Agent Identity

API 参考

文档版本 01

发布日期 2026-11-06



华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2026。 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


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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 使用前必读 1
2 API 概览 3
3 如何调用 API 4
3.1 构造请求 4
3.2 认证鉴权 6
3.3 返回结果 12
4 API 14
4.1 工作负载访问令牌 14
4.1.1 创建工作负载访问令牌（不以用户身份操作） 14
4.1.2 使用 JWT 创建工作负载访问令牌（以用户身份操作） 20
4.1.3 使用用户 ID 创建工作负载访问令牌（以用户身份操作） 26
4.2 凭证提供商 31
4.2.1 确认 OAuth 2.0 令牌的用户认证会话 32
4.2.2 获取与指定资源凭证提供者关联的 API 密钥 38
4.2.3 从资源凭证提供商处获取 OAuth 2.0 令牌 44
4.2.4 从 STS 凭证提供商获取 STS 凭证 53
4.3 OAuth2.0 流程 63
4.3.1 OAuth 2.0 推送授权请求（PAR）标准的授权 API 63
4.3.2 OAuth 2.0 标准授权回调 API 65
4.4 API 密钥凭证提供商 68
4.4.1 创建 API 密钥凭证提供商 68
4.4.2 查询 API 密钥凭证提供商列表 75
4.4.3 查询 API 密钥凭证提供商详情 80
4.4.4 更新 API 密钥凭证提供商 86
4.4.5 删除 API 密钥凭证提供商 93
4.5 OAuth2 凭证提供商 95
4.5.1 创建 OAuth2 凭证提供商 95
4.5.2 查询 OAuth2 凭证提供商列表 115
4.5.3 查询 OAuth2 凭证提供商详情 120
4.5.4 更新 OAuth2 凭证提供商 129
4.5.5 删除 OAuth2 凭证提供商 147
4.6 STS 凭证提供商 151

 版权所有 © 华为云计算技术有限公司

4.6.1 创建 STS 凭证提供商 151
4.6.2 查询 STS 凭证提供商列表 158
4.6.3 查询 STS 凭证提供商详情 163
4.6.4 更新 STS 凭证提供商 168
4.6.5 删除 STS 凭证提供商 175
4.7 工作负载身份 177
4.7.1 创建工作负载身份 178
4.7.2 查询工作负载身份列表 194
4.7.3 查询工作负载身份详情 200
4.7.4 更新工作负载身份 206
4.7.5 删除工作负载身份 223
4.7.6 查询工作负载身份的授权配置 226
4.8 令牌保险库 234
4.8.1 查询令牌保管库详情 234
4.8.2 更新令牌保管库配置 240
4.9 策略集 247
4.9.1 创建策略集 247
4.9.2 查询策略集列表 254
4.9.3 查询策略集详情 260
4.9.4 更新策略集 265
4.9.5 删除策略集 272
4.9.6 查询策略集关联的实体列表 275
4.10 策略 281
4.10.1 在指定策略集中创建策略 281
4.10.2 查询策略列表 289
4.10.3 查询策略详情 295
4.10.4 更新策略 301
4.10.5 删除策略 308
4.11 标签 315
4.11.1 查询项目标签列表 315
4.11.2 查询资源标签 320
4.11.3 查询资源实例列表 325
4.11.4 查询资源实例数量 332
4.11.5 向指定资源添加标签 338
4.11.6 从指定资源中删除标签 343
4.12 身份提供商 349
4.12.1 查询身份提供商 349
5 应用示例 353
5.1 配置 Agent 身份并获取访问令牌 353
6 权限和授权项 357
6.1 权限和授权项说明 357
6.2 身份策略授权参考 357

 版权所有 © 华为云计算技术有限公司

7 附录..... 378
7.1 状态码..... 378
7.2 错误码..... 380

 版权所有 © 华为云计算技术有限公司

1 使用前必读

概述

华为云智能体身份（Agent Identity）专门为Agent提供安全身份标识、安全凭证管理、细粒度访问控制的云服务，让智能体能够安全地调用各类第三方外部工具和华为云服务资源。

调用说明

智能体身份提供了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**。

同时智能体身份还提供多种编程语言的SDK供您使用，SDK的使用方法请参见**https://console.huaweicloud.com/apiexplorer/#/sdkcenter/AgentIdentity**。

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**中查询服务的终端节点。

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他们进行日常管理工作。

- 用户

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

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

- 区域（Region）

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

版权所有 © 华为云计算技术有限公司

详情请参见**区域和可用区**。

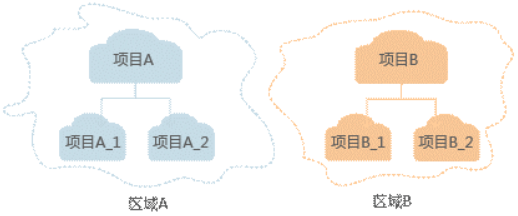
- 可用区（AZ，Availability Zone）

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

- 项目

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

  图 1-1 项目隔离模型

  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**》。

版权所有 © 华为云计算技术有限公司

2 API 概览

类型	子类型	说明
管控面	API密钥凭证提供商管理	对API密钥凭证提供商进行创建，查询，修改，删除操作。
	OAuth2凭证提供商管理	对OAuth2凭证提供商进行创建，查询，修改，删除操作。
	STS凭证提供商管理	对STS凭证提供商进行创建，查询，修改，删除操作。
	工作负载身份管理	对工作负载身份进行创建，查询，修改，删除操作。
	令牌保险库管理	对令牌保险库进行查询，修改操作。
	策略集管理	对策略集进行创建，查询，修改，删除操作。
	策略管理	对策略进行创建，查询，修改，删除操作。
	标签管理	对资源进行标签相关的创建，查询，删除操作。
	身份提供商查询	查询身份提供商列表。
凭证获取	从凭证提供商获取凭证	通过凭证提供商获取访问外部服务所需的凭证（API Key、OAuth2 Token或STS临时凭证）。
	OAuth2流程中使用的授权与回调接口	OAuth2流程中使用的授权与回调接口。
	获取工作负载访问令牌	签发工作负载访问令牌，支持以Agent身份或携带用户身份操作，用于访问其他服务。

 版权所有 © 华为云计算技术有限公司

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AgentIdentity服务的**创建工作负载身份**接口说明如何调用API。该API用于在AgentIdentity中注册一个工作负载身份，工作负载身份是Agent的身份标识，承载入站验证规则与出站凭证配置，用于Agent访问其他服务时进行身份认证与权限校验。

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

请求 URI

请求URI由如下部分组成。

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

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。

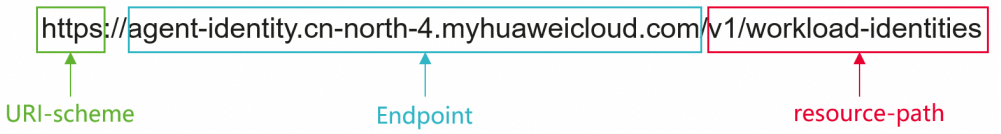
- **URI-scheme**：表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**中获取。例如Agent Identity服务在“华北-北京四”区域的Endpoint为“agent-identity.cn-north-4.myhuaweicloud.com”。
- **resource-path**：资源路径，也即API访问路径。从具体API的URI模块获取，例如“创建工作负载身份”接口的resource-path为“/v1/workload-identities”。
- **query-string**：查询参数，是可选部分，并不是每个API都有查询参数。第一个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。多个查询参数之间使用“&”分隔。

  例如您需要创建工作负载身份，在“华北-北京四”区域的Endpoint为agent-identity.cn-north-4.myhuaweicloud.com，并在**创建工作负载身份**接口的URI部分找到resource-path(/v1/workload-identities)，拼接起来如下所示。

  ```
  https://agent-identity.cn-north-4.myhuaweicloud.com/v1/workload-identities
  ```


版权所有 © 华为云计算技术有限公司

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**创建工作负载身份**接口的URI部分，您可以看到其请求方法为“POST”，则其请求为：

  ```
  POST https://agent-identity.cn-north-4.myhuaweicloud.com/v1/workload-identities
  ```

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”，有其他取值时会在具体接口中专门说明。
- **Authorization**：签名认证信息，可选，当使用AK/SK方式认证时，使用SDK对请求进行签名的过程中会自动填充该字段。AK/SK认证的详细说明请参见**AK/SK认证**。
- **X-Sdk-Date**：请求发送的时间，可选，当使用AK/SK方式认证时，使用SDK对请求进行签名的过程中会自动填充该字段。AK/SK认证的详细说明请参见**AK/SK认证**。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。
- **X-Project-ID**：子项目ID，可选，在多项目场景中使用。如果云服务资源创建在子项目中，AK/SK认证方式下，操作该资源的接口调用需要在请求消息头中携带X-Project-ID。
- **X-Domain-ID**：账号ID，可选。AK/SK认证方式下，全局服务的接口调用时，需在请求消息头中携带X-Domain-ID。

版权所有 © 华为云计算技术有限公司

对于**创建工作负载身份**接口，使用AK/SK方式认证时，添加消息头后的请求如下所示。

```
POST https://agent-identity.cn-north-4.myhuaweicloud.com/v1/workload-identities
Content-Type: application/json
X-Sdk-Date: 20260827T100000Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date, Signature=**********
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。如果请求消息体中参数值支持中文，则中文字符必须为UTF-8编码，并在Content-type中声明字符编码方式，例如：Content-Type: application/json; charset=utf-8。

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**创建工作负载身份**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，其中加粗的字段需要根据实际值填写。

- **name**为工作负载身份名称。
- **API_KEY**为入站验证方式。
- **22243eefff****为API Key的值，用于身份认证的密钥。
- **test-key-1**为API Key的名称，用于标识该Key。

```
POST https://agent-identity.cn-north-4.myhuaweicloud.com/v1/workload-identities
Content-Type: application/json
X-Sdk-Date: 20260827T100000Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date, Signature=**********

{
  "name": "name",
  "authorizer_type": "API_KEY",
  "authorizer_configuration": {
    "key_auth": {
      "api_keys": [
        {
          "api_key": "22243eefff**",
          "api_key_name": "test-key-1"
        }
      ]
    }
  }
}
```

到此为止，一个API请求所需要的内容已经准备完成，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。

3.2 认证鉴权

调用接口仅支持一种认证鉴权方式。

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

版权所有 © 华为云计算技术有限公司

AK/SK 认证

说明

AK/SK既可以使用永久访问密钥中的AK/SK，也可以使用临时访问密钥中的AK/SK，区别是临时访问密钥需要额外携带“X-Security-Token”Http Header头。

AK/SK签名认证方式仅支持消息体大小12M以内。

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**。

说明

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。

Java签名指导	**Go签名指导**	**Python签名指导**
C#签名指导	**JavaScript签名指导**	**PHP签名指导**
C++签名指导	**C签名指导**	**Android签名指导**

如果上述提供的签名SDK中没有你需要的开发语言，您可以基于**API的签名认证机制**，自己实现请求的签名。

签名示例

以下结合一个**Java Demo**来介绍如何对一个请求进行签名，并通过HTTP Client发送一个HTTPS请求的过程。如果您不使用Demo工程，也可以直接下载API网关签名工具在其他工程中引用。

1. 生成AK/SK。如果已生成过AK/SK，则可跳过此步骤，找到原来已下载的AK/SK文件，文件名一般为：credentials.csv。
   a. 登录**管理控制台**，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。
   b. 在左侧导航栏单击“访问密钥”，然后在页面中单击“新增访问密钥”。
   c. 在“新增访问密钥”弹窗的最下方，勾选理解上述建议的选项，然后单击“下一步”。
   d. 单击“确定”，访问密钥创建成功。
      - 在为账号用户创建访问密钥时，还需要进行身份验证，输入对应的验证码。
      - 如果开启了操作保护，在为IAM用户创建访问密钥时，也需要进行身份验证，输入对应的验证码。
   e. 单击“立即下载”，把访问密钥下载到本地。

版权所有 © 华为云计算技术有限公司

说明

为防止访问密钥泄露，建议您将其保存到安全的位置。

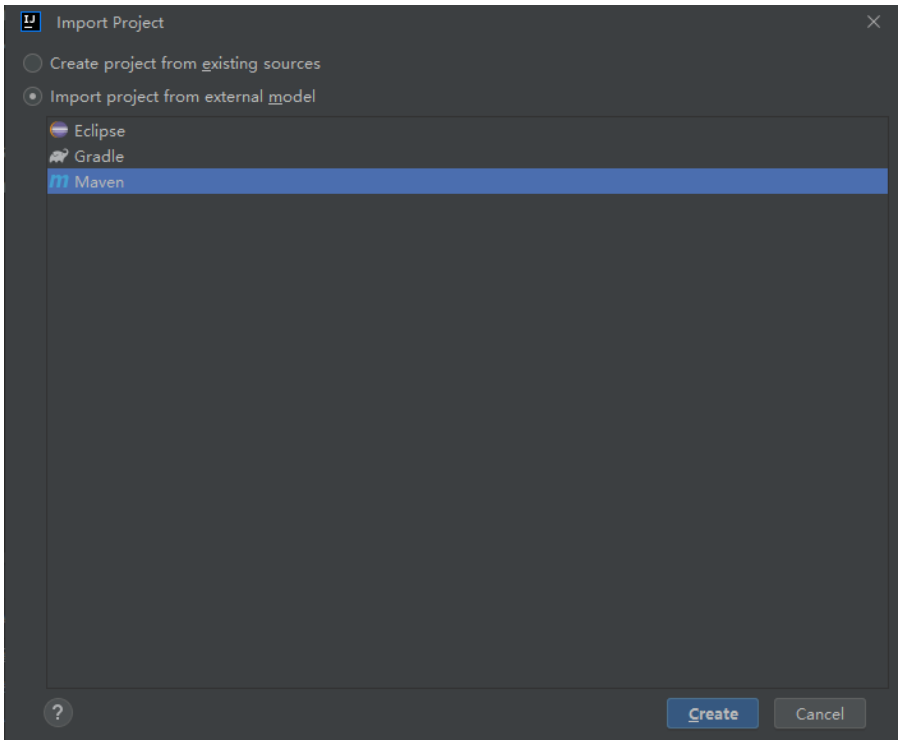
2. 把AK/SK设置为环境变量。

   本示例以Linux系统的操作为例，在本地环境将1中获取的AK/SK设置为环境变量

   a. 打开终端，执行以下命令编辑环境变量配置文件。
   ```
   vi ~/.bashrc
   ```
   b. 在文件中添加如下环境变量配置，然后保存文件并退出编辑器。
   ```
   export HUAWEICLOUD_SDK_AK="已获取的AK值"
   export HUAWEICLOUD_SDK_SK="已获取的SK值"
   ```
   c. 执行以下命令使配置文件生效。
   ```
   source ~/.bashrc
   ```
3. 获取示例代码，并解压缩。
4. 打开IDEA，在菜单栏选择“File > New > Project from Existing Sources”。

   选择解压后的“ApiGateway-java-sdk-*x.x.x*”文件夹，单击“OK”，导入示例工程。
5. 在“Import Project”页面，选择“Import project from external model”。

   选择“Maven”，最后单击“Create”。



6. IDEA支持在当前窗口或新窗口创建工程。此处，在弹窗中单击“New Window”。
7. 配置maven的settings.xml。

   a. 在profiles节点中添加如下内容：
   ```
   <profile>
       <id>MyProfile</id>
       <repositories>
           <repository>
               <id>HuaweiCloudSDK</id>
               <url>https://mirrors.huaweicloud.com/repository/maven/huaweicloudsdk/</url>
               <releases>
   ```

 版权所有 © 华为云计算技术有限公司

```
            <enabled>true</enabled>
        </releases>
        <snapshots>
            <enabled>false</enabled>
        </snapshots>
    </repository>
</repositories>
<pluginRepositories>
    <pluginRepository>
        <id>HuaweiCloudSDK</id>
        <url>https://mirrors.huaweicloud.com/repository/maven/huaweicloudsdk/</url>
        <releases>
            <enabled>true</enabled>
        </releases>
        <snapshots>
            <enabled>false</enabled>
        </snapshots>
    </pluginRepository>
</pluginRepositories>
</profile>
```

b. 在mirrors节点中增加：

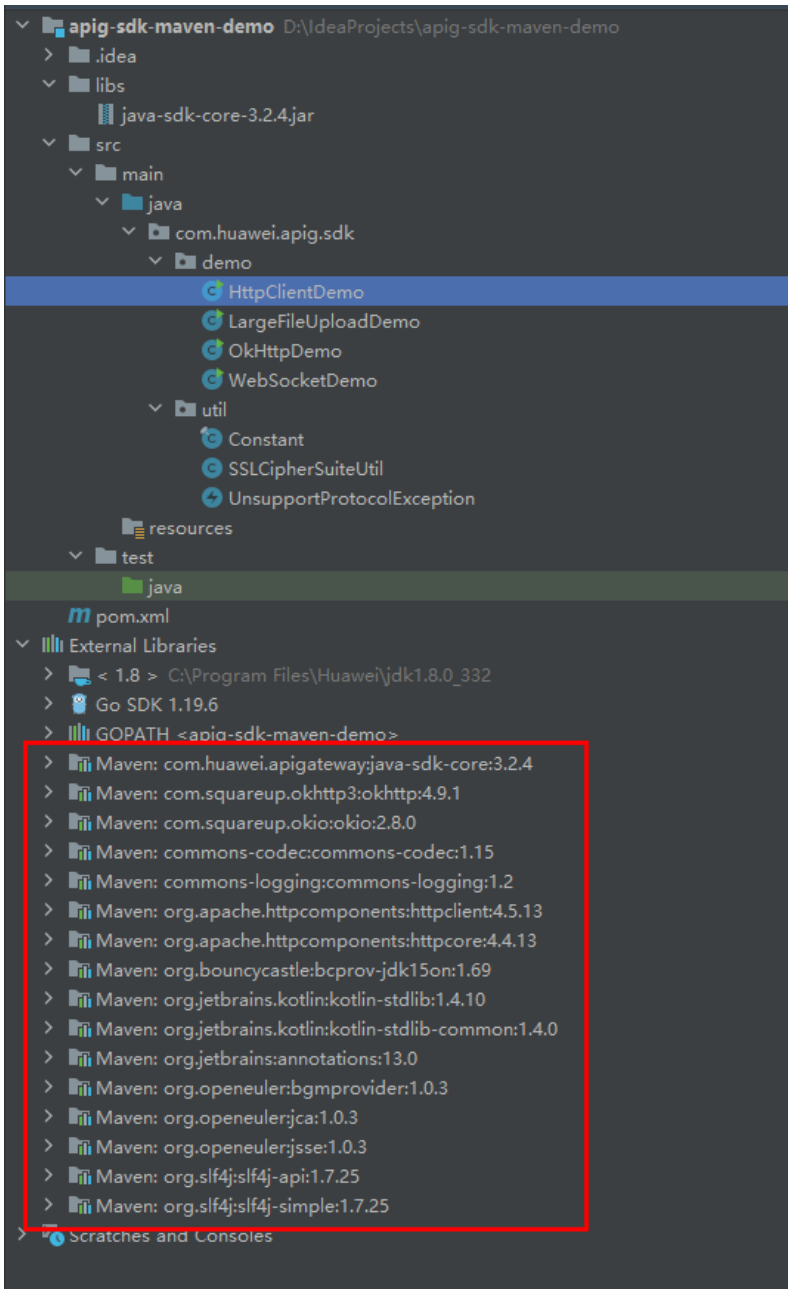
```
<mirror>
    <id>huaweicloud</id>
    <mirrorOf>*,!HuaweiCloudSDK</mirrorOf>
    <url>https://repo.huaweicloud.com/repository/maven/</url>
</mirror>
```

c. 增加activeProfiles标签激活配置：

```
<activeProfiles>
    <activeProfile>MyProfile</activeProfile>
</activeProfiles>
```

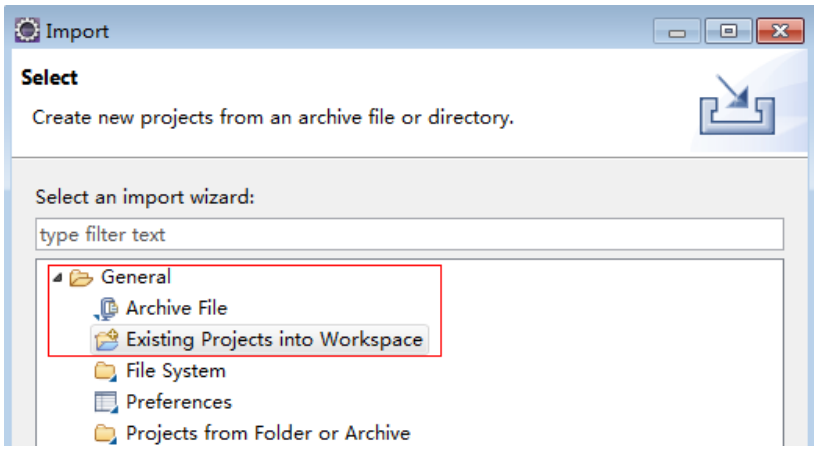
8. 下载Maven依赖，选择“pom.xml”并右键选择“Maven > Reload project”。

 版权所有 © 华为云计算技术有限公司

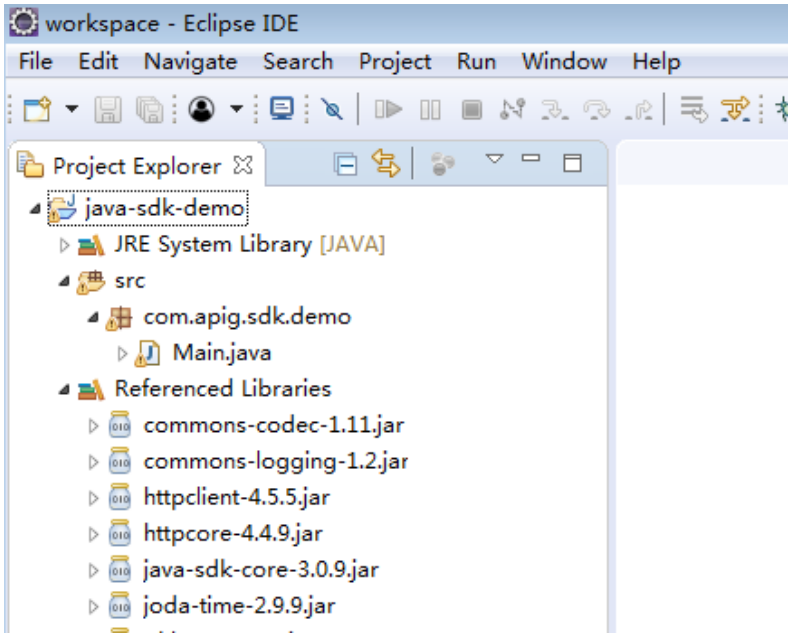


9. 打开Eclipse，在菜单栏选择“File > Import”，弹出“Import”对话框，选择“General > Existing Projects into Workspace”，选择解压后的“APIGW-java-sdk-*x.x.x*”文件夹。

 版权所有 © 华为云计算技术有限公司



10. 单击“Finish”，完成导入。导入后的示例工程如下所示。



11. 修改HttpClientDemo.java文件，把API信息和已设置的环境变量替换到对应位置。

    如下示例所示，加粗部分内容需要替换成实际值。

```
public class HttpClientDemo {
    private static final Logger LOGGER = LoggerFactory.getLogger(HttpClientDemo.class);
    public static void main(String[] args) throws Exception {
        // Create a new request.
        Request httpClientRequest = new Request();
        try {
            // HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK需替换为前面步骤中设置的环境变量值
            httpClientRequest.setKey(System.getenv("HUAWEICLOUD_SDK_AK"));
            httpClientRequest.setSecret(System.getenv("HUAWEICLOUD_SDK_SK"));
            // 设置API的请求方法
            httpClientRequest.setMethod("POST");
            // 设置API的请求路径，格式为https://{Endpoint}/{URI}
            httpClientRequest.setUrl("put your request url here");
            httpClientRequest.addHeader("Content-Type", "text/plain");
            // 设置API的请求Body体
            httpClientRequest.setBody("put your request body here");
        } catch (Exception e) {
            LOGGER.error(e.getMessage());
            return;
        }
```

 版权所有 © 华为云计算技术有限公司

```
        CloseableHttpClient client = null;
        try {
            // 对请求进行签名
            HttpRequestBase signedRequest = Client.sign(httpClientRequest,
Constant.SIGNATURE_ALGORITHM_SDK_HMAC_SHA256);
            if (Constant.DO_VERIFY) {
                // 创建httpClient并验证SSL证书
                HostName.setUrlHostName(httpClientRequest.getHost());
                client = (CloseableHttpClient)
SSLCipherSuiteUtil.createHttpClientWithVerify(Constant.INTERNATIONAL_PROTOCOL);
            } else {
                // 创建httpClient但不验证SSL证书
                client = (CloseableHttpClient)
SSLCipherSuiteUtil.createHttpClient(Constant.INTERNATIONAL_PROTOCOL);
            }
            HttpResponse response = client.execute(signedRequest);
            // 打印响应Body体信息
            HttpEntity resEntity = response.getEntity();
            if (resEntity != null) {
                String responseBody = EntityUtils.toString(resEntity, StandardCharsets.UTF_8);
                LOGGER.info("HTTP response body: {}", responseBody);
            }
        } catch (Exception e) {
            LOGGER.error(e.getMessage());
        } finally {
            if (client != null) {
                client.close();
            }
        }
    }
}
```

12. 运行HttpClientDemo.java，对请求进行签名、访问API并打印结果。

    显示**{"200": "sdk success"}**，表示签名成功，API请求成功发送到后端。

    如果改变AK或SK的值，API网关将返回的错误信息error_msg。

    您也可以通过这个视频教程了解AK/SK认证的使用：**https://bbs.huaweicloud.com/videos/100697**。

3.3 返回结果

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

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**创建工作负载身份**接口，如果调用后返回状态码为“201”，则表示请求成功。

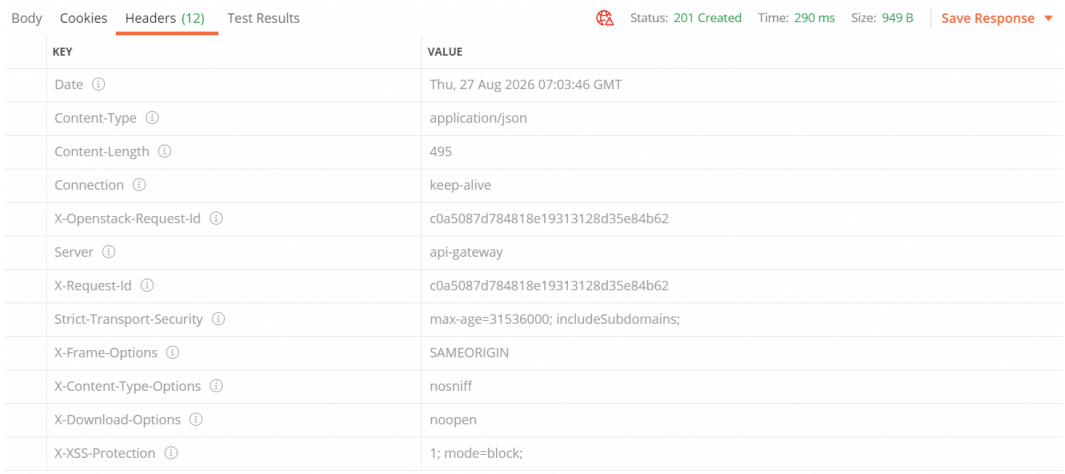
响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于**创建工作负载身份**接口，返回如**图1**所示的消息头。

版权所有 © 华为云计算技术有限公司

图 3-2 创建工作负载响应消息头



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**创建工作负载身份**接口，返回如下消息体。

