统一身份认证（新版）

API 参考

文档版本 01

发布日期 2024-09-04

华为云计算技术有限公司

商标声明


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

注意

您购买的产品、服务或特性等应受华为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

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

IAM除了支持界面控制台操作外，还提供API供您调用，您可以使用本文档提供的API对IAM进行相关操作，如创建用户、创建用户组等。在调用IAM的API之前，请确保已经充分了解IAM的相关概念，详细信息请参见：《统一身份认证用户指南》的“产品介绍”章节。

终端节点

IAM

终端节点即调用API的请求地址，不同服务在不同区域的终端节点不同，您可以从**地区和终端节点**中查询IAM的终端节点。

IAM的终端节点如**表1**所示。IAM是全局级服务，数据全局一份，IAM所有的API都可以使用全局服务的Endpoint调用；除了全局区域外，为了配合其他区域级云服务的API/CLI访问，IAM在其他区域（除全局服务外的所有区域）提供部分API，您可以根据需要选择就近区域的终端节点调用API。

表 1-1 IAM 的终端节点

区域名称	区域	终端节点（Endpoint）
全局	global	iam.myhuaweicloud.com
华北-北京一	cn-north-1	iam.cn-north-1.myhuaweicloud.com
华北-北京四	cn-north-4	iam.cn-north-4.myhuaweicloud.com
华东-上海一	cn-east-3	iam.cn-east-3.myhuaweicloud.com
华东-上海二	cn-east-2	iam.cn-east-2.myhuaweicloud.com

区域名称	区域	终端节点（Endpoint）
华南-广州	cn-south-1	iam.cn-south-1.myhuaweicloud.com
西南-贵阳一	cn-southwest-2	iam.cn-southwest-2.myhuaweicloud.com
中国-香港	ap-southeast-1	iam.ap-southeast-1.myhuaweicloud.com
亚太-曼谷	ap-southeast-2	iam.ap-southeast-2.myhuaweicloud.com
亚太-新加坡	ap-southeast-3	iam.ap-southeast-3.myhuaweicloud.com
亚太-雅加达	ap-southeast-4	iam.ap-southeast-4.myhuaweicloud.com
非洲-约翰内斯堡	af-south-1	iam.af-south-1.myhuaweicloud.com
拉美-圣地亚哥	la-south-2	iam.la-south-2.myhuaweicloud.com
土耳其-伊斯坦布尔	tr-west-1	iam.tr-west-1.myhuaweicloud.com

STS

STS的终端节点如表1-2所示。STS是区域级服务，数据在每个区域存储，您可以根据需要选择就近区域的终端节点调用API。

表 1-2 STS 的终端节点

区域名称	区域	终端节点（Endpoint）
华北-北京四	cn-north-4	sts.cn-north-4.myhuaweicloud.com
华东-上海一	cn-east-3	sts.cn-east-3.myhuaweicloud.com
华南-广州	cn-south-1	sts.cn-south-1.myhuaweicloud.com
西南-贵阳一	cn-southwest-2	sts.cn-southwest-2.myhuaweicloud.com
中国-香港	ap-southeast-1	sts.ap-southeast-1.myhuaweicloud.com
亚太-曼谷	ap-southeast-2	sts.ap-southeast-2.myhuaweicloud.com

区域名称	区域	终端节点（Endpoint）
亚太-新加坡	ap-southeast-3	sts.ap-southeast-3.myhuaweicloud.com
亚太-雅加达	ap-southeast-4	sts.ap-southeast-4.myhuaweicloud.com
非洲-约翰内斯堡	af-south-1	sts.af-south-1.myhuaweicloud.com
拉美-圣地亚哥	la-south-2	sts.la-south-2.myhuaweicloud.com
拉美-圣保罗一	sa-brazil-1	sts.sa-brazil-1.myhuaweicloud.com
土耳其-伊斯坦布尔	tr-west-1	sts.tr-west-1.myhuaweicloud.com

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。

- 区域（Region）

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

  详情请参见**区域和可用区**。

- 可用区（AZ，Availability Zone）

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

2 API 概览

类型	子类型	说明
管控面	IAM用户管理	对IAM用户进行创建，查询，修改，删除操作。
	凭据管理	对永久访问密钥进行创建，查询，修改，删除操作。 对用户登录信息进行创建，查询，修改，删除操作。
	MFA设备管理	对MFA设备进行启用，禁用，创建，查询，删除操作。
	安全设置	对账号的密码策略和登录策略进行查询和修改。
	用户组管理	对用户组进行创建，查询，修改，删除，添加用户，移除用户操作。
	身份策略管理	对身份策略进行创建，查询，删除操作。
	身份策略版本管理	对身份策略版本进行创建，查询，修改，删除操作。
	权限管理	对IAM身份进行附加身份策略，分离身份策略，查询身份策略操作。
	服务关联委托管理	对服务关联委托进行创建，查询，删除操作。
	服务主体查询	获取全部服务主体。
	授权概要查询	查询指定服务授权概要。查询已注册云服务列表。
	委托及信任委托管理	对委托及信任委托进行创建，查询，修改，删除操作。
	账号摘要查询	获取此账号中IAM主体使用情况和IAM配额的摘要信息。
	账号功能查询	获取此账号的功能状态。

类型	子类型	说明
	资源标签管理	对IAM资源进行标签相关的创建，查询，删除操作。
	非对称签名管理	设置租户开启或关闭非对称签名。 获取租户非对称签名开关状态。
临时安全凭证	通过委托或者信任委托获取临时访问密钥	通过委托或者信任委托获取临时访问密钥，临时访问密钥可用于对云资源发起访问。
	获取调用者身份信息	获取调用者（用户，委托等）身份信息。
	解密鉴权失败的原因	解密鉴权失败的原因。

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**通过委托或者信任委托获取临时安全凭证**接口说明如何调用API。该API通过切换已创建的IAM委托或者信任委托获取临时安全凭证，临时安全凭证是用户的访问令牌，承载身份与权限信息，用于调用其他API时进行请求签名。

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。

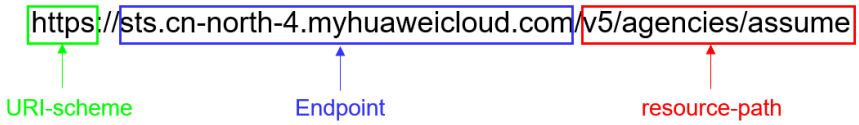
- **URI-scheme**：表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**处获取。例如STS服务在“华北-北京四”区域的Endpoint为“sts.cn-north-4.myhuaweicloud.com”。
- **resource-path**：资源路径，也即API访问路径。从具体API的URI模块获取，例如“通过委托或者信任委托获取临时安全凭证”API的resource-path为“/v5/agencies/assume”。
- **query-string**：查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要通过IAM在“华北-北京四”区域切换委托或者信任委托获取临时安全凭证，则需使用“华北-北京四”区域的Endpoint（sts.cn-

north-4.myhuaweicloud.com），并在**通过委托或者信任委托获取临时安全凭证**的URI部分找到resource-path（/v5/agencies/assume），拼接起来如下所示。

```
https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
```

图 3-1 URI 示意图



说明

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

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **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**通过委托或者信任委托获取临时安全凭证**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
```

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**：请求签名信息，必选。用户可以使用永久AK/SK或者临时安全凭证按照**AK/SK认证**对请求进行签名。

  说明

  API使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

  AK/SK认证的详细说明请参加**AK/SK认证**。
- **X-Project-ID**：子项目ID，可选，在多项目场景中使用。

- **X-Domain-ID**：账号ID (等同于 AccountId)。

对于**通过委托或者信任委托获取临时安全凭证**接口，添加消息头后的请求如下所示。

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
Content-Type: application/json
x-sdk-date: 20191115T033655Z
Authorization: SDK-HMAC-SHA256 Access=QTWAOYTTINDUT2QVKYUC, SignedHeaders=content-type;host;x-sdk-date, Signature=7be6668032f70418fcc22abc52071e57aff61b84a1d2381bb430d6870f4f6ebe
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求体中包含中文，中文字符必须采用UTF-8编码。

每个接口的消息体内容需要参考具体的API定义来填写，也不是每个请求都需要消息体，比如部分GET、DELETE操作就不需要消息体。

对于**通过委托或者信任委托获取临时安全凭证**接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***agency_urn***为目标委托的urn，***agency_session_name***为目标委托的会话名。

说明

duration_seconds参数定义了安全凭证的时效，下面示例中获取的安全凭证仅在1小时内有效。您还可以进一步限制安全凭证权限范围，详细定义请参见**通过委托或者信任委托获取临时安全凭证**。

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
Content-Type: application/json
x-sdk-date: xxxxxxxxxxxxxxxxx
Authorization: ********

{
  "duration_seconds": "3600"
  "agency_urn": "agency_urn",
  "agency_session_name": "agency_session_name",
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于**通过委托或者信任委托获取临时安全凭证**接口，返回的响应消息体中“credentials”就是需要获取的临时安全凭证。有了临时安全凭证之后，您就可以使用AK/SK认证调用其他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。

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。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

3.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**7.1 状态码**。

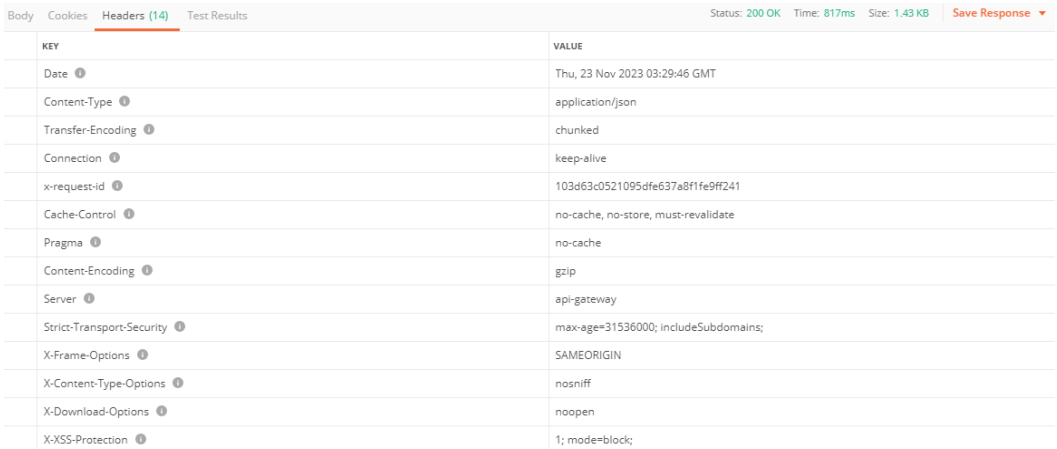
对于**通过委托或者信任委托获取临时安全凭证**接口，如果调用后返回状态码为“200”，则表示请求成功。

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**通过委托或者信任委托获取临时安全凭证**接口，返回如**图3-2**所示的消息头。

图 3-2 通过委托或者信任委托获取临时安全凭证的响应消息头



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**通过委托或者信任委托获取临时安全凭证**接口，返回如下消息体。

```
{
   "source_identity": "{source_identity}",
   "assumed_agency": {
      "urn": "sts::{account_id}::assumed-agency:{agency_name}/{agency_session_name}",
      "id": "{agency_id}:{agency_session_name}"
   },
   "credentials": {
   "access_key_id":"HSTANOXZU2UXBS55JLJ3",
   "secret_access_key":"EoWCQrr...SCcw4Whkt2aXKWAr",
   "security_token":"hQpjbi1XXXXXX...XXXXXbhBbA0TQ==",
   "expiration":"2022-09-07T03:27:51.158Z"
   }
}
```

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体格式示例如下所示。

```
{
   "error_code": "STS5.1106",
   "error_msg": "the agency 'iam::{account_id}:agency:{agency_name}' cannot be found"
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

4 API

4.1 IAM

4.1.1 IAM 用户管理

4.1.1.1 查询 IAM 用户列表

功能介绍

该接口可以用于查询IAM用户列表。

URI

GET /v5/users

表 4-1 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**

参数	是否必选	参数类型	描述
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**
group_id	否	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：200

表 4-2 响应 Body 参数

参数	参数类型	描述
users	Array of **User** objects	IAM用户列表。
page_info	**PageInfo** object	分页信息。

表 4-3 User

参数	参数类型	描述
description	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
user_name	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。
is_root_user	Boolean	IAM用户是否为根用户。
created_at	String	IAM用户创建时间。
user_id	String	IAM用户ID。
urn	String	统一资源名称。
enabled	Boolean	IAM用户是否启用。

表 4-4 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-5 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-6 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

- 查询所有用户列表。

  ```
  GET https://{endpoint}/v5/users
  ```

- 查询用户组xxx中的所有用户列表。

  ```
  GET https://{endpoint}/v5/users?group_id=xxx
  ```

响应示例

状态码：200

请求成功。

```
{
  "users" : [ {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.1.2 创建 IAM 用户

功能介绍

该接口可以用于创建IAM用户。

URI

POST /v5/users

请求参数

表 4-7 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。

参数	是否必选	参数类型	描述
description	否	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
enabled	是	Boolean	IAM用户是否启用。

响应参数

状态码：201

表 4-8 响应 Body 参数

参数	参数类型	描述
user	**User** object	IAM用户。

表 4-9 User

参数	参数类型	描述
description	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
user_name	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。
is_root_user	Boolean	IAM用户是否为根用户。
created_at	String	IAM用户创建时间。
user_id	String	IAM用户ID。
urn	String	统一资源名称。
enabled	Boolean	IAM用户是否启用。

状态码：400

表 4-10 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-11 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：409

表 4-12 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建名为name的IAM用户。

```
POST https://{endpoint}/v5/users

{
  "name" : "name",
  "description" : "description",
  "enabled" : true
}
```

响应示例

状态码：201

请求成功。


```
{
  "user" : {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true
  }
}
```

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**。

4.1.1.3 查询 IAM 用户最后登录时间

功能介绍

该接口可以用于查询IAM用户的最后登录时间。

URI

GET /v5/users/{user_id}/last-login

表 4-13 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：200

表 4-14 响应 Body 参数

参数	参数类型	描述
user_last_login	**UserLastLogin** object	IAM用户最后登录时间。

表 4-15 UserLastLogin

参数	参数类型	描述
last_login_at	String	IAM用户最后登录时间。若为null，则表示从未登录过。

状态码：403

表 4-16 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-17 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询IAM用户的最后登录时间。

```
GET https://{endpoint}/v5/users/{user_id}/last-login
```

响应示例

状态码：200

请求成功。

```
{
  "user_last_login" : {
    "last_login_at" : "2023-09-13T03:32:02.563Z"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.1.4 查询 IAM 用户详情

功能介绍

该接口可以用于查询IAM用户详情。

URI

GET /v5/users/{user_id}

表 4-18 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：200

表 4-19 响应 Body 参数

参数	参数类型	描述
user	**UserEx** object	IAM用户。

表 4-20 UserEx

参数	参数类型	描述
description	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
user_name	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。
is_root_user	Boolean	IAM用户是否为根用户。
created_at	String	IAM用户创建时间。
user_id	String	IAM用户ID。
urn	String	统一资源名称。
enabled	Boolean	IAM用户是否启用。
tags	Array of **Tag** objects	自定义标签列表。

表 4-21 Tag

参数	参数类型	描述
tag_key	String	标签键，可以包含任意语种字母、数字、空格以及"_"、"."、":"、"="、"+"、"-"、"@"符号的任意组合，但是首尾不能包含空格以及不能使用"_sys_"为开头，长度范围[1,64]。 最小长度：**1** 最大长度：**64**
tag_value	String	标签值，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，长度范围[0,128]。 最小长度：**0** 最大长度：**128**

状态码：403

表 4-22 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-23 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询IAM用户详情。

```
GET https://{endpoint}/v5/users/{user_id}
```

响应示例

状态码：200

请求成功。

```
{
  "user" : {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true,
    "tags" : [ {
      "tag_key" : "key",
      "tag_value" : "value"
    } ]
  }
}
```


状态码

状态码	描述
200	请求成功。
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**。

4.1.1.5 修改 IAM 用户信息

功能介绍

该接口可以用于修改IAM用户信息。

URI

PUT /v5/users/{user_id}

表 4-24 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

表 4-25 请求 Body 参数

参数	是否必选	参数类型	描述
new_user_name	否	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。
new_description	否	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
enabled	否	Boolean	IAM用户是否启用。

响应参数

状态码：200

表 4-26 响应 Body 参数

参数	参数类型	描述
user	**User** object	IAM用户。

表 4-27 User

参数	参数类型	描述
description	String	IAM用户描述信息，长度为0到255个字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。
user_name	String	IAM用户名，长度为1到64个字符，只包含字母、数字、"_"、"-"、"."和空格的字符串，且首位不能为数字。
is_root_user	Boolean	IAM用户是否为根用户。
created_at	String	IAM用户创建时间。
user_id	String	IAM用户ID。
urn	String	统一资源名称。
enabled	Boolean	IAM用户是否启用。

状态码：400

表 4-28 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-29 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。

参数	参数类型	描述
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-30 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-31 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

修改IAM用户信息。

```
PUT https://{endpoint}/v5/users/{user_id}

{
  "new_user_name" : "name",
  "new_description" : "description",
  "enabled" : true
}
```

响应示例

状态码：200

请求成功。

```
{
  "user" : {
```



```
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true,
    "tags" : [ {
      "tag_key" : "key",
      "tag_value" : "value"
    } ]
  }
}
```

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**。

4.1.1.6 删除 IAM 用户

功能介绍

该接口可以用于删除指定IAM用户。

URI

DELETE /v5/users/{user_id}

表 4-32 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-33 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-34 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-35 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除指定IAM用户。

```
DELETE https://{endpoint}/v5/users/{user_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.2 凭据管理

4.1.2.1 查询指定永久访问密钥最后使用时间

功能介绍

该接口可以用于查询IAM用户的指定永久访问密钥的最后使用时间。

URI

GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used

表 4-36 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
access_key_id	是	String	永久访问密钥ID，即AK。 最小长度：**1** 最大长度：**40**

请求参数

无

响应参数

状态码：200

表 4-37 响应 Body 参数

参数	参数类型	描述
access_key_last_used	**AccessKeyLastUsed** object	访问密钥的最后使用时间。

表 4-38 AccessKeyLastUsed

参数	参数类型	描述
last_used_at	String	访问密钥的最后使用时间。若不存在则表示从未使用过。

状态码：403

表 4-39 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-40 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询IAM用户的指定永久访问密钥的最后使用时间。

