eDIGTzSF4libxHV63ta4RLsKilox6aSRXEW7tYmFdkjLERTko6e",
  "refresh_token": "ESpjcsn8PO6I1ZBcdU0V919byfHCeOQH-iRrrS0b9Y8dgTEzjdQtiKx9ffuz76X6M7Es-sYh7UZAsUQwo42_2Xl19lBwshkkgvuRpmO0Suzl7C1ZeuPzFqVq1dVN3Dyd",
  "scope": "profile",
  "token_type": "Bearer",
  "expires_in": 1800
}
```

## 状态码

状态码	描述
200	授权成功。

## 错误码

请参见[错误码](#)。

## 4.1.3 统一认证获取 userinfo

### 功能介绍

统一认证获取userinfo.

### URI

GET /v1/open/login/userinfo

### 请求参数

表 4-5 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	获取的access_token。

### 响应参数

状态码： 200

表 4-6 响应 Body 参数

参数	参数类型	描述
id	String	用户id。
sub	String	用户名。
identity-id	String	账号id。
userAccount	String	账号。

### 请求示例

无

### 响应示例

```
{  
  "sub": "13739090031",  
  "identity-id": "16865386900050000000000001avatar-plamaste",  
  "userAccount": "13739090031",  
  "id": "16818102441480000000000000DESKTOP-59maste",  
  "tenant-id": "RoundTable"  
}
```



## 状态码

状态码	描述
200	获取用户信息。

## 错误码

请参见[错误码](#)

# 5 应用示例

## 5.1 获取 access\_token

### 操作场景

统一认证页面登录后获取到本次登录的code和state，随后根据code获取access\_token，可以参考此示例。

下面介绍如何调用圆桌[统一认证获取access\\_token](#)API，API的调用方法请参见[如何调用API](#)。

### 获取 access\_token

如下示例是获取access\_token最简单的配置。

```
POST https://avatar-apigw-external-lb.cn-north-4.myhuaweicloud.com/v1/open/login/oauth2/token
Content-Type: application/x-www-form-urlencoded
Accept: application/json
Form-Data:
client_id={ClientId}
client_secret={SECRET}
code=akaZnezUrkvT7KY4haEAo_KPiubG97fJZXuenXvTkMil_UF7JdWAg514j4r1-
PysxhoyppjIFVx6WE7nisqzvhCsfsQQORO8DjQunZu8nLnqO3EDE7LvBbVpjU-dTS_o
grant_type=authorization_code
```

## 5.2 获取用户信息

### 操作场景

在获取到access\_token后，需要根据access\_token获取userinfo完成整个OAuth2.0认证过程，可以参考此示例。

下面介绍如何调用圆桌[统一认证获取userinfo](#)API发布事件，API的调用方法请参见[如何调用API](#)。

### 获取用户信息

如下示例是获取用户信息最简单的配置。

```
GET https://roundtable-sit.ulanhba.huawei.com/open-login/userinfo
Content-Type: application/x-www-form-urlencoded
Accept: application/json
Authorization: Bearer ${上一步获取到的access_token}
```

# 6 权限和授权项

## 6.1 权限及授权项说明

如果您需要对您所拥有的开天企业工作台进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用开天企业工作台的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要为用户授予角色，才能使用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

### 📖 说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

账号具备所有接口的调用权限，如果使用账号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。例如，用户要调用接口来查询云服务器列表，那么这个IAM用户被授予的策略中必须包含允许“ecs:servers:list”的授权项，该接口才能调用成功。

## 支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给角色授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- 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](#)。

# 7 附录

## 7.1 状态码

状态码如表7-1所示。

表 7-1 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。
200	OK	接口调用成功
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。
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	Unprocessable Entity	请求格式正确，但是由于含有语义错误，无法响应。
429	TooManyRequests	表明请求超出了客户端访问频率的限制或者服务端接收到多于它能处理的请求。建议客户端读取相应的Retry-After首部，然后等待该首部指出的时间后再重试。
500	InternalServerError	表明服务端能被请求访问到，但是不能理解用户的请求。
501	Not Implemented	服务器不支持请求的功能，无法完成请求。
502	Bad Gateway	充当网关或代理的服务器，从远端服务器接收到了一个无效的请求。
503	ServiceUnavailable	被请求的服务无效。 建议直接修改该请求，不要重试该请求。
504	ServerTimeout	请求在给定的时间内无法完成。客户端仅在为请求指定超时（Timeout）参数时会得到该响应。
505	HTTP Version not supported	服务器不支持请求的HTTP协议的版本，无法完成处理。



## 7.2 错误码

状态码	错误码	错误信息	描述	修改建议
200	61010101	user_not_found	无法找到对应用户。	查看用户信息是否是有效地用户。
200	61010102	user_expired	用户已失效。	查看当前用户是否已失效。
200	61010103	invalid_request	请求缺少必要的参数。	检查传入的参数或请求头是否有遗漏。
200	61010104	unauthorized_client	未授权的client信息。	当前传入的client_id和client_secret有误。
200	61010105	access_denied	认证被拒绝。	client_id和client_secret不匹配。
200	61010106	unsupported_response_type	不支持的response_type。	response_type参数不正确。
200	61010107	invalid_scope	scope信息不匹配。	登录时的scope和token中的scope不匹配。
200	61010108	insufficient_scope	非法的 scope。	传入的scope信息不符合OAuth2.0规范。
200	61010201	invalid_client	client信息不匹配。	client_id信息不正确。
200	61010202	invalid_grant	无效的code，或grant_type异常。	code已经失效，重新获取。
200	61010203	invalid_token	token已失效。	token已失效，请刷新或重新登陆。
200	61010400	server_error	OAuth2.0认证出现异常。	OAuth2.0认证未知错误，联系开发进行排查。

# 8 修订记录

发布日期	修订记录
2023-08-29	第一次正式发布。