```
{
  "workload_identity": {
    "workload_identity_id": "684a2c3e5f1b9d0e7a3c4f56",
    "name": "my_workload_identity",
    "urn": "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/default/
<workload-identity-name>",
    "authorizer_type": "CUSTOM_JWT",
    "allowed_resource_oauth2_return_urls": [
      "https://example.com/oauth2/callback"
    ],
    "created_by": {
      "type": "SERVICE",
      "identifier": "service.AgentRuntime"
    },
    "created_at": {},
    "updated_at": {},
    "tags": [
      {
        "key": "key-1",
        "value": "value-1"
      }
    ]
  }
}
```

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

```
{
    "error_code": "AgentIdentity.0027",
    "error_msg": "workload identity already exists",
    "request_id": "***"
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

版权所有 © 华为云计算技术有限公司

4 API

4.1 工作负载访问令牌

4.1.1 创建工作负载访问令牌（不以用户身份操作）

功能介绍

创建工作负载访问令牌（不以用户身份操作）。

URI

POST /v1/workload-access-token

请求参数

表 4-1 请求 Body 参数

参数	是否必选	参数类型	描述
workload_name	是	String	**参数解释**: 已注册工作负载的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

 版权所有 © 华为云计算技术有限公司

响应参数

状态码：200

表 4-2 响应 Body 参数

参数	参数类型	描述
workload_access_token	String	**参数解释**： 表示工作负载和用户（或仅工作负载，如果不以用户身份操作）身份的不透明令牌。 **取值范围**： 长度为1~131072个字符。
expiration	String	**参数解释**： 工作负载访问令牌的过期时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。

状态码：400

表 4-3 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：401

表 4-4 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

表 4-5 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-6 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：429

版权所有 © 华为云计算技术有限公司

表 4-7 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：500

表 4-8 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

创建工作负载访问令牌。

```
POST https://{endpoint}/v1/workload-access-token

{
  "workload_name" : "my-workload-01"
}
```

响应示例

状态码：200

```
{
  "workload_access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expiration" : "2025-12-31T23:59:59Z"
}
```

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。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.1.2 使用 JWT 创建工作负载访问令牌（以用户身份操作）

功能介绍

使用JWT令牌为以用户身份操作的代理工作负载获取工作负载访问令牌。

URI

POST /v1/workload-access-token-for-jwt

请求参数

表 4-9 请求 Body 参数

参数	是否必选	参数类型	描述
workload_name	是	String	**参数解释**： 已注册工作负载的唯一标识符。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。
user_token	是	String	**参数解释**： 用户身份提供商颁发的OAuth 2.0令牌。 **约束限制**： 不涉及。 **取值范围**： 符合JWT格式，长度为1~131072个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

版权所有 © 华为云计算技术有限公司

表 4-10 响应 Body 参数

参数	参数类型	描述
workload_access_token	String	**参数解释**: 表示工作负载和用户（或仅工作负载，如果不以用户身份操作）身份的不透明令牌。 **取值范围**: 长度为1~131072个字符。
expiration	String	**参数解释**: 工作负载访问令牌的过期时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。

状态码：400

表 4-11 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：401

版权所有 © 华为云计算技术有限公司

表 4-12 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-13 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-14 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

版权所有 © 华为云计算技术有限公司

表 4-15 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：500

表 4-16 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

使用JWT创建工作负载访问令牌。

```
POST https://{endpoint}/v1/workload-access-token-for-jwt

{
  "workload_name" : "my-workload-01",
  "user_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

响应示例

状态码：200

```
{
  "workload_access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expiration" : "2025-12-31T23:59:59Z"
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常或JWKS获取失败（无法获取或验证JWT签名密钥）。
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.1.3 使用用户 ID 创建工作负载访问令牌（以用户身份操作）

功能介绍

使用用户ID为以用户身份操作的代理工作负载获取工作负载访问令牌。

URI

POST /v1/workload-access-token-for-user-id

请求参数

表 4-17 请求 Body 参数

参数	是否必选	参数类型	描述
workload_name	是	String	**参数解释**： 已注册工作负载的唯一标识符。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。
user_id	是	String	**参数解释**： 要获取访问令牌的用户ID。 **约束限制**： 不涉及。 **取值范围**： 长度为1~128个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

版权所有 © 华为云计算技术有限公司

表 4-18 响应 Body 参数

参数	参数类型	描述
workload_access_token	String	**参数解释**： 表示工作负载和用户（或仅工作负载，如果不以用户身份操作）身份的不透明令牌。 **取值范围**： 长度为1~131072个字符。
expiration	String	**参数解释**： 工作负载访问令牌的过期时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。

状态码：400

表 4-19 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：401

版权所有 © 华为云计算技术有限公司

表 4-20 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-21 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-22 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

版权所有 © 华为云计算技术有限公司

表 4-23 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：500

表 4-24 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

使用用户ID创建工作负载访问令牌。

```
POST https://{endpoint}/v1/workload-access-token-for-user-id

{
  "workload_name" : "my-workload-01",
  "user_id" : "user-12345"
}
```

响应示例

状态码：200

```
{
  "workload_access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expiration" : "2025-12-31T23:59:59Z"
}
```

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。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

4.2 凭证提供商

版权所有 © 华为云计算技术有限公司

4.2.1 确认 OAuth 2.0 令牌的用户认证会话

功能介绍

确认用户认证会话以获取资源的OAuth2.0令牌。

URI

POST /v1/resource-token-auth/complete

请求参数

表 4-25 请求 Body 参数

参数	是否必选	参数类型	描述
session_uri	是	String	**参数解释**: 用户认证会话的唯一标识符（跟踪OAuth2流程状态）。 **约束限制**: 不涉及。 **取值范围**: 必须以"urn:ietf:params:oauth:request_uri:"开头，后面跟随字母、数字、"."、"-"、"_"、"~"组成的字符串，长度为1~1024个字符。 **默认取值**: 不涉及。
user_identifier	是	UserIdentifier object	**参数解释**: 用于生成工作负载访问令牌的OAuth2.0令牌或用户ID，只需要其中一个字段（user_token或user_id）。 **约束限制**: user_token和user_id二选一。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-26 UserIdentifier

参数	是否必选	参数类型	描述
user_token	否	String	**参数解释**: 用于用户身份识别的OAuth2.0令牌。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
user_id	否	String	**参数解释**: 用于用户身份识别的用户ID。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

响应参数

状态码：200

无

状态码：400

表 4-27 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：401

表 4-28 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-29 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-30 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

表 4-31 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：500

版权所有 © 华为云计算技术有限公司

表 4-32 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

确认OAuth2.0令牌的用户认证会话。

```
POST https://{endpoint}/v1/resource-token-auth/complete

{
  "session_uri" : "urn:ietf:params:oauth:request_uri:abc123",
  "user_identifier" : {
    "user_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
  }
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	请求体异常（包括无效RAR详情验证）。
401	认证失败。

版权所有 © 华为云计算技术有限公司

状态码	描述
403	没有操作权限（包括缺少RAR授予的细粒度权限）。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

4.2.2 获取与指定资源凭证提供者关联的 API 密钥

功能介绍

获取与指定资源凭证提供者关联的API密钥。

URI

POST /v1/api-key

请求参数

表 4-33 请求 Body 参数

参数	是否必选	参数类型	描述
resource_credential_provider_name	是	String	**参数解释**: 要获取API密钥的资源凭证提供者名称。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
workload_access_token	否	String	**参数解释**: 请求API密钥的工作负载身份令牌。 **约束限制**: 不涉及。 **取值范围**: 长度为1~131072个字符。 **默认取值**: 不涉及。

响应参数

状态码：200

表 4-34 响应 Body 参数

参数	参数类型	描述
api_key	String	**参数解释**: 与请求的资源关联的API密钥。 **取值范围**: 长度为1~65536个字符。

状态码：400

表 4-35 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：401

表 4-36 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-37 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-38 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

表 4-39 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：500

版权所有 © 华为云计算技术有限公司

表 4-40 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

从资源凭证提供商获取API密钥。

```
POST https://{endpoint}/v1/api-key

{
  "resource_credential_provider_name" : "my-apikey-provider",
  "workload_access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

响应示例

状态码：200

```
{
  "api_key" : "sk-example1234567890abcdef"
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

版权所有 © 华为云计算技术有限公司

状态码	描述
401	认证失败。
403	没有操作权限。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

4.2.3 从资源凭证提供商处获取 OAuth 2.0 令牌

功能介绍

使用配置的流程返回指定资源的OAuth2.0令牌。

URI

POST /v1/oauth2/token

请求参数

表 4-41 请求 Body 参数

参数	是否必选	参数类型	描述
custom_parameters	否	Map<String,String>	**参数解释**: 授权请求的附加自定义参数（不会覆盖标准OAuth2参数）。 **约束限制**: 不涉及。 **取值范围**: 键值对，每个值长度为1~2048个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
custom_state	否	String	**参数解释**： 用于CSRF保护的不透明字符串（在回调URL响应中作为标准state参数返回）。 **约束限制**： 不涉及。 **取值范围**： 长度为1~4096个字符。 **默认取值**： 不涉及。
force_authentication	否	Boolean	**参数解释**： 是否发起新的3LO流程，无论现有会话如何。 **约束限制**： 不涉及。 **取值范围**： ● true：发起新的3LO流程。 ● false：使用现有会话。 **默认取值**： false
oauth2_flow	是	String	**参数解释**： 要执行的OAuth2流程类型。 **约束限制**： 不涉及。 **取值范围**： ● USER_FEDERATION：用户联合流程 ● M2M：机器对机器流程 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
resource_credential_provider_name	是	String	**参数解释**: 资源的凭证提供者名称。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**: 不涉及。
resource_oauth2_return_url	否	String	**参数解释**: 令牌检索后重定向的回调URL（必须为工作负载身份配置）。 **约束限制**: 不涉及。 **取值范围**: 必须以协议开头，长度为1~2048个字符。 **默认取值**: 不涉及。
scopes	否	Array of strings	**参数解释**: 请求的OAuth作用域（粗粒度权限，由rich_authorization_details补充细粒度控制）。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[1,50]，每个值长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
session_uri	否	String	**参数解释**： 用户认证会话的唯一标识符（跟踪OAuth2流程状态）。 **约束限制**： 不涉及。 **取值范围**： 必须以"urn:ietf:params:oauth:request_uri:"开头，后面跟随字母、数字、"."、"-"、"_"、"~"组成的字符串，长度为1~1024个字符。 **默认取值**： 不涉及。
workload_access_token	否	String	**参数解释**： 请求OAuth2.0令牌的工作负载身份令牌。 **约束限制**： 不涉及。 **取值范围**： 长度为1~131072个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

表 4-42 响应 Body 参数

参数	参数类型	描述
access_token	String	**参数解释**： 要使用的OAuth2.0访问令牌（如果请求了rich_authorization_details，则嵌入RAR授权详情声明）。 **取值范围**： 长度为1~131072个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
authorization_url	String	**参数解释**： 发起授权的URL（当需要用户授权时提供，包含编码的RAR详情以供用户同意）。 **取值范围**： 长度至少为1个字符。
session_status	String	**参数解释**： 用户授权会话的状态（决定OAuth2流程中的下一步操作）。 **取值范围**： ● IN_PROGRESS：进行中 ● FAILED：失败
session_uri	String	**参数解释**： 用户认证会话的唯一标识符（与请求的session_uri匹配）。 **取值范围**： 必须以"urn:ietf:params:oauth:request_uri:"开头，后面跟随字母、数字、"."、"-"、"_"、"~"组成的字符串，长度为1~1024个字符。

状态码：400

表 4-43 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：401

表 4-44 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-45 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-46 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

表 4-47 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：500

版权所有 © 华为云计算技术有限公司

表 4-48 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

从资源凭证提供商获取OAuth2.0令牌。

```
POST https://{endpoint}/v1/oauth2/token

{
  "oauth2_flow" : "USER_FEDERATION",
  "resource_credential_provider_name" : "my-oauth2-provider",
  "resource_oauth2_return_url" : "https://example.com/callback",
  "session_uri" : "urn:ietf:params:oauth:request_uri:abc123"
}
```

响应示例

状态码：200

```
{
  "access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "session_status" : "IN_PROGRESS",
  "session_uri" : "urn:ietf:params:oauth:request_uri:abc123"
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
200	请求成功（如果请求了RAR声明，则令牌中嵌入RAR声明）。
400	请求体异常（包括无效RAR类型/操作/位置验证）。
401	认证失败。
403	没有操作权限（包括RAR细粒度授权失败）。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

错误码

请参见**错误码**。

4.2.4 从 STS 凭证提供商获取 STS 凭证

功能介绍

从指定的STS凭证提供商获取临时STS凭证。

URI

POST /v1/sts/token

请求参数

表 4-49 请求 Body 参数

参数	是否必选	参数类型	描述
resource_credential_provider_name	是	String	**参数解释**： 要获取STS凭证的STS凭证提供商名称。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
workload_access_token	否	String	**参数解释**: 请求STS令牌的工作负载身份令牌。 **约束限制**: 不涉及。 **取值范围**: 长度为1~131072个字符。 **默认取值**: 不涉及。
agency_session_name	是	String	**参数解释**: 被代理委托会话的标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由字母、数字及"+", "=", ",", ".", "@", "-"组成，长度为2~64个字符。 **默认取值**: 不涉及。
duration_seconds	否	Integer	**参数解释**: 委托会话的持续时间，单位为秒。 **约束限制**: 不涉及。 **取值范围**: 900~43200。 **默认取值**: 3600
policy	否	String	**参数解释**: 要用作内联会话策略的JSON格式IAM策略。 **约束限制**: 不涉及。 **取值范围**: 长度为2~2048个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
source_identity	否	String	**参数解释**: 调用操作的主体的源身份。 **约束限制**: 不涉及。 **取值范围**: 只能由字母、数字及"+", "=", ",", ".", "@", "-"组成，长度为2~64个字符。 **默认取值**: 不涉及。
tags	否	Array of **StsTag** objects	**参数解释**: 标签列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[0,20]。 **默认取值**: 不涉及。
transitive_tag_keys	否	Array of strings	**参数解释**: 要设置为可传递的会话标签键列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[0,20]，每个值不能以"_sys_"开头，长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-50 StsTag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签的键标识符或名称。 **约束限制**： 不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 与标签键关联的字符串值。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

表 4-51 响应 Body 参数

参数	参数类型	描述
source_identity	String	**参数解释**： 调用操作的主体的源身份。 **取值范围**： 只能由字母、数字及"+", "=", ",", ".", "@", "-"组成，长度为2~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
assumed_agency	**assumed_agency** object	**参数解释**: 包含被代理委托的信息。包含urn和id两个子参数。 **取值范围**: 不涉及。
credentials	**credentials** object	**参数解释**: 用于API认证的凭证。 **取值范围**: 不涉及。

表 4-52 assumed_agency

参数	参数类型	描述
urn	String	**参数解释**: 被代理委托的URN。 **取值范围**: 长度最大为1500个字符。
id	String	**参数解释**: 包含委托ID和委托会话名称的唯一标识符。 **取值范围**: 只能由字母、数字及"+", "=", ",", ".", ":", "@", "-"组成，长度最大为256个字符。

表 4-53 credentials

参数	参数类型	描述
access_key_id	String	**参数解释**: 标识临时安全凭证的访问密钥ID。 **取值范围**: 长度为20个字符。
expiration	String	**参数解释**: 当前凭证过期的日期和时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
secret_access_key	String	**参数解释**: 可用于签署请求的秘密访问密钥。 **取值范围**: 长度为40个字符。
security_token	String	**参数解释**: 用户必须传递给服务API以使用临时凭证的令牌。 **取值范围**: 不涉及。

状态码：400

表 4-54 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：401

版权所有 © 华为云计算技术有限公司

表 4-55 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-56 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-57 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

版权所有 © 华为云计算技术有限公司

表 4-58 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：500

表 4-59 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

从STS凭证提供商获取STS凭证。

```
POST https://{endpoint}/v1/sts/token

{
  "resource_credential_provider_name" : "my-sts-provider",
  "agency_session_name" : "my-session",
  "workload_access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

响应示例

状态码：200

```
{
  "assumed_agency" : {
    "urn" : "urn:iam::12345678901234567890:agency:my-agency",
    "id" : "agency-id-session-name"
  },
  "credentials" : {
    "access_key_id" : "AKIAIOSFODNN7EXAMPLE",
    "secret_access_key" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "security_token" : "FwoGZXIvYXdzEBYaDH...",
    "expiration" : "2025-12-31T23:59:59Z"
  }
}
```

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。
404	未找到相应的资源。
429	请求过于频繁。
500	服务端异常。

版权所有 © 华为云计算技术有限公司

错误码

请参见**错误码**。

4.3 OAuth2.0 流程

4.3.1 OAuth 2.0 推送授权请求（PAR）标准的授权 API

功能介绍

遵循RFC 9126 PAR规范的核心OAuth2授权端点，仅通过request_uri参数接受授权请求以触发用户授权流程。

URI

GET /v1/oauth2/authorize

表 4-60 Query 参数

参数	是否必选	参数类型	描述
request_uri	是	String	**参数解释**： OAuth 2.0 PAR标准请求URI，引用OAuth2流程的授权参数。 **约束限制**： 不涉及。 **取值范围**： 必须以"urn:ietf:params:oauth:request_uri:"开头，后面跟随字母、数字、"."、"-"、"_"、"~"组成的字符串，长度为1~1024个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-61 响应 Body 参数

参数	参数类型	描述
error	String	**参数解释**： OAuth 2.0标准错误码，例如access_denied、invalid_request、invalid_client、unauthorized_client。 **取值范围**： 长度为1~128个字符。
error_description	String	**参数解释**： 人类可读的错误描述，URL编码以安全传输。 **取值范围**： 长度为1~2048个字符。

状态码：404

表 4-62 响应 Body 参数

参数	参数类型	描述
error	String	**参数解释**： OAuth 2.0标准错误码，例如access_denied、invalid_request、invalid_client、unauthorized_client。 **取值范围**： 长度为1~128个字符。
error_description	String	**参数解释**： 人类可读的错误描述，URL编码以安全传输。 **取值范围**： 长度为1~2048个字符。

状态码：500

版权所有 © 华为云计算技术有限公司

表 4-63 响应 Body 参数

参数	参数类型	描述
error	String	**参数解释**: OAuth 2.0标准错误码，例如access_denied、invalid_request、invalid_client、unauthorized_client。 **取值范围**: 长度为1~128个字符。
error_description	String	**参数解释**: 人类可读的错误描述，URL编码以安全传输。 **取值范围**: 长度为1~2048个字符。

请求示例

无

响应示例

无

状态码

状态码	描述
302	授权流程发起成功 - 通过Location头重定向到用户同意页面
400	OAuth2无效请求 - request_uri格式无效、授权请求已过期或参数格式错误
404	OAuth2无效请求 - 提供的request_uri未找到授权请求（无匹配的PAR注册）
500	OAuth2服务器错误 - OAuth2流程服务临时问题，无法处理授权请求

错误码

请参见**错误码**。

4.3.2 OAuth 2.0 标准授权回调 API

功能介绍

OAuth2重定向回调端点，用于在用户同意/拒绝后接收授权结果。

版权所有 © 华为云计算技术有限公司

URI

GET /v1/oauth2/callback/{credential_provider_id}

表 4-64 路径参数

参数	是否必选	参数类型	描述
credential_provider_id	是	String	**参数解释**: 凭证提供商的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: UUID格式。 **默认取值**: 不涉及。

表 4-65 Query 参数

参数	是否必选	参数类型	描述
code	否	String	**参数解释**: OAuth2.0标准授权码 - 一次性使用、短期有效的令牌，用于交换访问令牌。仅在授权成功时存在。 **约束限制**: 不涉及。 **取值范围**: 长度为1~8192个字符。 **默认取值**: 不涉及。
state	是	String	**参数解释**: OAuth2.0标准CSRF保护状态 - 不透明字符串，原始请求状态的回显。成功和错误时都存在。 **约束限制**: 不涉及。 **取值范围**: 长度为1~4096个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
error	否	String	**参数解释**: OAuth2.0标准错误码 - 仅在授权失败（拒绝/过期/无效）时存在。例如：access_denied、invalid_scope、server_error。 **约束限制**: 不涉及。 **取值范围**: 长度为1~128个字符。 **默认取值**: 不涉及。
error_description	否	String	**参数解释**: OAuth2.0标准错误描述 - 人类可读的错误信息，与error参数配对，URL编码以安全传输。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

无

请求示例

无

响应示例

无

版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
302	始终重定向到预配置的资源oauth2_return_url，并在查询参数中携带授权结果（成功：code+state	错误：error+error_description+state）

错误码

请参见**错误码**。

4.4 API 密钥凭证提供商

4.4.1 创建 API 密钥凭证提供商

功能介绍

创建一个新的API密钥凭证提供商。

URI

POST /v1/api-key-credential-providers

请求参数

表 4-66 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
api_key	是	String	**参数解释**： 用于与外部提供者进行身份验证的API密钥。 **约束限制**： 不涉及。 **取值范围**： 不能以空格开头或结尾，长度为1~4096个字符。 **默认取值**： 不涉及。
tags	否	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **约束限制**： 列表最多20个标签。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

表 4-67 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：201

表 4-68 响应 Body 参数

参数	参数类型	描述
credential_provider	**ApiKeyCredentialProvider** object	**参数解释**： API Key凭证提供商，用于配置通过API密钥进行身份验证的参数。 **取值范围**： 不涉及。

表 4-69 ApiKeyCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
api_key_secret	**Secret** object	**参数解释**： 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-70 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-71 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-72 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-73 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

表 4-74 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

创建API密钥凭证提供商。

```
POST https://{endpoint}/v1/api-key-credential-providers

{
  "name" : "my_apikeyprovider",
  "api_key" : "sk-example1234567890abcdef",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
```


版权所有 © 华为云计算技术有限公司

```
  } ]
}
```

响应示例

状态码：201

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_apikeyprovider",
    "urn" : "agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "api_key_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```

状态码

状态码	描述
201	请求成功。
400	请求体无效。
403	没有操作权限。
409	请求冲突。

错误码

请参见**错误码**。

4.4.2 查询 API 密钥凭证提供商列表

功能介绍

查询当前账号下的API密钥凭证提供商列表。支持分页查询，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/api-key-credential-providers

版权所有 © 华为云计算技术有限公司

表 4-75 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**: 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**: 不涉及。 **取值范围**: 1~200。 **默认取值**: 100。
marker	否	String	**参数解释**: 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：200

表 4-76 响应 Body 参数

参数	参数类型	描述
credential_providers	Array of **ApiKeyCredentialProviderSummary** objects	**参数解释**: API Key凭证提供商摘要信息。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-77 ApiKeyCredentialProviderSummary

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-78 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

版权所有 © 华为云计算技术有限公司

表 4-79 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**: 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**: 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**: 本页返回的条目数量。 **取值范围**: 不涉及。

状态码：400

表 4-80 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求示例

- 查询API密钥凭证提供商列表。

  ```
  GET https://{endpoint}/v1/api-key-credential-providers
  ```

- 分页查询API密钥凭证提供商列表。

  ```
  GET https://{endpoint}/v1/api-key-credential-providers?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "credential_providers" : [ {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_apikeyprovider_1",
    "urn" : "agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }, {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f57",
    "name" : "my_apikeyprovider_2",
    "urn" : "agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "tags" : [ {
      "key" : "key-2",
      "value" : "value-2"
    } ]
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "marker"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

错误码

请参见**错误码**。

4.4.3 查询 API 密钥凭证提供商详情

功能介绍

查询API密钥凭证提供商详情。

版权所有 © 华为云计算技术有限公司

URI

GET /v1/api-key-credential-providers/{credential_provider_name}

表 4-81 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：200

表 4-82 响应 Body 参数

参数	参数类型	描述
credential_provider	**ApiKeyCredentialProvider** object	**参数解释**: API Key凭证提供商，用于配置通过API密钥进行身份验证的参数。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-83 ApiKeyCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**: 凭证提供商的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**: 凭证提供商的唯一资源名称（URN）。 **取值范围**: 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
api_key_secret	**Secret** object	**参数解释**: 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**: 不涉及。
created_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-84 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-85 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-86 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-87 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