```
GET https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}/last-used
```

响应示例

状态码：200

请求成功。

```
{
  "access_key_last_used" : {
    "last_used_at" : "2023-09-13T06:51:20.550Z"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.2.2 修改指定永久访问密钥

功能介绍

该接口可以用于修改IAM用户的指定永久访问密钥。

URI

PUT /v5/users/{user_id}/access-keys/{access_key_id}

表 4-41 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
access_key_id	是	String	永久访问密钥ID，即AK。 最小长度：**1** 最大长度：**40**

请求参数

表 4-42 请求 Body 参数

参数	是否必选	参数类型	描述
status	是	String	访问密钥状态，可以为“启用”（active）或“停用”（inactive）。

响应参数

状态码：200

表 4-43 响应 Body 参数

参数	参数类型	描述
access_key	**AccessKeyMetadata** object	永久访问密钥。

表 4-44 AccessKeyMetadata

参数	参数类型	描述
user_id	String	IAM用户ID。
access_key_id	String	永久访问密钥ID，即AK。
created_at	String	访问密钥创建时间。
status	String	访问密钥状态，可以为“启用”（active）或“停用”（inactive）。

状态码：403

表 4-45 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-46 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

将IAM用户的指定永久访问密钥的状态置为启用。

```
PUT https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}

{
  "status" : "active"
}
```

响应示例

状态码：200

请求成功。

```
{
  "access_key" : {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.2.3 删除指定永久访问密钥

功能介绍

该接口可以用于删除IAM用户的指定永久访问密钥。

URI

DELETE /v5/users/{user_id}/access-keys/{access_key_id}

表 4-47 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
access_key_id	是	String	永久访问密钥ID，即AK。 最小长度：**1** 最大长度：**40**

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-48 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-49 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除IAM用户的指定永久访问密钥。

```
DELETE https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.2.4 查询所有永久访问密钥

功能介绍

该接口可以用于查询IAM用户的所有永久访问密钥。

URI

GET /v5/users/{user_id}/access-keys

表 4-50 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

表 4-51 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-52 响应 Body 参数

参数	参数类型	描述
access_keys	Array of **AccessKeyMetadata** objects	永久访问密钥列表。
page_info	**PageInfo** object	分页信息。

表 4-53 AccessKeyMetadata

参数	参数类型	描述
user_id	String	IAM用户ID。
access_key_id	String	永久访问密钥ID，即AK。
created_at	String	访问密钥创建时间。
status	String	访问密钥状态，可以为“启用”（active）或“停用”（inactive）。

表 4-54 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-55 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-56 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-57 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询IAM用户的所有永久访问密钥。

```
GET https://{endpoint}/v5/users/{user_id}/access-keys
```

响应示例

状态码：200

请求成功。

```
{
  "access_keys" : [ {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.2.5 创建永久访问密钥

功能介绍

该接口可以用于给IAM用户创建永久访问密钥。

访问密钥（Access Key ID/Secret Access Key，简称AK/SK），是您通过开发工具（API、CLI、SDK）访问的身份凭证，不用于登录控制台。系统通过AK识别访问用户的身份，通过SK进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

URI

POST /v5/users/{user_id}/access-keys

表 4-58 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：201

表 4-59 响应 Body 参数

参数	参数类型	描述
access_key	**AccessKey** object	创建的永久访问密钥。

表 4-60 AccessKey

参数	参数类型	描述
user_id	String	IAM用户ID。
access_key_id	String	创建的永久访问密钥ID，即AK。
created_at	String	访问密钥创建时间。
secret_access_key	String	创建的SK。
status	String	访问密钥状态，可以为“启用”（active）或“停用”（inactive）。

状态码：400

表 4-61 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-62 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-63 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

给IAM用户创建永久访问密钥。

```
POST https://{endpoint}/v5/users/{user_id}/access-keys
```

响应示例

状态码：201

请求成功。

```
{
  "access_key" : {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "secret_access_key" : "secret",
    "status" : "active"
  }
}
```

状态码

状态码	描述
201	请求成功。
400	请求体异常。

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**。

4.1.2.6 修改 IAM 用户密码

功能介绍

该接口可以用于IAM用户修改自己的密码。

URI

POST /v5/caller-password

请求参数

表 4-64 请求 Body 参数

参数	是否必选	参数类型	描述
new_password	是	String	IAM用户的新密码。
old_password	是	String	IAM用户的旧密码。

响应参数

状态码：200

请求成功。

状态码：400

表 4-65 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-66 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-67 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

IAM用户修改自己的密码。旧密码为Password1，新密码为Password2。

```
POST https://{endpoint}/v5/caller-password

{
  "new_password" : "Password2",
  "old_password" : "Password1"
}
```

响应示例

无

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。

错误码

请参见**错误码**。

4.1.2.7 查询 IAM 用户登录信息

功能介绍

该接口可以用于查询指定IAM用户的登录信息。

URI

GET /v5/users/{user_id}/login-profile

表 4-68 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：200

表 4-69 响应 Body 参数

参数	参数类型	描述
login_profile	**LoginProfile** object	IAM用户登录信息。

表 4-70 LoginProfile

参数	参数类型	描述
user_id	String	IAM用户ID。
password_reset_required	Boolean	IAM用户下次登录时是否需要修改密码。
password_expires_at	String	IAM用户密码过期时间。
created_at	String	IAM用户登录信息创建时间。

状态码：403

表 4-71 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-72 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定IAM用户的登录信息。

```
GET https://{endpoint}/v5/users/{user_id}/login-profile
```

响应示例

状态码：200

请求成功。

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```

状态码

状态码	描述
200	请求成功。

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**。

4.1.2.8 创建 IAM 用户登录信息

功能介绍

该接口可以用于创建指定IAM用户的登录信息。

URI

POST /v5/users/{user_id}/login-profile

表 4-73 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

表 4-74 请求 Body 参数

参数	是否必选	参数类型	描述
password	是	String	IAM用户的密码。
password_reset_required	是	Boolean	IAM用户下次登录时是否需要修改密码。

响应参数

状态码：201

表 4-75 响应 Body 参数

参数	参数类型	描述
login_profile	**LoginProfile** object	IAM用户登录信息。

表 4-76 LoginProfile

参数	参数类型	描述
user_id	String	IAM用户ID。
password_reset_required	Boolean	IAM用户下次登录时是否需要修改密码。
password_expires_at	String	IAM用户密码过期时间。
created_at	String	IAM用户登录信息创建时间。

状态码：400

表 4-77 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-78 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-79 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-80 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建指定IAM用户的登录信息，设置其密码为Password0，并要求下次登录时修改密码。

```
POST https://{endpoint}/v5/users/{user_id}/login-profile

{
  "password" : "Password0",
  "password_reset_required" : true
}
```

响应示例

状态码：201

请求成功。

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```

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。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.1.2.9 修改 IAM 用户登录信息

功能介绍

该接口可以用于修改指定IAM用户的登录信息。

URI

PUT /v5/users/{user_id}/login-profile

表 4-81 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

表 4-82 请求 Body 参数

参数	是否必选	参数类型	描述
password	否	String	IAM用户的密码。
password_reset_required	否	Boolean	IAM用户下次登录时是否需要修改密码。

响应参数

状态码：200

表 4-83 响应 Body 参数

参数	参数类型	描述
login_profile	**LoginProfile** object	IAM用户登录信息。

表 4-84 LoginProfile

参数	参数类型	描述
user_id	String	IAM用户ID。
password_reset_required	Boolean	IAM用户下次登录时是否需要修改密码。

参数	参数类型	描述
password_expires_at	String	IAM用户密码过期时间。
created_at	String	IAM用户登录信息创建时间。

状态码：400

表 4-85 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-86 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-87 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

修改指定IAM用户的登录信息，设置其密码为Password0，并要求下次登录时修改密码。

```
PUT https://{endpoint}/v5/users/{user_id}/login-profile

{
  "password" : "Password0",
  "password_reset_required" : true
}
```

响应示例

状态码：200

请求成功。

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```

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。

错误码

请参见**错误码**。

4.1.2.10 删除 IAM 用户登录信息

功能介绍

该接口可以用于删除指定IAM用户的登录信息。

URI

DELETE /v5/users/{user_id}/login-profile

表 4-88 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-89 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-90 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除指定IAM用户的登录信息。

```
DELETE https://{endpoint}/v5/users/{user_id}/login-profile
```

响应示例

无

状态码

状态码	描述
204	请求成功。

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**。

4.1.3 MFA 设备管理

4.1.3.1 列举全部 MFA 设备

功能介绍

该接口可以用于列举全部MFA设备。

URI

GET /v5/mfa-devices

表 4-91 Query 参数

参数	是否必选	参数类型	描述
user_id	否	String	IAM用户ID。
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-92 响应 Body 参数

参数	参数类型	描述
mfa_devices	Array of **MfaDeviceMetadata** objects	虚拟MFA设备列表。
page_info	**PageInfo** object	分页信息。

表 4-93 MfaDeviceMetadata

参数	参数类型	描述
serial_number	String	MFA设备序列号。
user_id	String	IAM用户ID。
enabled	Boolean	虚拟MFA设备是否开启。

表 4-94 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-95 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-96 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

- 列举全部MFA设备。

  ```
  GET https://{endpoint}/v5/mfa-devices
  ```

- 列举IAM用户xxx的全部MFA设备。

  ```
  GET https://{endpoint}/v5/mfa-devices?user_id=xxx
  ```

响应示例

状态码：200

请求成功。

```
{
  "mfa_devices" : [ {
    "serial_number" : "iam::accountid:mfa:name",
    "user_id" : "xxx",
    "enabled" : true
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.3.2 启用 MFA 设备

功能介绍

该接口可以用于启用指定的MFA设备并将其与指定的IAM用户关联。

URI

POST /v5/mfa-devices/enable

请求参数

表 4-97 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
serial_number	是	String	MFA设备序列号。 最大长度：**150**
authentication_code_first	是	String	设备发出的验证码。 最大长度：**12**
authentication_code_second	是	String	设备发出的后续验证码。 最大长度：**12**

响应参数

状态码：200

请求成功。

状态码：400

表 4-98 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-99 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-100 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

启用序列号为iam::accountid:mfa:name的MFA设备并将其与IAM用户xxx关联。

```
POST https://{endpoint}/v5/mfa-devices/enable

{
  "user_id" : "xxx",
  "serial_number" : "iam::accountid:mfa:name",
  "authentication_code_first" : "123456",
  "authentication_code_second" : "123456"
}
```

响应示例

无

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。

错误码

请参见**错误码**。

4.1.3.3 禁用 MFA 设备

功能介绍

该接口可以用于禁用指定的MFA设备并删除其与对应IAM用户的关联。

URI

POST /v5/mfa-devices/disable

请求参数

表 4-101 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
serial_number	是	String	MFA设备序列号。 最大长度：**150**

响应参数

状态码：200

请求成功。

状态码：400

表 4-102 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-103 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

参数	参数类型	描述
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-104 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

禁用序列号为iam::accountid:mfa:name的MFA设备并删除其与IAM用户xxx的关联。

```
POST https://{endpoint}/v5/mfa-devices/disable

{
  "user_id" : "xxx",
  "serial_number" : "iam::accountid:mfa:name"
}
```

响应示例

无

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。

错误码

请参见**错误码**。

4.1.3.4 创建 MFA 设备

功能介绍

该接口可以用于创建MFA设备。

URI

POST /v5/virtual-mfa-devices

请求参数

表 4-105 请求 Body 参数

参数	是否必选	参数类型	描述
virtual_mfa_device_name	是	String	MFA设备名称，长度为1到64个字符，只包含字母、数字、"_"和"-"的字符串。 最小长度：**1** 最大长度：**64**
user_id	是	String	IAM用户ID。

响应参数

状态码：201

表 4-106 响应 Body 参数

参数	参数类型	描述
virtual_mfa_device	**VirtualMfaDevice** object	MFA设备。

表 4-107 VirtualMfaDevice

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

状态码：400

表 4-108 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-109 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-110 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-111 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

为IAM用户xxx创建名为name的MFA设备。

```
POST https://{endpoint}/v5/virtual-mfa-devices

{
  "virtual_mfa_device_name" : "name",
  "user_id" : "xxx"
}
```

响应示例

状态码：201

请求成功。

```
{
  "virtual_mfa_device" : {
    "serial_number" : "iam::accountid:mfa:name",
    "base32_string_seed" : "seed"
  }
}
```

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。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.1.3.5 删除 MFA 设备

功能介绍

该接口可以用于删除MFA设备。

URI

DELETE /v5/virtual-mfa-devices

表 4-112 Query 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。
serial_number	是	String	MFA设备序列号。 最大长度：**150**

请求参数

无

响应参数

状态码：204

请求成功。

状态码：400

表 4-113 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-114 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-115 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除IAM用户xxx的序列号为iam::accountid:mfa:name的MFA设备。

```
DELETE https://{endpoint}/v5/virtual-mfa-devices?user_id=xxx&serial_number=iam%3A%3Aaccountid%3Amfa%3Aname
```

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。

错误码

请参见**错误码**。

4.1.4 安全设置

4.1.4.1 查询账号的 Token 策略

功能介绍

查询账号的Token策略，Token策略控制账号下的所有身份类型（IAM用户、委托、联邦用户）是否允许获取Token（联邦认证获取的unscoped token不受Token策略影响）。

URI

GET /v5/token-policy

请求参数

无

响应参数

状态码：200

表 4-116 响应 Body 参数

参数	参数类型	描述
token_policy	**TokenPolicy** object	账号的Token策略

表 4-117 TokenPolicy

参数	参数类型	描述
token_enabled	Boolean	是否允许获取Token，默认为true，设置为false后将不允许获取账号下所有身份类型（IAM用户、委托、联邦用户）的Token（联邦认证获取的unscoped token不受Token策略影响）。

状态码：403

表 4-118 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

查询账号的Token策略

```
GET https://{endpoint}/v5/token-policy
```

响应示例

状态码：200

请求成功。

```
{
  "token_policy" : {
    "token_enabled" : true
  }
}
```

状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.4.2 修改账号的 Token 策略

功能介绍

修改账号的Token策略，Token策略控制账号下的所有身份类型（IAM用户、委托、联邦用户）是否允许获取Token（联邦认证获取的unscoped token不受Token策略影响）。

URI

PUT /v5/token-policy

请求参数

表 4-119 请求 Body 参数

参数	是否必选	参数类型	描述
token_enabled	否	Boolean	是否允许获取Token，默认为true，设置为false后将不允许获取账号下所有身份类型（IAM用户、委托、联邦用户）的Token（联邦认证获取的unscoped token不受Token策略影响）。

响应参数

状态码：200

表 4-120 响应 Body 参数

参数	参数类型	描述
token_policy	**TokenPolicy** object	账号的Token策略

表 4-121 TokenPolicy

参数	参数类型	描述
token_enabled	Boolean	是否允许获取Token，默认为true，设置为false后将不允许获取账号下所有身份类型（IAM用户、委托、联邦用户）的Token（联邦认证获取的unscoped token不受Token策略影响）。

状态码：400

表 4-122 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-123 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

修改账号的Token策略。

```
PUT https://{endpoint}/v5/token-policy

{
```

```
  "token_enabled" : true
}
```

响应示例

状态码：200

请求成功。

```
{
  "token_policy" : {
    "token_enabled" : true
  }
}
```

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**。

4.1.4.3 查询账号密码策略

功能介绍

该接口可以用于查询账号密码策略。

URI

GET /v5/password-policy

请求参数

无

响应参数

状态码：200

表 4-124 响应 Body 参数

参数	参数类型	描述
password_policy	**PasswordPolicy** object	密码策略。

表 4-125 PasswordPolicy

参数	参数类型	描述
maximum_consecutive_identical_chars	Integer	同一字符连续出现的最大次数。
maximum_password_length	Integer	密码最大字符数。
minimum_password_age	Integer	密码最短使用时间（分钟）。
minimum_password_length	Integer	密码最小字符数。
password_reuse_prevention	Integer	密码不能与历史密码重复次数。
password_not_username_or_invert	Boolean	密码是否可以是用户名或用户名的反序。默认值为true，为true时表示密码不可以是用户名或用户名的反序。
password_requirements	String	设置密码必须包含的字符要求。
password_validity_period	Integer	密码有效期（天）。
password_char_combination	Integer	至少包含字符种类的个数。
allow_user_to_change_password	Boolean	是否允许IAM用户修改自己的密码，不适用于根用户。

状态码：403

表 4-126 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

查询账号密码策略。

```
GET https://{endpoint}/v5/password-policy
```

响应示例

状态码：200

请求成功。

```
{
  "password_policy" : {
    "maximum_consecutive_identical_chars" : 0,
    "maximum_password_length" : 32,
    "minimum_password_age" : 0,
    "minimum_password_length" : 8,
    "password_reuse_prevention" : 1,
    "password_not_username_or_invert" : true,
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "password_validity_period" : 180,
    "password_char_combination" : 2,
    "allow_user_to_change_password" : true
  }
}
```

状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.4.4 修改账号密码策略

功能介绍

该接口可以用于修改账号密码策略。

URI

PUT /v5/password-policy

请求参数

表 4-127 请求 Body 参数

参数	是否必选	参数类型	描述
maximum_consecutive_identical_chars	否	Integer	同一字符连续出现的最大次数，取值范围为[0,32]。 最小值：**0** 最大值：**32**
minimum_password_age	否	Integer	密码最短使用时间（分钟），取值范围为[0,1440]。 最小值：**0** 最大值：**1440**
minimum_password_length	否	Integer	密码最小字符数，取值范围为[8,32]。 最小值：**8** 最大值：**32**
password_reuse_prevention	否	Integer	密码不能与历史密码重复次数，取值范围为[0,24]。 最小值：**0** 最大值：**24**
password_not_username_or_invert	否	Boolean	密码是否可以是用户名或用户名的反序。默认值为true，为true时表示密码不可以是用户名或用户名的反序。
password_validity_period	否	Integer	密码有效期（天），取值范围为[0,180]。 最小值：**0** 最大值：**180**
password_char_combination	否	Integer	至少包含字符种类的个数，取值范围为[2,4]。 最小值：**2** 最大值：**4**
allow_user_to_change_password	否	Boolean	是否允许IAM用户修改自己的密码，不适用于根用户。