查询API密钥凭证提供商详情。

```
GET https://{endpoint}/v1/api-key-credential-providers/{credential_provider_name}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_apikeyprovider",
    "urn" : "agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "api_key_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.4.4 更新 API 密钥凭证提供商

功能介绍

更新指定API密钥凭证提供商的API密钥。

URI

PUT /v1/api-key-credential-providers/{credential_provider_name}

表 4-88 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

表 4-89 请求 Body 参数

参数	是否必选	参数类型	描述
api_key	否	String	**参数解释**: 更新后的API密钥。 **约束限制**: 不涉及。 **取值范围**: 不能以空格开头或结尾，长度为1~4096个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-90 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**: 标签键，用于标识标签的名称。 **约束限制**: 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**: 不涉及。
value	是	String	**参数解释**: 标签值，用于标识标签的具体内容。 **约束限制**: 不涉及。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

响应参数

状态码：200

表 4-91 响应 Body 参数

参数	参数类型	描述
credential_provider	**ApiKeyCredentialProvider** object	**参数解释**： API Key凭证提供商，用于配置通过API密钥进行身份验证的参数。 **取值范围**： 不涉及。

表 4-92 ApiKeyCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
api_key_secret	**Secret** object	**参数解释**： 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-93 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

表 4-94 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-95 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：404

表 4-96 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

表 4-97 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

更新API密钥凭证提供商的API密钥。

```
PUT https://{endpoint}/v1/api-key-credential-providers/{credential_provider_name}

{
  "api_key" : "sk-example1234567890abcdef"
}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_idapi_key_credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_apikeyprovider",
    "urn" : "agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "api_key_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-04 14:13:20",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

版权所有 © 华为云计算技术有限公司

状态码	描述
409	请求冲突。

错误码

请参见**错误码**。

4.4.5 删除 API 密钥凭证提供商

功能介绍

删除指定的API密钥凭证提供商。

URI

DELETE /v1/api-key-credential-providers/{credential_provider_name}

表 4-98 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：204

无

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-99 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-100 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

删除API密钥凭证提供商。

```
DELETE https://{endpoint}/v1/api-key-credential-providers/{credential_provider_name}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.5 OAuth2 凭证提供商

4.5.1 创建 OAuth2 凭证提供商

功能介绍

创建一个新的OAuth2凭证提供商。

URI

POST /v1/oauth2-credential-providers

版权所有 © 华为云计算技术有限公司

请求参数

表 4-101 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。
credential_provider_vendor	是	String	**参数解释**： 支持的OAuth2提供商类型。 **约束限制**： 不涉及。 **取值范围**： ● MicrosoftOauth2：微软OAuth2 ● GoogleOauth2：谷歌OAuth2 ● GithubOauth2：GitHub OAuth2 ● CustomOauth2：自定义OAuth2 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
oauth2_provider_config_input	是	**Oauth2ProviderConfigInput** object	**参数解释**: OAuth2提供商配置输入（UNION类型）。 **约束限制**: 只能指定以下一种配置：microsoft_oauth2_provider_config、google_oauth2_provider_config、github_oauth2_provider_config或custom_oauth2_provider_config。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-102 Oauth2ProviderConfigInput

参数	是否必选	参数类型	描述
microsoft_oauth2_provider_config	否	**MicrosoftOauth2ProviderConfigInput** object	**参数解释**: Microsoft OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
google_oauth2_provider_config	否	**GoogleOauth2ProviderConfigInput** object	**参数解释**: Google OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
github_oauth2_provider_config	否	**GithubOauth2ProviderConfigInput** object	**参数解释**: GitHub OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
custom_oauth2_provider_config	否	**CustomOauth2ProviderConfigInput** object	**参数解释**: 自定义OAuth2提供商的输入配置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-103 MicrosoftOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。
tenant_id	是	String	**参数解释**: Microsoft OAuth2提供商的租户ID（Tenant ID），用于标识Microsoft OAuth2认证的租户。 **约束限制**: 不涉及。 **取值范围**: 可取值common、organizations、consumers，或符合UUID格式的租户ID，或由英文字母、数字及"."、"_"、"-"组成，长度为1~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-104 GoogleOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

表 4-105 GithubOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

表 4-106 CustomOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
oauth2_discovery	是	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **约束限制**: discovery_url和authorization_server_metadata二选一。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-107 Oauth2Discovery

参数	是否必选	参数类型	描述
discovery_url	否	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。 **默认取值**: 不涉及。
authorization_server_metadata	否	**Oauth2AuthorizationServerMetadata** object	**参数解释**: OAuth2提供商的授权服务器元数据。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-108 Oauth2AuthorizationServerMetadata

参数	是否必选	参数类型	描述
authorization_endpoint	是	String	**参数解释**: 授权服务器的授权端点。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
issuer	是	String	**参数解释**: 授权服务器的签发者标识。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
token_endpoint	是	String	**参数解释**: 授权服务器的令牌端点。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
response_types	否	Array of strings	**参数解释**: 支持的响应类型列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[1,20]，每个元素为1~50个字符的字符串。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
token_endpoint_auth_methods	否	Array of strings	**参数解释**: 令牌端点支持的客户端认证方法列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[1,2]。 **默认取值**: 不涉及。

表 4-109 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**: 标签键，用于标识标签的名称。 **约束限制**: 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**: 不涉及。
value	是	String	**参数解释**: 标签值，用于标识标签的具体内容。 **约束限制**: 不涉及。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

响应参数

状态码：201

表 4-110 响应 Body 参数

参数	参数类型	描述
credential_provider	**Oauth2CredentialProvider** object	**参数解释**： OAuth2凭证提供商，用于配置通过OAuth2协议获取外部服务访问凭证的参数。 **取值范围**： 不涉及。

表 4-111 Oauth2CredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
credential_provider_vendor	String	**参数解释**： 支持的OAuth2提供商类型。 **取值范围**： • MicrosoftOauth2：微软OAuth2 • GoogleOauth2：谷歌OAuth2 • GithubOauth2：GitHub OAuth2 • CustomOauth2：自定义OAuth2

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
client_secret	**Secret** object	**参数解释**: 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**: 不涉及。
callback_url	String	**参数解释**: OAuth2 提供方认证完成后跳转回调的URL。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
created_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
oauth2_provider_config_output	**Oauth2ProviderConfigOutput** object	**参数解释**: OAuth2提供商配置输出（UNION类型）。 **取值范围**: 不涉及。
tags	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-112 Secret

参数	参数类型	描述
secret_id	String	**参数解释**: 凭证ID，唯一标识CSMS中的凭证。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**: 凭证名称，CSMS中存储的凭证名称。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-113 Oauth2ProviderConfigOutput

参数	参数类型	描述
microsoft_oauth2_provider_config	**MicrosoftOauth2ProviderConfigOutput** object	**参数解释**: Microsoft OAuth2提供商的输出配置。 **取值范围**: 不涉及。
google_oauth2_provider_config	**GoogleOauth2ProviderConfigOutput** object	**参数解释**: Google OAuth2提供商的输出配置。 **取值范围**: 不涉及。
github_oauth2_provider_config	**GithubOauth2ProviderConfigOutput** object	**参数解释**: GitHub OAuth2提供商的输出配置。 **取值范围**: 不涉及。
custom_oauth2_provider_config	**CustomOauth2ProviderConfigOutput** object	**参数解释**: 自定义OAuth2提供商的输出配置。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-114 MicrosoftOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-115 GoogleOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-116 GithubOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-117 CustomOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-118 Oauth2Discovery

参数	参数类型	描述
discovery_url	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。
authorization_server_metadata	**Oauth2AuthorizationServerMetadata** object	**参数解释**: OAuth2提供商的授权服务器元数据。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-119 Oauth2AuthorizationServerMetadata

参数	参数类型	描述
authorization_endpoint	String	**参数解释**: 授权服务器的授权端点。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
issuer	String	**参数解释**: 授权服务器的签发者标识。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
token_endpoint	String	**参数解释**: 授权服务器的令牌端点。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
response_types	Array of strings	**参数解释**: 支持的响应类型列表。 **取值范围**: 数组长度范围[1,20]，每个元素为1~50个字符的字符串。
token_endpoint_auth_methods	Array of strings	**参数解释**: 令牌端点支持的客户端认证方法列表。 **取值范围**: 数组长度范围[1,2]。

表 4-120 Tag

参数	参数类型	描述
key	String	**参数解释**: 标签键，用于标识标签的名称。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-121 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-122 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

表 4-123 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

表 4-124 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

创建Microsoft OAuth2凭证提供商。

```
POST https://{endpoint}/v1/oauth2-credential-providers

{
  "name" : "my_microsoft_oauthprovider",
  "credential_provider_vendor" : "MicrosoftOauth2",
  "oauth2_provider_config_input" : {
    "microsoft_oauth2_provider_config" : {
      "client_id" : "285624f5-5958-4f36-b171-168303615bce",
      "client_secret" : "28365081388-oovo6094eg8opo187jn0mstj8s2cevku",
```


版权所有 © 华为云计算技术有限公司

```
    "tenant_id" : "285624f5-5958-4f36-b171-168303615bce"
   }
  },
  "tags" : [ {
   "key" : "key-1",
   "value" : "value-1"
  } ]
}
```

响应示例

状态码：201

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_microsoft_oauthprovider",
    "urn" : "agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "credential_provider_vendor" : "MicrosoftOauth2",
    "client_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "callback_url" : "https://agent-identity.cn-north-4.myhuaweicloud.com/v1/oauth2/callback/
9c38be75-5973-4709-a211-7e2c438c250d",
    "oauth2_provider_config_output" : {
      "microsoft_oauth2_provider_config" : {
        "oauth2_discovery" : {
          "discovery_url" : "https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration",
          "authorization_server_metadata" : null
        },
        "client_id" : "285624f5-5958-4f36-b171-168303615bce"
      },
      "google_oauth2_provider_config" : null,
      "github_oauth2_provider_config" : null,
      "custom_oauth2_provider_config" : null
    },
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-04 14:13:20",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```

状态码

状态码	描述
201	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。
429	请求过于频繁。

 版权所有 © 华为云计算技术有限公司

错误码

请参见**错误码**。

4.5.2 查询 OAuth2 凭证提供商列表

功能介绍

查询当前账号下的OAuth2凭证提供商列表。支持分页查询，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/oauth2-credential-providers

表 4-125 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**： 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**： 不涉及。 **取值范围**： 1~200。 **默认取值**： 100。
marker	否	String	**参数解释**： 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**： 不涉及。

请求参数

无

版权所有 © 华为云计算技术有限公司

响应参数

状态码：200

表 4-126 响应 Body 参数

参数	参数类型	描述
credential_providers	Array of **Oauth2CredentialProviderSummary** objects	**参数解释**： OAuth2凭证提供商摘要信息。 **取值范围**： 不涉及。
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-127 Oauth2CredentialProviderSummary

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
credential_provider_vendor	String	**参数解释**： 支持的OAuth2提供商类型。 **取值范围**： ● MicrosoftOauth2：微软OAuth2 ● GoogleOauth2：谷歌OAuth2 ● GithubOauth2：GitHub OAuth2 ● CustomOauth2：自定义OAuth2
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-128 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

表 4-129 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

表 4-130 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

- 查询OAuth2凭证提供商列表。

  ```
  GET https://{endpoint}/v1/oauth2-credential-providers
  ```

- 分页查询OAuth2凭证提供商列表。

  ```
  GET https://{endpoint}/v1/oauth2-credential-providers?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "credential_providers" : [ {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_microsoft_oauthprovider",
    "urn" : "agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "credential_provider_vendor" : "MicrosoftOauth2",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : "marker"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

版权所有 © 华为云计算技术有限公司

错误码

请参见**错误码**。

4.5.3 查询 OAuth2 凭证提供商详情

功能介绍

查询OAuth2凭证提供商详情。

URI

GET /v1/oauth2-credential-providers/{credential_provider_name}

表 4-131 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：200

表 4-132 响应 Body 参数

参数	参数类型	描述
credential_provider	**Oauth2CredentialProvider** object	**参数解释**: OAuth2凭证提供商，用于配置通过OAuth2协议获取外部服务访问凭证的参数。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-133 Oauth2CredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**: 凭证提供商的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**: 凭证提供商的唯一资源名称（URN）。 **取值范围**: 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
credential_provider_vendor	String	**参数解释**: 支持的OAuth2提供商类型。 **取值范围**: ● MicrosoftOauth2：微软OAuth2 ● GoogleOauth2：谷歌OAuth2 ● GithubOauth2：GitHub OAuth2 ● CustomOauth2：自定义OAuth2
client_secret	**Secret** object	**参数解释**: 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**: 不涉及。
callback_url	String	**参数解释**: OAuth2 提供方认证完成后跳转回调的URL。 **取值范围**: 必须以https://开头，长度为1~2048个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
oauth2_provider_config_output	**Oauth2ProviderConfigOutput** object	**参数解释**： OAuth2提供商配置输出（UNION类型）。 **取值范围**： 不涉及。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-134 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

表 4-135 Oauth2ProviderConfigOutput

参数	参数类型	描述
microsoft_oauth2_provider_config	**MicrosoftOauth2ProviderConfigOutput** object	**参数解释**: Microsoft OAuth2提供商的输出配置。 **取值范围**: 不涉及。
google_oauth2_provider_config	**GoogleOauth2ProviderConfigOutput** object	**参数解释**: Google OAuth2提供商的输出配置。 **取值范围**: 不涉及。
github_oauth2_provider_config	**GithubOauth2ProviderConfigOutput** object	**参数解释**: GitHub OAuth2提供商的输出配置。 **取值范围**: 不涉及。
custom_oauth2_provider_config	**CustomOauth2ProviderConfigOutput** object	**参数解释**: 自定义OAuth2提供商的输出配置。 **取值范围**: 不涉及。

表 4-136 MicrosoftOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

版权所有 © 华为云计算技术有限公司

表 4-137 GoogleOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-138 GithubOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-139 CustomOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
client_id	String	**参数解释**： OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**： 长度为1~256个字符。

表 4-140 Oauth2Discovery

参数	参数类型	描述
discovery_url	String	**参数解释**： OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **取值范围**： 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。
authorization_server_metadata	**Oauth2AuthorizationServerMetadata** object	**参数解释**： OAuth2提供商的授权服务器元数据。 **取值范围**： 不涉及。

表 4-141 Oauth2AuthorizationServerMetadata

参数	参数类型	描述
authorization_endpoint	String	**参数解释**： 授权服务器的授权端点。 **取值范围**： 必须以https://开头，长度为1~2048个字符。
issuer	String	**参数解释**： 授权服务器的签发者标识。 **取值范围**： 必须以https://开头，长度为1~2048个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
token_endpoint	String	**参数解释**： 授权服务器的令牌端点。 **取值范围**： 必须以https://开头，长度为1~2048个字符。
response_types	Array of strings	**参数解释**： 支持的响应类型列表。 **取值范围**： 数组长度范围[1,20]，每个元素为1~50个字符的字符串。
token_endpoint_auth_methods	Array of strings	**参数解释**： 令牌端点支持的客户端认证方法列表。 **取值范围**： 数组长度范围[1,2]。

表 4-142 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-143 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-144 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

查询OAuth2凭证提供商详情。

```
GET https://{endpoint}/v1/oauth2-credential-providers/{credential_provider_name}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_microsoft_oauthprovider",
    "urn" : "agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "credential_provider_vendor" : "MicrosoftOauth2",
    "client_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "callback_url" : "https://agent-identity.cn-north-4.myhuaweicloud.com/v1/oauth2/callback/
9c38be75-5973-4709-a211-7e2c438c250d",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "oauth2_provider_config_output" : {
      "microsoft_oauth2_provider_config" : {
        "oauth2_discovery" : {
          "discovery_url" : "https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration",
          "authorization_server_metadata" : null
        },
        "client_id" : "285624f5-5958-4f36-b171-168303615bce"
      },
      "google_oauth2_provider_config" : null,
      "github_oauth2_provider_config" : null,
      "custom_oauth2_provider_config" : null
    }
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

版权所有 © 华为云计算技术有限公司

错误码

请参见**错误码**。

4.5.4 更新 OAuth2 凭证提供商

功能介绍

更新指定的OAuth2凭证提供商。

URI

PUT /v1/oauth2-credential-providers/{credential_provider_name}

表 4-145 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-146 请求 Body 参数

参数	是否必选	参数类型	描述
oauth2_provider_config_input	否	**Oauth2ProviderConfigInput** object	**参数解释**: OAuth2提供商配置输入（UNION类型）。 **约束限制**: 只能指定以下一种配置：microsoft_oauth2_provider_config、google_oauth2_provider_config、github_oauth2_provider_config或custom_oauth2_provider_config。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-147 Oauth2ProviderConfigInput

参数	是否必选	参数类型	描述
microsoft_oauth2_provider_config	否	**MicrosoftOauth2ProviderConfigInput** object	**参数解释**: Microsoft OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
google_oauth2_provider_config	否	**GoogleOauth2ProviderConfigInput** object	**参数解释**: Google OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
github_oauth2_provider_config	否	**GithubOauth2ProviderConfigInput** object	**参数解释**: GitHub OAuth2提供商集成的配置设置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
custom_oauth2_provider_config	否	**CustomOauth2ProviderConfigInput** object	**参数解释**: 自定义OAuth2提供商的输入配置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-148 MicrosoftOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。
tenant_id	是	String	**参数解释**: Microsoft OAuth2提供商的租户ID（Tenant ID），用于标识Microsoft OAuth2认证的租户。 **约束限制**: 不涉及。 **取值范围**: 可取值common、organizations、consumers，或符合UUID格式的租户ID，或由英文字母、数字及"."、"_"、"-"组成，长度为1~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-149 GoogleOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

表 4-150 GithubOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

表 4-151 CustomOauth2ProviderConfigInput

参数	是否必选	参数类型	描述
client_id	是	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **约束限制**: 不涉及。 **取值范围**: 长度为1~256个字符。 **默认取值**: 不涉及。
client_secret	是	String	**参数解释**: OAuth2应用的客户端密钥（Client Secret），用于OAuth2认证流程中的应用身份验证。 **约束限制**: 不涉及。 **取值范围**: 长度为1~2048个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
oauth2_discovery	是	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **约束限制**: discovery_url和authorization_server_metadata二选一。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-152 Oauth2Discovery

参数	是否必选	参数类型	描述
discovery_url	否	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。 **默认取值**: 不涉及。
authorization_server_metadata	否	**Oauth2AuthorizationServerMetadata** object	**参数解释**: OAuth2提供商的授权服务器元数据。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-153 Oauth2AuthorizationServerMetadata

参数	是否必选	参数类型	描述
authorization_endpoint	是	String	**参数解释**: 授权服务器的授权端点。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
issuer	是	String	**参数解释**: 授权服务器的签发者标识。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
token_endpoint	是	String	**参数解释**: 授权服务器的令牌端点。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，长度为1~2048个字符。 **默认取值**: 不涉及。
response_types	否	Array of strings	**参数解释**: 支持的响应类型列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[1,20]，每个元素为1~50个字符的字符串。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
token_endpoint_auth_methods	否	Array of strings	**参数解释**: 令牌端点支持的客户端认证方法列表。 **约束限制**: 不涉及。 **取值范围**: 数组长度范围[1,2]。 **默认取值**: 不涉及。

表 4-154 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**: 标签键，用于标识标签的名称。 **约束限制**: 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**: 不涉及。
value	是	String	**参数解释**: 标签值，用于标识标签的具体内容。 **约束限制**: 不涉及。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

响应参数

状态码：200

表 4-155 响应 Body 参数

参数	参数类型	描述
credential_provider	**Oauth2CredentialProvider** object	**参数解释**： OAuth2凭证提供商，用于配置通过OAuth2协议获取外部服务访问凭证的参数。 **取值范围**： 不涉及。

表 4-156 Oauth2CredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
credential_provider_vendor	String	**参数解释**： 支持的OAuth2提供商类型。 **取值范围**： • MicrosoftOauth2：微软OAuth2 • GoogleOauth2：谷歌OAuth2 • GithubOauth2：GitHub OAuth2 • CustomOauth2：自定义OAuth2

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
client_secret	**Secret** object	**参数解释**: 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**: 不涉及。
callback_url	String	**参数解释**: OAuth2 提供方认证完成后跳转回调的URL。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
created_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
oauth2_provider_config_output	**Oauth2ProviderConfigOutput** object	**参数解释**: OAuth2提供商配置输出（UNION类型）。 **取值范围**: 不涉及。
tags	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-157 Secret

参数	参数类型	描述
secret_id	String	**参数解释**: 凭证ID，唯一标识CSMS中的凭证。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
secret_name	String	**参数解释**: 凭证名称，CSMS中存储的凭证名称。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-158 Oauth2ProviderConfigOutput

参数	参数类型	描述
microsoft_oauth2_provider_config	**MicrosoftOauth2ProviderConfigOutput** object	**参数解释**: Microsoft OAuth2提供商的输出配置。 **取值范围**: 不涉及。
google_oauth2_provider_config	**GoogleOauth2ProviderConfigOutput** object	**参数解释**: Google OAuth2提供商的输出配置。 **取值范围**: 不涉及。
github_oauth2_provider_config	**GithubOauth2ProviderConfigOutput** object	**参数解释**: GitHub OAuth2提供商的输出配置。 **取值范围**: 不涉及。
custom_oauth2_provider_config	**CustomOauth2ProviderConfigOutput** object	**参数解释**: 自定义OAuth2提供商的输出配置。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-159 MicrosoftOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-160 GoogleOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-161 GithubOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-162 CustomOauth2ProviderConfigOutput

参数	参数类型	描述
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。
client_id	String	**参数解释**: OAuth2应用的客户端ID（Client ID），用于标识接入OAuth2认证流程的应用。 **取值范围**: 长度为1~256个字符。

表 4-163 Oauth2Discovery

参数	参数类型	描述
discovery_url	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。
authorization_server_metadata	**Oauth2AuthorizationServerMetadata** object	**参数解释**: OAuth2提供商的授权服务器元数据。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-164 Oauth2AuthorizationServerMetadata

参数	参数类型	描述
authorization_endpoint	String	**参数解释**： 授权服务器的授权端点。 **取值范围**： 必须以https://开头，长度为1~2048个字符。
issuer	String	**参数解释**： 授权服务器的签发者标识。 **取值范围**： 必须以https://开头，长度为1~2048个字符。
token_endpoint	String	**参数解释**： 授权服务器的令牌端点。 **取值范围**： 必须以https://开头，长度为1~2048个字符。
response_types	Array of strings	**参数解释**： 支持的响应类型列表。 **取值范围**： 数组长度范围[1,20]，每个元素为1~50个字符的字符串。
token_endpoint_auth_methods	Array of strings	**参数解释**： 令牌端点支持的客户端认证方法列表。 **取值范围**： 数组长度范围[1,2]。

表 4-165 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-166 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-167 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

表 4-168 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：429

表 4-169 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

更新OAuth2凭证提供商的client_secret和tenant_id。

```
PUT https://{endpoint}/v1/oauth2-credential-providers/{credential_provider_name}

{
  "oauth2_provider_config_input" : {
    "microsoft_oauth2_provider_config" : {
      "client_id" : "285624f5-5958-4f36-b171-168303615bce",
      "client_secret" : "285624f5-5958-4f36-b171-168303615bce",
      "tenant_id" : "285624f5-5958-4f36-b171-168303615bce"
    }
```


版权所有 © 华为云计算技术有限公司

```
  }
}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_microsoft_oauthprovider",
    "urn" : "agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/
<name>",
    "credential_provider_vendor" : "MicrosoftOauth2",
    "client_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "callback_url" : "https://agent-identity.cn-north-4.myhuaweicloud.com/v1/oauth2/callback/
9c38be75-5973-4709-a211-7e2c438c250d",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-04 14:13:20",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ],
    "oauth2_provider_config_output" : {
      "microsoft_oauth2_provider_config" : {
        "oauth2_discovery" : {
          "discovery_url" : "https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration",
          "authorization_server_metadata" : null
        },
        "client_id" : "285624f5-5958-4f36-b171-168303615bce"
      }
    }
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。
429	请求过于频繁。

错误码

请参见**错误码**。

4.5.5 删除 OAuth2 凭证提供商

功能介绍

删除指定的OAuth2凭证提供商。

版权所有 © 华为云计算技术有限公司

URI

DELETE /v1/oauth2-credential-providers/{credential_provider_name}

表 4-170 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：204

无

状态码：400

表 4-171 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-172 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-173 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：429

表 4-174 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

删除OAuth2凭证提供商。

```
DELETE https://{endpoint}/v1/oauth2-credential-providers/{credential_provider_name}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。
429	请求过于频繁。

错误码

请参见**错误码**。

4.6 STS 凭证提供商

4.6.1 创建 STS 凭证提供商

功能介绍

创建一个新的STS凭证提供商。

URI

POST /v1/sts-credential-providers

版权所有 © 华为云计算技术有限公司

请求参数

表 4-175 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。
agency_urn	是	String	**参数解释**: IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。 **默认取值**: 不涉及。
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-176 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：201

表 4-177 响应 Body 参数

参数	参数类型	描述
credential_provider	**StsCredentialProvider** object	**参数解释**： STS凭证提供商，用于配置通过IAM委托获取临时访问凭证的参数。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-178 StsCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 不涉及。
agency_urn	String	**参数解释**： IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-179 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-180 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-181 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-182 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

创建STS凭证提供商。

```
POST https://{endpoint}/v1/sts-credential-providers

{
  "name" : "my_stsprovider",
  "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ]
}
```

响应示例

状态码：201

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_stsprovider",
    "urn" : "agentIdentity:<region>:<account-id>:stsCredentialProvider:tokenVault/<token-vault-id>/<name>",
    "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
```


版权所有 © 华为云计算技术有限公司

```
  }]
 }
}
```

状态码

状态码	描述
201	请求成功。
400	请求体异常。
403	没有操作权限。
409	请求冲突。

错误码

请参见**错误码**。

4.6.2 查询 STS 凭证提供商列表

功能介绍

查询当前账号下的STS凭证提供商列表。支持分页查询，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/sts-credential-providers

表 4-183 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**: 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**: 不涉及。 **取值范围**: 1~200。 **默认取值**: 100。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
marker	否	String	**参数解释**： 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：200

表 4-184 响应 Body 参数

参数	参数类型	描述
credential_providers	Array of **StsCredentialProviderSummary** objects	**参数解释**： STS凭证提供商摘要信息。 **取值范围**： 不涉及。
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-185 StsCredentialProviderSummary