响应参数

状态码：200

表 4-128 响应 Body 参数

参数	参数类型	描述
password_policy	**PasswordPolicy** object	密码策略。

表 4-129 PasswordPolicy

参数	参数类型	描述
maximum_consecutive_identical_chars	Integer	同一字符连续出现的最大次数。
maximum_password_length	Integer	密码最大字符数。
minimum_password_age	Integer	密码最短使用时间（分钟）。
minimum_password_length	Integer	密码最小字符数。
password_reuse_prevention	Integer	密码不能与历史密码重复次数。
password_not_username_or_invert	Boolean	密码是否可以是用户名或用户名的反序。默认值为true，为true时表示密码不可以是用户名或用户名的反序。
password_requirements	String	设置密码必须包含的字符要求。
password_validity_period	Integer	密码有效期（天）。
password_char_combination	Integer	至少包含字符种类的个数。
allow_user_to_change_password	Boolean	是否允许IAM用户修改自己的密码，不适用于根用户。

状态码：400

表 4-130 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-131 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

修改账号密码策略。

```
PUT https://{endpoint}/v5/password-policy

{
  "maximum_consecutive_identical_chars" : 0,
  "minimum_password_age" : 0,
  "minimum_password_length" : 8,
  "password_reuse_prevention" : 1,
  "password_not_username_or_invert" : true,
  "password_validity_period" : 180,
  "password_char_combination" : 2,
  "allow_user_to_change_password" : true
}
```

响应示例

状态码：200

请求成功。

```
{
  "password_policy" : {
    "maximum_consecutive_identical_chars" : 0,
    "maximum_password_length" : 32,
    "minimum_password_age" : 0,
    "minimum_password_length" : 8,
    "password_reuse_prevention" : 1,
    "password_not_username_or_invert" : true,
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "password_validity_period" : 180,
    "password_char_combination" : 2,
    "allow_user_to_change_password" : true
  }
}
```

状态码

状态码	描述
200	请求成功。

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**。

4.1.4.5 查询账号登录策略

功能介绍

该接口可以用于查询账号登录策略。

URI

GET /v5/login-policy

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
login_policy	**LoginPolicy** object	登录策略。

表 4-133 LoginPolicy

参数	参数类型	描述
user_validity_period	Integer	如果IAM用户在该值设置的有效期（天）内未登录，则被停用，不适用于根用户。
custom_info_for_login	String	登录提示信息。
lockout_duration	Integer	IAM用户登录锁定时长（分钟）。
login_failed_times	Integer	限定时间内登录失败次数。

参数	参数类型	描述
period_with_login_failures	Integer	限定时间长度（分钟）。
session_timeout	Integer	登录会话失效时间。
show_recent_login_info	Boolean	是否显示最近一次的登录信息。
allow_address_netmasks	Array of **AllowAddressNetmask** objects	允许访问的IP地址或网段。
allow_ip_ranges	Array of **AllowIpRange** objects	允许访问的IP地址区间。

表 4-134 AllowAddressNetmask

参数	参数类型	描述
address_netmask	String	IP地址或网段，例如"192.168.0.1/24"。 最大长度：**50**
description	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

表 4-135 AllowIpRange

参数	参数类型	描述
ip_range	String	IP地址区间，例如"0.0.0.0-255.255.255.255"。 最大长度：**50**
description	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

状态码：403

表 4-136 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

查询账号登录策略。

```
GET https://{endpoint}/v5/login-policy
```

响应示例

状态码：200

请求成功。

```
{
  "login_policy" : {
    "user_validity_period" : 0,
    "custom_info_for_login" : "info",
    "lockout_duration" : 15,
    "login_failed_times" : 5,
    "period_with_login_failures" : 15,
    "session_timeout" : 60,
    "show_recent_login_info" : false,
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "description"
    } ],
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "description"
    } ]
  }
}
```

状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.4.6 修改账号登录策略

功能介绍

该接口可以用于修改账号登录策略。

URI

PUT /v5/login-policy

请求参数

表 4-137 请求 Body 参数

参数	是否必选	参数类型	描述
user_validity_period	否	Integer	如果IAM用户在该值设置的有效期（天）内未登录，则被停用，不适用于根用户，取值范围为[0,240]。 最小值：**0** 最大值：**240**
custom_info_for_login	否	String	登录提示信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**64**
lockout_duration	否	Integer	IAM用户登录锁定时长（分钟），取值范围为[15,1440]。 最小值：**15** 最大值：**1440**
login_failed_times	否	Integer	限定时间内登录失败次数，取值范围为[3,10]。 最小值：**3** 最大值：**10**
period_with_login_failures	否	Integer	限定时间长度（分钟），取值范围为[15,60]。 最小值：**15** 最大值：**60**
session_timeout	否	Integer	登录会话失效时间，取值范围为[15,1440]。 最小值：**15** 最大值：**1440**

参数	是否必选	参数类型	描述
show_recent_login_info	否	Boolean	是否显示最近一次的登录信息。
allow_address_netmasks	否	Array of **AllowAddressNetmask** objects	允许访问的IP地址或网段，例如"xxx.xxx.xxx.xxx/24"。
allow_ip_ranges	否	Array of **AllowIpRange** objects	允许访问的IP地址区间，取值为IP地址区间，例如"0.0.0.0-255.255.255.255"。

表 4-138 AllowAddressNetmask

参数	是否必选	参数类型	描述
address_netmask	是	String	IP地址或网段，例如"192.168.0.1/24"。 最大长度：**50**
description	否	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

表 4-139 AllowIpRange

参数	是否必选	参数类型	描述
ip_range	是	String	IP地址区间，例如"0.0.0.0-255.255.255.255"。 最大长度：**50**
description	否	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

响应参数

状态码：200

表 4-140 响应 Body 参数

参数	参数类型	描述
login_policy	**LoginPolicy** object	登录策略。

表 4-141 LoginPolicy

参数	参数类型	描述
user_validity_period	Integer	如果IAM用户在该值设置的有效期（天）内未登录，则被停用，不适用于根用户。
custom_info_for_login	String	登录提示信息。
lockout_duration	Integer	IAM用户登录锁定时长（分钟）。
login_failed_times	Integer	限定时间内登录失败次数。
period_with_login_failures	Integer	限定时间长度（分钟）。
session_timeout	Integer	登录会话失效时间。
show_recent_login_info	Boolean	是否显示最近一次的登录信息。
allow_address_netmasks	Array of **AllowAddressNetmask** objects	允许访问的IP地址或网段。
allow_ip_ranges	Array of **AllowIpRange** objects	允许访问的IP地址区间。

表 4-142 AllowAddressNetmask

参数	参数类型	描述
address_netmask	String	IP地址或网段，例如"192.168.0.1/24"。 最大长度：**50**
description	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

表 4-143 AllowIpRange

参数	参数类型	描述
ip_range	String	IP地址区间，例如"0.0.0.0-255.255.255.255"。 最大长度：**50**
description	String	描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**255**

状态码：400

表 4-144 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-145 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

修改账号登录策略。

```
PUT https://{endpoint}/v5/login-policy

{
  "user_validity_period" : 0,
  "custom_info_for_login" : "info",
  "lockout_duration" : 15,
  "login_failed_times" : 5,
  "period_with_login_failures" : 15,
  "session_timeout" : 60,
  "show_recent_login_info" : false,
```

```
  "allow_address_netmasks" : [ {
    "address_netmask" : "192.168.0.1/24",
    "description" : "description"
  } ],
  "allow_ip_ranges" : [ {
    "ip_range" : "0.0.0.0-255.255.255.255",
    "description" : "description"
  } ]
}
```

响应示例

状态码：200

请求成功。

```
{
  "login_policy" : {
    "user_validity_period" : 0,
    "custom_info_for_login" : "info",
    "lockout_duration" : 15,
    "login_failed_times" : 5,
    "period_with_login_failures" : 15,
    "session_timeout" : 60,
    "show_recent_login_info" : false,
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "description"
    } ],
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "description"
    } ]
  }
}
```

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**。

4.1.5 用户组管理

4.1.5.1 查询用户组列表

功能介绍

该接口可以用于查询用户组列表。

URI

GET /v5/groups

表 4-146 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**
user_id	否	String	IAM用户ID。

请求参数

无

响应参数

状态码：200

表 4-147 响应 Body 参数

参数	参数类型	描述
groups	Array of **Group** objects	用户组列表。
page_info	**PageInfo** object	分页信息。

表 4-148 Group

参数	参数类型	描述
group_id	String	用户组ID。
group_name	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。

参数	参数类型	描述
created_at	String	用户组创建时间。
urn	String	统一资源名称。
description	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

表 4-149 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-150 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-151 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

- 查询所有用户组列表。

  ```
  GET https://{endpoint}/v5/groups
  ```

- 查询IAM用户xxx所在的所有用户组列表。

  ```
  GET https://{endpoint}/v5/groups?user_id=xxx
  ```

响应示例

状态码：200

请求成功。

```
{
  "groups" : [ {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.5.2 创建用户组

功能介绍

该接口可以用于创建用户组。

URI

POST /v5/groups

请求参数

表 4-152 请求 Body 参数

参数	是否必选	参数类型	描述
group_name	是	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。
description	否	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

响应参数

状态码：201

表 4-153 响应 Body 参数

参数	参数类型	描述
group	**Group** object	用户组。

表 4-154 Group

参数	参数类型	描述
group_id	String	用户组ID。
group_name	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。
created_at	String	用户组创建时间。
urn	String	统一资源名称。
description	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

状态码：400

表 4-155 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-156 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：409

表 4-157 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建名为name的用户组。

```
POST https://{endpoint}/v5/groups

{
  "group_name" : "name",
  "description" : "description"
}
```

响应示例

状态码：201

请求成功。

```
{
  "group" : {
```



```
  "group_id" : "string",
  "group_name" : "name",
  "created_at" : "2023-09-11T10:13:25.414Z",
  "urn" : "iam::accountid:group:name",
  "description" : "description"
 }
}
```

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**。

4.1.5.3 查询用户组详情

功能介绍

该接口可以用于查询用户组详情。

URI

GET /v5/groups/{group_id}

表 4-158 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：200

表 4-159 响应 Body 参数

参数	参数类型	描述
group	**Group** object	用户组。

表 4-160 Group

参数	参数类型	描述
group_id	String	用户组ID。
group_name	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。
created_at	String	用户组创建时间。
urn	String	统一资源名称。
description	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

状态码：403

表 4-161 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-162 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

参数	参数类型	描述
request_id	String	请求ID。

请求示例

查询用户组详情。

```
GET https://{endpoint}/v5/groups/{group_id}
```

响应示例

状态码：200

请求成功。

```
{
  "group" : {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.5.4 修改用户组

功能介绍

该接口可以用于修改用户组信息。

URI

PUT /v5/groups/{group_id}

表 4-163 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-164 请求 Body 参数

参数	是否必选	参数类型	描述
new_group_name	否	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。
new_group_description	否	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

响应参数

状态码：200

表 4-165 响应 Body 参数

参数	参数类型	描述
group	**Group** object	用户组。

表 4-166 Group

参数	参数类型	描述
group_id	String	用户组ID。
group_name	String	用户组名，长度为1到128个字符，可包含中文、英文、数字、空格、"_"、"-"、"{"和"}"的字符串。
created_at	String	用户组创建时间。
urn	String	统一资源名称。

参数	参数类型	描述
description	String	用户组描述信息，长度为0到255字符，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。

状态码：400

表 4-167 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-168 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-169 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-170 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

修改用户组信息。

```
PUT https://{endpoint}/v5/groups/{group_id}

{
  "new_group_name" : "name",
  "new_group_description" : "description"
}
```

响应示例

状态码：200

请求成功。

```
{
  "group" : {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  }
}
```

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**。

4.1.5.5 删除用户组

功能介绍

该接口可以用于删除用户组。

URI

DELETE /v5/groups/{group_id}

表 4-171 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-172 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-173 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。

参数	参数类型	描述
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-174 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除用户组。

```
DELETE https://{endpoint}/v5/groups/{group_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.5.6 添加 IAM 用户到用户组

功能介绍

该接口可以用于添加IAM用户到用户组。

URI

POST /v5/groups/{group_id}/add-user

表 4-175 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-176 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

响应参数

状态码：200

请求成功。

状态码：400

表 4-177 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-178 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

参数	参数类型	描述
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-179 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-180 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

添加IAM用户xxx到指定用户组。

```
POST https://{endpoint}/v5/groups/{group_id}/add-user

{
  "user_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	请求体异常。

状态码	描述
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**。

4.1.5.7 移除用户组中的 IAM 用户

功能介绍

该接口可以用于移除用户组中的IAM用户。

URI

POST /v5/groups/{group_id}/remove-user

表 4-181 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-182 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

响应参数

状态码：200

请求成功。

状态码：403

表 4-183 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-184 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

移除指定用户组中的IAM用户xxx。

```
POST https://{endpoint}/v5/groups/{group_id}/remove-user

{
  "user_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.6 身份策略管理

4.1.6.1 查询所有身份策略

功能介绍

该接口可以用于查询所有身份策略，包含系统预置身份策略和自定义身份策略。

URI

GET /v5/policies

表 4-185 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**
policy_type	否	String	身份策略类型，可以为“自定义”（custom）或“系统预置”（system）。
path_prefix	否	String	资源路径前缀，由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。 最大长度：**512**
only_attached	否	Boolean	是否仅列举存在附加实体的身份策略。 缺省值：**false**

请求参数

表 4-186 请求 Header 参数

参数	是否必选	参数类型	描述
X-Language	否	String	选择接口返回的信息的语言，可以为中文（"zh-cn"）或英文（"en-us"），默认为中文。 缺省值：**zh-cn**

响应参数

状态码：200

表 4-187 响应 Body 参数

参数	参数类型	描述
policies	Array of **Policy** objects	身份策略列表。
page_info	**PageInfo** object	分页信息。

表 4-188 Policy

参数	参数类型	描述
policy_type	String	身份策略类型，可以为“自定义”（custom）或“系统预置”（system）。
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
default_version_id	String	默认版本号。
attachment_count	Integer	附加了本身份策略的实体数量。

参数	参数类型	描述
description	String	身份策略描述。
created_at	String	身份策略创建时间。
updated_at	String	身份策略默认版本最近一次的更新时间。

表 4-189 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：403

表 4-190 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

查询所有身份策略。

```
GET https://{endpoint}/v5/policies
```

响应示例

状态码：200

请求成功。

```
{
  "policies" : [ {
    "policy_type" : "custom",
    "policy_name" : "name",
```

```
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```


状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.6.2 创建自定义身份策略

功能介绍

该接口可以用于创建一个默认版本为v1的新自定义身份策略。

URI

POST /v5/policies

请求参数

表 4-191 请求 Body 参数

参数	是否必选	参数类型	描述
policy_name	是	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
path	否	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。

参数	是否必选	参数类型	描述

policy_document	是	String	自定义身份策略或系统预置身份策略的策略文档的json格式。下面的字符*= < > ( ) /*是语法中的特殊字符，不包含在身份策略中。
			问号*?*表示元素是可选的。例如*sid_block?*。
			竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
			当一个元素允许多个值时，使用重复值,以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
			下面的递归文法描述了身份策略的语法：
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,
			<resource_string>, ...]
			
			<condition_block> = "Condition" :
			{ <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  ...
			}

参数	是否必选	参数类型	描述
			<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
description	否	String	身份策略描述。

响应参数

状态码：201

表 4-192 响应 Body 参数

参数	参数类型	描述
policy	**Policy** object	身份策略。

表 4-193 Policy

参数	参数类型	描述
policy_type	String	身份策略类型，可以为“自定义”（custom）或“系统预置”（system）。
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
default_version_id	String	默认版本号。
attachment_count	Integer	附加了本身份策略的实体数量。
description	String	身份策略描述。
created_at	String	身份策略创建时间。

参数	参数类型	描述
updated_at	String	身份策略默认版本最近一次的更新时间。

状态码：400

表 4-194 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-195 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：409

表 4-196 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建一个名为name的新自定义身份策略。

```
POST https://{endpoint}/v5/policies

{
```

```
  "policy_name" : "name",
  "path" : "",
  "policy_document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
  "description" : "description"
}
```

响应示例

状态码：201

请求成功。

```
{
  "policy" : {
    "policy_type" : "custom",
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  }
}
```

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**。

4.1.6.3 通过身份策略 ID 获取身份策略

功能介绍

该接口可以用于通过身份策略ID获取身份策略信息。

URI

GET /v5/policies/{policy_id}

表 4-197 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-198 请求 Header 参数

参数	是否必选	参数类型	描述
X-Language	否	String	选择接口返回的信息的语言，可以为中文（"zh-cn"）或英文（"en-us"），默认为中文。 缺省值：**zh-cn**

响应参数

状态码：200

表 4-199 响应 Body 参数

参数	参数类型	描述
policy	**Policy** object	身份策略。

表 4-200 Policy

参数	参数类型	描述
policy_type	String	身份策略类型，可以为“自定义”（custom）或“系统预置”（system）。
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。

参数	参数类型	描述
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
default_version_id	String	默认版本号。
attachment_count	Integer	附加了本身份策略的实体数量。
description	String	身份策略描述。
created_at	String	身份策略创建时间。
updated_at	String	身份策略默认版本最近一次的更新时间。

状态码：403

表 4-201 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-202 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

通过身份策略ID获取身份策略信息。

```
GET https://{endpoint}/v5/policies/{policy_id}
```

响应示例

状态码：200

请求成功。

```
{
  "policy" : {
    "policy_type" : "custom",
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.6.4 删除自定义身份策略

功能介绍

该接口可以用于删除一个存在的自定义身份策略，必须确保该自定义身份策略没有附加在任何IAM用户、用户组、委托或信任委托上。

URI

DELETE /v5/policies/{policy_id}

表 4-203 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-204 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-205 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-206 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除指定自定义身份策略。

```
DELETE https://{endpoint}/v5/policies/{policy_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.6.5 为指定身份策略创建一个新版本

功能介绍

该接口可以用于为指定身份策略创建一个新版本。

URI

POST /v5/policies/{policy_id}/versions

表 4-207 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-208 请求 Body 参数

参数	是否必选	参数类型	描述

policy_document	是	String	自定义身份策略或系统预置身份策略的策略文档的json格式。下面的字符*= < > ( ) /*是语法中的特殊字符，不包含在身份策略中。
			问号*?*表示元素是可选的。例如*sid_block?*。
			竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
			当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
			下面的递归文法描述了身份策略的语法：
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,
			<resource_string>, ...]
			