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 不涉及。
agency_urn	String	**参数解释**： IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-186 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

表 4-187 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

表 4-188 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

- 查询STS凭证提供商列表。

  ```
  GET https://{endpoint}/v1/sts-credential-providers
  ```

- 分页查询STS凭证提供商列表。

  ```
  GET https://{endpoint}/v1/sts-credential-providers?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "credential_providers" : [ {
```


版权所有 © 华为云计算技术有限公司

```
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_stsprovider",
    "urn" : "agentIdentity:<region>:<account-id>:stsCredentialProvider:tokenVault/<token-vault-id>/<name>",
    "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : "marker"
  }
}
```


状态码

状态码	描述
200	请求成功。
400	请求体异常。

错误码

请参见**错误码**。

4.6.3 查询 STS 凭证提供商详情

功能介绍

查询STS凭证提供商详情。

URI

GET /v1/sts-credential-providers/{credential_provider_name}

版权所有 © 华为云计算技术有限公司

表 4-189 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：200

表 4-190 响应 Body 参数

参数	参数类型	描述
credential_provider	**StsCredentialProvider** object	**参数解释**： STS凭证提供商，用于配置通过IAM委托获取临时访问凭证的参数。 **取值范围**： 不涉及。

表 4-191 StsCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 不涉及。
agency_urn	String	**参数解释**： IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-192 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-193 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：404

表 4-194 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

查询STS凭证提供商详情。

```
GET https://{endpoint}/v1/sts-credential-providers/{credential_provider_name}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_stsprovider",
    "urn" : "agentIdentity:<region>:<account-id>:stsCredentialProvider:tokenVault/<token-vault-id>/<name>",
    "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.6.4 更新 STS 凭证提供商

功能介绍

更新指定的STS凭证提供商。

URI

PUT /v1/sts-credential-providers/{credential_provider_name}

表 4-195 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**: 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-196 请求 Body 参数

参数	是否必选	参数类型	描述
agency_urn	否	String	**参数解释**: IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。 **默认取值**: 不涉及。
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-197 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

表 4-198 响应 Body 参数

参数	参数类型	描述
credential_provider	**StsCredentialProvider** object	**参数解释**： STS凭证提供商，用于配置通过IAM委托获取临时访问凭证的参数。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-199 StsCredentialProvider

参数	参数类型	描述
credential_provider_id	String	**参数解释**： 凭证提供商的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 凭证提供商的唯一资源名称（URN）。 **取值范围**： 不涉及。
agency_urn	String	**参数解释**： IAM委托的统一资源名称（URN），用于获取IAM临时凭证，在IAM控制台的「委托」页面中获取，需确保该委托的信任策略允许 AgentIdentity 服务执行 sts:agencies:assume 动作。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-200 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-201 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-202 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-203 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

更新STS凭证提供商的agency_urn和标签。

```
PUT https://{endpoint}/v1/sts-credential-providers/{credential_provider_name}

{
  "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ]
}
```

响应示例

状态码：200

```
{
  "credential_provider" : {
    "credential_provider_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_stsprovider",
    "urn" : "agentIdentity:<region>:<account-id>:stsCredentialProvider:tokenVault/<token-vault-id>/<name>",
    "agency_urn" : "iam::3fd23817bd85480e8dc4f520075de348:agency:provider",
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
```


版权所有 © 华为云计算技术有限公司

```
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.6.5 删除 STS 凭证提供商

功能介绍

删除指定的STS凭证提供商。

URI

DELETE /v1/sts-credential-providers/{credential_provider_name}

表 4-204 路径参数

参数	是否必选	参数类型	描述
credential_provider_name	是	String	**参数解释**： 凭证提供商名称，用于唯一标识一个凭证提供商。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。

请求参数

无

版权所有 © 华为云计算技术有限公司

响应参数

状态码：204

无

状态码：400

表 4-205 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-206 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

删除STS凭证提供商。

```
DELETE https://{endpoint}/v1/sts-credential-providers/{credential_provider_name}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.7 工作负载身份

版权所有 © 华为云计算技术有限公司

4.7.1 创建工作负载身份

功能介绍

创建一个新的工作负载身份。工作负载身份用于为工作负载（如Agent运行时）提供统一的身份标识，支持配置自定义JWT、IAM、API Key等多种授权方式，实现对入站请求的身份验证和授权。

URI

POST /v1/workload-identities

请求参数

表 4-207 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。
allowed_resource_oauth2_return_urls	否	Array of strings	**参数解释**： 工作负载身份关联的资源OAuth2回调地址列表。用于指定OAuth2授权流程中允许的回调地址，确保令牌仅返回到受信任的URL。 **约束限制**： 列表最多允许20个回调地址。 **取值范围**： 符合URL格式的字符串，必须以协议开头（如https://），长度为1~2048个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
authorizer_type	是	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **约束限制**： 创建工作负载身份时必填，创建后不可修改。 **取值范围**： • CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 • IAM：IAM授权，通过华为云IAM服务进行身份验证。 • API_KEY：API Key授权，通过预置的API密钥进行身份验证。 • NONE：无授权，不进行入站请求身份验证。 **默认取值**： 不涉及。
authorizer_configuration	否	**AuthorizerConfiguration** object	**参数解释**： 入站授权配置，用于定义工作负载身份如何验证入站请求的身份。根据授权类型（authorizer_type）的不同，需要配置对应的授权参数。 **约束限制**： 当authorizer_type为CUSTOM_JWT时，需配置custom_jwt；当authorizer_type为API_KEY时，需配置key_auth。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表，用于为工作负载身份添加标签，便于分类和管理。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-208 AuthorizerConfiguration

参数	是否必选	参数类型	描述
custom_jwt	否	**CustomJWTAuthorizerConfiguration** object	**参数解释**: 自定义JWT授权配置，用于配置通过外部身份提供商签发的JWT令牌进行入站请求身份验证的参数。当authorizer_type为CUSTOM_JWT时使用此配置。 **约束限制**: 仅当authorizer_type为CUSTOM_JWT时有效。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
key_auth	否	**KeyAuthAuthorizerConfiguration** object	**参数解释**: API Key授权配置，用于配置通过预置API密钥进行入站请求身份验证的参数。当authorizer_type为API_KEY时使用此配置。 **约束限制**: 仅当authorizer_type为API_KEY时有效。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-209 CustomJWTAuthorizerConfiguration

参数	是否必选	参数类型	描述
discovery_url	是	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。 **默认取值**: 不涉及。
allowed_audience	否	Array of strings	**参数解释**: 允许的JWT受众（audience）值列表。入站JWT令牌中的aud声明必须匹配此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。
allowed_clients	否	Array of strings	**参数解释**: 允许的JWT客户端标识（client_id）列表。入站JWT令牌中的client_id声明必须匹配此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
allowed_scopes	否	Array of strings	**参数解释**: 允许的JWT scope值列表。入站JWT令牌中的scope声明必须包含此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、":"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。
custom_claims	否	Array of **CustomClaimValidation** objects	**参数解释**: 自定义声明（claim）验证规则列表，用于对入站JWT令牌中的自定义声明字段进行匹配验证。 **约束限制**: 列表最多允许100条规则。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-210 CustomClaimValidation

参数	是否必选	参数类型	描述
authorizing_claim_match_value	是	**AuthorizingClaimMatchValue** object	**参数解释**: 授权声明匹配值，定义入站JWT令牌中声明字段值与预期值之间的匹配关系。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
inbound_token_claim_name	是	String	**参数解释**： 需要验证的自定义声明字段名称。入站JWT令牌中必须包含此声明字段，且其值需满足匹配规则。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"、":"组成，长度为1~255个字符。 **默认取值**： 不涉及。
inbound_token_claim_value_type	是	String	**参数解释**： 声明字段值的数据类型，用于确定如何解析和匹配入站JWT令牌中的声明值。 **约束限制**： 不涉及。 **取值范围**： ● STRING：字符串类型，声明值为单个字符串。 ● STRING_ARRAY：字符串数组类型，声明值为字符串列表。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-211 AuthorizingClaimMatchValue

参数	是否必选	参数类型	描述
claim_match_operator	是	String	**参数解释**: 声明匹配操作符，定义声明字段值与匹配值之间的关系类型。 **约束限制**: 不涉及。 **取值范围**: • EQUALS：等于，声明值必须完全等于匹配值。 • CONTAINS：包含，声明值（字符串）必须包含匹配值。 • CONTAINS_ANY：包含任意一个，声明值（数组）中至少包含匹配值列表中的一个元素。 **默认取值**: 不涉及。
claim_match_value	是	ClaimMatchValue object	**参数解释**: 声明匹配值，指定用于与入站JWT令牌中声明字段值进行比对的预期值。根据声明值类型（STRING或STRING_ARRAY），使用match_value_string或match_value_string_list。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-212 ClaimMatchValue

参数	是否必选	参数类型	描述
match_value_string	否	String	**参数解释**: 字符串类型的匹配值，当inbound_token_claim_value_type为STRING时使用。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"_"、"."、"-"组成，长度为1~255个字符。 **默认取值**: 不涉及。
match_value_string_list	否	Array of strings	**参数解释**: 字符串数组类型的匹配值列表项，当inbound_token_claim_value_type为STRING_ARRAY时使用。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"_"、"."、"-"组成，单个值长度为1~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-213 KeyAuthAuthorizerConfiguration

参数	是否必选	参数类型	描述
api_keys	是	Array of **ApiKeyInfo** objects	**参数解释**： API密钥信息列表，用于配置一个或多个API密钥。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。 **约束限制**： 列表最多允许10个API密钥。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

表 4-214 ApiKeyInfo

参数	是否必选	参数类型	描述
api_key	是	String	**参数解释**： API密钥值。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。如果为空，系统将自动生成一个随机字符串。 **约束限制**： 不涉及。 **取值范围**： 不能以空格开头或结尾，长度为1~1024个字符。 **默认取值**： 不涉及。
api_key_name	否	String	**参数解释**： API密钥名称，用于标识和区分不同的API密钥。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为0~64个字符。 **默认取值**： 空字符串。

版权所有 © 华为云计算技术有限公司

表 4-215 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：201

表 4-216 响应 Body 参数

参数	参数类型	描述
workload_identity	**WorkloadIdentity** object	**参数解释**： 工作负载身份的详细信息，包含名称、URN、授权类型、API密钥凭证、创建者、创建时间、更新时间和标签等。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-217 WorkloadIdentity

参数	参数类型	描述
workload_identity_id	String	**参数解释**： 工作负载身份的唯一标识。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 工作负载身份的唯一资源名称（URN），由系统自动生成，用于全局唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
allowed_resource_oauth2_return_urls	Array of strings	**参数解释**： 工作负载身份关联的资源OAuth2回调地址列表。 **取值范围**： 符合URL格式的字符串，必须以协议开头（如https://），长度为1~2048个字符。
authorizer_type	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **取值范围**： ● CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 ● IAM：IAM授权，通过华为云IAM服务进行身份验证。 ● API_KEY：API Key授权，通过预置的API密钥进行身份验证。 ● NONE：无授权，不进行入站请求身份验证。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
api_key_secret	**Secret** object	**参数解释**: 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**: 不涉及。
created_by	**CreatedBy** object	**参数解释**: 工作负载身份的创建者信息，包含创建者类型和创建者标识。 **取值范围**: 不涉及。
created_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **取值范围**: 不涉及。

表 4-218 Secret

参数	参数类型	描述
secret_id	String	**参数解释**: 凭证ID，唯一标识CSMS中的凭证。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-219 CreatedBy

参数	参数类型	描述
type	String	**参数解释**： 工作负载身份创建者类型，标识创建者是由用户还是由服务创建的。 **取值范围**： ● CUSTOMER：由用户创建。 ● SERVICE：由服务自动创建。
identifier	String	**参数解释**： 工作负载身份创建者标识。当创建者类型为CUSTOMER时，标识为用户的账号ID；当创建者类型为SERVICE时，标识为服务名称。 **取值范围**： 不涉及。

表 4-220 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-221 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-222 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

- 创建使用自定义JWT授权的工作负载身份。

```
POST https://{endpoint}/v1/workload-identities

{
  "name" : "my_workload_identity",
  "allowed_resource_oauth2_return_urls" : [ "https://example.com/oauth2/callback" ],
  "authorizer_type" : "CUSTOM_JWT",
  "authorizer_configuration" : {
    "custom_jwt" : {
      "discovery_url" : "https://example.com/.well-known/openid-configuration",
      "allowed_audience" : [ "example-audience" ],
      "allowed_clients" : [ "example-client-id" ],
      "allowed_scopes" : [ "read", "write" ],
      "custom_claims" : [ {
        "inbound_token_claim_name" : "tenant",
        "inbound_token_claim_value_type" : "STRING",
        "authorizing_claim_match_value" : {
          "claim_match_operator" : "EQUALS",
          "claim_match_value" : {
            "match_value_string" : "acme"
          }
        }
      }, {
        "inbound_token_claim_name" : "roles",
        "inbound_token_claim_value_type" : "STRING_ARRAY",
        "authorizing_claim_match_value" : {
          "claim_match_operator" : "CONTAINS_ANY",
          "claim_match_value" : {
            "match_value_string_list" : [ "admin", "editor" ]
```


版权所有 © 华为云计算技术有限公司

```
        }
      }
    } ]
  }
 },
 "tags" : [ {
  "key" : "key-1",
  "value" : "value-1"
 } ]
}
```

- 创建使用API Key授权的工作负载身份。

```
POST https://{endpoint}/v1/workload-identities

{
 "name" : "my_workload_identity",
 "authorizer_type" : "API_KEY",
 "authorizer_configuration" : {
  "key_auth" : {
   "api_keys" : [ {
    "api_key" : "22243eefff**",
    "api_key_name" : "test-key-1"
   }, {
    "api_key" : "22243eefff**",
    "api_key_name" : "test-key-2"
   } ]
  }
 }
}
```

响应示例

状态码：201

```
{
  "workload_identity" : {
    "workload_identity_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_workload_identity",
    "urn" : "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-
directory-id>/<workload-identity-name>",
    "authorizer_type" : "CUSTOM_JWT",
    "api_key_secret" : "null,",
    "allowed_resource_oauth2_return_urls" : [ "https://example.com/oauth2/callback" ],
    "created_by" : {
      "type" : "SERVICE",
      "identifier" : "service.AgentRuntime"
    },
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```

状态码

状态码	描述
201	请求成功。
400	请求体异常。
409	请求冲突。

 版权所有 © 华为云计算技术有限公司

错误码

请参见**错误码**。

4.7.2 查询工作负载身份列表

功能介绍

查询当前账号下的工作负载身份列表。支持分页查询，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/workload-identities

表 4-223 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**： 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**： 不涉及。 **取值范围**： 1~200。 **默认取值**： 100。
marker	否	String	**参数解释**： 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**： 不涉及。

请求参数

无

版权所有 © 华为云计算技术有限公司

响应参数

状态码：200

表 4-224 响应 Body 参数

参数	参数类型	描述
workload_identities	Array of **WorkloadIdentitySummary** objects	**参数解释**： 工作负载身份摘要信息列表。 **取值范围**： 不涉及。
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-225 WorkloadIdentitySummary

参数	参数类型	描述
workload_identity_id	String	**参数解释**： 工作负载身份的唯一标识。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 工作负载身份的唯一资源名称（URN），由系统自动生成，用于全局唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
authorizer_type	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **取值范围**： • CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 • IAM：IAM授权，通过华为云IAM服务进行身份验证。 • API_KEY：API Key授权，通过预置的API密钥进行身份验证。 • NONE：无授权，不进行入站请求身份验证。
created_by	**CreatedBy** object	**参数解释**： 工作负载身份的创建者信息，包含创建者类型和创建者标识。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-226 CreatedBy

参数	参数类型	描述
type	String	**参数解释**： 工作负载身份创建者类型，标识创建者是由用户还是由服务创建的。 **取值范围**： ● CUSTOMER：由用户创建。 ● SERVICE：由服务自动创建。
identifier	String	**参数解释**： 工作负载身份创建者标识。当创建者类型为CUSTOMER时，标识为用户的账号ID；当创建者类型为SERVICE时，标识为服务名称。 **取值范围**： 不涉及。

表 4-227 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

版权所有 © 华为云计算技术有限公司

表 4-228 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

表 4-229 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求示例

- 查询工作负载身份列表。

  ```
  GET https://{endpoint}/v1/workload-identities
  ```

- 分页查询工作负载身份列表。

  ```
  GET https://{endpoint}/v1/workload-identities?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "workload_identities" : [ {
    "workload_identity_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "workload_identity_1",
    "urn" : "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>",
    "authorizer_type" : "CUSTOM_JWT",
    "created_by" : {
      "type" : "SERVICE",
      "identifier" : "service.AgentRuntime"
    },
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }, {
    "workload_identity_id" : "684a2c3e5f1b9d0e7a3c4f57",
    "name" : "workload_identity_2",
    "urn" : "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>",
    "authorizer_type" : "API_KEY",
    "created_by" : {
      "type" : "CUSTOMER",
      "identifier" : 12345678901234567890
    },
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-03 00:00:00",
    "tags" : [ {
      "key" : "key-2",
      "value" : "value-2"
    } ]
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "marker"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.7.3 查询工作负载身份详情

功能介绍

根据工作负载身份名称查询指定工作负载身份的详细信息，包括名称、URN、授权类型、创建者、标签等。

URI

GET /v1/workload-identities/{workload_identity_name}

表 4-230 路径参数

参数	是否必选	参数类型	描述
workload_identity_name	是	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：200

表 4-231 响应 Body 参数

参数	参数类型	描述
workload_identity	WorkloadIdentity object	**参数解释**： 工作负载身份的详细信息，包含名称、URN、授权类型、API密钥凭证、创建者、创建时间、更新时间和标签等。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-232 WorkloadIdentity

参数	参数类型	描述
workload_identity_id	String	**参数解释**： 工作负载身份的唯一标识。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 工作负载身份的唯一资源名称（URN），由系统自动生成，用于全局唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
allowed_resource_oauth2_return_urls	Array of strings	**参数解释**： 工作负载身份关联的资源OAuth2回调地址列表。 **取值范围**： 符合URL格式的字符串，必须以协议开头（如https://），长度为1~2048个字符。
authorizer_type	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **取值范围**： ● CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 ● IAM：IAM授权，通过华为云IAM服务进行身份验证。 ● API_KEY：API Key授权，通过预置的API密钥进行身份验证。 ● NONE：无授权，不进行入站请求身份验证。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
api_key_secret	**Secret** object	**参数解释**： 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**： 不涉及。
created_by	**CreatedBy** object	**参数解释**： 工作负载身份的创建者信息，包含创建者类型和创建者标识。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-233 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-234 CreatedBy

参数	参数类型	描述
type	String	**参数解释**： 工作负载身份创建者类型，标识创建者是由用户还是由服务创建的。 **取值范围**： ● CUSTOMER：由用户创建。 ● SERVICE：由服务自动创建。
identifier	String	**参数解释**： 工作负载身份创建者标识。当创建者类型为CUSTOMER时，标识为用户的账号ID；当创建者类型为SERVICE时，标识为服务名称。 **取值范围**： 不涉及。

表 4-235 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-236 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-237 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

查询工作负载身份详情。

```
GET https://{endpoint}/v1/workload-identities/{workload_identity_name}
```

响应示例

状态码：200

```
{
  "workload_identity" : {
    "workload_identity_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "name" : "my_workload_identity",
    "urn" : "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>",
    "allowed_resource_oauth2_return_urls" : [ "https://example.com/oauth2/callback" ],
    "authorizer_type" : "API_KEY",
    "api_key_secret" : {
      "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
      "secret_name" : "test-secret"
    },
    "created_by" : {
      "type" : "SERVICE",
      "identifier" : "service.AgentRuntime"
    },
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "tags" : [ {
      "key" : "key-1",
```


版权所有 © 华为云计算技术有限公司

```
    "value" : "value-1"
  } ]
 }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.7.4 更新工作负载身份

功能介绍

更新指定工作负载身份的配置信息，包括OAuth2回调地址、授权配置和标签等。

URI

PUT /v1/workload-identities/{workload_identity_name}

表 4-238 路径参数

参数	是否必选	参数类型	描述
workload_identity_name	是	String	**参数解释**: 工作负载身份名称，用于唯一标识一个工作负载身份。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-239 请求 Body 参数

参数	是否必选	参数类型	描述
allowed_resource_oauth2_return_urls	否	Array of strings	**参数解释**： 工作负载身份关联的资源OAuth2回调地址列表。用于指定OAuth2授权流程中允许的回调地址，确保令牌仅返回到受信任的URL。 **约束限制**： 列表最多允许20个回调地址。 **取值范围**： 符合URL格式的字符串，必须以协议开头（如https://），长度为1~2048个字符。 **默认取值**： 不涉及。
authorizer_configuration	否	**AuthorizerConfiguration** object	**参数解释**： 入站授权配置，用于定义工作负载身份如何验证入站请求的身份。根据授权类型（authorizer_type）的不同，需要配置对应的授权参数。 **约束限制**： 当authorizer_type为CUSTOM_JWT时，需配置custom_jwt；当authorizer_type为API_KEY时，需配置key_auth。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表，用于为工作负载身份添加标签，便于分类和管理。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-240 AuthorizerConfiguration

参数	是否必选	参数类型	描述
custom_jwt	否	**CustomJWTAuthorizerConfiguration** object	**参数解释**: 自定义JWT授权配置，用于配置通过外部身份提供商签发的JWT令牌进行入站请求身份验证的参数。当authorizer_type为CUSTOM_JWT时使用此配置。 **约束限制**: 仅当authorizer_type为CUSTOM_JWT时有效。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
key_auth	否	**KeyAuthAuthorizerConfiguration** object	**参数解释**: API Key授权配置，用于配置通过预置API密钥进行入站请求身份验证的参数。当authorizer_type为API_KEY时使用此配置。 **约束限制**: 仅当authorizer_type为API_KEY时有效。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-241 CustomJWTAuthorizerConfiguration

参数	是否必选	参数类型	描述
discovery_url	是	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **约束限制**: 不涉及。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。 **默认取值**: 不涉及。
allowed_audience	否	Array of strings	**参数解释**: 允许的JWT受众（audience）值列表。入站JWT令牌中的aud声明必须匹配此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。
allowed_clients	否	Array of strings	**参数解释**: 允许的JWT客户端标识（client_id）列表。入站JWT令牌中的client_id声明必须匹配此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
allowed_scopes	否	Array of strings	**参数解释**: 允许的JWT scope值列表。入站JWT令牌中的scope声明必须包含此列表中的某个值才能通过验证。 **约束限制**: 列表最多允许100个值。 **取值范围**: 只能由英文字母、数字及"."、"_"、":"、"-"组成，单个值长度为1~256个字符。 **默认取值**: 不涉及。
custom_claims	否	Array of **CustomClaimValidation** objects	**参数解释**: 自定义声明（claim）验证规则列表，用于对入站JWT令牌中的自定义声明字段进行匹配验证。 **约束限制**: 列表最多允许100条规则。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-242 CustomClaimValidation

参数	是否必选	参数类型	描述
authorizing_claim_match_value	是	**AuthorizingClaimMatchValue** object	**参数解释**: 授权声明匹配值，定义入站JWT令牌中声明字段值与预期值之间的匹配关系。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
inbound_token_claim_name	是	String	**参数解释**： 需要验证的自定义声明字段名称。入站JWT令牌中必须包含此声明字段，且其值需满足匹配规则。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"、":"组成，长度为1~255个字符。 **默认取值**： 不涉及。
inbound_token_claim_value_type	是	String	**参数解释**： 声明字段值的数据类型，用于确定如何解析和匹配入站JWT令牌中的声明值。 **约束限制**： 不涉及。 **取值范围**： ● STRING：字符串类型，声明值为单个字符串。 ● STRING_ARRAY：字符串数组类型，声明值为字符串列表。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-243 AuthorizingClaimMatchValue

参数	是否必选	参数类型	描述
claim_match_operator	是	String	**参数解释**： 声明匹配操作符，定义声明字段值与匹配值之间的关系类型。 **约束限制**： 不涉及。 **取值范围**： • EQUALS：等于，声明值必须完全等于匹配值。 • CONTAINS：包含，声明值（字符串）必须包含匹配值。 • CONTAINS_ANY：包含任意一个，声明值（数组）中至少包含匹配值列表中的一个元素。 **默认取值**： 不涉及。
claim_match_value	是	**ClaimMatchValue** object	**参数解释**： 声明匹配值，指定用于与入站JWT令牌中声明字段值进行比对的预期值。根据声明值类型（STRING或STRING_ARRAY），使用match_value_string或match_value_string_list。 **约束限制**： 不涉及。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-244 ClaimMatchValue

参数	是否必选	参数类型	描述
match_value_string	否	String	**参数解释**： 字符串类型的匹配值，当inbound_token_claim_value_type为STRING时使用。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"组成，长度为1~255个字符。 **默认取值**： 不涉及。
match_value_string_list	否	Array of strings	**参数解释**： 字符串数组类型的匹配值列表项，当inbound_token_claim_value_type为STRING_ARRAY时使用。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"组成，单个值长度为1~255个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-245 KeyAuthAuthorizerConfiguration

参数	是否必选	参数类型	描述
api_keys	是	Array of **ApiKeyInfo** objects	**参数解释**： API密钥信息列表，用于配置一个或多个API密钥。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。 **约束限制**： 列表最多允许10个API密钥。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

表 4-246 ApiKeyInfo

参数	是否必选	参数类型	描述
api_key	是	String	**参数解释**： API密钥值。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。如果为空，系统将自动生成一个随机字符串。 **约束限制**： 不涉及。 **取值范围**： 不能以空格开头或结尾，长度为1~1024个字符。 **默认取值**： 不涉及。
api_key_name	否	String	**参数解释**： API密钥名称，用于标识和区分不同的API密钥。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为0~64个字符。 **默认取值**： 空字符串。

版权所有 © 华为云计算技术有限公司

表 4-247 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

表 4-248 响应 Body 参数

参数	参数类型	描述
workload_identity	**WorkloadIdentity** object	**参数解释**： 工作负载身份的详细信息，包含名称、URN、授权类型、API密钥凭证、创建者、创建时间、更新时间和标签等。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-249 WorkloadIdentity

参数	参数类型	描述
workload_identity_id	String	**参数解释**： 工作负载身份的唯一标识。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
name	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
urn	String	**参数解释**： 工作负载身份的唯一资源名称（URN），由系统自动生成，用于全局唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
allowed_resource_oauth2_return_urls	Array of strings	**参数解释**： 工作负载身份关联的资源OAuth2回调地址列表。 **取值范围**： 符合URL格式的字符串，必须以协议开头（如https://），长度为1~2048个字符。
authorizer_type	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **取值范围**： ● CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 ● IAM：IAM授权，通过华为云IAM服务进行身份验证。 ● API_KEY：API Key授权，通过预置的API密钥进行身份验证。 ● NONE：无授权，不进行入站请求身份验证。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
api_key_secret	**Secret** object	**参数解释**： 凭证信息，包含凭证ID和凭证名称。用于API Key授权方式下，标识存储在CSMS（凭证管理服务）中的API密钥凭证。 **取值范围**： 不涉及。
created_by	**CreatedBy** object	**参数解释**： 工作负载身份的创建者信息，包含创建者类型和创建者标识。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-250 Secret

参数	参数类型	描述
secret_id	String	**参数解释**： 凭证ID，唯一标识CSMS中的凭证。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
secret_name	String	**参数解释**： 凭证名称，CSMS中存储的凭证名称。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

表 4-251 CreatedBy

参数	参数类型	描述
type	String	**参数解释**： 工作负载身份创建者类型，标识创建者是由用户还是由服务创建的。 **取值范围**： ● CUSTOMER：由用户创建。 ● SERVICE：由服务自动创建。
identifier	String	**参数解释**： 工作负载身份创建者标识。当创建者类型为CUSTOMER时，标识为用户的账号ID；当创建者类型为SERVICE时，标识为服务名称。 **取值范围**： 不涉及。

表 4-252 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-253 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-254 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-255 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

表 4-256 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

更新工作负载身份的OAuth2回调地址和API Key授权配置。

```
PUT https://{endpoint}/v1/workload-identities/{workload_identity_name}

{
  "allowed_resource_oauth2_return_urls" : [ "https://example.com/oauth2/callback", "https://example.com/oauth2/callback2" ],
  "authorizer_configuration" : {
    "key_auth" : {
      "api_keys" : [ {
        "api_key" : "22243eefff**",
```


版权所有 © 华为云计算技术有限公司

```
      "api_key_name" : "test-key-1"
    }, {
      "api_key" : "22243eefff**",
      "api_key_name" : "test-key-2"
    } ]
  }
 }
}
```

响应示例

状态码：200

```
{
 "workload_identity" : {
  "workload_identity_id" : "684a2c3e5f1b9d0e7a3c4f56",
  "name" : "my_workload_identity",
  "urn" : "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>",
  "authorizer_type" : "API_KEY",
  "api_key_secret" : {
   "secret_id" : "285624f5-5958-4f36-b171-168303615bce",
   "secret_name" : "test-secret"
  },
  "allowed_resource_oauth2_return_urls" : [ "https://example.com/oauth2/callback", "https://example.com/oauth2/callback2" ],
  "created_by" : {
   "type" : "SERVICE",
   "identifier" : "service.AgentRuntime"
  },
  "created_at" : "2025-01-01 00:00:00",
  "updated_at" : "2025-01-03 00:00:00",
  "tags" : [ {
   "key" : "key-1",
   "value" : "value-1"
  } ]
 }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
403	没有操作权限。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.7.5 删除工作负载身份

功能介绍

删除指定的工作负载身份。删除后，该工作负载身份将不再可用，与之关联的授权配置也将一并删除。

URI

DELETE /v1/workload-identities/{workload_identity_name}

表 4-257 路径参数

参数	是否必选	参数类型	描述
workload_identity_name	是	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：204

无

状态码：400

表 4-258 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

表 4-259 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：404

表 4-260 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

表 4-261 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

删除工作负载身份。

```
DELETE https://{endpoint}/v1/workload-identities/{workload_identity_name}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。
403	没有操作权限。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.7.6 查询工作负载身份的授权配置

功能介绍

查询指定工作负载身份的授权配置信息，包括授权类型和具体的授权配置（如自定义JWT配置或API Key配置）。

版权所有 © 华为云计算技术有限公司

URI

GET /v1/workload-identities/{workload_identity_name}/authorizer-configuration

表 4-262 路径参数

参数	是否必选	参数类型	描述
workload_identity_name	是	String	**参数解释**: 工作负载身份名称，用于唯一标识一个工作负载身份。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：200

表 4-263 响应 Body 参数

参数	参数类型	描述
workload_identity_authorizer_configuration	**WorkloadIdentityAuthorizerConfiguration** object	**参数解释**: 工作负载身份的授权配置信息，包含工作负载身份名称、授权类型和授权配置。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-264 WorkloadIdentityAuthorizerConfiguration

参数	参数类型	描述
workload_identity_name	String	**参数解释**： 工作负载身份名称，用于唯一标识一个工作负载身份。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~56个字符。
authorizer_type	String	**参数解释**： 授权类型，用于指定工作负载身份的入站请求身份验证方式。不同的授权类型对应不同的授权配置。 **取值范围**： • CUSTOM_JWT：自定义JWT授权，通过外部身份提供商的JWT令牌进行身份验证。 • IAM：IAM授权，通过华为云IAM服务进行身份验证。 • API_KEY：API Key授权，通过预置的API密钥进行身份验证。 • NONE：无授权，不进行入站请求身份验证。
authorizer_configuration	**AuthorizerConfiguration** object	**参数解释**： 入站授权配置，用于定义工作负载身份如何验证入站请求的身份。根据授权类型（authorizer_type）的不同，需要配置对应的授权参数。 **取值范围**： 不涉及。

表 4-265 AuthorizerConfiguration

参数	参数类型	描述
custom_jwt	**CustomJWTAuthorizerConfiguration** object	**参数解释**： 自定义JWT授权配置，用于配置通过外部身份提供商签发的JWT令牌进行入站请求身份验证的参数。当authorizer_type为CUSTOM_JWT时使用此配置。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
key_auth	KeyAuthAuthorizerConfiguration object	**参数解释**： API Key授权配置，用于配置通过预置API密钥进行入站请求身份验证的参数。当authorizer_type为API_KEY时使用此配置。 **取值范围**： 不涉及。

表 4-266 CustomJWTAuthorizerConfiguration

参数	参数类型	描述
discovery_url	String	**参数解释**： OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **取值范围**： 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。
allowed_audience	Array of strings	**参数解释**： 允许的JWT受众（audience）值列表。入站JWT令牌中的aud声明必须匹配此列表中的某个值才能通过验证。 **取值范围**： 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。
allowed_clients	Array of strings	**参数解释**： 允许的JWT客户端标识（client_id）列表。入站JWT令牌中的client_id声明必须匹配此列表中的某个值才能通过验证。 **取值范围**： 只能由英文字母、数字及"."、"_"、"-"组成，单个值长度为1~256个字符。
allowed_scopes	Array of strings	**参数解释**： 允许的JWT scope值列表。入站JWT令牌中的scope声明必须包含此列表中的某个值才能通过验证。 **取值范围**： 只能由英文字母、数字及"."、"_"、":"、"-"组成，单个值长度为1~256个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
custom_claims	Array of **CustomClaimValidation** objects	**参数解释**： 自定义声明（claim）验证规则列表，用于对入站JWT令牌中的自定义声明字段进行匹配验证。 **取值范围**： 不涉及。

表 4-267 CustomClaimValidation

参数	参数类型	描述
authorizing_claim_match_value	**AuthorizingClaimMatchValue** object	**参数解释**： 授权声明匹配值，定义入站JWT令牌中声明字段值与预期值之间的匹配关系。 **取值范围**： 不涉及。
inbound_token_claim_name	String	**参数解释**： 需要验证的自定义声明字段名称。入站JWT令牌中必须包含此声明字段，且其值需满足匹配规则。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"、":"组成，长度为1~255个字符。
inbound_token_claim_value_type	String	**参数解释**： 声明字段值的数据类型，用于确定如何解析和匹配入站JWT令牌中的声明值。 **取值范围**： • STRING：字符串类型，声明值为单个字符串。 • STRING_ARRAY：字符串数组类型，声明值为字符串列表。

版权所有 © 华为云计算技术有限公司

表 4-268 AuthorizingClaimMatchValue

参数	参数类型	描述
claim_match_operator	String	**参数解释**： 声明匹配操作符，定义声明字段值与匹配值之间的关系类型。 **取值范围**： • EQUALS：等于，声明值必须完全等于匹配值。 • CONTAINS：包含，声明值（字符串）必须包含匹配值。 • CONTAINS_ANY：包含任意一个，声明值（数组）中至少包含匹配值列表中的一个元素。
claim_match_value	**ClaimMatchValue** object	**参数解释**： 声明匹配值，指定用于与入站JWT令牌中声明字段值进行比对的预期值。根据声明值类型（STRING或STRING_ARRAY），使用match_value_string或match_value_string_list。 **取值范围**： 不涉及。

表 4-269 ClaimMatchValue

参数	参数类型	描述
match_value_string	String	**参数解释**： 字符串类型的匹配值，当inbound_token_claim_value_type为STRING时使用。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"组成，长度为1~255个字符。
match_value_string_list	Array of strings	**参数解释**： 字符串数组类型的匹配值列表项，当inbound_token_claim_value_type为STRING_ARRAY时使用。 **取值范围**： 只能由英文字母、数字及"_"、"."、"-"组成，单个值长度为1~255个字符。

版权所有 © 华为云计算技术有限公司

表 4-270 KeyAuthAuthorizerConfiguration

参数	参数类型	描述
api_keys	Array of **ApiKeyInfo** objects	**参数解释**： API密钥信息列表，用于配置一个或多个API密钥。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。 **取值范围**： 不涉及。

表 4-271 ApiKeyInfo

参数	参数类型	描述
api_key	String	**参数解释**： API密钥值。在密钥轮换期间，列表中的任意一个密钥均可用于身份验证。如果为空，系统将自动生成一个随机字符串。 **取值范围**： 不能以空格开头或结尾，长度为1~1024个字符。
api_key_name	String	**参数解释**： API密钥名称，用于标识和区分不同的API密钥。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为0~64个字符。

状态码：400

表 4-272 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-273 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求示例

查询工作负载身份的授权配置。

```
GET https://{endpoint}/v1/workload-identities/{workload_identity_name}/authorizer-configuration
```

响应示例

状态码：200

```
{
  "workload_identity_authorizer_configuration" : {
    "workload_identity_name" : "my_workload_identity",
    "authorizer_type" : "API_KEY",
    "authorizer_configuration" : {
      "key_auth" : {
        "api_keys" : [ {
          "api_key" : "22243eefff**",
          "api_key_name" : "test-key-1"
        }, {
          "api_key" : "22243eefff**",
          "api_key_name" : "test-key-2"
        } ]
      }
    }
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.8 令牌保险库

4.8.1 查询令牌保管库详情

功能介绍

查询令牌保管库详情。

URI

GET /v1/token-vaults/{token_vault_id}

版权所有 © 华为云计算技术有限公司

表 4-274 路径参数

参数	是否必选	参数类型	描述
token_vault_id	是	String	**参数解释**: Token Vault的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。 **默认取值**: default。

请求参数

无

响应参数

状态码：200

表 4-275 响应 Body 参数

参数	参数类型	描述
token_vault	**TokenVault** object	**参数解释**: Token Vault对象，用于管理密钥存储和策略集配置。 **取值范围**: 不涉及。

表 4-276 TokenVault

参数	参数类型	描述
token_vault_id	String	**参数解释**: Token Vault的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
urn	String	**参数解释**： Token Vault对象的统一资源标识（URN）。 **取值范围**： 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
kms_configuration	**KmsConfiguration** object	**参数解释**： KMS密钥配置，用于指定Token Vault使用的KMS密钥类型和密钥ID。 **取值范围**： 不涉及。
policy_engine_configuration	**PolicyEngineConfiguration** object	**参数解释**： TokenVault关联的策略集配置。 **取值范围**： 不涉及。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。

表 4-277 KmsConfiguration

参数	参数类型	描述
key_type	String	**参数解释**： KMS密钥类型，用于指定Token Vault使用的KMS密钥类型。 **取值范围**： • CustomerManagedKey：客户管理密钥 • ServiceManagedKey：服务管理密钥

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
kms_key_id	String	**参数解释**： KMS密钥ID，用于标识Token Vault使用的KMS密钥。 **取值范围**： 不涉及。

表 4-278 PolicyEngineConfiguration

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。
mode	String	**参数解释**： 策略集的强制模式。LOG_ONLY模式下策略集会根据策略评估每个操作并记录是否允许或拒绝的跟踪，但不强制执行决策。ENFORCE模式下策略集会根据策略评估操作并通过允许或拒绝来强制执行决策。 **取值范围**： ● LOG_ONLY：仅记录模式，策略集评估操作但不强制执行决策。建议在启用强制执行前使用此模式测试和验证策略。 ● ENFORCE：强制执行模式，策略集评估操作并强制执行决策。

表 4-279 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-280 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-281 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

查询令牌保管库详情。

```
GET https://{endpoint}/v1/token-vaults/{token_vault_id}
```

响应示例

状态码：200

```
{
  "token_vault" : {
    "token_vault_id" : "default",
    "urn" : "agentIdentity:cn-north-4:123456789012:tokenVault:default",
    "kms_configuration" : {
      "key_type" : "CustomerManagedKey",
      "kms_key_id" : "12345678-1234-1234-1234-123456789012"
    },
    "policy_engine_configuration" : {
      "policy_engine_id" : "abc123def456",
      "mode" : "LOG_ONLY"
    },
    "updated_at" : "2025-01-01 00:00:00",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ]
  }
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.8.2 更新令牌保管库配置

功能介绍

更新令牌保管库配置，包括KMS和策略集设置。

URI

PUT /v1/token-vaults/{token_vault_id}

表 4-282 路径参数

参数	是否必选	参数类型	描述
token_vault_id	是	String	**参数解释**: Token Vault的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。 **默认取值**: default。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-283 请求 Body 参数

参数	是否必选	参数类型	描述
policy_engine_configuration	是	PolicyEngineConfiguration object	**参数解释**: TokenVault关联的策略集配置。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-284 PolicyEngineConfiguration

参数	是否必选	参数类型	描述
policy_engine_id	否	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
mode	否	String	**参数解释**： 策略集的强制模式。LOG_ONLY模式下策略集会根据策略评估每个操作并记录是否允许或拒绝的跟踪，但不强制执行决策。ENFORCE模式下策略集会根据策略评估操作并通过允许或拒绝来强制执行决策。 **约束限制**： 不涉及。 **取值范围**： • LOG_ONLY：仅记录模式，策略集评估操作但不强制执行决策。建议在启用强制执行前使用此模式测试和验证策略。 • ENFORCE：强制执行模式，策略集评估操作并强制执行决策。 **默认取值**： LOG_ONLY。

响应参数

状态码：200

表 4-285 响应 Body 参数

参数	参数类型	描述
token_vault	**TokenVault** object	**参数解释**： Token Vault对象，用于管理密钥存储和策略集配置。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-286 TokenVault

参数	参数类型	描述
token_vault_id	String	**参数解释**: Token Vault的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
urn	String	**参数解释**: Token Vault对象的统一资源标识（URN）。 **取值范围**: 只能由英文字母、数字及"/"、"="、"_"、":"、"-"组成，长度为16~1500个字符。
kms_configuration	**KmsConfiguration** object	**参数解释**: KMS密钥配置，用于指定Token Vault使用的KMS密钥类型和密钥ID。 **取值范围**: 不涉及。
policy_engine_configuration	**PolicyEngineConfiguration** object	**参数解释**: TokenVault关联的策略集配置。 **取值范围**: 不涉及。
updated_at	String	**参数解释**: UTC时间戳，记录资源的创建或更新时间。 **取值范围**: 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
tags	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-287 KmsConfiguration

参数	参数类型	描述
key_type	String	**参数解释**： KMS密钥类型，用于指定Token Vault使用的KMS密钥类型。 **取值范围**： ● CustomerManagedKey：客户管理密钥 ● ServiceManagedKey：服务管理密钥
kms_key_id	String	**参数解释**： KMS密钥ID，用于标识Token Vault使用的KMS密钥。 **取值范围**： 不涉及。

表 4-288 PolicyEngineConfiguration

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。
mode	String	**参数解释**： 策略集的强制模式。LOG_ONLY模式下策略集会根据策略评估每个操作并记录是否允许或拒绝的跟踪，但不强制执行决策。ENFORCE模式下策略集会根据策略评估操作并通过允许或拒绝来强制执行决策。 **取值范围**： ● LOG_ONLY：仅记录模式，策略集评估操作但不强制执行决策。建议在启用强制执行前使用此模式测试和验证策略。 ● ENFORCE：强制执行模式，策略集评估操作并强制执行决策。

版权所有 © 华为云计算技术有限公司

表 4-289 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-290 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：404

表 4-291 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

为TokenVault绑定策略集。

```
PUT https://{endpoint}/v1/token-vaults/{token_vault_id}

{
  "policy_engine_configuration" : {
    "policy_engine_id" : "abc123def456",
    "mode" : "ENFORCE"
  }
}
```

响应示例

状态码：200

```
{
  "token_vault" : {
    "token_vault_id" : "default",
    "urn" : "agentIdentity:cn-north-4:123456789012:tokenVault:default",
    "kms_configuration" : {
      "key_type" : "CustomerManagedKey",
      "kms_key_id" : "12345678-1234-1234-1234-123456789012"
    },
    "policy_engine_configuration" : {
      "policy_engine_id" : "abc123def456",
```


版权所有 © 华为云计算技术有限公司

```
    "mode" : "ENFORCE"
  },
  "updated_at" : "2025-01-02 00:00:00",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ]
 }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.9 策略集

4.9.1 创建策略集

功能介绍

创建一个新的策略集。

URI

POST /v1/policy-engines

版权所有 © 华为云计算技术有限公司

请求参数

表 4-292 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**： 策略集名称，由用户指定且不可变。 **约束限制**： 不涉及。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。 **默认取值**： 不涉及。
type	是	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **约束限制**： 不涉及。 **取值范围**： ● GATEWAY：用于网关的策略集，可绑定到网关实例。 ● TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。 **默认取值**： 不涉及。
description	否	String	**参数解释**： 策略集的可读描述。 **约束限制**： 不涉及。 **取值范围**： 长度为1~4096个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表，用于为工作负载身份添加标签，便于分类和管理。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-293 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**: 标签键，用于标识标签的名称。 **约束限制**: 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**: 不涉及。
value	是	String	**参数解释**: 标签值，用于标识标签的具体内容。 **约束限制**: 不涉及。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

响应参数

状态码：201

表 4-294 响应 Body 参数

参数	参数类型	描述
policy_engine	**PolicyEngine** object	**参数解释**： 策略集对象。 **取值范围**： 不涉及。

表 4-295 PolicyEngine

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。
name	String	**参数解释**： 策略集名称，由用户指定且不可变。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
type	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **取值范围**： • GATEWAY：用于网关的策略集，可绑定到网关实例。 • TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。
description	String	**参数解释**： 策略集的可读描述。 **取值范围**： 长度为1~4096个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
urn	String	**参数解释**： 策略集的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

表 4-296 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-297 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-298 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

创建策略集。

```
POST https://{endpoint}/v1/policy-engines

{
  "name" : "my_policy_engine",
  "type" : "GATEWAY",
  "description" : "Example policy engine",
  "tags" : [ {
    "key" : "environment",
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ]
}
```

响应示例

状态码：201

```
{
  "policy_engine" : {
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy_engine",
    "type" : "GATEWAY",
    "urn" : "agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>",
    "description" : "Example policy engine",
```


版权所有 © 华为云计算技术有限公司

```
  "tags" : [ {
    "key" : "environment",
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ],
  "created_at" : "2025-01-01 00:00:00",
  "updated_at" : "2025-01-01 00:00:00"
 }
}
```


状态码

状态码	描述
201	请求成功。
400	请求体异常。
409	请求冲突。

错误码

请参见**错误码**。

4.9.2 查询策略集列表

功能介绍

查询策略集列表。支持按类型过滤，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/policy-engines

版权所有 © 华为云计算技术有限公司

表 4-299 Query 参数

参数	是否必选	参数类型	描述
type	否	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **约束限制**： 不涉及。 **取值范围**： ● GATEWAY：用于网关的策略集，可绑定到网关实例。 ● TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。 **默认取值**： 不涉及。
limit	否	Integer	**参数解释**： 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**： 不涉及。 **取值范围**： 1~200。 **默认取值**： 100。
marker	否	String	**参数解释**： 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

无

响应参数

状态码：200

表 4-300 响应 Body 参数

参数	参数类型	描述
policy_engines	Array of **PolicyEngineSummary** objects	**参数解释**： 策略集列表。为 Array of PolicyEngineSummary objects。 **取值范围**： 不涉及。
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-301 PolicyEngineSummary

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。
name	String	**参数解释**： 策略集名称，由用户指定且不可变。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
type	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **取值范围**： • GATEWAY：用于网关的策略集，可绑定到网关实例。 • TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。
urn	String	**参数解释**： 策略集的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

表 4-302 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

表 4-303 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-304 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

- 查询策略集列表。

  ```
  GET https://{endpoint}/v1/policy-engines
  ```

- 按类型过滤查询策略集列表。

  ```
  GET https://{endpoint}/v1/policy-engines?type=GATEWAY
  ```

响应示例

状态码：200

```
{
  "policy_engines" : [ {
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy_engine_1",
    "type" : "GATEWAY",
    "urn" : "agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>",
    "tags" : [ {
      "key" : "environment",
      "value" : "production"
    } ],
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00"
  }, {
    "policy_engine_id" : "385624f5-5958-4f36-b171-168303615bcg",
    "name" : "my_policy_engine_2",
    "type" : "TOKEN_VAULT",
    "urn" : "agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>",
```


版权所有 © 华为云计算技术有限公司

```
    "tags" : [ {
      "key" : "team",
      "value" : "platform"
    } ],
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00"
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "marker"
  }
}
```


状态码

状态码	描述
200	请求成功。
400	请求体异常。

错误码

请参见**错误码**。

4.9.3 查询策略集详情

功能介绍

查询策略集详情。

URI

GET /v1/policy-engines/{policy_engine_id}

表 4-305 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

无

响应参数

状态码：200

表 4-306 响应 Body 参数

参数	参数类型	描述
policy_engine	**PolicyEngine** object	**参数解释**： 策略集对象。 **取值范围**： 不涉及。

表 4-307 PolicyEngine

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。
name	String	**参数解释**： 策略集名称，由用户指定且不可变。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
type	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **取值范围**： • GATEWAY：用于网关的策略集，可绑定到网关实例。 • TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
description	String	**参数解释**： 策略集的可读描述。 **取值范围**： 长度为1~4096个字符。
urn	String	**参数解释**： 策略集的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

表 4-308 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-309 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-310 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

无

响应示例

状态码：200

```
{
  "policy_engine" : {
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy_engine",
    "type" : "GATEWAY",
    "description" : "Example policy engine",
    "urn" : "agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>",
    "tags" : [ {
      "key" : "environment",
      "value" : "production"
    }, {
      "key" : "team",
      "value" : "platform"
    } ],
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00"
  }
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.9.4 更新策略集

功能介绍

更新策略集的描述和标签。

URI

PUT /v1/policy-engines/{policy_engine_id}

表 4-311 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-312 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	**参数解释**: 策略集的更新描述。 **约束限制**: 不涉及。 **取值范围**: 长度为1~4096个字符。 **默认取值**: 不涉及。
tags	否	Array of **Tag** objects	**参数解释**: 自定义标签列表，用于为工作负载身份添加标签，便于分类和管理。 **约束限制**: 列表最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

表 4-313 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**: 标签键，用于标识标签的名称。 **约束限制**: 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：200

表 4-314 响应 Body 参数

参数	参数类型	描述
policy_engine	**PolicyEngine** object	**参数解释**： 策略集对象。 **取值范围**： 不涉及。

表 4-315 PolicyEngine

参数	参数类型	描述
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
name	String	**参数解释**： 策略集名称，由用户指定且不可变。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
type	String	**参数解释**： 策略集类型，用于按类型过滤策略集。不指定时返回所有类型的策略集。 **取值范围**： • GATEWAY：用于网关的策略集，可绑定到网关实例。 • TOKEN_VAULT：用于TokenVault的策略集，只能绑定到TokenVault实例。
description	String	**参数解释**： 策略集的可读描述。 **取值范围**： 长度为1~4096个字符。
urn	String	**参数解释**： 策略集的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。
tags	Array of **Tag** objects	**参数解释**： 自定义标签列表。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

表 4-316 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-317 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-318 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-319 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

更新策略集的描述和标签。

```
PUT https://{endpoint}/v1/policy-engines/{policy_engine_id}

{
  "description" : "Updated description",
  "tags" : [ {
    "key" : "environment",
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ]
}
```

响应示例

状态码：200

```
{
  "policy_engine" : {
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy_engine",
    "type" : "GATEWAY",
    "description" : "Updated description",
    "urn" : "agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>",
    "tags" : [ {
      "key" : "environment",
```


版权所有 © 华为云计算技术有限公司

```
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ],
  "created_at" : "2025-01-01 00:00:00",
  "updated_at" : "2025-01-03 00:00:00"
 }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.9.5 删除策略集

功能介绍

删除指定的策略集。

URI

DELETE /v1/policy-engines/{policy_engine_id}

表 4-320 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

无

响应参数

状态码：204

无

状态码：400

表 4-321 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-322 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：409

表 4-323 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求示例

删除策略集。

```
DELETE https://{endpoint}/v1/policy-engines/{policy_engine_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.9.6 查询策略集关联的实体列表