			<condition_block> = "Condition" :
			{ <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },

参数	是否必选	参数类型	描述
			<condition_type_string> : { <condition_key_string> : <condition_value_list> }, ... } <condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
set_as_default	否	Boolean	是否设置为默认版本。 缺省值：**false**

响应参数

状态码：201

表 4-209 响应 Body 参数

参数	参数类型	描述
policy_version	**PolicyVersion** object	身份策略版本信息。

表 4-210 PolicyVersion

参数	参数类型	描述

document	String	自定义身份策略或系统预置身份策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在身份策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了身份策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

参数	参数类型	描述
version_id	String	身份策略版本号，以"v"开头后跟数字，例如"v5"。
is_default	Boolean	是否为默认版本。
created_at	String	身份策略版本创建时间。

状态码：400

表 4-211 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-212 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-213 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-214 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

为指定身份策略创建一个新版本，并置为默认版本。

```
POST https://{endpoint}/v5/policies/{policy_id}/versions

{
  "policy_document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
  "set_as_default" : true
}
```

响应示例

状态码：201

请求成功。

```
{
  "policy_version" : {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v2",
    "is_default" : true,
    "created_at" : "2023-09-25T08:00:51.537Z"
  }
}
```

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。
404	未找到相应的资源。
409	请求冲突。

错误码

请参见**错误码**。

4.1.6.6 查询指定身份策略的所有版本

功能介绍

该接口可以用于查询指定身份策略的所有版本信息。

URI

GET /v5/policies/{policy_id}/versions

表 4-215 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

表 4-216 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-217 响应 Body 参数

参数	参数类型	描述
versions	Array of **PolicyVersion** objects	身份策略版本列表。
page_info	**PageInfo** object	分页信息。

表 4-218 PolicyVersion

参数	参数类型	描述

document	String	自定义身份策略或系统预置身份策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在身份策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了身份策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

参数	参数类型	描述
version_id	String	身份策略版本号，以"v"开头后跟数字，例如"v5"。
is_default	Boolean	是否为默认版本。
created_at	String	身份策略版本创建时间。

表 4-219 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：403

表 4-220 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-221 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定身份策略的所有版本信息。

```
GET https://{endpoint}/v5/policies/{policy_id}/versions
```

响应示例

状态码：200

请求成功。

```
{
  "versions" : [ {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v1",
    "is_default" : true,
    "created_at" : "2023-09-25T09:03:24.786Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.6.7 查询指定身份策略版本

功能介绍

该接口可以用于查询指定身份策略的指定版本的相关信息，包括身份策略文档。

URI

GET /v5/policies/{policy_id}/versions/{version_id}

表 4-222 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
version_id	是	String	身份策略版本号，以"v"开头后跟数字的字符串，例如"v5"。

请求参数

无

响应参数

状态码：200

表 4-223 响应 Body 参数

参数	参数类型	描述
policy_version	**PolicyVersion** object	身份策略版本信息。

表 4-224 PolicyVersion

参数	参数类型	描述

document	String	自定义身份策略或系统预置身份策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在身份策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了身份策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

参数	参数类型	描述
version_id	String	身份策略版本号，以"v"开头后跟数字，例如"v5"。
is_default	Boolean	是否为默认版本。
created_at	String	身份策略版本创建时间。

状态码：403

表 4-225 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-226 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定身份策略的指定版本的相关信息。

```
GET https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}
```

响应示例

状态码：200

请求成功。

```
{
  "policy_version" : {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v1",
```

```
    "is_default" : true,
    "created_at" : "2023-09-25T08:00:51.537Z"
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.6.8 删除指定身份策略版本

功能介绍

该接口可以用于删除指定身份策略的指定版本。默认身份策略版本不能被删除。

URI

DELETE /v5/policies/{policy_id}/versions/{version_id}

表 4-227 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
version_id	是	String	身份策略版本号，以"v"开头后跟数字的字符串，例如"v5"。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-228 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-229 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-230 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除指定身份策略的指定版本。

```
DELETE https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.6.9 将指定身份策略版本设置为默认版本

功能介绍

该接口可以用于将指定身份策略的指定版本设置为默认版本。

URI

POST /v5/policies/{policy_id}/versions/{version_id}/set-default

表 4-231 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
version_id	是	String	身份策略版本号，以"v"开头后跟数字的字符串，例如"v5"。

请求参数

无

响应参数

状态码：200

请求成功。

状态码：403

表 4-232 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-233 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-234 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

将指定身份策略的指定版本设置为默认版本。

```
POST https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}/set-default
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7 权限管理

4.1.7.1 为委托或信任委托附加身份策略

功能介绍

该接口可以用于为指定委托或信任委托附加指定身份策略。

URI

POST /v5/policies/{policy_id}/attach-agency

表 4-235 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-236 请求 Body 参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

响应参数

状态码：200

请求成功。

状态码：403

表 4-237 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-238 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-239 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

为委托xxx附加指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-agency

{
```

```
  "agency_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.2 为用户组附加身份策略

功能介绍

该接口可以用于为指定用户组附加指定身份策略。

URI

POST /v5/policies/{policy_id}/attach-group

表 4-240 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-241 请求 Body 参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

响应参数

状态码：200

请求成功。

状态码：403

表 4-242 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-243 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-244 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

为用户组xxx附加指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-group

{
  "group_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.3 为 IAM 用户附加身份策略

功能介绍

该接口可以用于为指定IAM用户附加指定身份策略。

URI

POST /v5/policies/{policy_id}/attach-user

表 4-245 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-246 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

响应参数

状态码：200

请求成功。

状态码：403

表 4-247 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-248 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-249 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

参数	参数类型	描述
request_id	String	请求ID。

请求示例

为IAM用户xxx附加指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-user

{
  "user_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.4 从委托或信任委托分离身份策略

功能介绍

该接口可以用于从指定委托或信任委托中分离指定身份策略。

URI

POST /v5/policies/{policy_id}/detach-agency

表 4-250 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-251 请求 Body 参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

响应参数

状态码：200

请求成功。

状态码：403

表 4-252 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-253 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-254 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

从委托xxx中分离指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-agency

{
  "agency_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.5 从用户组分离身份策略

功能介绍

该接口可以用于从指定用户组分离指定身份策略。

URI

POST /v5/policies/{policy_id}/detach-group

表 4-255 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-256 请求 Body 参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

响应参数

状态码：200

请求成功。

状态码：403

表 4-257 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-258 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-259 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

从用户组xxx中分离指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-group

{
  "group_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.6 从 IAM 用户分离身份策略

功能介绍

该接口可以用于从指定的IAM用户分离指定身份策略。

URI

POST /v5/policies/{policy_id}/detach-user

表 4-260 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-261 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

响应参数

状态码：200

请求成功。

状态码：403

表 4-262 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-263 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。

参数	参数类型	描述
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-264 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

从IAM用户xxx中分离指定身份策略。

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-user

{
  "user_id" : "xxx"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.7 查询指定身份策略附加的所有实体

功能介绍

该接口可用于查询指定身份策略附加的所有实体。

URI

GET /v5/policies/{policy_id}/attached-entities

表 4-265 路径参数

参数	是否必选	参数类型	描述
policy_id	是	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

表 4-266 Query 参数

参数	是否必选	参数类型	描述
entity_type	否	String	实体类型，包含user、 group 和 agency三种类型。
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-267 响应 Body 参数

参数	参数类型	描述
policy_agencies	Array of **PolicyAgency** objects	委托及信任委托列表。
policy_groups	Array of **PolicyGroup** objects	用户组列表。
policy_users	Array of **PolicyUser** objects	IAM用户列表。
page_info	**PageInfo** object	分页信息。

表 4-268 PolicyAgency

参数	参数类型	描述
agency_id	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
attached_at	String	身份策略的附加时间。

表 4-269 PolicyGroup

参数	参数类型	描述
group_id	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
attached_at	String	身份策略的附加时间。

表 4-270 PolicyUser

参数	参数类型	描述
user_id	String	IAM用户ID。
attached_at	String	身份策略的附加时间。

表 4-271 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：403

表 4-272 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-273 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定身份策略附加的所有实体。

```
GET https://{endpoint}/v5/policies/{policy_id}/attached-entities
```

响应示例

状态码：200

请求成功。

```
{
  "policy_agencies" : [ {
```

```
    "agency_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "policy_groups" : [ {
    "group_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "policy_users" : [ {
    "user_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 3
  }
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.7.8 查询指定委托或信任委托附加的所有身份策略

功能介绍

该接口可用于查询指定委托或信任委托附加的所有身份策略。

URI

GET /v5/agencies/{agency_id}/attached-policies

表 4-274 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

表 4-275 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-276 响应 Body 参数

参数	参数类型	描述
attached_policies	Array of **AttachedPolicy** objects	身份策略列表。
page_info	**PageInfo** object	分页信息。

表 4-277 AttachedPolicy

参数	参数类型	描述
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。
attached_at	String	身份策略的附加时间。

表 4-278 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-279 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-280 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-281 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定委托附加的所有身份策略。

```
GET https://{endpoint}/v5/agencies/{agency_id}/attached-policies
```

响应示例

状态码：200

请求成功。

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.7.9 查询指定用户组附加的所有身份策略

功能介绍

该接口可用于查询指定用户组附加的所有身份策略。

URI

GET /v5/groups/{group_id}/attached-policies

表 4-282 路径参数

参数	是否必选	参数类型	描述
group_id	是	String	用户组ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

表 4-283 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-284 响应 Body 参数

参数	参数类型	描述
attached_policies	Array of **AttachedPolicy** objects	身份策略列表。
page_info	**PageInfo** object	分页信息。

表 4-285 AttachedPolicy

参数	参数类型	描述
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。
attached_at	String	身份策略的附加时间。

表 4-286 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-287 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-288 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

参数	参数类型	描述
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-289 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定用户组附加的所有身份策略。

```
GET https://{endpoint}/v5/groups/{group_id}/attached-policies
```

响应示例

状态码：200

请求成功。

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 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。

错误码

请参见**错误码**。

4.1.7.10 查询指定 IAM 用户附加的所有身份策略

功能介绍

该接口可用于查询指定IAM用户附加的所有身份策略。

URI

GET /v5/users/{user_id}/attached-policies

表 4-290 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	IAM用户ID。

表 4-291 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-292 响应 Body 参数

参数	参数类型	描述
attached_policies	Array of **AttachedPolicy** objects	身份策略列表。
page_info	**PageInfo** object	分页信息。

表 4-293 AttachedPolicy

参数	参数类型	描述
policy_name	String	身份策略名称，长度为1到128个字符，只包含字母、数字、"_"、"+"、"="、"."、"@"和"-"的字符串。
policy_id	String	身份策略ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
urn	String	统一资源名称。
attached_at	String	身份策略的附加时间。

表 4-294 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-295 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-296 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-297 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定IAM用户附加的所有身份策略。

```
GET https://{endpoint}/v5/users/{user_id}/attached-policies
```

响应示例

状态码：200

请求成功。

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

状态码

状态码	描述
200	请求成功。

状态码	描述
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**。

4.1.8 授权概要查询

4.1.8.1 查询指定服务授权概要

功能介绍

该接口可以用于查询指定云服务的授权概要。

URI

GET /v5/authorization-schemas/services/{service_code}

表 4-298 路径参数

参数	是否必选	参数类型	描述
service_code	是	String	服务名称缩写，长度为1到56个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：200

表 4-299 响应 Body 参数

参数	参数类型	描述
version	String	服务授权概要的版本号。
actions	Array of **Action** objects	云服务支持的授权项列表。

参数	参数类型	描述
resources	Array of **Resource** objects	云服务支持的资源列表。
conditions	Array of **Condition** objects	云服务支持的条件键列表。
operations	Array of **Operation** objects	云服务支持的操作列表。

表 4-300 Action

参数	参数类型	描述
name	String	三段式的授权项名称，例如"iam:policies:createV5"。
access_level	String	在策略中使用此授权项时授予的访问级别。
permission_only	Boolean	该授权项是否仅作为权限点，不对应任何操作。
description	**Description** object	描述信息。
aliases	Array of strings	授权项别名列表，用以兼容授权项改名或者拆分新授权项的场景。
resources	Array of **ActionAssociatedResource** objects	与该授权项关联的资源列表，用于定义授权项的资源级权限。
condition_keys	Array of strings	该授权项支持的，且与资源无关的服务自定义条件属性以及部分全局属性。

表 4-301 ActionAssociatedResource

参数	参数类型	描述
urn_template	String	统一资源名称模板，表示可以通过这类资源的统一资源名称对该授权项进行资源粒度的授权。

参数	参数类型	描述
required	Boolean	标识该资源类型是否是这个授权项必选的，即授权项一定涉及对这类资源的操作；例如subnet是vpc:subnets:get的必选资源类型；而ou是organizations::tagResource的可选资源类型，因为organizations::tagResource操作的资源还可能是account或者policy。
condition_keys	Array of strings	针对该授权项和资源的服务自定义条件属性以及部分全局属性，只有授权项和资源同时匹配时才会生效。

表 4-302 Resource

参数	参数类型	描述
type_name	String	云服务资源类型名称。
urn_template	String	统一资源名称模板，表示可以通过这类资源的统一资源名称对该授权项进行资源粒度的授权。

表 4-303 Condition

参数	参数类型	描述
key	String	条件键的名称。
value_type	String	条件值的数据类型。
multi_valued	Boolean	条件值是否为多值。
description	**Description** object	描述信息。

表 4-304 Description

参数	参数类型	描述
en_US	String	英文描述。 最小长度：**1** 最大长度：**1500**

参数	参数类型	描述
zh_CN	String	中文描述。 最小长度：**1** 最大长度：**1500**

表 4-305 Operation

参数	参数类型	描述
operation_id	String	OpenAPI的操作标识符。 最小长度：**1** 最大长度：**64**
operation_action	String	三段式的授权项名称，例如"iam:policies:createV5"。
dependent_actions	Array of strings	该操作可能需要的其他授权项授权。

状态码：404

表 4-306 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询指定云服务的授权概要。

```
GET https://{endpoint}/v5/authorization-schemas/services/{service_code}
```

响应示例

状态码：200

请求成功。

```
{
  "version" : "v1",
  "actions" : [ {
    "name" : "sts:agencies:assume",
    "access_level" : "write",
    "permission_only" : false,
    "description" : {
```

```
      "en_US" : "Grants permission to obtain a set of temporary credentials that you can use to access
resources that you might not normally have access to.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:ExternalId", "sts:SourceIdentity", "sts:TransitiveTagKeys",
"sts:AgencySessionName" ]
  }, {
    "name" : "sts::getCallerIdentity",
    "access_level" : "read",
    "permission_only" : false,
    "description" : {
      "en_US" : "Grants permission to obtain details about the IAM identity whose credentials are used to call
the API.",
      "zh_CN" : "..."
    }
  }, {
    "name" : "sts::decodeAuthorizationMessage",
    "access_level" : "write",
    "permission_only" : false,
    "description" : {
      "en_US" : "Grants permission to decode additional information about the authorization status of a
request from an encoded message returned in response to a request.",
      "zh_CN" : "..."
    }
  }, {
    "name" : "sts::setSourceIdentity",
    "access_level" : "write",
    "permission_only" : true,
    "description" : {
      "en_US" : "Grants permission to set a source identity on a STS session.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:SourceIdentity" ]
  }, {
    "name" : "sts::tagSession",
    "access_level" : "tagging",
    "permission_only" : true,
    "description" : {
      "en_US" : "Grants permission to add tags to a STS session.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:TransitiveTagKeys" ]
  } ],
  "resources" : [ {
    "type_name" : "assumed-agency",
    "urn_template" : "sts::<account-id>:assumed-agency:<agency-name>/<session-name>"
  } ],
  "conditions" : [ {
    "key" : "sts:ExternalId",
    "value_type" : "string",
    "multi_valued" : false,
    "description" : {
      "en_US" : "Filters access by the external ID that is passed in the request.",
      "zh_CN" : "..."
    }
  }, {
    "key" : "sts:SourceIdentity",
```

```
  "value_type" : "string",
  "multi_valued" : false,
  "description" : {
    "en_US" : "Filters access by the source identity that is passed in the request.",
    "zh_CN" : "..."
  }
 }, {
  "key" : "sts:TransitiveTagKeys",
  "value_type" : "string",
  "multi_valued" : true,
  "description" : {
    "en_US" : "Filters access by the transitive tag keys that are passed in the request.",
    "zh_CN" : "..."
  }
 }, {
  "key" : "sts:AgencySessionName",
  "value_type" : "string",
  "multi_valued" : false,
  "description" : {
    "en_US" : "Filters access by the agency session name required when you assume an agency.",
    "zh_CN" : "..."
  }
 } ],
 "operations" : [ {
  "operation_id" : "AssumeAgency",
  "operation_action" : "sts:agencies:assume",
  "dependent_actions" : [ "sts::tagSession", "sts::setSourceIdentity" ]
 }, {
  "operation_id" : "GetCallerIdentity",
  "operation_action" : "sts::getCallerIdentity"
 }, {
  "operation_id" : "DecodeAuthorizationMessage",
  "operation_action" : "sts::decodeAuthorizationMessage"
 } ]
}
```


状态码

状态码	描述
200	请求成功。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.1.8.2 查询已注册云服务列表

功能介绍

该接口可以用于查询已注册云服务列表。

URI

GET /v5/authorization-schemas/registered-services

表 4-307 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-308 响应 Body 参数

参数	参数类型	描述
service_codes	Array of strings	服务名称缩写列表。
page_info	**PageInfo** object	分页信息。

表 4-309 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

请求示例

查询已注册云服务列表。

```
GET https://{endpoint}/v5/authorization-schemas/registered-services
```

响应示例

状态码：200

请求成功。

```
{
  "service_codes" : [ "service1", "service2" ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 2
  }
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见**错误码**。

4.1.8.3 获取全部服务主体

功能介绍

该接口可以用于获取全部服务主体。

URI

GET /v5/service-principals

表 4-310 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

请求参数

表 4-311 请求 Header 参数

参数	是否必选	参数类型	描述
X-Language	否	String	选择接口返回的信息的语言，可以为中文（"zh-cn"）或英文（"en-us"），默认为中文。 缺省值：**zh-cn**

响应参数

状态码：200

表 4-312 响应 Body 参数

参数	参数类型	描述
service_principals	Array of **ServicePrincipalMetadata** objects	服务主体列表。
page_info	**PageInfo** object	分页信息。

表 4-313 ServicePrincipalMetadata

参数	参数类型	描述
service_principal	String	服务主体，由"service."开头，后跟一个长度为1到56个字符，只包含字母、数字和"-"的字符串。
service_catalog	String	云服务名称。 最小长度：**1** 最大长度：**64**
display_name	String	用于显示的服务主体名称。
description	String	服务主体的描述。

表 4-314 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：400

表 4-315 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

请求示例

获取全部服务主体。

```
GET https://{endpoint}/v5/service-principals
```

响应示例

状态码：200

请求成功。

```
{
  "service_principals" : [ {
    "service_principal" : "service.xxx",
    "service_catalog" : "XXX",
    "display_name" : "display_name",
    "description" : "description"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

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**。

4.1.9 委托及信任委托管理

4.1.9.1 创建服务关联委托

功能介绍

该接口可以用于创建服务关联委托。

URI

PUT /v5/service-linked-agencies

请求参数

表 4-316 请求 Body 参数

参数	是否必选	参数类型	描述
service_principal	是	String	服务主体，由"service."开头，后跟一个长度为1到56个字符，只包含字母、数字和"-"的字符串。
description	否	String	服务关联委托描述信息，不能包含特定字符"@"、"#"、"%"、"&"、"<"、">"、"\"、"$"、"^"和"*"的字符串。 最大长度：**1000**

响应参数

状态码：201

表 4-317 响应 Body 参数

参数	参数类型	描述
agency	**Agency** object	委托或信任委托。

表 4-318 Agency

参数	参数类型	描述
urn	String	统一资源名称。

参数	参数类型	描述

trust_policy	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在信任策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了信任策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

参数	参数类型	描述
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
created_at	String	委托或信任委托创建时间。
description	String	委托或信任委托描述信息。
max_session_duration	Integer	委托或信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
agency_id	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
agency_name	String	委托或信任委托名称，长度为1到64个字符，只包含字母、数字、"_"、"+"、"="、","、"."、"@"和"-"的字符串。
trust_domain_id	String	被委托方账号ID，仅存在于委托中，不存在于信任委托中。
trust_domain_name	String	被委托方账号名，仅存在于委托中，不存在于信任委托中。

状态码：403

表 4-319 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-320 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-321 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建服务主体为service.xxx的服务关联委托。

```
PUT https://{endpoint}/v5/service-linked-agencies

{
  "service_principal" : "service.xxx",
  "description" : "description"
}
```

响应示例

状态码：201

请求成功。

```
{
  "agency" : {
    "urn" : "iam::accountid:agency:service-linked-agency/service.xxx/name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"Service\":[\"service.xxx\"]}}]}",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "service-linked-agency/service.xxx/",
    "agency_id" : "id",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  }
}
```


状态码

状态码	描述
201	请求成功。
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**。

4.1.9.2 删除服务关联委托

功能介绍

该接口可以用于服务关联委托删除自己。

URI

DELETE /v5/service-linked-agencies/{agency_id}

表 4-322 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：202

表 4-323 响应 Body 参数

参数	参数类型	描述
deletion_task_id	String	删除任务ID。

状态码：403

表 4-324 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-325 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-326 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

以服务关联委托的身份删除自己。

```
DELETE https://{endpoint}/v5/service-linked-agencies/{agency_id}
```

响应示例

状态码：202

请求成功。

```
{
  "deletion_task_id" : "task"
}
```

状态码

状态码	描述
202	请求成功。
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**。

4.1.9.3 获取服务关联委托删除状态

功能介绍

该接口可以用于获取服务关联委托删除状态。

URI

GET /v5/service-linked-agencies/deletion-task/{deletion_task_id}

表 4-327 路径参数

参数	是否必选	参数类型	描述
deletion_task_id	是	String	删除任务ID。 最小长度：**1** 最大长度：**1000**

请求参数

无

响应参数

状态码：200

表 4-328 响应 Body 参数

参数	参数类型	描述
status	String	删除任务状态。
reason	String	删除失败的原因。

参数	参数类型	描述
agency_usage_list	Array of AgencyUsage objects	该服务关联委托正在被使用的场景列表。

表 4-329 AgencyUsage

参数	参数类型	描述
region	String	区域名称。
resources	Array of strings	统一资源名称列表。

状态码：403

表 4-330 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-331 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

获取服务关联委托删除状态。

```
GET https://{endpoint}/v5/service-linked-agencies/deletion-task/{deletion_task_id}
```

响应示例

状态码：200

请求成功。

```
{
  "status" : "succeeded"
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.1.9.4 查询指定条件下的委托及信任委托列表

功能介绍

该接口可以用于查询指定条件下的委托及信任委托列表。

URI

GET /v5/agencies

表 4-332 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示的条目数量，范围为1到200条，默认为100条。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	分页标记，长度为4到400个字符，只包含字母、数字、"+"、"/"、"="、"-"和"_"的字符串。 最小长度：**4** 最大长度：**400**

参数	是否必选	参数类型	描述
path_prefix	否	String	资源路径前缀，由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。 最大长度：**512**

请求参数

无

响应参数

状态码：200

表 4-333 响应 Body 参数

参数	参数类型	描述
agencies	Array of **Agency** objects	委托及信任委托列表。
page_info	**PageInfo** object	分页信息。

表 4-334 Agency

参数	参数类型	描述
urn	String	统一资源名称。

参数	参数类型	描述

trust_policy	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在信任策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了信任策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

参数	参数类型	描述
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
created_at	String	委托或信任委托创建时间。
description	String	委托或信任委托描述信息。
max_session_duration	Integer	委托或信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
agency_id	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
agency_name	String	委托或信任委托名称，长度为1到64个字符，只包含字母、数字、"_"、"+"、"="、","、"."、"@"和"-"的字符串。
trust_domain_id	String	被委托方账号ID，仅存在于委托中，不存在于信任委托中。
trust_domain_name	String	被委托方账号名，仅存在于委托中，不存在于信任委托中。

表 4-335 PageInfo

参数	参数类型	描述
next_marker	String	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。
current_count	Integer	本页返回条目数量。

状态码：403

表 4-336 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。

参数	参数类型	描述
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

查询所有委托及信任委托列表。

```
GET https://{endpoint}/v5/agencies
```

响应示例

状态码：200

请求成功。

```
{
  "agencies" : [ {
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.9.5 创建信任委托

功能介绍

该接口可以用于创建信任委托。

说明

信任委托只能授予身份策略且仅兼容支持身份策略的云服务，详情见《统一身份认证用户指南》的“支持身份策略与信任委托的云服务列表”章节。

URI

POST /v5/agencies

请求参数

表 4-337 请求 Body 参数

参数	是否必选	参数类型	描述
agency_name	是	String	信任委托名称，长度为1到64个字符，只包含字母、数字、"_"、"+"、"="、","、"."、"@"和"-"的字符串。
path	否	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。

参数	是否必选	参数类型	描述

trust_policy	是	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) /*是语法中的特殊字符，不包含在信任策略中。
			问号*?*表示元素是可选的。例如*sid_block?*。
			竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
			当一个元素允许多个值时，使用重复值,以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
			下面的递归文法描述了信任策略的语法：
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <principal_block>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<principal_block> = ("Principal" |
			"NotPrincipal") : <principal_map>
			
			<principal_map> =
			{ <principal_map_entry>,
			<principal_map_entry>, ... }
			
			<principal_map_entry> = ("IAM" |
			"Service") : [<principal_id_string>, ... |
			<service_principal_string>, ...]
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,
			<resource_string>, ...]
			
			<condition_block> = "Condition" :

参数	是否必选	参数类型	描述

			{ <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  ...
			}
			
			<condition_value_list> =
			(<condition_value> |
			[<condition_value>,
			<condition_value>, ...])
			
			<condition_value> = "string"

max_session_duration	否	Integer	信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
description	否	String	信任委托描述信息，默认为空串，字符串最大长度为1000。 最大长度：**1000**

响应参数

状态码：201

表 4-338 响应 Body 参数

参数	参数类型	描述
agency	**TrustAgency** object	信任委托。

表 4-339 TrustAgency

参数	参数类型	描述
urn	String	统一资源名称。

参数	参数类型	描述

trust_policy	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在信任策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了信任策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

参数	参数类型	描述
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
created_at	String	信任委托创建时间。
description	String	信任委托描述信息。
max_session_duration	Integer	信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
agency_id	String	信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
agency_name	String	信任委托名称，长度为1到64个字符，只包含字母、数字、"_"、"+"、"="、","、"."、"@"和"-"的字符串。
trust_domain_id	String	被委托方账号ID，仅存在于委托中，不存在于信任委托中。
trust_domain_name	String	被委托方账号名，仅存在于委托中，不存在于信任委托中。

状态码：400

表 4-340 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-341 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

参数	参数类型	描述
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：409

表 4-342 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

创建名为name的信任委托。

```
POST https://{endpoint}/v5/agencies

{
  "agency_name" : "name",
  "path" : "",
  "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
  "max_session_duration" : 3600,
  "description" : "description"
}
```

响应示例

状态码：201

请求成功。

```
{
  "agency" : {
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  }
}
```


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**。

4.1.9.6 查询委托或信任委托详情

功能介绍

该接口可以用于查询委托或信任委托详情。

URI

GET /v5/agencies/{agency_id}

表 4-343 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：200

表 4-344 响应 Body 参数

参数	参数类型	描述
agency	**AgencyEx** object	委托或信任委托。

表 4-345 AgencyEx

参数	参数类型	描述
urn	String	统一资源名称。

参数	参数类型	描述

trust_policy	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) |*是语法中的特殊字符，不包含在信任策略中。
		问号*?*表示元素是可选的。例如*sid_block?*。
		竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
		当一个元素允许多个值时，使用重复值*,*以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
		下面的递归文法描述了信任策略的语法：
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

参数	参数类型	描述
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
created_at	String	委托或信任委托创建时间。
description	String	委托或信任委托描述信息。
max_session_duration	Integer	委托或信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
path	String	资源路径，默认为空串。由若干段字符串拼接而成，每段先包含一个或多个字母、数字、"."、","、"+"、"@"、"="、"_"或"-"，并以"/"结尾，例如"foo/bar/"。
agency_id	String	委托或信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
agency_name	String	委托或信任委托名称，长度为1到64个字符，只包含字母、数字、"_"、"+"、"="、","、"."、"@"和"-"的字符串。
trust_domain_id	String	被委托方账号ID，仅存在于委托中，不存在于信任委托中。
trust_domain_name	String	被委托方账号名，仅存在于委托中，不存在于信任委托中。
tags	Array of **Tag** objects	自定义标签列表。

表 4-346 Tag

参数	参数类型	描述
tag_key	String	标签键，可以包含任意语种字母、数字、空格以及"_"、"."、":"、"="、"+"、"-"、"@"符号的任意组合，但是首尾不能包含空格以及不能使用"_sys_"为开头，长度范围[1,64]。 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
tag_value	String	标签值，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，长度范围[0,128]。 最小长度：**0** 最大长度：**128**

状态码：403

表 4-347 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-348 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

查询委托详情。

```
GET https://{endpoint}/v5/agencies/{agency_id}
```

响应示例

状态码：200

请求成功。

```
{
  "agency" : {
```

```
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null,
    "tags" : [ {
      "tag_key" : "key",
      "tag_value" : "value"
    } ]
  }
}
```


状态码

状态码	描述
200	请求成功。
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**。

4.1.9.7 修改信任委托

功能介绍

该接口可以用于修改信任委托。

URI

PUT /v5/agencies/{agency_id}

表 4-349 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-350 请求 Body 参数

参数	是否必选	参数类型	描述
max_session_duration	否	Integer	信任委托最大会话时长，默认为3600秒，取值范围为[3600,43200]。
description	否	String	信任委托描述信息。 最大长度：**1000**

响应参数

状态码：200

请求成功。

状态码：400

表 4-351 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-352 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-353 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-354 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

修改信任委托。

```
PUT https://{endpoint}/v5/agencies/{agency_id}

{
  "max_session_duration" : 3600,
  "description" : "description"
}
```

响应示例

无

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**。

4.1.9.8 删除信任委托

功能介绍

该接口可以用于删除信任委托。

URI

DELETE /v5/agencies/{agency_id}

表 4-355 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

无

响应参数

状态码：204

请求成功。

状态码：403

表 4-356 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-357 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-358 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除信任委托。

```
DELETE https://{endpoint}/v5/agencies/{agency_id}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
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**。

4.1.9.9 修改信任委托信任策略

功能介绍

该接口可以用于修改信任委托信任策略。

URI

PUT /v5/agencies/{agency_id}/trust-policy

表 4-359 路径参数

参数	是否必选	参数类型	描述
agency_id	是	String	信任委托ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。

请求参数

表 4-360 请求 Body 参数

参数	是否必选	参数类型	描述

trust_policy	是	String	信任委托信任策略的策略文档的json格式。下面的字符*= < > ( ) /*是语法中的特殊字符，不包含在信任策略中。
			问号*?*表示元素是可选的。例如*sid_block?*。
			竖线*|*表示可选项，括号定义了可选项的范围。例如*("Allow" | "Deny")*。
			当一个元素允许多个值时，使用重复值,以及*...*表示。例如*[<policy_statement>, <policy_statement>, ...]*。
			下面的递归文法描述了信任策略的语法：
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <principal_block>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<principal_block> = ("Principal" |
			"NotPrincipal") : <principal_map>
			
			<principal_map> =
			{ <principal_map_entry>,
			<principal_map_entry>, ... }
			
			<principal_map_entry> = ("IAM" |
			"Service") : [<principal_id_string>, ... |
			<service_principal_string>, ...]
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]

参数	是否必选	参数类型	描述

			<resource_block> = ("Resource" | "NotResource") : [<resource_string>, <resource_string>, ...]
			
			<condition_block> = "Condition" : { <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
			  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
			  ...
			}
			
			<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...])
			
			<condition_value> = "string"

响应参数

状态码：200

请求成功。

状态码：400

表 4-361 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-362 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-363 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-364 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

修改信任委托信任策略。

```
PUT https://{endpoint}/v5/agencies/{agency_id}/trust-policy

{
  "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}"
}
```

响应示例

无

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**。

4.1.10 账号功能管理

4.1.10.1 获取此账号中 IAM 实体使用情况和 IAM 配额的摘要信息

功能介绍

该接口可以用于获取此账号中IAM实体使用情况和IAM配额的摘要信息。

URI

GET /v5/account-summary

请求参数

无

响应参数

状态码：200

表 4-365 响应 Body 参数

参数	参数类型	描述
attached_policies_per_agency_quota	Integer	附加到委托或信任委托上的身份策略的最大数量。
attached_policies_per_group_quota	Integer	附加到用户组上的身份策略的最大数量。
attached_policies_per_user_quota	Integer	附加到IAM用户上的身份策略的最大数量。
policies_quota	Integer	自定义身份策略的最大数量。
policy_size_quota	Integer	身份策略及信任策略的策略文档的最大字符数，不包括空格。
versions_per_policy_quota	Integer	自定义身份策略同一时刻保留的最大版本数量。
policies	Integer	此账号中当前创建的自定义身份策略数量。
agencies	Integer	此账号中当前创建的委托及信任委托的总数量。
agencies_quota	Integer	此账号能够创建的委托及信任委托的总数上限。

参数	参数类型	描述
users	Integer	此账号当前创建的IAM用户数量，包括根用户。
users_quota	Integer	此账号能够创建的IAM用户数上限，包括根用户。
groups	Integer	此账号当前创建的用户组数量。
groups_quota	Integer	此账号能够创建的用户组数上限。
root_user_mfa_enabled	Integer	根用户绑定的已启用MFA的数量。

状态码：404

表 4-366 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

获取此账号中IAM实体使用情况和IAM配额的摘要信息。

```
GET https://{endpoint}/v5/account-summary
```

响应示例

状态码：200

请求成功。

```
{
  "attached_policies_per_agency_quota" : 10,
  "attached_policies_per_group_quota" : 10,
  "attached_policies_per_user_quota" : 10,
  "policies_quota" : 1500,
  "policy_size_quota" : 6144,
  "versions_per_policy_quota" : 5,
  "policies" : 133,
  "agencies" : 50,
  "agencies_quota" : 50,
  "users" : 135,
  "users_quota" : 500,
  "groups" : 34,
  "groups_quota" : 500,
  "root_user_mfa_enabled" : 0
}
```


状态码

状态码	描述
200	请求成功。
404	未找到相应的资源。

错误码

请参见**错误码**。

4.1.10.2 设置账号开启或关闭非对称签名

功能介绍

该接口用于设置账号开启或关闭非对称签名功能。

URI

PUT /v5/asymmetric-signature-switch

请求参数

表 4-367 请求 Body 参数

参数	是否必选	参数类型	描述
asymmetric_signature	是	**AsymmetricSignature** object	设置账号是否开启非对称签名功能。