功能介绍

查询指定策略集关联的实体（网关和令牌保管库）列表。支持分页查询，可通过limit和marker参数控制返回结果的数量和起始位置。

URI

GET /v1/policy-engines/{policy_engine_id}/attachments

版权所有 © 华为云计算技术有限公司

表 4-324 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**： 不涉及。

表 4-325 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**： 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**： 不涉及。 **取值范围**： 1~200。 **默认取值**： 100。
marker	否	String	**参数解释**： 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**： 不涉及。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

无

响应参数

状态码：200

表 4-326 响应 Body 参数

参数	参数类型	描述
attachments	Array of **PolicyEngineAttachmentSummary** objects	**参数解释**： 策略集关联列表。 **取值范围**： 不涉及。
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-327 PolicyEngineAttachmentSummary

参数	参数类型	描述
entity_type	String	**参数解释**： 可关联到策略集的实体类型。 **取值范围**： • GATEWAY：网关 • TOKEN_VAULT：Token Vault
entity_id	String	**参数解释**： 关联实体的唯一标识符。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
mode	String	**参数解释**： 策略集的强制模式。LOG_ONLY模式下策略集会根据策略评估每个操作并记录是否允许或拒绝的跟踪，但不强制执行决策。ENFORCE模式下策略集会根据策略评估操作并通过允许或拒绝来强制执行决策。 **取值范围**： ● LOG_ONLY：仅记录模式，策略集评估操作但不强制执行决策。建议在启用强制执行前使用此模式测试和验证策略。 ● ENFORCE：强制执行模式，策略集评估操作并强制执行决策。
attached_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

表 4-328 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-329 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-330 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

- 查询策略集关联的实体列表。

  ```
  GET https://{endpoint}/v1/policy-engines/{policy_engine_id}/attachments
  ```

- 分页查询策略集关联的实体列表。

  ```
  GET https://{endpoint}/v1/policy-engines/{policy_engine_id}/attachments?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "attachments" : [ {
    "entity_type" : "GATEWAY",
    "entity_id" : "b2fc0463-8b28-46c5-87ba-6267295ffc57",
    "mode" : "LOG_ONLY",
    "attached_at" : "2025-01-01 00:00:00"
  }, {
    "entity_type" : "TOKEN_VAULT",
    "entity_id" : "default",
    "mode" : "ENFORCE",
    "attached_at" : "2025-01-02 00:00:00"
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "marker"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.10 策略

4.10.1 在指定策略集中创建策略

功能介绍

在指定策略集中创建策略。

URI

POST /v1/policy-engines/{policy_engine_id}/policies

表 4-331 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-332 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	**参数解释**: 策略名称，用于标识和区分不同的策略。 **约束限制**: 不涉及。 **取值范围**: 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。 **默认取值**: 不涉及。
description	否	String	**参数解释**: 策略的可读描述。 **约束限制**: 不涉及。 **取值范围**: 长度为1~4096个字符。 **默认取值**: 不涉及。
definition	是	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **约束限制**: 只能指定cedar成员。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
validation_mode	否	String	**参数解释**: 策略创建/更新的验证模式。 **约束限制**: 不涉及。 **取值范围**: • FAIL_ON_ANY_FINDINGS: 如果Cedar分析器报告任何发现则失败（默认）。 • IGNORE_ALL_FINDINGS: 即使检测到发现也允许创建/更新。 **默认取值**: FAIL_ON_ANY_FINDINGS

表 4-333 PolicyDefinition

参数	是否必选	参数类型	描述
cedar	是	CedarPolicy object	**参数解释**: Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **约束限制**: 不涉及。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-334 CedarPolicy

参数	是否必选	参数类型	描述
statement	是	String	**参数解释**： Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **约束限制**： 不涉及。 **取值范围**： 长度为34~10000个字符。

响应参数

状态码：202

表 4-335 响应 Body 参数

参数	参数类型	描述
policy	**Policy** object	**参数解释**： 策略对象。 **取值范围**： 不涉及。

表 4-336 Policy

参数	参数类型	描述
policy_id	String	**参数解释**： 策略ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。
name	String	**参数解释**： 策略名称，用于标识和区分不同的策略。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
description	String	**参数解释**: 策略的可读描述。 **取值范围**: 长度为1~4096个字符。
urn	String	**参数解释**: 策略的统一资源名称（URN）。 **取值范围**: 长度为1~1024个字符。
pending_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。
active_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。
status	String	**参数解释**: 策略的当前状态。 **取值范围**: ● CREATING：策略正在创建中 ● ACTIVE：策略已激活并可用 ● UPDATING：策略正在更新中 ● DELETING：策略正在删除中 ● CREATE_FAILED：策略创建失败 ● UPDATE_FAILED：策略更新失败 ● DELETE_FAILED：策略删除失败
status_reasons	Array of strings	**参数解释**: 关于策略状态的额外信息，提供关于任何失败或策略创建过程当前状态的详细信息。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

表 4-337 PolicyDefinition

参数	参数类型	描述
cedar	**CedarPolicy** object	**参数解释**： Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **取值范围**： 不涉及。

表 4-338 CedarPolicy

参数	参数类型	描述
statement	String	**参数解释**： Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **取值范围**： 长度为34~10000个字符。

版权所有 © 华为云计算技术有限公司

状态码：400

表 4-339 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-340 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

在指定策略集中创建策略。

```
POST https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies

{
  "name" : "my_policy",
  "description" : "Example policy",
  "definition" : {
    "cedar" : {
      "statement" : "permit(principal, action, resource);"
    }
  }
}
```

响应示例

状态码：202

```
{
  "policy" : {
    "policy_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy",
    "description" : "Example policy",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "active_definition" : null,
    "status" : "CREATING",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce"
  }
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
202	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.10.2 查询策略列表

功能介绍

查询策略列表。

URI

GET /v1/policy-engines/{policy_engine_id}/policies

表 4-341 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-342 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**: 每页显示的条目数量，用于控制单次查询返回的工作负载身份数量。 **约束限制**: 不涉及。 **取值范围**: 1~200。 **默认取值**: 100。
marker	否	String	**参数解释**: 分页标记，用于指定查询的起始位置，配合limit使用。当返回结果中存在next_marker时，使用该值作为下一次请求的marker参数以获取下一页数据。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成，长度为4~400个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：200

表 4-343 响应 Body 参数

参数	参数类型	描述
policies	Array of **PolicySummary** objects	**参数解释**: 策略列表。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
page_info	**PageInfo** object	**参数解释**： 分页信息，包含下一页标记和当前页返回条目数量。 **取值范围**： 不涉及。

表 4-344 PolicySummary

参数	参数类型	描述
policy_id	String	**参数解释**： 策略ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。
name	String	**参数解释**： 策略名称，用于标识和区分不同的策略。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
description	String	**参数解释**： 策略的可读描述。 **取值范围**： 长度为1~4096个字符。
urn	String	**参数解释**： 策略的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
status	String	**参数解释**： 策略的当前状态。 **取值范围**： ● CREATING：策略正在创建中 ● ACTIVE：策略已激活并可用 ● UPDATING：策略正在更新中 ● DELETING：策略正在删除中 ● CREATE_FAILED：策略创建失败 ● UPDATE_FAILED：策略更新失败 ● DELETE_FAILED：策略删除失败
status_reasons	Array of strings	**参数解释**： 关于策略状态的额外信息，提供关于任何失败或策略创建过程当前状态的详细信息。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

版权所有 © 华为云计算技术有限公司

表 4-345 PageInfo

参数	参数类型	描述
next_marker	String	**参数解释**： 下一页标记，配合limit参数使用。如果存在，则表示还有后续的条目未显示在当前返回体中。请使用该值作为下一次请求的分页标记参数以获得下一页信息。请反复调用该接口直至该字段不存在。 **取值范围**： 只能由英文字母、数字及"+"、"/"、"="、"-"、"_"组成。
current_count	Integer	**参数解释**： 本页返回的条目数量。 **取值范围**： 不涉及。

状态码：400

表 4-346 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求示例

- 查询策略列表。

  ```
  GET https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies
  ```

- 分页查询策略列表。

  ```
  GET https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies?limit=10&marker=xxx
  ```

响应示例

状态码：200

```
{
  "policies" : [ {
    "policy_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy_1",
    "description" : "Example policy for allowing read access to resources",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "active_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "status" : "ACTIVE",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce"
  }, {
    "policy_id" : "385624f5-5958-4f36-b171-168303615bcg",
    "name" : "my_policy_2",
    "description" : "Example policy for allowing write access to resources",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "active_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "status" : "CREATE_FAILED",
    "status_reasons" : [ "Invalid syntax in statement", "Missing required principal type" ],
    "created_at" : "2025-01-02 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce"
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "marker"
  }
}
```

状态码

状态码	描述
200	请求成功。

版权所有 © 华为云计算技术有限公司

状态码	描述
400	请求体异常。

错误码

请参见**错误码**。

4.10.3 查询策略详情

功能介绍

查询策略详情。

URI

GET /v1/policy-engines/{policy_engine_id}/policies/{policy_id}

表 4-347 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。
policy_id	是	String	**参数解释**: 策略ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

无

响应参数

状态码：200

表 4-348 响应 Body 参数

参数	参数类型	描述
policy	**Policy** object	**参数解释**： 策略对象。 **取值范围**： 不涉及。

表 4-349 Policy

参数	参数类型	描述
policy_id	String	**参数解释**： 策略ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。
name	String	**参数解释**： 策略名称，用于标识和区分不同的策略。 **取值范围**： 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
description	String	**参数解释**： 策略的可读描述。 **取值范围**： 长度为1~4096个字符。
urn	String	**参数解释**： 策略的统一资源名称（URN）。 **取值范围**： 长度为1~1024个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
pending_definition	**PolicyDefinition** object	**参数解释**： 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**： 不涉及。
active_definition	**PolicyDefinition** object	**参数解释**： 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**： 不涉及。
status	String	**参数解释**： 策略的当前状态。 **取值范围**： ● CREATING：策略正在创建中 ● ACTIVE：策略已激活并可用 ● UPDATING：策略正在更新中 ● DELETING：策略正在删除中 ● CREATE_FAILED：策略创建失败 ● UPDATE_FAILED：策略更新失败 ● DELETE_FAILED：策略删除失败
status_reasons	Array of strings	**参数解释**： 关于策略状态的额外信息，提供关于任何失败或策略创建过程当前状态的详细信息。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

表 4-350 PolicyDefinition

参数	参数类型	描述
cedar	**CedarPolicy** object	**参数解释**： Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **取值范围**： 不涉及。

表 4-351 CedarPolicy

参数	参数类型	描述
statement	String	**参数解释**： Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **取值范围**： 长度为34~10000个字符。

状态码：400

版权所有 © 华为云计算技术有限公司

表 4-352 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

表 4-353 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

查询策略详情。

```
GET https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies/{policy_id}
```

响应示例

状态码：200

```
{
  "policy" : {
    "policy_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy",
    "description" : "Example policy",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "active_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "status" : "ACTIVE",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-01 00:00:00"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

4.10.4 更新策略

功能介绍

更新策略。

URI

PUT /v1/policy-engines/{policy_engine_id}/policies/{policy_id}

表 4-354 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。
policy_id	是	String	**参数解释**: 策略ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-355 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	**参数解释**: 策略的更新描述。 **约束限制**: 不涉及。 **取值范围**: 长度为1~4096个字符。 **默认取值**: 不涉及。
definition	否	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **约束限制**: 只能指定cedar成员。 **取值范围**: 不涉及。 **默认取值**: 不涉及。
validation_mode	否	String	**参数解释**: 策略创建/更新的验证模式。 **约束限制**: 不涉及。 **取值范围**: • FAIL_ON_ANY_FINDINGS：如果Cedar分析器报告任何发现则失败（默认）。 • IGNORE_ALL_FINDINGS：即使检测到发现也允许创建/更新。 **默认取值**: FAIL_ON_ANY_FINDINGS

版权所有 © 华为云计算技术有限公司

表 4-356 PolicyDefinition

参数	是否必选	参数类型	描述
cedar	是	CedarPolicy object	**参数解释**： Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **约束限制**： 不涉及。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

表 4-357 CedarPolicy

参数	是否必选	参数类型	描述
statement	是	String	**参数解释**： Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **约束限制**： 不涉及。 **取值范围**： 长度为34~10000个字符。

响应参数

状态码：202

表 4-358 响应 Body 参数

参数	参数类型	描述
policy	Policy object	**参数解释**： 策略对象。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-359 Policy

参数	参数类型	描述
policy_id	String	**参数解释**: 策略ID，系统自动生成的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。
name	String	**参数解释**: 策略名称，用于标识和区分不同的策略。 **取值范围**: 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
description	String	**参数解释**: 策略的可读描述。 **取值范围**: 长度为1~4096个字符。
urn	String	**参数解释**: 策略的统一资源名称（URN）。 **取值范围**: 长度为1~1024个字符。
pending_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。
active_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
status	String	**参数解释**： 策略的当前状态。 **取值范围**： ● CREATING：策略正在创建中 ● ACTIVE：策略已激活并可用 ● UPDATING：策略正在更新中 ● DELETING：策略正在删除中 ● CREATE_FAILED：策略创建失败 ● UPDATE_FAILED：策略更新失败 ● DELETE_FAILED：策略删除失败
status_reasons	Array of strings	**参数解释**： 关于策略状态的额外信息，提供关于任何失败或策略创建过程当前状态的详细信息。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

版权所有 © 华为云计算技术有限公司

表 4-360 PolicyDefinition

参数	参数类型	描述
cedar	CedarPolicy object	**参数解释**: Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **取值范围**: 不涉及。

表 4-361 CedarPolicy

参数	参数类型	描述
statement	String	**参数解释**: Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **取值范围**: 长度为34~10000个字符。

状态码：400

表 4-362 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-363 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

更新策略的描述和定义。

```
PUT https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies/{policy_id}

{
  "description" : "Updated description for the policy",
  "definition" : {
    "cedar" : {
      "statement" : "permit(principal, action, resource);"
    }
```


版权所有 © 华为云计算技术有限公司

```
  }
}
```

响应示例

状态码：202

```
{
  "policy" : {
    "policy_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy",
    "description" : "Updated description for the policy",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource when principal == User::\"alice\");"
      }
    },
    "active_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "status" : "UPDATING",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce"
  }
}
```

状态码

状态码	描述
202	请求成功。
400	请求体异常。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.10.5 删除策略

功能介绍

删除指定的策略。

URI

DELETE /v1/policy-engines/{policy_engine_id}/policies/{policy_id}

版权所有 © 华为云计算技术有限公司

表 4-364 路径参数

参数	是否必选	参数类型	描述
policy_engine_id	是	String	**参数解释**: 策略集ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。 **默认取值**: 不涉及。
policy_id	是	String	**参数解释**: 策略ID，系统自动生成的唯一标识符。 **约束限制**: 不涉及。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。 **默认取值**: 不涉及。

请求参数

无

响应参数

状态码：202

表 4-365 响应 Body 参数

参数	参数类型	描述
policy	**Policy** object	**参数解释**: 策略对象。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-366 Policy

参数	参数类型	描述
policy_id	String	**参数解释**: 策略ID，系统自动生成的唯一标识符。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~128个字符。
name	String	**参数解释**: 策略名称，用于标识和区分不同的策略。 **取值范围**: 只能以英文字母开头，由英文字母、数字及"_"组成，长度为1~48个字符。
description	String	**参数解释**: 策略的可读描述。 **取值范围**: 长度为1~4096个字符。
urn	String	**参数解释**: 策略的统一资源名称（URN）。 **取值范围**: 长度为1~1024个字符。
pending_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。
active_definition	**PolicyDefinition** object	**参数解释**: 策略定义结构，封装不同的策略格式和语言，用于定义访问控制规则。这是一个UNION类型，只能指定以下一种成员。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
status	String	**参数解释**： 策略的当前状态。 **取值范围**： ● CREATING：策略正在创建中 ● ACTIVE：策略已激活并可用 ● UPDATING：策略正在更新中 ● DELETING：策略正在删除中 ● CREATE_FAILED：策略创建失败 ● UPDATE_FAILED：策略更新失败 ● DELETE_FAILED：策略删除失败
status_reasons	Array of strings	**参数解释**： 关于策略状态的额外信息，提供关于任何失败或策略创建过程当前状态的详细信息。 **取值范围**： 不涉及。
created_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
updated_at	String	**参数解释**： UTC时间戳，记录资源的创建或更新时间。 **取值范围**： 使用UTC+0时间格式，格式为yyyy-MM-ddTHH:mm:ssZ。例如：2025-01-01T00:00:00Z。
policy_engine_id	String	**参数解释**： 策略集ID，系统自动生成的唯一标识符。 **取值范围**： 只能由英文字母、数字及"-"、"_"组成，长度为12~59个字符。

版权所有 © 华为云计算技术有限公司

表 4-367 PolicyDefinition

参数	参数类型	描述
cedar	CedarPolicy object	**参数解释**: Cedar策略定义，用于封装Cedar语法的访问控制策略语句。 **取值范围**: 不涉及。

表 4-368 CedarPolicy

参数	参数类型	描述
statement	String	**参数解释**: Cedar策略语句，定义授权逻辑。该语句遵循Cedar语法，指定主体、操作、资源和条件，用于细粒度访问控制。 **取值范围**: 长度为34~10000个字符。

状态码：400

表 4-369 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

表 4-370 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：409

版权所有 © 华为云计算技术有限公司

表 4-371 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

删除策略。

```
DELETE https://{endpoint}/v1/policy-engines/{policy_engine_id}/policies/{policy_id}
```

响应示例

状态码：202

```
{
  "policy" : {
    "policy_id" : "285624f5-5958-4f36-b171-168303615bce",
    "name" : "my_policy",
    "urn" : "agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>",
    "pending_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "active_definition" : {
      "cedar" : {
        "statement" : "permit(principal, action, resource);"
      }
    },
    "status" : "DELETING",
    "created_at" : "2025-01-01 00:00:00",
    "updated_at" : "2025-01-02 00:00:00",
    "policy_engine_id" : "285624f5-5958-4f36-b171-168303615bce"
```


版权所有 © 华为云计算技术有限公司

```
  }
}
```

状态码

状态码	描述
202	请求成功。
400	请求体异常。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.11 标签

4.11.1 查询项目标签列表

功能介绍

查询项目下某资源类型的所有标签，按key聚合去重。

URI

GET /v1/{resource_type}/tags

版权所有 © 华为云计算技术有限公司

表 4-372 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**： 资源类型，用于指定要操作的资源类型。 **约束限制**： 不涉及。 **取值范围**： ● oauth2CredentialProvider：OAuth2凭证提供商 ● apiKeyCredentialProvider：API Key凭证提供商 ● stsCredentialProvider：STS凭证提供商 ● tokenVault：令牌保管库 ● workloadIdentityDirectory：工作负载身份目录 ● workloadIdentity：工作负载身份 ● policyEngine：策略集 **默认取值**： 不涉及。

表 4-373 Query 参数

参数	是否必选	参数类型	描述
offset	否	Integer	**参数解释**： 分页偏移量，从第一条数据偏移offset条数据后开始查询。 **约束限制**： 不涉及。 **取值范围**： 最小值为0。 **默认取值**： 0。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**： 每页返回的最大资源数量，用于分页查询。 **约束限制**： 不涉及。 **取值范围**： 1~1000。 **默认取值**： 1000。

请求参数

无

响应参数

状态码：200

表 4-374 响应 Body 参数

参数	参数类型	描述
tags	Array of **GroupedTag** objects	**参数解释**： 项目标签聚合列表，按key聚合去重。 **取值范围**： 不涉及。
total_count	Integer	**参数解释**： 标签key总数。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-375 GroupedTag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
values	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-376 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：403

表 4-377 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

- 查询项目标签列表。

  ```
  GET https://{endpoint}/v1/{resource_type}/tags
  ```

- 分页查询项目标签列表。

  ```
  GET https://{endpoint}/v1/{resource_type}/tags?offset=0&limit=10
  ```

响应示例

状态码：200

```
{
  "tags" : [ {
    "key" : "environment",
    "values" : [ "production", "staging" ]
  }, {
    "key" : "team",
    "values" : [ "platform" ]
  } ],
  "total_count" : 2
}
```


版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
200	请求成功。
400	请求体异常。
403	没有操作权限。

错误码

请参见**错误码**。

4.11.2 查询资源标签

功能介绍

查询指定资源的标签列表。

URI

GET /v1/{resource_type}/{resource_id}/tags

版权所有 © 华为云计算技术有限公司

表 4-378 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**： 资源类型，用于指定要操作的资源类型。 **约束限制**： 不涉及。 **取值范围**： ● oauth2CredentialProvider：OAuth2凭证提供商 ● apiKeyCredentialProvider：API Key凭证提供商 ● stsCredentialProvider：STS凭证提供商 ● tokenVault：令牌保管库 ● workloadIdentityDirectory：工作负载身份目录 ● workloadIdentity：工作负载身份 ● policyEngine：策略集 **默认取值**： 不涉及。
resource_id	是	String	**参数解释**： 资源ID，用于唯一标识一个资源。 **约束限制**： 不涉及。 **取值范围**： 只能由字母、数字、"-"和"_"组成，长度为1~64个字符。 **默认取值**： 不涉及。

请求参数

无

响应参数

状态码：200

版权所有 © 华为云计算技术有限公司

表 4-379 响应 Body 参数

参数	参数类型	描述
tags	Array of **Tag** objects	**参数解释**： 资源标签列表。 **取值范围**： 不涉及。

表 4-380 Tag

参数	参数类型	描述
key	String	**参数解释**： 标签键，用于标识标签的名称。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-381 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-382 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-383 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

查询资源标签。

```
GET https://{endpoint}/v1/{resource_type}/{resource_id}/tags
```

响应示例

状态码：200

```
{
  "tags" : [ {
    "key" : "environment",
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

版权所有 © 华为云计算技术有限公司

状态码	描述
403	没有操作权限。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.11.3 查询资源实例列表

功能介绍

根据标签过滤条件查询资源实例列表。

URI

POST /v1/{resource_type}/resource-instances/filter

表 4-384 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**： 资源类型，用于指定要操作的资源类型。 **约束限制**： 不涉及。 **取值范围**： • oauth2CredentialProvider：OAuth2凭证提供商 • apiKeyCredentialProvider：API Key凭证提供商 • stsCredentialProvider：STS凭证提供商 • tokenVault：令牌保管库 • workloadIdentityDirectory：工作负载身份目录 • workloadIdentity：工作负载身份 • policyEngine：策略集 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-385 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	**参数解释**： 每页返回的最大资源数量，用于分页查询。 **约束限制**： 不涉及。 **取值范围**： 1~1000。 **默认取值**： 1000。
offset	否	Integer	**参数解释**： 分页偏移量，从第一条数据偏移offset条数据后开始查询。 **约束限制**： 不涉及。 **取值范围**： 最小值为0。 **默认取值**： 0。

请求参数

表 4-386 请求 Body 参数

参数	是否必选	参数类型	描述
without_any_tag	否	Boolean	**参数解释**： 是否查询不带标签的资源。当该字段为true时，查询所有不带标签的资源，此时忽略"tags"字段。 **约束限制**： 不涉及。 **取值范围**： ● true：查询不带标签的资源。 ● false：按tags字段过滤。 **默认取值**： false

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **TagFilter** objects	**参数解释**： 标签过滤条件列表，用于按标签过滤资源实例。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]，最多包含20个key，每个key下的value最多20个。 **默认取值**： 不涉及。
matches	否	Array of **Match** objects	**参数解释**： 搜索字段列表，用于按资源名称过滤。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]。 **默认取值**： 不涉及。

表 4-387 TagFilter

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识要过滤的标签名称。 **约束限制**： 不涉及。 **取值范围**： 长度为1~128个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
values	是	Array of strings	**参数解释**： 标签值列表，用于标识要过滤的标签值。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]，每个值最大长度255个字符。 **默认取值**： 不涉及。

表 4-388 Match

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 搜索字段的键，用于指定按哪个字段进行搜索。 **约束限制**： 不涉及。 **取值范围**： ● resource_name：按资源名称搜索。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 搜索字段的值，用于指定搜索的关键字。 **约束限制**： 不涉及。 **取值范围**： 每个值最大长度255个unicode字符。 **默认取值**： 不涉及。

响应参数

状态码：200

版权所有 © 华为云计算技术有限公司

表 4-389 响应 Body 参数

参数	参数类型	描述
resources	Array of **ResourceItem** objects	**参数解释**: 资源实例列表。 **取值范围**: 不涉及。
total_count	Integer	**参数解释**: 总记录数。 **取值范围**: 不涉及。

表 4-390 ResourceItem

参数	参数类型	描述
resource_id	String	**参数解释**: 资源ID，用于唯一标识一个资源。 **取值范围**: 不涉及。
resource_name	String	**参数解释**: 资源名称。 **取值范围**: 不涉及。
tags	Array of **Tag** objects	**参数解释**: 标签列表。 **取值范围**: 不涉及。

表 4-391 Tag

参数	参数类型	描述
key	String	**参数解释**: 标签键，用于标识标签的名称。 **取值范围**: 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
value	String	**参数解释**： 标签值，用于标识标签的具体内容。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。

状态码：400

表 4-392 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-393 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

根据标签过滤条件查询资源实例列表。

```
POST https://{endpoint}/v1/{resource_type}/resource-instances/filter

{
  "without_any_tag" : false,
  "tags" : [ {
    "key" : "environment",
    "values" : [ "production" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "my_resource"
  } ]
}
```

响应示例

状态码：200

```
{
  "resources" : [ {
    "resource_id" : "684a2c3e5f1b9d0e7a3c4f56",
    "resource_name" : "my_workload_identity_1",
    "tags" : [ {
      "key" : "environment",
      "value" : "production"
    }, {
```


版权所有 © 华为云计算技术有限公司

```
      "key" : "team",
      "value" : "platform"
    } ]
  }, {
    "resource_id" : "684a2c3e5f1b9d0e7a3c4f57",
    "resource_name" : "my_token_vault_1",
    "tags" : [ {
      "key" : "environment",
      "value" : "staging"
    } ]
  } ],
  "total_count" : 2
}
```