表 4-368 AsymmetricSignature

参数	是否必选	参数类型	描述
asymmetric_signature_switch	是	Boolean	非对称签名开关。

响应参数

状态码：204

请求成功。

状态码：403

表 4-369 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

设置账号开启非对称签名。

```
PUT https://{endpoint}/v5/asymmetric-signature-switch

{
  "asymmetric_signature" : {
    "asymmetric_signature_switch" : true
  }
}
```

响应示例

无

状态码

状态码	描述
204	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.10.3 获取账号非对称签名开关状态

功能介绍

该接口用于获取账号非对称签名开关的状态。

URI

GET /v5/asymmetric-signature-switch

请求参数

无

响应参数

状态码：200

表 4-370 响应 Body 参数

参数	参数类型	描述
asymmetric_signature	AsymmetricSignatureWithDomainId object	账号非对称签名开关信息。

表 4-371 AsymmetricSignatureWithDomainId

参数	参数类型	描述
domain_id	String	账号ID。
asymmetric_signature_switch	Boolean	非对称签名开关。

状态码：403

表 4-372 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

请求示例

获取账号非对称签名开关状态。

```
GET https://{endpoint}/v5/asymmetric-signature-switch
```

响应示例

状态码：200

请求成功。

```
{
  "asymmetric_signature" : {
    "asymmetric_signature_switch" : true,
    "domain_id" : "xxxxx"
  }
}
```

状态码

状态码	描述
200	请求成功。
403	没有操作权限。

错误码

请参见**错误码**。

4.1.11 资源标签管理

4.1.11.1 为 IAM 资源打上标签

功能介绍

该接口可以用于为IAM资源打上标签。

URI

POST /v5/{resource_type}/{resource_id}/tags/create

表 4-373 路径参数

参数	是否必选	参数类型	描述
resource_id	是	String	资源ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
resource_type	是	String	资源类型，可以为“信任委托”（trust agency）或“IAM用户”（user）。

请求参数

表 4-374 请求 Body 参数

参数	是否必选	参数类型	描述
tags	否	Array of **Tag** objects	自定义标签列表。 数组长度：**1 - 20**

表 4-375 Tag

参数	是否必选	参数类型	描述
tag_key	是	String	标签键，可以包含任意语种字母、数字、空格以及"_"、"."、":"、"="、"+"、"-"、"@"符号的任意组合，但是首尾不能包含空格以及不能使用"_sys_"为开头，长度范围[1,64]。 最小长度：**1** 最大长度：**64**
tag_value	是	String	标签值，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，长度范围[0,128]。 最小长度：**0** 最大长度：**128**

响应参数

状态码：200

表 4-376 响应 Body 参数

参数	参数类型	描述
tags	Array of **Tag** objects	自定义标签列表。

表 4-377 Tag

参数	参数类型	描述
tag_key	String	标签键，可以包含任意语种字母、数字、空格以及"_"、"."、":"、"="、"+"、"-"、"@"符号的任意组合，但是首尾不能包含空格以及不能使用"_sys_"为开头，长度范围[1,64]。 最小长度：**1** 最大长度：**64**
tag_value	String	标签值，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，长度范围[0,128]。 最小长度：**0** 最大长度：**128**

状态码：400

表 4-378 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-379 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-380 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-381 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

为指定IAM资源打上一个标签，标签键为key，标签值为value。

```
POST https://{endpoint}/v5/{resource_type}/{resource_id}/tags/create

{
  "tags" : [ {
    "tag_key" : "key",
    "tag_value" : "value"
  } ]
}
```

响应示例

状态码：200

请求成功。

```
{
  "tags" : [ {
    "tag_key" : "key",
    "tag_value" : "value"
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	请求体异常。

状态码	描述
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**。

4.1.11.2 删除指定资源的部分标签

功能介绍

该接口可以用于删除指定资源的部分标签。

URI

DELETE /v5/{resource_type}/{resource_id}/tags/delete

表 4-382 路径参数

参数	是否必选	参数类型	描述
resource_id	是	String	资源ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
resource_type	是	String	资源类型，可以为“信任委托”（trust agency）或“IAM用户”（user）。

请求参数

表 4-383 请求 Body 参数

参数	是否必选	参数类型	描述
[数组元素]	否	Array of strings	待删除的标签键列表。 数组长度：**1 - 20**

响应参数

状态码：200

请求成功。

状态码：400

表 4-384 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-385 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-386 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

状态码：409

表 4-387 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

删除指定资源的两个标签，其标签键分别为key1、key2。

```
DELETE https://{endpoint}/v5/{resource_type}/{resource_id}/tags/delete

[ "key1", "key2" ]
```

响应示例

无

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**。

4.1.11.3 获取指定资源的所有标签

功能介绍

该接口可以用于获取指定资源的所有标签。

URI

GET /v5/{resource_type}/{resource_id}/tags

表 4-388 路径参数

参数	是否必选	参数类型	描述
resource_id	是	String	资源ID，长度为1到64个字符，只包含字母、数字和"-"的字符串。
resource_type	是	String	资源类型，可以为“信任委托”（trust agency）或“IAM用户”（user）。

请求参数

无

响应参数

状态码：200

表 4-389 响应 Body 参数

参数	参数类型	描述
tags	Array of **Tag** objects	自定义标签列表。

表 4-390 Tag

参数	参数类型	描述
tag_key	String	标签键，可以包含任意语种字母、数字、空格以及"_"、"."、":"、"="、"+"、"-"、"@"符号的任意组合，但是首尾不能包含空格以及不能使用"_sys_"为开头，长度范围[1,64]。 最小长度：**1** 最大长度：**64**
tag_value	String	标签值，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，长度范围[0,128]。 最小长度：**0** 最大长度：**128**

状态码：403

表 4-391 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-392 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求ID。

请求示例

获取指定资源的所有标签。

```
GET https://{endpoint}/v5/{resource_type}/{resource_id}/tags
```

响应示例

状态码：200

请求成功。

```
{
  "tags" : [ {
    "tag_key" : "key",
    "tag_value" : "value"
  } ]
}
```

状态码

状态码	描述
200	请求成功。
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**。

4.2 STS

4.2.1 临时安全凭证

4.2.1.1 通过委托或者信任委托获取临时安全凭证

功能介绍

通过委托或者信任委托获取临时安全凭证，临时安全凭证可用于对云资源发起访问。

URI

POST /v5/agencies/assume

请求参数

表 4-393 请求 Header 参数

参数	是否必选	参数类型	描述
X-Security-Token	否	String	通过临时安全凭证调用接口时，需要提供“X-Security-Token”Http头，取值为临时安全凭证的security_token字段。

表 4-394 请求 Body 参数

参数	是否必选	参数类型	描述
duration_seconds	否	Integer	获得的临时安全凭证的有效时间（单位秒）。请注意，该时间需要小于委托本身设置的最大会话持续时间，同时在携带X-Security-Token的Header头时该时间不能超过3600秒。 最小值：**900** 最大值：**43200** 缺省值：**3600**
external_id	否	String	外部ID，防止混淆代理人问题。 最小长度：**2** 最大长度：**1224**
policy	否	String	自定义策略，限制本次会话获得的临时安全凭证的权限范围不会超过该自定义策略指定的权限。 最小长度：**2** 最大长度：**2048**
policy_ids	否	Array of strings	预置策略列表，限制本次会话获得的临时安全凭证的权限范围不会超过该预置策略指定的权限。 最大长度：**64**

参数	是否必选	参数类型	描述
agency_urn	是	String	目标委托的URN。 最大长度：**1500**
agency_session_name	是	String	委托会话的会话名。 最小长度：**2** 最大长度：**128**
serial_number	否	String	调用者绑定的MFA设备的序列号。 最小长度：**9** 最大长度：**256**
token_code	否	String	调用者绑定的MFA设备上的6位数字码。 最小长度：**6** 最大长度：**6**
source_identity	否	String	调用链里最初调用者所声明的身份。 最小长度：**2** 最大长度：**64**
tags	否	Array of **TagDto** objects	自定义标签列表。
transitive_tag_keys	否	Array of strings	随着临时安全凭证调用链持续透传的标签键列表。

表 4-395 TagDto

参数	是否必选	参数类型	描述
key	是	String	标签键。 最小长度：**1** 最大长度：**128**
value	是	String	标签值，取值可以为空字符串，不可以为null。 最小长度：**0** 最大长度：**255**

响应参数

状态码：200

表 4-396 响应 Body 参数

参数	参数类型	描述
source_identity	String	调用链里最初调用者所声明的身份。 最小长度：**2** 最大长度：**64**
assumed_agency	**AssumedAgencyDto** object	目标委托信息。
credentials	**CredentialsDto** object	生成的临时安全凭证。

表 4-397 AssumedAgencyDto

参数	参数类型	描述
urn	String	目标委托的URN。 最大长度：**1500**
id	String	目标委托的唯一标志，包含了委托ID和委托会话名称信息。 最大长度：**256**

表 4-398 CredentialsDto

参数	参数类型	描述
access_key_id	String	临时安全凭证的AK。 最小长度：**20** 最大长度：**20**
expiration	String	临时安全凭证的失效时间。
secret_access_key	String	临时安全凭证的SK。 最小长度：**40** 最大长度：**40**
security_token	String	临时安全凭证的security_token。

状态码：400

表 4-399 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-400 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
encoded_authorization_message	String	加密后的认证失败信息，可以通过STS5解密接口进行解密。

状态码：404

表 4-401 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：500

表 4-402 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

请求示例

通过账号27680d67da6b47eb82d00a1a118be145下的委托Y0yfCQYJGO获取临时安全凭证。

```
POST https://{endpoint}/v5/agencies/assume

{
```

```
  "duration_seconds" : 3600,
  "agency_urn" : "iam::27680d67da6b47eb82d00a1a118be145:agency:Y0yfCQYJGO",
  "agency_session_name" : "session1"
}
```

响应示例

状态码：200

请求成功。

```
{
  "assumed_agency" : {
    "urn" : "sts::{account_id}::assumed-agency:{agency_name}/{agency_session_name}",
    "id" : "{agency_id}:{agency_session_name}"
  },
  "credentials" : {
    "access_key_id" : "HSTANO...XBS55JLJ3",
    "secret_access_key" : "EoWCQrr...SCcw4Whkt2aXKWAr",
    "security_token" : "hQpjbi1XXXXXX...XXXXXKbhBbA0TQ==",
    "expiration" : "2022-09-07T03:27:51.158Z"
  }
}
```

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	未找到对应资源。
500	服务端异常。

错误码

请参见**错误码**。

4.2.2 调用者信息查询

4.2.2.1 获取调用者身份信息

功能介绍

获取调用者（用户，委托等）身份信息。

URI

GET /v5/caller-identity

请求参数

表 4-403 请求 Header 参数

参数	是否必选	参数类型	描述
X-Security-Token	否	String	通过临时安全凭证调用接口时，需要提供“X-Security-Token”Http头，取值为临时安全凭证的security_token字段。

响应参数

状态码：200

表 4-404 响应 Body 参数

参数	参数类型	描述
account_id	String	账号ID。 最大长度：**64**
principal_urn	String	主体URN。 最小长度：**4** 最大长度：**1024**
principal_id	String	主体ID。 最小长度：**2** 最大长度：**256**

状态码：500

表 4-405 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

请求示例

获取调用者身份信息。

```
GET https://{endpoint}/v5/caller-identity
```

响应示例

状态码：200

请求成功。

```
{
  "account_id" : "27680d67da6b47eb82d00a1a118be145",
  "principal_urn" : "iam::27680d67da6b47eb82d00a1a118be145:user:user-name",
  "principal_id" : "user-id"
}
```

状态码

状态码	描述
200	请求成功。
500	服务端异常。

错误码

请参见**错误码**。

4.2.3 鉴权结果查询

4.2.3.1 解密鉴权失败的原因

功能介绍

解密鉴权失败的原因。

URI

POST /v5/decode-authorization-message

请求参数

表 4-406 请求 Header 参数

参数	是否必选	参数类型	描述
X-Security-Token	否	String	通过临时安全凭证调用接口时，需要提供“X-Security-Token”Http头，取值为临时安全凭证的security_token字段。

表 4-407 请求 Body 参数

参数	是否必选	参数类型	描述
encoded_message	是	String	加密的鉴权失败原因，字符串长度范围[1,10240]。 最小长度：**1** 最大长度：**10240**

响应参数

状态码：200

表 4-408 响应 Body 参数

参数	参数类型	描述
decoded_message	String	鉴权失败原因的明文。 最小长度：**1** 最大长度：**10240**

状态码：400

表 4-409 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：403

表 4-410 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

状态码：500

表 4-411 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

请求示例

解密鉴权失败的原因。

```
POST https://{endpoint}/v5/decode-authorization-message

{
  "encoded_message" : "HY0L8G1lOe3rcfgxfKVP+AK+S33eYp/rHQ4I0kJed9...rwaYmLp+pt/ICBwk"
}
```

响应示例

状态码：200

请求成功。

```
{
  "decoded_message" : "{\"context\":{\"user_profile\":...\"failure\":\"implicit deny by identity-based policy\"}"
}
```

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。
500	服务端异常。

错误码

请参见**错误码**。

4.3 Access Analyzer

4.3.1 分析器

4.3.1.1 检索分析器的列表

功能介绍

检索分析器的列表。

URI

GET /v5/analyzers

表 4-412 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	单页最大结果数。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	页面标记。 最小长度：**4** 最大长度：**400**
type	否	String	分析器的类型。 ● account：账号级外部访问分析器 ● organization：组织级外部访问分析器 ● account_unused_access：账号级未使用访问分析器 ● organization_unused_access：组织级未使用访问分析器 ● account_iam_best_practice：账号级IAM最佳实践分析器

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
analyzers	Array of **AnalyzerSummary** objects	分析器列表信息。
page_info	**PageInfo** object	页面的信息。

表 4-414 AnalyzerSummary

参数	参数类型	描述
configuration	**AnalyzerConfiguration** object	分析器的配置项。
created_at	String	分析器创建的时间。
id	String	分析器的唯一标识符。
last_analyzed_resource	String	最近分析的资源的唯一资源标识符。
last_resource_analyzed_at	String	最近一次分析资源的时间。
last_all_analyzed_at	String	最近一次分析全量资源的时间。
name	String	分析器的名称。
organization_id	String	组织ID。
status	String	分析器的状态。 • active：激活 • creating：创建中 • disabled：禁用 • failed：创建失败
status_reason	**StatusReason** object	提供有关分析器当前状态的更多详细信息。
tags	Array of **Tag** objects	自定义标签列表。

参数	参数类型	描述
type	String	分析器的类型。 • account: 账号级外部访问分析器 • organization：组织级外部访问分析器 • account_unused_access：账号级未使用访问分析器 • organization_unused_access：组织级未使用访问分析器 • account_iam_best_practice：账号级IAM最佳实践分析器
urn	String	分析器的唯一资源标识符。

表 4-415 AnalyzerConfiguration

参数	参数类型	描述
unused_access	**unused_access** object	未使用的访问分析器的配置项。

表 4-416 unused_access

参数	参数类型	描述
unused_access_age	Integer	生成分析结果的预设天数。 最小值：**1** 最大值：**180** 缺省值：**90**
unused_analysis_rule	**UnusedAnalysisRule** object	未使用分析规则。

表 4-417 UnusedAnalysisRule

参数	参数类型	描述
exclusions	Array of **UnusedAnalysisRuleCriteria** objects	排除规则。

表 4-418 UnusedAnalysisRuleCriteria

参数	参数类型	描述
account_ids	Array of strings	账号ID列表。 最小长度：**1** 最大长度：**36** 数组长度：**1 - 2000**
resource_tags	Array of **Tag** objects	资源标签列表。 数组长度：**1 - 20**

表 4-419 StatusReason

参数	参数类型	描述
code	String	分析器当前状态的原因。 • delegated_administrator_deregistered：委托管理员未注册 • trusted_service_disabled：可信服务未开启 • internal_error：内部错误 • organization_deleted：组织已删除 • service_linked_agency_creation_failed：服务关联委托创建失败
details	String	分析器当前状态的详细原因。

表 4-420 Tag

参数	参数类型	描述
key	String	标签键。
value	String	与标签键关联的字符串值。

表 4-421 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。

参数	参数类型	描述
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

检索分析器的列表。

```
GET https://{hostname}/v5/analyzers
```

响应示例

状态码：200

OK

```
{
  "analyzers" : [ {
    "created_at" : "2023-09-07T07:26:23.440Z",
    "id" : "{analyzer_id}",
    "last_analyzed_resource" : "iam::{domain_id}:agency:{agency_name}",
    "last_resource_analyzed_at" : "2023-09-07T07:26:23.440Z",
    "name" : "my-analyzer",
    "status" : "active",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ],
    "type" : "account",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.1.2 创建分析器

功能介绍

为您的账号或者组织创建分析器。

URI

POST /v5/analyzers

请求参数

表 4-422 请求 Body 参数

参数	是否必选	参数类型	描述
configuration	否	**AnalyzerConfiguration** object	分析器的配置项。
name	是	String	分析器的名称。
tags	否	Array of **Tag** objects	自定义标签列表。 数组长度：**1 - 20**
type	是	String	分析器的类型。 • account: 账号级外部访问分析器 • organization：组织级外部访问分析器 • account_unused_access：账号级未使用访问分析器 • organization_unused_access：组织级未使用访问分析器 • account_iam_best_practice：账号级IAM最佳实践分析器

表 4-423 AnalyzerConfiguration

参数	是否必选	参数类型	描述
unused_access	否	**unused_access** object	未使用的访问分析器的配置项。

表 4-424 unused_access

参数	是否必选	参数类型	描述
unused_access_age	否	Integer	生成分析结果的预设天数。 最小值：**1** 最大值：**180** 缺省值：**90**
unused_analysis_rule	否	**UnusedAnalysisRule** object	未使用分析规则。

表 4-425 UnusedAnalysisRule

参数	是否必选	参数类型	描述
exclusions	否	Array of **UnusedAnalysisRuleCriteria** objects	排除规则。

表 4-426 UnusedAnalysisRuleCriteria

参数	是否必选	参数类型	描述
account_ids	否	Array of strings	账号ID列表。 最小长度：**1** 最大长度：**36** 数组长度：**1 - 2000**
resource_tags	否	Array of **Tag** objects	资源标签列表。 数组长度：**1 - 20**

表 4-427 Tag

参数	是否必选	参数类型	描述
key	是	String	标签键。
value	是	String	与标签键关联的字符串值。

响应参数

状态码：201

表 4-428 响应 Body 参数

参数	参数类型	描述
id	String	分析器的唯一标识符。
urn	String	分析器的唯一资源标识符。

请求示例

为您的账号或者组织创建分析器。

```
POST https://{hostname}/v5/analyzers

{
  "name" : "my-analyzer",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ],
  "type" : "account"
}
```

响应示例

状态码：201

Created

```
{
  "id" : "{analyzer_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
}
```

状态码

状态码	描述
201	Created

错误码

请参见**错误码**。

4.3.1.3 显示指定的分析器

功能介绍

检索有关指定分析器的信息。

URI

GET /v5/analyzers/{analyzer_id}

表 4-429 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

表 4-430 响应 Body 参数

参数	参数类型	描述
analyzer	**AnalyzerSummary** object	包含有关分析器的信息。

表 4-431 AnalyzerSummary

参数	参数类型	描述
configuration	**AnalyzerConfiguration** object	分析器的配置项。
created_at	String	分析器创建的时间。
id	String	分析器的唯一标识符。
last_analyzed_resource	String	最近分析的资源的唯一资源标识符。
last_resource_analyzed_at	String	最近一次分析资源的时间。
last_all_analyzed_at	String	最近一次分析全量资源的时间。
name	String	分析器的名称。
organization_id	String	组织ID。

参数	参数类型	描述
status	String	分析器的状态。 • active：激活 • creating：创建中 • disabled：禁用 • failed：创建失败
status_reason	**StatusReason** object	提供有关分析器当前状态的更多详细信息。
tags	Array of **Tag** objects	自定义标签列表。
type	String	分析器的类型。 • account: 账号级外部访问分析器 • organization：组织级外部访问分析器 • account_unused_access：账号级未使用访问分析器 • organization_unused_access：组织级未使用访问分析器 • account_iam_best_practice：账号级IAM最佳实践分析器
urn	String	分析器的唯一资源标识符。

表 4-432 AnalyzerConfiguration

参数	参数类型	描述
unused_access	**unused_access** object	未使用的访问分析器的配置项。

表 4-433 unused_access

参数	参数类型	描述
unused_access_age	Integer	生成分析结果的预设天数。 最小值：**1** 最大值：**180** 缺省值：**90**
unused_analysis_rule	**UnusedAnalysisRule** object	未使用分析规则。

表 4-434 UnusedAnalysisRule

参数	参数类型	描述
exclusions	Array of **UnusedAnalysisRuleCriteria** objects	排除规则。

表 4-435 UnusedAnalysisRuleCriteria

参数	参数类型	描述
account_ids	Array of strings	账号ID列表。 最小长度：**1** 最大长度：**36** 数组长度：**1 - 2000**
resource_tags	Array of **Tag** objects	资源标签列表。 数组长度：**1 - 20**

表 4-436 StatusReason

参数	参数类型	描述
code	String	分析器当前状态的原因。 • delegated_administrator_deregistered：委托管理员未注册 • trusted_service_disabled：可信服务未开启 • internal_error：内部错误 • organization_deleted：组织已删除 • service_linked_agency_creation_failed：服务关联委托创建失败
details	String	分析器当前状态的详细原因。

表 4-437 Tag

参数	参数类型	描述
key	String	标签键。
value	String	与标签键关联的字符串值。

请求示例

检索有关指定分析器的信息。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}
```

响应示例

状态码：200

OK

```
{
  "analyzer" : {
    "created_at" : "2023-09-07T07:51:10.502Z",
    "id" : "{analyzer_id}",
    "last_analyzed_resource" : "iam::{domain_id}:agency:{agency_name}",
    "last_resource_analyzed_at" : "2023-09-07T07:51:10.502Z",
    "name" : "my-analyzer",
    "status" : "active",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ],
    "type" : "account",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.1.4 删除指定的分析器

功能介绍

删除指定的分析器。分析器生成的所有检查结果都将被删除。

URI

DELETE /v5/analyzers/{analyzer_id}

表 4-438 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：204

Deleted

无

请求示例

删除指定的分析器。

```
DELETE https://{hostname}/v5/analyzers/{analyzer_id}
```

响应示例

无

状态码

状态码	描述
204	Deleted

错误码

请参见**错误码**。

4.3.1.5 更新指定分析器的配置

功能介绍

更新指定分析器的配置。

URI

PUT /v5/analyzers/{analyzer_id}

表 4-439 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-440 请求 Body 参数

参数	是否必选	参数类型	描述
configuration	否	**AnalyzerConfiguration** object	分析器的配置项。

表 4-441 AnalyzerConfiguration

参数	是否必选	参数类型	描述
unused_access	否	**unused_access** object	未使用的访问分析器的配置项。

表 4-442 unused_access

参数	是否必选	参数类型	描述
unused_access_age	否	Integer	生成分析结果的预设天数。 最小值：**1** 最大值：**180** 缺省值：**90**
unused_analysis_rule	否	**UnusedAnalysisRule** object	未使用分析规则。

表 4-443 UnusedAnalysisRule

参数	是否必选	参数类型	描述
exclusions	否	Array of **UnusedAnalysisRuleCriteria** objects	排除规则。

表 4-444 UnusedAnalysisRuleCriteria

参数	是否必选	参数类型	描述
account_ids	否	Array of strings	账号ID列表。 最小长度：**1** 最大长度：**36** 数组长度：**1 - 2000**
resource_tags	否	Array of **Tag** objects	资源标签列表。 数组长度：**1 - 20**

表 4-445 Tag

参数	是否必选	参数类型	描述
key	是	String	标签键。
value	是	String	与标签键关联的字符串值。

响应参数

状态码：200

OK

无

请求示例

更新指定分析器的配置。

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}

{
  "configuration" : {
    "unused_access" : {
      "unused_access_age" : 30,
      "unused_analysis_rule" : {
        "exclusions" : [ {
          "account_ids" : [ "123", "456" ]
        }, {
          "resource_tags" : [ {
            "key" : "key-1",
            "value" : "value-1"
          }, {
            "key" : "key-2",
            "value" : "value-2"
          } ]
        } ]
      }
    }
  }
}
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.1.6 立即开始扫描应用于指定资源的策略

功能介绍

立即开始扫描应用于指定资源的策略。

URI

POST /v5/analyzers/{analyzer_id}/scan

表 4-446 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-447 请求 Body 参数

参数	是否必选	参数类型	描述
resource_id	否	String	资源的唯一标识符。 最小长度：**1** 最大长度：**36**
resource_owner_account	是	String	拥有资源的账号ID。
resource_project_id	否	String	资源所属的项目标识符 最大长度：**36**

参数	是否必选	参数类型	描述
resource_urn	是	String	资源的唯一资源标识符。
finding_type	否	String	访问分析结果类型。 ● external_access：外部访问 ● unused_iam_user_access_key：未使用访问密钥 ● unused_iam_user_password：未使用密码 ● unused_permission：未使用权限 ● unused_iam_agency：未使用委托 ● iam_bp_root_user_has_access_key：为根用户绑定AK/SK ● iam_bp_access_api_with_password：使用密码访问API ● iam_bp_login_protection_disabled：未开启登录保护 ● iam_bp_mfa_unconfigured：未绑定MFA ● iam_bp_assign_high_risk_sys_policy_or_role_to_user：为用户授予高风险系统策略或角色 ● iam_bp_attach_high_risk_sys_identity_policy_to_user：为用户授予高风险系统身份策略 ● iam_bp_assign_high_risk_sys_policy_or_role_to_agency：为委托授予高风险系统策略或角色 ● iam_bp_attach_high_risk_sys_identity_policy_to_agency：为委托授予高风险系统身份策略

响应参数

状态码：200

OK

无

请求示例

立即开始扫描应用于指定资源的策略。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/scan

{
  "resource_owner_account" : "{analyzer_id}",
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "resource_id" : "{agency_id}"
}
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.2 存档规则

4.3.2.1 为指定的分析器创建存档规则

功能介绍

为指定的分析器创建存档规则。存档规则会自动存档符合您在创建规则时所定义条件的新结果。

URI

POST /v5/analyzers/{analyzer_id}/archive-rules

表 4-448 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-449 请求 Body 参数

参数	是否必选	参数类型	描述
filters	是	Array of **FindingFilter** objects	匹配要返回的访问分析结果的筛选器。 数组长度：**1 - 10**
name	是	String	创建存档规则的名称。

表 4-450 FindingFilter

参数	是否必选	参数类型	描述
criterion	是	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。

参数	是否必选	参数类型	描述
key	是	String	过滤键。 ● resource：资源URN ● resource_type：资源类型 ● resource_owner_account：资源所有者账号 ● is_public：公共访问权限 ● id：分析结果ID ● status：分析结果类型 ● principal_type：主体类型 ● principal_identifier：主体Identifier ● change_type：分析结果状态的变化 ● existing_finding_id：已有分析结果ID ● existing_finding_status：已有分析结果状态 ● condition.g:PrincipalUrn：主体URN ● condition.g:PrincipalId：主体ID ● condition.g:PrincipalAccount：主体账号 ● condition.g:PrincipalOrgId：主体OrgID ● condition.g:PrincipalOrgPath：主体组织路径 ● condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID ● condition.g:SourceIp：源IP ● condition.g:SourceVpc：源VPC ● condition.g:SourceVpce：源VPCE ● finding_type：分析结果类型

表 4-451 Criterion

参数	是否必选	参数类型	描述
contains	否	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	否	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	否	Boolean	要匹配筛选器的“存在”运算符。
neq	否	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

响应参数

状态码：201

表 4-452 响应 Body 参数

参数	参数类型	描述
id	String	存档规则的唯一标识符。
urn	String	存档规则的唯一资源标识符。

请求示例

为指定的分析器创建存档规则 存档规则会自动存档符合您在创建规则时所定义条件的新结果。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ],
  "name" : "my-archive-rules"
}
```

响应示例

状态码：201

Created


```
{
  "id" : "{archive_rule_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
}
```

状态码

状态码	描述
201	Created

错误码

请参见**错误码**。

4.3.2.2 检索为指定分析器创建的存档规则的列表

功能介绍

检索为指定分析器创建的存档规则列表。

URI

GET /v5/analyzers/{analyzer_id}/archive-rules

表 4-453 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

表 4-454 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	单页最大结果数。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	页面标记。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-455 响应 Body 参数

参数	参数类型	描述
archive_rules	Array of **ArchiveRuleSummary** objects	为指定分析器创建的存档规则的列表。
page_info	**PageInfo** object	页面的信息。

表 4-456 ArchiveRuleSummary

参数	参数类型	描述
created_at	String	创建存档规则的时间。
filters	Array of **FindingFilter** objects	匹配要返回的访问分析结果的筛选器。
id	String	存档规则的唯一标识符。
name	String	创建存档规则的名称。
updated_at	String	上次更新存档规则的时间。
urn	String	存档规则的唯一资源标识符。

表 4-457 FindingFilter

参数	参数类型	描述
criterion	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。

参数	参数类型	描述
key	String	过滤键。 ● resource：资源URN ● resource_type：资源类型 ● resource_owner_account：资源所有者账号 ● is_public：公共访问权限 ● id：分析结果ID ● status：分析结果类型 ● principal_type：主体类型 ● principal_identifier：主体Identifier ● change_type：分析结果状态的变化 ● existing_finding_id：已有分析结果ID ● existing_finding_status：已有分析结果状态 ● condition.g:PrincipalUrn：主体URN ● condition.g:PrincipalId：主体ID ● condition.g:PrincipalAccount：主体账号 ● condition.g:PrincipalOrgId：主体OrgID ● condition.g:PrincipalOrgPath：主体组织路径 ● condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID ● condition.g:SourceIp：源IP ● condition.g:SourceVpc：源VPC ● condition.g:SourceVpce：源VPCE ● finding_type：分析结果类型

表 4-458 Criterion

参数	参数类型	描述
contains	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	Boolean	要匹配筛选器的“存在”运算符。

参数	参数类型	描述
neq	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

表 4-459 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

检索为指定分析器创建的存档规则的列表。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules
```

响应示例

状态码：200

OK

```
{
  "archive_rules" : [ {
    "created_at" : "2023-09-07T08:35:41.997Z",
    "filters" : [ {
      "criterion" : {
        "eq" : [ "iam:agency" ]
      },
      "key" : "resource_type"
    } ],
    "id" : "{archive_rule_id}",
    "name" : "my-archive-rules",
    "updated_at" : "2023-09-07T08:35:41.997Z",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.2.3 检索有关存档规则的信息

功能介绍

检索有关存档规则的信息。

URI

GET /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

表 4-460 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
archive_rule_id	是	String	存档规则的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

表 4-461 响应 Body 参数

参数	参数类型	描述
archive_rule	**ArchiveRuleSummary** object	分析器创建的存档规则。

表 4-462 ArchiveRuleSummary

参数	参数类型	描述
created_at	String	创建存档规则的时间。
filters	Array of **FindingFilter** objects	匹配要返回的访问分析结果的筛选器。
id	String	存档规则的唯一标识符。
name	String	创建存档规则的名称。
updated_at	String	上次更新存档规则的时间。
urn	String	存档规则的唯一资源标识符。

表 4-463 FindingFilter

参数	参数类型	描述
criterion	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。

参数	参数类型	描述
key	String	过滤键。 ● resource：资源URN ● resource_type：资源类型 ● resource_owner_account：资源所有者账号 ● is_public：公共访问权限 ● id：分析结果ID ● status：分析结果类型 ● principal_type：主体类型 ● principal_identifier：主体Identifier ● change_type：分析结果状态的变化 ● existing_finding_id：已有分析结果ID ● existing_finding_status：已有分析结果状态 ● condition.g:PrincipalUrn：主体URN ● condition.g:PrincipalId：主体ID ● condition.g:PrincipalAccount：主体账号 ● condition.g:PrincipalOrgId：主体OrgID ● condition.g:PrincipalOrgPath：主体组织路径 ● condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID ● condition.g:SourceIp：源IP ● condition.g:SourceVpc：源VPC ● condition.g:SourceVpce：源VPCE ● finding_type：分析结果类型

表 4-464 Criterion

参数	参数类型	描述
contains	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	Boolean	要匹配筛选器的“存在”运算符。

参数	参数类型	描述
neq	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

请求示例

检索有关存档规则的信息。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}
```

响应示例

状态码：200

OK

```
{
  "archive_rule" : {
    "created_at" : "2023-09-07T08:35:41.997Z",
    "filters" : [ {
      "criterion" : {
        "eq" : [ "iam:agency" ]
      },
      "key" : "resource_type"
    } ],
    "id" : "{archive_rule_id}",
    "name" : "my-archive-rules",
    "updated_at" : "2023-09-07T08:35:41.997Z",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.2.4 删除指定的存档规则

功能介绍

删除指定的存档规则。

URI

DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

表 4-465 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
archive_rule_id	是	String	存档规则的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：204

Deleted

无

请求示例

删除指定的存档规则。