状态码

状态码	描述
200	请求成功。
400	请求体异常。
403	没有操作权限。

错误码

请参见**错误码**。

4.11.4 查询资源实例数量

功能介绍

根据标签过滤条件查询资源实例数量。

URI

POST /v1/{resource_type}/resource-instances/count

版权所有 © 华为云计算技术有限公司

表 4-394 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**： 资源类型，用于指定要操作的资源类型。 **约束限制**： 不涉及。 **取值范围**： ● oauth2CredentialProvider：OAuth2凭证提供商 ● apiKeyCredentialProvider：API Key凭证提供商 ● stsCredentialProvider：STS凭证提供商 ● tokenVault：令牌保管库 ● workloadIdentityDirectory：工作负载身份目录 ● workloadIdentity：工作负载身份 ● policyEngine：策略集 **默认取值**： 不涉及。

请求参数

表 4-395 请求 Body 参数

参数	是否必选	参数类型	描述
without_any_tag	否	Boolean	**参数解释**： 是否查询不带标签的资源。当该字段为true时，查询所有不带标签的资源，此时忽略"tags"字段。 **约束限制**： 不涉及。 **取值范围**： ● true：查询不带标签的资源。 ● false：按tags字段过滤。 **默认取值**： false

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
tags	否	Array of **TagFilter** objects	**参数解释**： 标签过滤条件列表，用于按标签过滤资源实例。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]，最多包含20个key，每个key下的value最多20个。 **默认取值**： 不涉及。
matches	否	Array of **Match** objects	**参数解释**： 搜索字段列表，用于按资源名称过滤。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]。 **默认取值**： 不涉及。

表 4-396 TagFilter

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识要过滤的标签名称。 **约束限制**： 不涉及。 **取值范围**： 长度为1~128个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
values	是	Array of strings	**参数解释**： 标签值列表，用于标识要过滤的标签值。 **约束限制**： 不涉及。 **取值范围**： 数组长度范围[0,20]，每个值最大长度255个字符。 **默认取值**： 不涉及。

表 4-397 Match

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 搜索字段的键，用于指定按哪个字段进行搜索。 **约束限制**： 不涉及。 **取值范围**： ● resource_name：按资源名称搜索。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 搜索字段的值，用于指定搜索的关键字。 **约束限制**： 不涉及。 **取值范围**： 每个值最大长度255个unicode字符。 **默认取值**： 不涉及。

响应参数

状态码：200

版权所有 © 华为云计算技术有限公司

表 4-398 响应 Body 参数

参数	参数类型	描述
total_count	Integer	**参数解释**: 总记录数。 **取值范围**: 不涉及。

状态码：400

表 4-399 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

版权所有 © 华为云计算技术有限公司

表 4-400 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

根据标签过滤条件查询资源实例数量。

```
POST https://{endpoint}/v1/{resource_type}/resource-instances/count

{
  "tags" : [ {
    "key" : "environment",
    "values" : [ "production" ]
  } ]
}
```

响应示例

状态码：200

```
{
  "total_count" : 2
}
```

状态码

状态码	描述
200	查询成功。

版权所有 © 华为云计算技术有限公司

状态码	描述
400	请求体异常。
403	没有操作权限。

错误码

请参见**错误码**。

4.11.5 向指定资源添加标签

功能介绍

向指定资源添加标签。

URI

POST /v1/{resource_type}/{resource_id}/tags/create

表 4-401 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**: 资源类型，用于指定要操作的资源类型。 **约束限制**: 不涉及。 **取值范围**: • oauth2CredentialProvider：OAuth2凭证提供商 • apiKeyCredentialProvider：API Key凭证提供商 • stsCredentialProvider：STS凭证提供商 • tokenVault：令牌保管库 • workloadIdentityDirectory：工作负载身份目录 • workloadIdentity：工作负载身份 • policyEngine：策略集 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
resource_id	是	String	**参数解释**: 资源ID，用于唯一标识一个资源。 **约束限制**: 不涉及。 **取值范围**: 只能由字母、数字、"-"和"_"组成，长度为1~64个字符。 **默认取值**: 不涉及。

请求参数

表 4-402 请求 Body 参数

参数	是否必选	参数类型	描述
tags	是	Array of **Tag** objects	**参数解释**: 自定义标签列表。 **约束限制**: 列表最少1个，最多20个标签。 **取值范围**: 不涉及。 **默认取值**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-403 Tag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。
value	是	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：204

无

状态码：400

表 4-404 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

状态码：403

表 4-405 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

状态码：404

表 4-406 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

请求示例

向指定资源添加标签。

```
POST https://{endpoint}/v1/{resource_type}/{resource_id}/tags/create

{
  "tags" : [ {
    "key" : "environment",
    "value" : "production"
  }, {
    "key" : "team",
    "value" : "platform"
  } ]
}
```

响应示例

无

版权所有 © 华为云计算技术有限公司

状态码

状态码	描述
204	请求成功。
400	请求体异常。
403	没有操作权限。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.11.6 从指定资源中删除标签

功能介绍

从指定资源中删除标签。

URI

POST /v1/{resource_type}/{resource_id}/tags/delete

版权所有 © 华为云计算技术有限公司

表 4-407 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	**参数解释**： 资源类型，用于指定要操作的资源类型。 **约束限制**： 不涉及。 **取值范围**： ● oauth2CredentialProvider：OAuth2凭证提供商 ● apiKeyCredentialProvider：API Key凭证提供商 ● stsCredentialProvider：STS凭证提供商 ● tokenVault：令牌保管库 ● workloadIdentityDirectory：工作负载身份目录 ● workloadIdentity：工作负载身份 ● policyEngine：策略集 **默认取值**： 不涉及。
resource_id	是	String	**参数解释**： 资源ID，用于唯一标识一个资源。 **约束限制**： 不涉及。 **取值范围**： 只能由字母、数字、"-"和"_"组成，长度为1~64个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

请求参数

表 4-408 请求 Body 参数

参数	是否必选	参数类型	描述
tags	是	Array of **UnTag** objects	**参数解释**： 自定义标签列表，指定要删除的标签。 **约束限制**： 列表最多20个标签。 **取值范围**： 不涉及。 **默认取值**： 不涉及。

表 4-409 UnTag

参数	是否必选	参数类型	描述
key	是	String	**参数解释**： 标签键，用于标识标签的名称。 **约束限制**： 首尾不能包含空格，不能以"_sys_"开头。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"符号的任意组合，长度为1~128个字符。 **默认取值**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	是否必选	参数类型	描述
value	否	String	**参数解释**： 标签值，用于标识标签的具体内容。 **约束限制**： 不涉及。 **取值范围**： 可以包含任意语种字母、数字、空格以及"_"、"."、":"、"/"、"="、"+"、"-"、"@"、"&"符号的任意组合，可以是空字符串，长度为0~255个字符。 **默认取值**： 不涉及。

响应参数

状态码：204

无

状态码：400

表 4-410 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

参数	参数类型	描述
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：403

表 4-411 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**： 错误码。 **取值范围**： 不涉及。
error_msg	String	**参数解释**： 错误信息。 **取值范围**： 不涉及。
request_id	String	**参数解释**： 请求ID。 **取值范围**： 不涉及。
encoded_authorization_message	String	**参数解释**： 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**： 不涉及。

状态码：404

版权所有 © 华为云计算技术有限公司

表 4-412 响应 Body 参数

参数	参数类型	描述
error_code	String	**参数解释**: 错误码。 **取值范围**: 不涉及。
error_msg	String	**参数解释**: 错误信息。 **取值范围**: 不涉及。
request_id	String	**参数解释**: 请求ID。 **取值范围**: 不涉及。
encoded_authorization_message	String	**参数解释**: 加密后的认证失败信息，可以通过STS5解密接口进行解密。 **取值范围**: 不涉及。

请求示例

从指定资源中删除标签。

```
POST https://{endpoint}/v1/{resource_type}/{resource_id}/tags/delete

{
  "tags" : [ {
    "key" : "environment"
  }, {
    "key" : "team"
  } ]
}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	请求体异常。

版权所有 © 华为云计算技术有限公司

状态码	描述
403	没有操作权限。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.12 身份提供商

4.12.1 查询身份提供商

功能介绍

查询身份提供商列表。

URI

GET /v1/identity-providers

请求参数

无

响应参数

状态码：200

表 4-413 响应 Body 参数

参数	参数类型	描述
identity_providers	Array of **IdentityProviderListSummary** objects	**参数解释**： 身份提供者列表。 **取值范围**： 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-414 IdentityProviderListSummary

参数	参数类型	描述
identity_provider	String	**参数解释**: 身份提供者编码，用于唯一标识一个身份提供者。 **取值范围**: 只能由英文字母、数字及"-"、"_"组成，长度为1~64个字符。
display_name	String	**参数解释**: 身份提供商的名称。 **取值范围**: 不涉及。
oauth2_discovery	**Oauth2Discovery** object	**参数解释**: OAuth2提供商的发现信息（UNION类型）。 **取值范围**: 不涉及。

表 4-415 Oauth2Discovery

参数	参数类型	描述
discovery_url	String	**参数解释**: OpenID Connect发现地址（Discovery URL），用于获取身份提供商的OIDC配置信息，包括签发者地址、JWKS端点等。 **取值范围**: 必须以https://开头，且以/.well-known/openid-configuration结尾，长度为1~2048个字符。
authorization_server_metadata	**Oauth2AuthorizationServerMetadata** object	**参数解释**: OAuth2提供商的授权服务器元数据。 **取值范围**: 不涉及。

版权所有 © 华为云计算技术有限公司

表 4-416 Oauth2AuthorizationServerMetadata

参数	参数类型	描述
authorization_endpoint	String	**参数解释**: 授权服务器的授权端点。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
issuer	String	**参数解释**: 授权服务器的签发者标识。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
token_endpoint	String	**参数解释**: 授权服务器的令牌端点。 **取值范围**: 必须以https://开头，长度为1~2048个字符。
response_types	Array of strings	**参数解释**: 支持的响应类型列表。 **取值范围**: 数组长度范围[1,20]，每个元素为1~50个字符的字符串。
token_endpoint_auth_methods	Array of strings	**参数解释**: 令牌端点支持的客户端认证方法列表。 **取值范围**: 数组长度范围[1,2]。

请求示例

查询身份提供商列表。

```
GET https://{endpoint}/v1/identity-providers
```

响应示例

状态码：200

```
{
  "identity_providers" : [ {
    "identity_provider" : "MicrosoftOauth2",
    "display_name" : "Microsoft",
    "oauth2_discovery" : {
      "discovery_url" : "https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration"
    }
  }, {
```


版权所有 © 华为云计算技术有限公司

```
    "identity_provider" : "GoogleOauth2",
    "display_name" : "Google",
    "oauth2_discovery" : {
      "discovery_url" : "https://accounts.google.com/.well-known/openid-configuration"
    }
  }, {
    "identity_provider" : "GithubOauth2",
    "display_name" : "GitHub",
    "oauth2_discovery" : {
      "authorization_server_metadata" : {
        "authorization_endpoint" : "https://github.com/login/oauth/authorize",
        "issuer" : "https://token.actions.githubusercontent.com",
        "token_endpoint" : "https://github.com/login/oauth/access_token",
        "response_types" : [ "code", "token", "id_token", "code token", "code id_token", "token id_token",
"code token id_token" ],
        "token_endpoint_auth_methods" : [ "client_secret_post", "client_secret_basic" ]
      }
    }
  } ]
}
```


状态码

状态码	描述
200	请求成功。

错误码

请参见**错误码**。

版权所有 © 华为云计算技术有限公司

5 应用示例

5.1 配置 Agent 身份并获取访问令牌

场景描述

在企业办公自动化场景中，AI Agent需要访问员工的Microsoft数据，以便自动处理邮件分类、文件整理等任务，这涉及到复杂的OAuth 2.0授权流程。

本示例展示如何通过AgentIdentity简化Agent访问Microsoft的开发复杂度，让开发者无需关心OAuth 2.0的底层细节。

总体思路

1. 为Agent创建工作负载身份。

2. 配置Microsoft OAuth2凭证。

3. 获取工作负载访问令牌。

4. 获取Microsoft访问令牌。

涉及的接口如下：

- **创建工作负载身份**
- **创建OAuth2凭证提供商**
- **使用用户ID创建工作负载访问令牌（以用户身份操作）**
- **从资源凭证提供商处获取OAuth 2.0令牌**

步骤1：创建工作负载身份

URI：POST /v1/workload-identities

API文档详情请参见：**创建工作负载身份**

- 请求示例：

```
POST https://{endpoint}/v1/workload-identities

{
  "name": "my_workload_identity",
  "allowed_resource_oauth2_return_urls": [
    "https://example.com/oauth2/callback"
  ],
```


版权所有 © 华为云计算技术有限公司

```
  "authorizer_type": "CUSTOM_JWT",
  "authorizer_configuration": {
    "custom_jwt": {
      "discovery_url": "https://example.com/.well-known/openid-configuration",
      "allowed_audience": ["example-audience"],
      "allowed_clients": ["example-client-id"],
      "allowed_scopes": ["read","write"],
      "custom_claims": [
        {
          "inbound_token_claim_name": "tenant",
          "inbound_token_claim_value_type": "STRING",
          "authorizing_claim_match_value": {
            "claim_match_operator": "EQUALS",
            "claim_match_value": {"match_value_string": "acme"}
          }
        }
      ]
    }
  }
}
```

- 响应示例：

```
{
  "workload_identity": {
    "workload_identity_id": "684a2c3e5f1b9d0e7a3c4f56",
    "name": "my_workload_identity",
    "urn": "agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>",
    "authorizer_type": "CUSTOM_JWT",
    "api_key_secret": null,
    "allowed_resource_oauth2_return_urls": [
      "https://example.com/oauth2/callback"
    ],
    "created_by": {"type": "SERVICE","identifier": "service.AgentRuntime"},
    "created_at": "2025-12-01T08:00:00Z",
    "updated_at": "2025-12-01T08:00:00Z",
    "tags": null
  }
}
```

步骤2：创建Microsoft OAuth2凭证提供商

URI：POST /v1/oauth2-credential-providers

API文档详情请参见：**创建OAuth2凭证提供商**

- 请求示例：

```
POST https://{endpoint}/v1/oauth2-credential-providers

{
  "name": "my_microsoft_oauthprovider",
  "credential_provider_vendor": "MicrosoftOauth2",
  "oauth2_provider_config_input": {
    "microsoft_oauth2_provider_config": {
      "client_id": "285634f5-5958-4f36-b171-168305215bce",
      "client_secret": "28365081388-oovo6094eg8opo187jn0mstj8s2cevku",
      "tenant_id": "285634f5-5958-4f36-b171-168305215bce"
    }
  }
}
```

- 响应示例：

```
{
  "credential_provider": {
    "credential_provider_id": "684a2c3e5f1b9d0e7a3c4f56",
    "name": "my_microsoft_oauthprovider",
    "urn": "agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/<name>",
    "credential_provider_vendor": "MicrosoftOauth2",
    "client_secret": {
```


版权所有 © 华为云计算技术有限公司

```
    "secret_id": "285624f5-5958-4f36-b171-168303615bce",
    "secret_name": "test-secret"
   },
   "callback_url": "https://agent-identity.cn-north-4.myhuaweicloud.com/v1/oauth2/callback/
9c38be75-5973-4709-a211-7e2c438c250d",
   "created_at": "2025-12-01T08:00:00Z",
   "updated_at": "2025-12-01T08:00:00Z",
   "oauth2_provider_config_output": {
    "microsoft_oauth2_provider_config": {
     "oauth2_discovery": {
      "discovery_url": "https://login.microsoftonline.com/common/v2.0/.well-known/openid-
configuration",
      "authorization_server_metadata": null
     },
     "client_id": "285624f5-5958-4f36-b171-168303615bce"
    },
    "google_oauth2_provider_config": null,
    "github_oauth2_provider_config": null,
    "custom_oauth2_provider_config": null
   },
   "tags": null
  }
}
```


注：需在 Microsoft Entra ID 中完成配置，将回调地址添加为应用的 Redirect URI。

步骤3：获取工作负载访问令牌

URI：POST /v1/workload-access-token-for-user-id

API文档详情请参见：**使用用户ID创建工作负载访问令牌（以用户身份操作）**

- 请求示例：

```
POST https://{endpoint}/v1/workload-access-token-for-user-id

{
  "workload_name" : "my_workload_identity",
  "user_id" : "user-12345"
}
```

- 响应示例：

```
{
  "workload_access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expiration": "2025-12-31T23:59:59Z"
}
```

在三种获取工作负载访问令牌的方法中，/v1/workload-access-token（不带用户）签出的WAT不能用于USER_FEDERATION流程；USER_FEDERATION必须使用-for-user-id或-for-jwt。

步骤4：获取Microsoft访问令牌

URI：POST /v1/oauth2/token

API文档详情请参见：**从资源凭证提供商处获取OAuth 2.0令牌**

- 请求示例：

```
POST https://{endpoint}/v1/oauth2/token

{
  "custom_state": "string",
  "force_authentication": false,
  "oauth2_flow": "USER_FEDERATION",
  "resource_credential_provider_name": "my_microsoft_oauthprovider",
  "scopes": ["openid", "email", "profile"],
  "workload_access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

 版权所有 © 华为云计算技术有限公司

- 响应示例（首次调用，USER_FEDERATION）：

```
{
  "authorization_url": "https://{endpoint}/v1/oauth2/authorize?request_uri=urn%3Aietf%3Aparams
%3Aoauth%3Arequest_uri%3A8f14e45f...",
  "session_status": "IN_PROGRESS",
  "session_uri": "urn:ietf:params:oauth:request_uri:abc123"
}
```

Agent 收到首次响应后，将 authorization_url 提供给最终用户，用户在浏览器中打开该链接，登录 Microsoft 账号并同意授权。授权完成后，系统自动完成令牌交换。Agent 携带首次返回的 session_uri 和相同的工作负载访问令牌轮询本接口，待 session_status 变为 SUCCEEDED 后，即可获取 access_token。

- 请求示例（授权后调用，USER_FEDERATION）：

```
POST https://{endpoint}/v1/oauth2/token

{
  "custom_state": "string",
  "force_authentication": false,
  "oauth2_flow": "USER_FEDERATION",
  "resource_credential_provider_name": "my_microsoft_oauthprovider",
  "workload_access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "session_uri": "urn:ietf:params:oauth:request_uri:abc123"
}
```

- 响应示例（用户已完成授权）：

```
{
  "session_uri": "urn:ietf:params:oauth:request_uri:abc123",
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...",
  "expires_at": "2025-12-31T23:59:59Z"
}
```

可根据session_status判断流程状态：IN_PROGRESS表示等待用户授权，可间隔数秒后重新轮询；SUCCEEDED表示授权完成，使用access_token访问Microsoft服务；FAILED表示授权失败（如用户取消授权），需重新发起。Agent获取到访问令牌后，可在令牌有效期内使用该令牌访问Microsoft服务，例如调用 Microsoft Graph 查询邮件：

```
GET https://graph.microsoft.com/v1.0/me/messages
Authorization: Bearer <access_token>
```

 版权所有 © 华为云计算技术有限公司

6 权限和授权项

6.1 权限和授权项说明

如果您需要对您所拥有的AgentIdentity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），如果账号所具备的权限功能已经能满足您的要求，您可以跳过本章节，不影响您使用RGC服务的其他功能。

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

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

例如，用户要授予创建工作负载身份的权限，那么这个IAM用户被授予的策略中必须包含允许“agentIdentity::createWorkloadIdentity”的授权项，该接口才能调用成功。

6.2 身份策略授权参考

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

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

SCP不直接进行授权，只划定权限边界。将SCP绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM身份策略授予权限的有效性受SCP限制，只有在SCP允许范围内的权限才能生效。

IAM服务与Organizations服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：**IAM服务与Organizations服务权限访问控制的区别**。

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

版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑IAM自定义身份策略，请参考**创建自定义身份策略**。
- 如何使用这些元素编辑SCP自定义策略，请参考**创建SCP**。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read和Write等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于Agent Identity定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在身份策略语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于Agent Identity定义的条件键的详细信息请参见**条件（Condition）**。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的API访问。详细信息请参见**身份策略兼容性说明**。

您可以在身份策略语句的Action元素中指定以下Agent Identity的相关操作。

表 6-1 Agent Identity 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::createApiKeyCredentialProvider	授予创建API密钥凭证提供者的权限。	Write	apiKeyCredentialProvider *	-	-
			tokenVault *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::listApiKeyCredentialProviders	授予查询API密钥凭证提供者列表的权限。	List	apiKeyCredentialProvider *	-	-
			tokenVault *	-	
agentIdentity::getApiKeyCredentialProvider	授予查询API密钥凭证提供者详情的权限。	Read	apiKeyCredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
agentIdentity::updateApiKeyCredentialProvider	授予更新API密钥凭证提供者的权限。	Write	apiKeyCredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::deleteApiKeyCredentialProvider	授予删除API密钥凭证提供者的权限。	Write	apiKeyCredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::createOauth2CredentialProvider	授予创建OAuth2凭证提供者的权限。	Write	oauth2CredentialProvider *	-	-
			tokenVault *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::listOauth2CredentialProviders	授予查询OAuth2凭证提供者列表的权限。	List	oauth2CredentialProvider *	-	-
			tokenVault *	-	
agentIdentity::getOauth2CredentialProvider	授予查询OAuth2凭证提供者详情的权限。	Read	oauth2CredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
agentIdentity::updateOauth2CredentialProvider	授予更新OAuth2凭证提供者的权限。	Write	oauth2CredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::deleteOauth2CredentialProvider	授予删除OAuth2凭证提供者的权限。	Write	oauth2CredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
agentIdentity::createStsCredentialProvider	授予创建STS凭证提供者的权限。	Write	stsCredentialProvider *	-	-
			tokenVault *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::listStsCredentialProviders	授予查询STS凭证提供者列表的权限。	List	stsCredentialProvider *	-	-
			tokenVault *	-	
agentIdentity::getStsCredentialProvider	授予查询STS凭证提供者详情的权限。	Read	stsCredentialProvider *	g:ResourceTag/<tag-key>	-

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			token Vault *	g:ResourceTag/<tag-key>	
agentIdentity::updateStsCredentialProvider	授予更新STS凭证提供者的权限。	Write	stsCredentialProvider *	g:ResourceTag/<tag-key>	-
			token Vault *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::deleteStsCredentialProvider	授予删除STS凭证提供者的权限。	Write	stsCredentialProvider *	g:ResourceTag/<tag-key>	-
			token Vault *	g:ResourceTag/<tag-key>	
agentIdentity::createWorkloadIdentity	授予创建工作负载身份的权限。	Write	workloadIdentity Directory *	-	-
			workloadIdentity *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::listWorkloadIdentity	授予查询工作负载身份列表的权限。	List	workloadIdentityDirectory *	-	-
			workloadIdentity *	-	
agentIdentity::getWorkloadIdentity	授予查询工作负载身份详情的权限。	Read	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	
agentIdentity::getAuthorizerConfiguration	授予查询工作负载身份授权配置的权限。	Read	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	
			-	agentIdentity:authorizerType	
agentIdentity::updateWorkloadIdentity	授予更新工作负载身份的权限。	Write	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::deleteWorkloadIdentity	授予删除工作负载身份的权限。	Write	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	
agentIdentity:tokenVault:get	授予查询令牌保管库详情的权限。	Read	tokenVault *	g:ResourceTag/<tag-key>	-
agentIdentity:tokenVault:update	授予更新令牌保管库配置的权限。	Write	tokenVault *	g:ResourceTag/<tag-key>	-
agentIdentity::getResourceApiKey	授予获取与API密钥凭证提供者关联的API密钥的权限。	Read	apiKeyCredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
			-	• agentIdentity:workloadIdentityName • agentIdentity:workloadIdentityDirectoryId	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::getResourceOauth2Token	授予通过OAuth2两方/三方授权流程获取访问令牌，以访问外部资源的权限。	Read	oauth2CredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
			-	• agentIdentity:workloadIdentityName • agentIdentity:workloadIdentityDirectoryId	
agentIdentity::completeResourceTokenAuth	授予通过OAuth2三方授权流程获取访问令牌，以访问外部资源的权限。	Read	oauth2CredentialProvider *	g:ResourceTag/<tag-key>	-
			tokenVault *	g:ResourceTag/<tag-key>	
			-	• agentIdentity:workloadIdentityName • agentIdentity:workloadIdentityDirectoryId	
agentIdentity::getResourceStsToken	授予从STS凭证提供者获取IAM临时凭证的权限。	Read	stsCredentialProvider *	g:ResourceTag/<tag-key>	-

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			token Vault *	g:ResourceTag/<tag-key>	
			-	• agentIdentity:workloadIdentityName • agentIdentity:workloadIdentityDirectoryId	
agentIdentity::createWorkloadAccessToken	授予获取代理工作负载访问令牌的权限。	Write	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	
agentIdentity::createWorkloadAccessTokenForJWT	授予使用JWT令牌获取代表用户操作的代理工作负载访问令牌的权限。	Write	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• agentIdentity:inboundJwtClaim/client_id • agentIdentity:inboundJwtClaim/iss • agentIdentity:inboundJwtClaim/scope • agentIdentity:inboundJwtClaim/sub • agentIdentity:inboundJwtClaim/aud	
agentIdentity::createWorkloadAccessTokenForUserId	授予使用用户ID获取代表用户操作的代理工作负载访问令牌的权限。	Write	workloadIdentityDirectory *	g:ResourceTag/<tag-key>	-
			workloadIdentity *	g:ResourceTag/<tag-key>	
			-	agentIdentity:userId	
agentIdentity:policyEngine:create	授予创建策略引擎的权限。	Write	policyEngine *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity:policyEngine:list	授予查询策略引擎列表的权限。	List	policyEngine *	-	-
agentIdentity:policyEngine:get	授予查询策略引擎详情的权限。	Read	policyEngine *	g:ResourceTag/<tag-key>	-
agentIdentity:policyEngine:update	授予更新策略引擎的权限。	Write	policyEngine *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity:policyEngine:delete	授予删除策略引擎的权限。	Write	policyEngine *	g:ResourceTag/<tag-key>	-
agentIdentity:policyEngine:listAttachments	授予查询策略引擎绑定列表的权限。	Read	policyEngine *	g:ResourceTag/<tag-key>	-
agentIdentity::createPolicy	授予创建策略的权限。	Write	policyEngine *	g:ResourceTag/<tag-key>	-
			policy *	-	
agentIdentity::listPolicies	授予查询策略列表的权限。	List	policyEngine *	g:ResourceTag/<tag-key>	-
			policy *	-	
agentIdentity::getPolicy	授予查询策略详情的权限。	Read	policyEngine *	g:ResourceTag/<tag-key>	-
			policy *	-	
agentIdentity::updatePolicy	授予更新策略的权限。	Write	policyEngine *	g:ResourceTag/<tag-key>	-

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			policy *	-	
agentIdentity::deletePolicy	授予删除策略的权限。	Write	policyEngine *	g:ResourceTag/<tag-key>	-
			policy *	-	
agentIdentity::tagResource	授予创建标签权限。	Tagging	workloadIdentityDirectory	g:ResourceTag/<tag-key>	-
			tokenVault	g:ResourceTag/<tag-key>	
			workloadIdentity	g:ResourceTag/<tag-key>	
			stsCredentialProvider	g:ResourceTag/<tag-key>	
			oauth2CredentialProvider	g:ResourceTag/<tag-key>	
			apiKeyCredentialProvider	g:ResourceTag/<tag-key>	
			policyEngine	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
agentIdentity::unTagResource	授予删除标签权限。	Tagging	workloadIdentityDirectory	g:ResourceTag/<tag-key>	-
			tokenVault	g:ResourceTag/<tag-key>	
			workloadIdentity	g:ResourceTag/<tag-key>	
			stsCredentialProvider	g:ResourceTag/<tag-key>	
			oauth2CredentialProvider	g:ResourceTag/<tag-key>	
			apiKeyCredentialProvider	g:ResourceTag/<tag-key>	
			policyEngine	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
agentIdentity::listTagsForResource	授予查询指定资源标签的权限。	List	workloadIdentityDirectory	g:ResourceTag/<tag-key>	-
			tokenVault	g:ResourceTag/<tag-key>	

版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			workloadIdentity	g:ResourceTag/<tag-key>	
			stsCredentialProvider	g:ResourceTag/<tag-key>	
			oauth2CredentialProvider	g:ResourceTag/<tag-key>	
			apiKeyCredentialProvider	g:ResourceTag/<tag-key>	
			policyEngine	g:ResourceTag/<tag-key>	
agentIdentity::listTags	授予标签获取列表权限。	List	-	-	-
agentIdentity::listResourcesByTag	授予标签查询资源列表权限。	List	-	g:TagKeys	-

Agent Identity的API通常对应着一个或多个授权项。表6-2展示了API与授权项的关系，以及该API需要依赖的授权项。

表 6-2 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/api-key-credential-providers	agentIdentity::createApiKeyCredentialProvider	• csms:secret:create • kms:cmk:createDataKey
GET /v1/api-key-credential-providers	agentIdentity::listApiKeyCredentialProviders	-

版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/api-key-credential-providers/{credential_provider_name}	agentIdentity::getApiKeyCredentialProvider	-
PUT /v1/api-key-credential-providers/{credential_provider_name}	agentIdentity::updateApiKeyCredentialProvider	• csms:secret:createVersion • kms:cmk:createDataKey
DELETE /v1/api-key-credential-providers/{credential_provider_name}	agentIdentity::deleteApiKeyCredentialProvider	csms:secret:delete
POST /v1/oauth2-credential-providers	agentIdentity::createOauth2CredentialProvider	• csms:secret:create • kms:cmk:createDataKey
GET /v1/oauth2-credential-providers	agentIdentity::listOauth2CredentialProviders	-
GET /v1/oauth2-credential-providers/{credential_provider_name}	agentIdentity::getOauth2CredentialProvider	-
PUT /v1/oauth2-credential-providers/{credential_provider_name}	agentIdentity::updateOauth2CredentialProvider	• csms:secret:createVersion • kms:cmk:createDataKey
DELETE /v1/oauth2-credential-providers/{credential_provider_name}	agentIdentity::deleteOauth2CredentialProvider	csms:secret:delete
POST /v1/sts-credential-providers	agentIdentity::createStsCredentialProvider	iam:agencies:pass
GET /v1/sts-credential-providers	agentIdentity::listStsCredentialProviders	-

版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/sts-credential-providers/{credential_provider_name}	agentIdentity::getStsCredentialProvider	-
PUT /v1/sts-credential-providers/{credential_provider_name}	agentIdentity::updateStsCredentialProvider	iam:agencies:pass
DELETE /v1/sts-credential-providers/{credential_provider_name}	agentIdentity::deleteStsCredentialProvider	-
POST /v1/workload-identities	agentIdentity::createWorkloadIdentity	• csms:secret:create • kms:cmk:createDataKey
GET /v1/workload-identities	agentIdentity::listWorkloadIdentity	-
GET /v1/workload-identities/{workload_identity_name}	agentIdentity::getWorkloadIdentity	-
GET /v1/workload-identities/{workload_identity_name}/authorizer-configuration	agentIdentity::getAuthorizerConfiguration	• csms:secret:getVersion • kms:cmk:decryptDataKey
PUT /v1/workload-identities/{workload_identity_name}	agentIdentity::updateWorkloadIdentity	• csms:secret:createVersion • kms:cmk:createDataKey
DELETE /v1/workload-identities/{workload_identity_name}	agentIdentity::deleteWorkloadIdentity	csms:secret:delete
GET /v1/token-vaults/{token_vault_id}	agentIdentity:tokenVault:get	-

版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/token-vaults/{token_vault_id}	agentIdentity:tokenVault:update	-
POST /v1/api-key	agentIdentity::getResourceApiKey	• csms:secret:getVersion • kms:cmk:decryptDataKey
POST /v1/oauth2/token	agentIdentity::getResourceOauth2Token	• csms:secret:getVersion • kms:cmk:decryptDataKey
POST /v1/sts/token	agentIdentity::getResourceStsToken	-
POST /v1/resource-token-auth/complete	agentIdentity::completeResourceTokenAuth	-
POST /v1/workload-access-token	agentIdentity::createWorkloadAccessToken	-
POST /v1/workload-access-token-for-jwt	agentIdentity::createWorkloadAccessTokenForJWT	-
POST /v1/workload-access-token-for-user-id	agentIdentity::createWorkloadAccessTokenForUserId	-
POST /v1/policy-engines	agentIdentity:policyEngine:create	-
GET /v1/policy-engines	agentIdentity:policyEngine:list	-
GET /v1/policy-engines/{policy_engine_id}	agentIdentity:policyEngine:get	-
PUT /v1/policy-engines/{policy_engine_id}	agentIdentity:policyEngine:update	-
DELETE /v1/policy-engines/{policy_engine_id}	agentIdentity:policyEngine:delete	-
GET /v1/policy-engines/{policy_engine_id}/attachments	agentIdentity:policyEngine:listAttachments	-

版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/policy-engines/{policy_engine_id}/policies	agentIdentity::createPolicy	-
GET /v1/policy-engines/{policy_engine_id}/policies	agentIdentity::listPolicies	-
GET /v1/policy-engines/{policy_engine_id}/policies/{policy_id}	agentIdentity::getPolicy	-
PUT /v1/policy-engines/{policy_engine_id}/policies/{policy_id}	agentIdentity::updatePolicy	-
DELETE /v1/policy-engines/{policy_engine_id}/policies/{policy_id}	agentIdentity::deletePolicy	-
POST /v1/{resource_type}/{resource_id}/tags/create	agentIdentity::tagResource	-
-	agentIdentity::unTagResource	-
GET /v1/{resource_type}/{resource_id}/tags	agentIdentity::listTagsForResource	-
GET /v1/{resource_type}/tags	agentIdentity::listTags	-
POST /v1/{resource_type}/resource-instances/filter	agentIdentity::listResourcesByTag	-
POST /v1/{resource_type}/resource-instances/count	agentIdentity::listResourcesByTag	-

版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）用于定义身份策略生效的资源范围。如表6-3中某项操作已指定了对应的资源类型，则在包含该操作的身份策略语句中选择填写对应资源的URN时，身份策略仅对该指定资源生效；未填写对应资源的URN时，身份策略将对指定资源类型下所有资源生效；如未指定资源类型，Resource默认取值为“*”，身份策略将作用于所有资源。此外，您也可在身份策略中设置条件，进一步精细化限定资源类型。

Agent Identity定义了以下可以在自定义身份策略的Resource元素中使用的资源类型。

表 6-3 Agent Identity 支持的资源类型

资源类型	URN
apiKeyCredentialProvider	agentIdentity:<region>:<account-id>:apiKeyCredentialProvider:tokenVault/<token-vault-id>/<name>
policyEngine	agentIdentity:<region>:<account-id>:policyEngine:<policy-engine-id>
workloadIdentityDirectory	agentIdentity:<region>:<account-id>:workloadIdentityDirectory:<workload-directory-id>
oauth2CredentialProvider	agentIdentity:<region>:<account-id>:oauth2CredentialProvider:tokenVault/<token-vault-id>/<name>
stsCredentialProvider	agentIdentity:<region>:<account-id>:stsCredentialProvider:tokenVault/<token-vault-id>/<name>
policy	agentIdentity:<region>:<account-id>:policy:policyEngine/<policy-engine-id>/<policy-id>
tokenVault	agentIdentity:<region>:<account-id>:tokenVault:<token-vault-id>
workloadIdentity	agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括**条件键**和**运算符**。

- 条件键表示身份策略语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：**全局条件键**。
  - 服务级条件键（前缀通常为服务缩写，如agent identity:）仅适用于对应服务的操作，详情请参见**表6-4**。

版权所有 © 华为云计算技术有限公司

  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：**运算符**。

Agent Identity支持的服务级条件键

Agent Identity定义了以下可以在自定义身份策略的Condition元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表 6-4 Agent Identity 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
agentIdentity:authorizerType	string	单值	按工作负载身份授权配置的类型筛选访问权限。
agentIdentity:workloadIdentityName	string	单值	按工作负载身份的名称过滤访问权限。
agentIdentity:workloadIdentityDirectoryId	string	单值	按工作负载身份目录的标识过滤访问权限。
agentIdentity:inboundJwtClaim/client_id	string	单值	按请求中传入的JWT里的client_id声明过滤访问权限。
agentIdentity:inboundJwtClaim/iss	string	单值	按请求中传入的JWT里的签发者（iss）声明过滤访问权限。
agentIdentity:inboundJwtClaim/scope	string	多值	按请求中传入的JWT里的作用域（scope）声明过滤访问权限。
agentIdentity:inboundJwtClaim/sub	string	单值	按请求中传入的JWT里的主体（sub）声明过滤访问权限。
agentIdentity:inboundJwtClaim/aud	string	多值	按请求中传入的JWT里的受众（aud）声明过滤访问权限。
agentIdentity:userId	string	单值	按请求中传入的静态用户ID值过滤访问权限。

版权所有 © 华为云计算技术有限公司

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	错误码说明
100	Continue	继续请求。 这个临时响应用来通知客户端，它的部分请求已经被服务器接收，且仍未被拒绝。
101	Switching Protocols	切换协议。只能切换到更高级的协议。 例如，切换到HTTP的新版本协议。
200	OK	请求成功并返回资源。
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。

版权所有 © 华为云计算技术有限公司

状态码	编码	错误码说明
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。

 版权所有 © 华为云计算技术有限公司

状态码	编码	错误码说明
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。

7.2 错误码

调用接口出错后，将不会返回结果数据。调用方可根据每个接口对应的错误码来定位错误原因。当调用出错时，HTTP 请求返回一个4xx或5xx的HTTP状态码。返回的消息

版权所有 © 华为云计算技术有限公司

体中是具体的错误代码及错误信息。在调用方找不到错误原因时，可以联系华为云客服，并提供错误码，以便我们尽快帮您解决问题。

错误响应 Body 体格式说明

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_code": "AgentIdentity.0027",
   "error_msg": "workload identity already exists",
   "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
```

其中，error_code表示错误码，error_msg表示错误描述信息，request_id表示本次请求的ID。

特别地，如果是因为缺少权限而出错时，错误相应的Body体格式如下所示。

```
{
   "error_code": "AgentIdentity.0027",
   "error_msg": "workload identity already exists",
   "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
   "encoded_authorization_message": "xxx...xxx"
}
```

其中，encoded_authorization_message为该场景下额外提供的字段，表示加密后的认证失败信息，可以通过STS5解密接口进行解密。

错误码说明

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

表 7-2 错误码

状态码	错误码	错误信息	描述	处理措施
403	AgentIdentity.0001	access denied: {0}	访问被拒绝: {0}	请检查用户是否有对应资源的操作权限
400	AgentIdentity.0002	missing header x-user-profile	缺少请求头 x-user-profile	请确认请求头中包含 x-user-profile
400	AgentIdentity.0007	invalid marker	无效的分页标记	请检查分页参数 marker 是否合法
400	AgentIdentity.0031	invalid agency urn	无效的 agency URN	请检查 agency URN 格式是否正确
400	AgentIdentity.0032	duplicate key for: {0}	重复键: {0}	请确保键值唯一，不重复
400	AgentIdentity.0054	tag limit exceeded	标签数量超限	请减少标签数量
400	AgentIdentity.0056	tag policy violation	标签策略违规	请检查标签是否符合标签策略要求

版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	AgentIdentity.0057	policy validation failed	策略验证失败	请检查策略语法是否正确
404	AgentIdentity.0034	no such resource	资源不存在	请确认资源 ID 是否正确
429	AgentIdentity.0053	too many requests, please retry later	请求过多，请稍后重试	请稍后重试
400	AgentIdentity.0003	the credential provider vendor not supported	不支持该凭据提供者厂商	请确认凭证提供商类型是否支持
404	AgentIdentity.0004	no such credential provider	凭据提供者不存在	请确认凭证提供商名称是否正确
409	AgentIdentity.0005	credential provider already exists	凭据提供者已存在	请更换名称或使用已有凭证提供商
400	AgentIdentity.0049	oauth2 credential provider quota exceeded	OAuth2 凭据提供者配额超限	请申请提升配额或删除不用的凭证提供商
400	AgentIdentity.0050	api key credential provider quota exceeded	API Key 凭据提供者配额超限	请申请提升配额或删除不用的凭证提供商
400	AgentIdentity.0051	sts credential provider quota exceeded	STS 凭据提供者配额超限	请申请提升配额或删除不用的凭证提供商
400	AgentIdentity.0006	invalid OIDC configuration	无效的 OIDC 配置	请检查 OIDC 配置参数是否正确
400	AgentIdentity.0008	invalid URL and must end with '/.well-known/openid-configuration'	无效的 URL，必须以 /.well-known/openid-configuration 结尾	请确保 URL 以 /.well-known/openid-configuration 结尾
400	AgentIdentity.0009	HTTPS protocol required for {0}	{0} 需要 HTTPS 协议	请确保使用 HTTPS 协议
400	AgentIdentity.0010	invalid OIDC metadata	无效的 OIDC 元数据	请检查 OIDC 元数据格式是否正确
400	AgentIdentity.0011	Well-Known endpoint unreachable	Well-Known 端点不可达	请确认端点地址可访问且网络连通
400	AgentIdentity.0012	JWKS endpoint unreachable	JWKS 端点不可达	请确认 JWKS 端点地址可访问且网络连通
400	AgentIdentity.0013	JWKS keys array is empty	JWKS keys 数组为空	请确认 JWKS 端点返回的密钥数组非空

 版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	AgentIdentity.0014	invalid jwks format	无效的 JWKS 格式	请检查 JWKS 格式是否符合标准
400	AgentIdentity.0015	authorization_endpoint is required	authorization_endpoint 为必填项	请确认 OIDC 配置中包含 authorization_endpoint
400	AgentIdentity.0016	id_token_signing_alg_values_supported is required	id_token_signing_alg_values_supported 为必填项	请确认 OIDC 配置中包含签名算法列表
400	AgentIdentity.0017	id_token_signing_alg_values_supported must include RS256	id_token_signing_alg_values_supported 必须包含 RS256	请确保签名算法列表包含 RS256
400	AgentIdentity.0020	issuer is required	issuer 为必填项	请确认 OIDC 配置中包含 issuer 字段
400	AgentIdentity.0021	token_endpoint is required	token_endpoint 为必填项	请确认 OIDC 配置中包含 token_endpoint 字段
404	AgentIdentity.0022	no such token vault	Token Vault 不存在	请确认 Token Vault ID 是否正确
404	AgentIdentity.0023	no such workload identity	工作负载身份不存在	请确认工作负载身份名称是否正确
403	AgentIdentity.0024	workloadIdentity is linked to a service and cannot be deleted by the caller	工作负载身份已关联服务，调用方无权删除	请确认该工作负载身份未被服务关联
409	AgentIdentity.0027	workload identity already exists	工作负载身份已存在	请更换名称或使用已有工作负载身份
400	AgentIdentity.0048	workload identity quota exceeded	工作负载身份配额超限	请申请提升配额或删除不用的工作负载身份
400	AgentIdentity.0025	authorizer type does not match authorizer configuration	授权器类型与授权器配置不匹配	请确认授权者类型与配置一致
400	AgentIdentity.0026	invalid custom claims	无效的自定义 claims	请检查自定义声明格式是否正确
409	AgentIdentity.0028	authorizer configuration already exists	授权器配置已存在	请确认是否已存在授权者配置
404	AgentIdentity.0030	no such authorizer configuration	授权器配置不存在	请确认授权者配置名称是否正确

 版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
404	AgentIdentity.0036	no such policy engine	策略集不存在	请确认策略引擎名称是否正确
409	AgentIdentity.0037	policy engine already exists	策略集已存在	请更换名称或使用已有策略引擎
409	AgentIdentity.0038	policy engine has attachments and cannot be deleted	策略集存在关联绑定，无法删除	请先删除关联的附件再删除策略引擎
409	AgentIdentity.0039	policy engine contains policies and cannot be deleted	策略集包含策略，无法删除	请先删除关联的策略再删除策略引擎
400	AgentIdentity.0041	policy engine type mismatch	策略集类型不匹配	请确认策略引擎类型与操作一致
400	AgentIdentity.0042	policy engine quota exceeded	策略集配额超限	请申请提升配额或删除不用的策略引擎
400	AgentIdentity.0052	total policy size exceeds the policy engine limit	策略总大小超出策略集限制	请减小策略总大小或申请提升配额
400	AgentIdentity.0043	policy quota exceeded	策略配额超限	请申请提升配额或删除不用的策略
400	AgentIdentity.0044	policy is in a transitional state and cannot be modified	策略处于过渡状态，无法修改	请稍后重试，等待策略状态稳定
400	AgentIdentity.0045	policy size limit exceeded	策略大小超限	请减小策略内容大小
404	AgentIdentity.0046	no such policy	策略不存在	请确认策略名称是否正确
409	AgentIdentity.0047	policy already exists	策略已存在	请更换名称或使用已有策略
400	AgentIdentity.1001	bad request	请求无效	请检查请求参数是否正确
409	AgentIdentity.1002	concurrent modification	并发修改冲突	请稍后重试
400	AgentIdentity.1003	CSMS service rate limit exceeded	CSMS 服务限流	请稍后重试
400	AgentIdentity.1004	invalid CSMS secret format	无效的 CSMS 密钥格式	请检查密钥格式是否正确
404	AgentIdentity.1005	CSMS secret not found	CSMS 密钥不存在	请确认密钥 ID 是否正确

版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
500	AgentIdentity.1006	CSMS service internal error	CSMS 服务内部错误	请联系技术支持
400	AgentIdentity.1007	invalid resource id	无效的资源 ID	请检查资源 ID 格式是否正确
429	AgentIdentityTokenVault.0429	Too Many Requests	请求过多	请降低请求频率，稍后重试
400	AgentIdentityTokenVault.1001	Workload Access Token is invalid or expired	Workload Access Token 无效或已过期	请检查并更新 Workload Access Token
400	AgentIdentityTokenVault.1002	The identity in the request does not match the session identity information	请求中的身份与会话身份信息不匹配	请确保请求中的身份信息与创建会话时一致
400	AgentIdentityTokenVault.1003	Session workload identity mismatch	会话工作负载身份不匹配	请检查请求的工作负载身份是否正确
400	AgentIdentityTokenVault.1004	Identity is empty	身份为空	请提供有效的身份信息
404	AgentIdentityTokenVault.1005	Session not found	会话未找到	请检查会话URI是否正确或会话是否已过期
400	AgentIdentityTokenVault.1006	Failed to get oauth2 token: {0}	获取 OAuth2 token 失败	请检查 OAuth2 配置或联系管理员
403	AgentIdentityTokenVault.1007	access denied: {0}	访问被拒绝	请检查用户是否有对应资源的操作权限
400	AgentIdentityTokenVault.1008	Invalid resource URN	无效的资源 URN	请检查资源 URN 格式是否正确
400	AgentIdentityTokenVault.1009	Conflict: both workload_access_token and security_token are provided	冲突的 token（同时提供了 workload_access_token 和 security_token）	请只提供一种认证方式
400	AgentIdentityTokenVault.1010	Resource oauth2 return url is not in the allowed list for workload identity/ resource_oauth2_return_url should not be set for M2M flow	无效的资源 OAuth2 返回 URL	请检查 OAuth2 返回 URL 配置
400	AgentIdentityTokenVault.1011	Workload identity urn is invalid	无效的工作负载身份 URN	请检查工作负载身份 URN 格式
400	AgentIdentityTokenVault.1012	OAuth2 token has expired	OAuth2 token 已过期	请刷新或重新获取 OAuth2 token

 版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	AgentIdentityTokenVault.1013	STS5 error message or Assume agency failed	STS5 Assume 失败	请检查 STS 配置或联系管理员
400	AgentIdentityTokenVault.1014	Session {0} status is invalid	会话状态无效	请检查会话状态或重新创建会话
400	AgentIdentityTokenVault.1015	User ID and user token cannot both exist	身份不明确（User ID 和 user token 同时存在）	请只提供一种用户身份标识
400	AgentIdentityTokenVault.1016	custom_state is required	custom_state 是必需的	请提供 custom_state 参数
400	AgentIdentityTokenVault.1017	Credential provider ID mismatch	凭证提供者 ID 不匹配	请检查凭证提供者 ID 是否与请求一致
400	AgentIdentityTokenVault.1018	Invalid request URI format: {0}. Expected format: urn:ietf:params:oauth:request_uri:[a-zA-Z0-9-._~]+ with length between 1 and 1024	无效的会话 URI 格式	请按照指定格式提供 request_uri
400	AgentIdentityTokenVault.1019	Invalid user token	无效的用户 token	请检查并更新用户 token
400	AgentIdentityTokenVault.1020	custom_parameters should not be set for M2M flow	M2M 流程不应设置 custom_parameters	请移除 custom_parameters 参数
400	AgentIdentityTokenVault.1021	Failed to parse client_credentials token response	解析 client_credentials token 响应失败	请检查 OAuth2 服务端响应
400	AgentIdentityTokenVault.1022	Failed to request client_credentials token	请求 client_credentials token 失败	请检查 OAuth2 配置或联系管理员
404	AgentIdentityTokenVault.1101	Resource not found: {0}	资源未找到	请检查资源名称或 URN 是否正确
404	AgentIdentityTokenVault.1102	agency with urn {0} cannot be found	agency 未找到	请检查 agency URN 是否正确
400	AgentIdentityDirectoryService.2002	invalid custom claim validation config	自定义声明验证配置无效	请检查 JWT 自定义声明验证配置
400	AgentIdentityDirectoryService.2003	failed to discover provider metadata	Provider 元数据发现失败	请检查 JWT 配置中的 discovery_url 是否可访问

 版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	AgentIdentityDirectoryService.2004	failed to parse JWT token	JWT 解析失败	请检查 user_token 格式是否正确
400	AgentIdentityDirectoryService.2005	failed to verify JWT claims	JWT Claims 验证失败	请检查 JWT 中的声明信息
400	AgentIdentityDirectoryService.2006	invalid JWT audience	无效的 audience	请检查 JWT 中的 aud 声明
400	AgentIdentityDirectoryService.2007	invalid JWT client ID	无效的 client_id	请检查 JWT 中的 client_id 声明
400	AgentIdentityDirectoryService.2008	invalid JWT scope	无效的 scope	请检查 JWT 中的 scope 声明
400	AgentIdentityDirectoryService.2009	invalid custom claim	无效的自定义声明	请检查 JWT 中的自定义声明
400	AgentIdentityDirectoryService.3003	both source_ip and source_vpce are missing in context_attributes	缺少 source_ip 和 source_vpce	请确认请求包含 source_ip 或 source_vpce
400	AgentIdentityDirectoryService.3004	invalid source_vpce	source_vpce 格式无效	请检查 x-source-vpce 请求头格式（需为 UUID）
400	AgentIdentityDirectoryService.3005	invalid user_profile	user_profile 格式无效	请检查 x-user-profile 请求头 JSON 格式
400	AgentIdentityDirectoryService.3006	missing user_profile	缺少 user_profile	请确认请求头中包含 x-user-profile
400	AgentIdentityDirectoryService.3007	missing context_attributes	缺少上下文属性	请确认请求头中包含 x-context-attributes
400	AgentIdentityDirectoryService.3008	invalid context_attributes	上下文属性格式无效	请检查 x-context-attributes 请求头 JSON 格式
400	AgentIdentityDirectoryService.3009	resource urn {urn} in the request is invalid	无效的资源 URN	请检查资源 URN 格式是否正确

 版权所有 © 华为云计算技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	AgentIdentityDirectoryService.3010	security token format is invalid	无效的安全令牌	请检查 x-security-token 请求头
400	AgentIdentityDirectoryService.3011	security token key with issuer {issuer} cannot be found	安全令牌密钥未找到	请联系管理员检查安全令牌配置
400	AgentIdentityDirectoryService.3012	unknown security token key version {version}	未知的安全令牌密钥版本	请检查安全令牌版本
400	AgentIdentityDirectoryService.3013	principal id {id} in the user profile is invalid	无效的 Principal ID	请检查 Principal ID 格式
404	AgentIdentityDirectoryService.3014	user id {user_id} in the user profile cannot be found	用户未找到	请检查用户 ID 是否正确

版权所有 © 华为云计算技术有限公司