```
DELETE https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}
```

响应示例

无

状态码

状态码	描述
204	Deleted

错误码

请参见**错误码**。

4.3.2.5 更新指定存档规则的条件和值

功能介绍

更新指定存档规则的条件和值。

URI

PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

表 4-466 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
archive_rule_id	是	String	存档规则的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-467 请求 Body 参数

参数	是否必选	参数类型	描述
filters	是	Array of **FindingFilter** objects	匹配要返回的访问分析结果的筛选器。 数组长度：**1 - 10**

表 4-468 FindingFilter

参数	是否必选	参数类型	描述
criterion	是	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。

参数	是否必选	参数类型	描述
key	是	String	过滤键。 ● resource：资源URN ● resource_type：资源类型 ● resource_owner_account：资源所有者账号 ● is_public：公共访问权限 ● id：分析结果ID ● status：分析结果类型 ● principal_type：主体类型 ● principal_identifier：主体Identifier ● change_type：分析结果状态的变化 ● existing_finding_id：已有分析结果ID ● existing_finding_status：已有分析结果状态 ● condition.g:PrincipalUrn：主体URN ● condition.g:PrincipalId：主体ID ● condition.g:PrincipalAccount：主体账号 ● condition.g:PrincipalOrgId：主体OrgID ● condition.g:PrincipalOrgPath：主体组织路径 ● condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID ● condition.g:SourceIp：源IP ● condition.g:SourceVpc：源VPC ● condition.g:SourceVpce：源VPCE ● finding_type：分析结果类型

表 4-469 Criterion

参数	是否必选	参数类型	描述
contains	否	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	否	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	否	Boolean	要匹配筛选器的“存在”运算符。
neq	否	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

响应参数

状态码：200

OK

无

请求示例

更新指定存档规则的条件和值。

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  }, {
    "criterion" : {
      "eq" : [ "obs:bucket" ]
    },
    "key" : "resource_type"
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.2.6 应用存档规则

功能介绍

以追溯方式将存档规则应用于符合存档规则条件的现有结果。

URI

POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply

表 4-470 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
archive_rule_id	是	String	存档规则的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

OK

无

请求示例

以追溯方式将存档规则应用于符合存档规则条件的现有结果。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.3 分析结果

4.3.3.1 检索指定分析器生成的访问分析结果列表

功能介绍

检索指定分析器生成的访问分析结果列表。

URI

POST /v5/analyzers/{analyzer_id}/findings

表 4-471 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-472 请求 Body 参数

参数	是否必选	参数类型	描述
filters	否	Array of **FindingFilter** objects	匹配要返回的访问分析结果的筛选器。 数组长度：**1 - 20**
limit	否	Integer	单页最大结果数。
marker	否	String	页面标记。

表 4-473 FindingFilter

参数	是否必选	参数类型	描述
criterion	是	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。
key	是	String	过滤键。 • resource：资源URN • resource_type：资源类型 • resource_owner_account：资源所有者账号 • is_public：公共访问权限 • id：分析结果ID • status：分析结果类型 • principal_type：主体类型 • principal_identifier：主体Identifier • change_type：分析结果状态的变化 • existing_finding_id：已有分析结果ID • existing_finding_status：已有分析结果状态 • condition.g:PrincipalUrn：主体URN • condition.g:PrincipalId：主体ID • condition.g:PrincipalAccount：主体账号 • condition.g:PrincipalOrgId：主体OrgID • condition.g:PrincipalOrgPath：主体组织路径 • condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID • condition.g:SourceIp：源IP • condition.g:SourceVpc：源VPC • condition.g:SourceVpce：源VPCE • finding_type：分析结果类型

表 4-474 Criterion

参数	是否必选	参数类型	描述
contains	否	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	否	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	否	Boolean	要匹配筛选器的“存在”运算符。
neq	否	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

响应参数

状态码：200

表 4-475 响应 Body 参数

参数	参数类型	描述
findings	Array of **FindingSummary** objects	访问分析结果列表。
page_info	**PageInfo** object	页面的信息。

表 4-476 FindingSummary

参数	参数类型	描述
action	Array of strings	允许外部主体使用的操作。
analyzed_at	String	分析资源的时间。
condition	Array of **FindingCondition** objects	分析的策略语句中导致访问分析结果的条件。
created_at	String	生成访问分析结果的时间。

参数	参数类型	描述
finding_type	String	访问分析结果类型。 • external_access：外部访问 • unused_iam_user_access_key：未使用访问密钥 • unused_iam_user_password：未使用密码 • unused_permission：未使用权限 • unused_iam_agency：未使用委托 • iam_bp_root_user_has_access_key：为根用户绑定AK/SK • iam_bp_access_api_with_password：使用密码访问API • iam_bp_login_protection_disabled：未开启登录保护 • iam_bp_mfa_unconfigured：未绑定MFA • iam_bp_assign_high_risk_sys_policy_or_role_to_user：为用户授予高风险系统策略或角色 • iam_bp_attach_high_risk_sys_identity_policy_to_user：为用户授予高风险系统身份策略 • iam_bp_assign_high_risk_sys_policy_or_role_to_agency：为委托授予高风险系统策略或角色 • iam_bp_attach_high_risk_sys_identity_policy_to_agency：为委托授予高风险系统身份策略
id	String	访问分析结果的唯一标识符。
is_public	Boolean	表示生成访问分析结果的策略是否允许公共访问资源。
principal	**FindingPrincipal** object	访问信任区内资源的外部主体。
resource	String	资源的唯一资源标识符。
resource_id	String	资源的唯一标识符。 最小长度：**1** 最大长度：**36**
resource_owner_account	String	拥有资源的账号ID。

参数	参数类型	描述
resource_project_id	String	资源所属的项目标识符 最大长度：**36**
resource_type	String	资源的类型。 ● iam:agency：IAM委托 ● iam:user：IAM用户 ● kms:cmk：DEW共享密钥 ● obs:bucket：OBS桶 ● swr:repo：SWR镜像仓库 ● cbr:backup：CBR备份 ● ims:image：IMS镜像
sources	Array of strings	访问分析结果的来源，这指示如何授予生成访问分析结果的访问权限。
status	String	访问分析结果当前状态。 ● active：活跃 ● archived：已归档 ● resolved：已解决
updated_at	String	更新访问分析结果的时间。

表 4-477 FindingCondition

参数	参数类型	描述
key	String	条件"键"的标识符或名称。
value	String	条件"键"对应的"值"。

表 4-478 FindingPrincipal

参数	参数类型	描述
identifier	String	主体身份的标识符。

参数	参数类型	描述
type	String	主体身份的类型。 ● all_principal：所有主体 ● account：账号 ● all_user_in_account： 账号下所有用户 ● all_agency_in_account： 账号下所有委托 ● all_identity_provider_in_account：账号下所有身份提供商 ● specific_user：特定用户 ● specific_agency：特定委托 ● specific_group：特定用户组 ● specific_identity_provider：特定身份提供商

表 4-479 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

检索指定分析器生成的结果列表。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/findings

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ],
  "limit" : 100,
  "marker" : "{marker_string}"
}
```

响应示例

状态码：200

OK

```
{
  "findings" : [ {
    "action" : [ "sts:agencies:assume" ],
    "analyzed_at" : "2023-09-07T08:04:41.698Z",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
    } ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "id" : "{finding_id}",
    "is_public" : false,
    "principal" : {
      "identifier" : "{domain_id}",
      "type" : "account"
    },
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "resource_owner_account" : "{domain_id}",
    "resource_id" : "{agency_id}",
    "resource_type" : "iam:agency",
    "status" : "active",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.3.2 更新指定结果的状态

功能介绍

更新指定访问分析结果的状态。

URI

PUT /v5/analyzers/{analyzer_id}/findings

表 4-480 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-481 请求 Body 参数

参数	是否必选	参数类型	描述
ids	否	Array of strings	要更新的访问分析结果唯一标识符数组。 数组长度：**1 - 50**
resource_urn	否	String	资源的唯一资源标识符。
status	是	String	要更新的访问分析结果状态。 • active：活跃 • archived：已存档

响应参数

状态码：200

OK

无

请求示例

更新指定结果的状态。

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}/findings

{
  "ids" : [ "{finding_id}" ],
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "status" : "active"
}
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.3.3 检索有关指定结果的信息

功能介绍

检索有关指定结果的信息。

URI

GET /v5/analyzers/{analyzer_id}/findings/{finding_id}

表 4-482 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
finding_id	是	String	访问分析结果的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

表 4-483 响应 Body 参数

参数	参数类型	描述
finding	**Finding** object	访问分析结果。

表 4-484 Finding

参数	参数类型	描述
action	Array of strings	允许外部主体使用的操作。
analyzed_at	String	分析资源的时间。
condition	Array of **FindingCondition** objects	分析的策略语句中导致访问分析结果的条件。
created_at	String	生成访问分析结果的时间。

参数	参数类型	描述
finding_details	Array of **FindingDetails** objects	访问分析结果的详细信息。
finding_type	String	访问分析结果类型。 • external_access：外部访问 • unused_iam_user_access_key：未使用访问密钥 • unused_iam_user_password：未使用密码 • unused_permission：未使用权限 • unused_iam_agency：未使用委托 • iam_bp_root_user_has_access_key：为根用户绑定AK/SK • iam_bp_access_api_with_password：使用密码访问API • iam_bp_login_protection_disabled：未开启登录保护 • iam_bp_mfa_unconfigured：未绑定MFA • iam_bp_assign_high_risk_sys_policy_or_role_to_user：为用户授予高风险系统策略或角色 • iam_bp_attach_high_risk_sys_identity_policy_to_user：为用户授予高风险系统身份策略 • iam_bp_assign_high_risk_sys_policy_or_role_to_agency：为委托授予高风险系统策略或角色 • iam_bp_attach_high_risk_sys_identity_policy_to_agency：为委托授予高风险系统身份策略
id	String	访问分析结果的唯一标识符。
is_public	Boolean	表示生成访问分析结果的策略是否允许公共访问资源。
principal	**FindingPrincipal** object	访问信任区内资源的外部主体。
resource	String	资源的唯一资源标识符。
resource_id	String	资源的唯一标识符。 最小长度：**1** 最大长度：**36**

参数	参数类型	描述
resource_owner_account	String	拥有资源的账号ID。
resource_project_id	String	资源所属的项目标识符 最大长度：**36**
resource_type	String	资源的类型。 • iam:agency：IAM委托 • iam:user：IAM用户 • kms:cmk：DEW共享密钥 • obs:bucket：OBS桶 • swr:repo：SWR镜像仓库 • cbr:backup：CBR备份 • ims:image：IMS镜像
sources	Array of strings	访问分析结果的来源，这指示如何授予生成访问分析结果的访问权限。
status	String	访问分析结果当前状态。 • active：活跃 • archived：已归档 • resolved：已解决
updated_at	String	更新访问分析结果的时间。

表 4-485 FindingDetails

参数	参数类型	描述
external_access_details	**ExternalAccessDetails** object	外部访问分析详细结果。
unused_iam_user_access_key_details	**UnusedIamUserAccessKeyDetails** object	未使用密钥分析详细结果。
unused_iam_user_password_details	**UnusedIamUserPasswordDetails** object	未使用用户密码分析详细结果。
unused_permission_details	**UnusedPermissionDetails** object	未使用权限分析详细结果。
unused_iam_agency_details	**UnusedIamAgencyDetails** object	未使用委托分析详细结果。

参数	参数类型	描述
iam_bp_root_user_has_access_key_details	**IamBpRootUserHasAccessKeyDetails** object	Root用户有访问密钥分析详细结果。
iam_bp_access_api_with_password_details	**IamBpAccessApiWithPasswordDetails** object	使用密码访问API分析详细结果。
iam_bp_login_protection_disabled_details	**IamBpLoginProtectionDisabledDetails** object	登录保护未开启分析详细结果。
iam_bp_mfa_unconfigured_details	**IamBpMfaUnconfiguredDetails** object	未绑定MFA分析详细结果。
iam_bp_assign_high_risk_sys_policy_or_role_to_user_details	**IamBpAssignHighRiskSysPolicyOrRoleToUserDetails** object	为IAM用户授予高风险系统策略或角色分析详细结果。
iam_bp_attach_high_risk_sys_identity_policy_to_user_details	**IamBpAttachHighRiskSysIdentityPolicyToUserDetails** object	为IAM用户授予高风险系统身份策略分析详细结果。
iam_bp_assign_high_risk_sys_policy_or_role_to_agency_details	**IamBpAssignHighRiskSysPolicyOrRoleToAgencyDetails** object	为IAM委托授予高风险系统权限或角色分析详细结果。
iam_bp_attach_high_risk_sys_identity_policy_to_agency_details	**IamBpAttachHighRiskSysIdentityPolicyToAgencyDetails** object	为IAM委托授予高风险系统身份策略分析详细结果。

表 4-486 ExternalAccessDetails

参数	参数类型	描述
action	Array of strings	允许外部主体使用的操作。
condition	Array of **FindingCondition** objects	分析的策略语句中导致访问分析结果的条件。
is_public	Boolean	表示生成访问分析结果的策略是否允许公共访问资源。
principal	**FindingPrincipal** object	访问信任区内资源的外部主体。

参数	参数类型	描述
sources	Array of strings	访问分析结果的来源，这指示如何授予生成访问分析结果的访问权限。

表 4-487 FindingCondition

参数	参数类型	描述
key	String	条件"键"的标识符或名称。
value	String	条件"键"对应的"值"。

表 4-488 UnusedIamUserAccessKeyDetails

参数	参数类型	描述
access_key_id	String	用户访问密钥唯一标识符（ID）。
last_accessed	String	用户访问密钥的最后访问时间。

表 4-489 UnusedIamUserPasswordDetails

参数	参数类型	描述
last_accessed	String	用户密码的最后访问时间。

表 4-490 UnusedPermissionDetails

参数	参数类型	描述
service	String	权限对应的云服务名称。
last_accessed	String	用户使用云服务的最后访问时间。
actions	Array of **UnusedAction** objects	未使用的操作列表。

表 4-491 UnusedAction

参数	参数类型	描述
action	String	授权项名称。
last_accessed	AnyType	用户使用授权项的最后访问时间。

表 4-492 UnusedIamAgencyDetails

参数	参数类型	描述
last_accessed	String	用户使用委托的最后访问时间。

表 4-493 IamBpRootUserHasAccessKeyDetails

参数	参数类型	描述
access_key_id	String	用户访问密钥唯一标识符（ID）。 最小长度：**1** 最大长度：**40**
last_accessed	String	用户访问密钥的最后访问时间。
created_at	String	用户访问密钥的创建时间。

表 4-494 IamBpAccessApiWithPasswordDetails

参数	参数类型	描述
user_id	String	用户的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
last_access_api_with_pwd_at	String	用户使用密码访问API的最后时间。
user_created_at	String	用户的创建时间。

表 4-495 IamBpLoginProtectionDisabledDetails

参数	参数类型	描述
user_id	String	用户的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
user_created_at	String	用户的创建时间。

表 4-496 IamBpMfaUnconfiguredDetails

参数	参数类型	描述
user_id	String	用户的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
user_created_at	String	用户的创建时间。

表 4-497 IamBpAssignHighRiskSysPolicyOrRoleToUserDetails

参数	参数类型	描述
user_id	String	用户的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
permission_name	String	权限名称。

表 4-498 IamBpAttachHighRiskSysIdentityPolicyToUserDetails

参数	参数类型	描述
user_id	String	用户的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
policy_name	String	策略名称。

表 4-499 IamBpAssignHighRiskSysPolicyOrRoleToAgencyDetails

参数	参数类型	描述
agency_id	String	委托的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
permission_name	String	权限名称。

表 4-500 IamBpAttachHighRiskSysIdentityPolicyToAgencyDetails

参数	参数类型	描述
agency_id	String	委托的唯一标识符（ID）。 最小长度：**1** 最大长度：**36**
policy_name	String	策略名称。

表 4-501 FindingPrincipal

参数	参数类型	描述
identifier	String	主体身份的标识符。
type	String	主体身份的类型。 ● all_principal：所有主体 ● account：账号 ● all_user_in_account： 账号下所有用户 ● all_agency_in_account： 账号下所有委托 ● all_identity_provider_in_account：账号下所有身份提供商 ● specific_user：特定用户 ● specific_agency：特定委托 ● specific_group：特定用户组 ● specific_identity_provider：特定身份提供商

请求示例

检索有关指定结果的信息。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/findings/{finding_id}
```

响应示例

状态码：200

OK

```
{
  "finding" : {
    "action" : [ "obs:bucket:listBucket" ],
    "analyzed_at" : "2023-09-07T08:04:41.698Z",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
```

```
  } ],
  "created_at" : "2023-09-07T08:04:41.698Z",
  "id" : "{finding_id}",
  "is_public" : false,
  "principal" : {
    "identifier" : "{domain_id}",
    "type" : "account"
  },
  "resource" : "obs:{region_id}::bucket:{bucket_name}",
  "resource_owner_account" : "{domain_id}",
  "resource_type" : "obs:bucket",
  "sources" : [ "bucket_policy" ],
  "status" : "active",
  "updated_at" : "2023-09-07T08:04:41.698Z"
 }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.4 访问预览

4.3.4.1 创建访问预览

功能介绍

创建访问预览。

URI

POST /v5/analyzers/{analyzer_id}/access-previews

表 4-502 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-503 请求 Body 参数

参数	是否必选	参数类型	描述
configurations	是	**Configuration** object	访问预览配置。
resource_urn	是	String	资源的唯一资源标识符。

表 4-504 Configuration

参数	是否必选	参数类型	描述
iam_agency	否	**IAMAgency** object	IAM信任委托。
obs_bucket	否	**OBSBucket** object	OBS桶。
kms_cmk	否	**KMSCmk** object	KMS密钥。

表 4-505 IAMAgency

参数	是否必选	参数类型	描述
trust_policy	是	String	该策略JSON格式策略文档。

表 4-506 OBSBucket

参数	是否必选	参数类型	描述
bucket_acl	否	String	桶ACL xml文件的string格式。
bucket_policy	否	String	该策略JSON格式策略文档。

表 4-507 KMSCmk

参数	是否必选	参数类型	描述
grants	是	String	用于加密密钥的授权。

响应参数

状态码：201

表 4-508 响应 Body 参数

参数	参数类型	描述
access_preview_id	String	访问预览的唯一标识符。

请求示例

创建访问预览。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/access-previews

{
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "configurations" : {
    "iam_agency" : {
      "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Condition\":{\"StringMatch\":{\"g:PrincipalOrgId\":
[\"org_id\"]}},\"Action\":[\"sts:agencies:assume\",\"sts::tagSession\",\"sts::setSourceIdentity\"],\"Effect
\":\"Allow\",\"Principal\":{\"IAM\":[\"dd...\"]}}]}"
    }
  }
}
```

响应示例

状态码：201

Created

```
{
  "access_preview_id" : "{access_preview_id}"
}
```

状态码

状态码	描述
201	Created

错误码

请参见**错误码**。

4.3.4.2 获取所有访问预览

功能介绍

获取所有访问预览。

URI

GET /v5/analyzers/{analyzer_id}/access-previews

表 4-509 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**

表 4-510 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	单页最大结果数。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	页面标记。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-511 响应 Body 参数

参数	参数类型	描述
access_previews	Array of **AccessPreviewSummary** objects	访问预览列表。
page_info	**PageInfo** object	页面的信息。

表 4-512 AccessPreviewSummary

参数	参数类型	描述
access_preview_id	String	访问预览的唯一标识符。
analyzer_id	String	分析器的唯一标识符。

参数	参数类型	描述
created_at	String	访问预览创建时间。
status	String	访问预览的状态。 • creating：创建中 • completed：创建成功 • failed：创建失败
status_reason	**PreviewStatusReason** object	提供有关访问预览当前状态的更多详细信息。

表 4-513 PreviewStatusReason

参数	参数类型	描述
code	String	访问预览当前状态的原因。

表 4-514 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

获取所有的访问预览。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/access-previews
```

响应示例

状态码：200

OK

```
{
  "access_previews" : [ {
    "analyzer_id" : "{analyzer_id}",
    "created_at" : "2023-09-07T08:35:41.997Z",
    "access_preview_id" : "{access_preview_id}",
    "status" : "completed"
  } ],
  "page_info" : {
```

```
    "current_count" : 1,
    "next_marker" : null
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.4.3 获取相关访问预览的信息

功能介绍

获取相关访问预览的信息。

URI

GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}

表 4-515 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
access_preview_id	是	String	访问预览的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

表 4-516 响应 Body 参数

参数	参数类型	描述
access_preview	**AccessPreview** object	访问预览。

表 4-517 AccessPreview

参数	参数类型	描述
access_preview_id	String	访问预览的唯一标识符。
analyzer_id	String	分析器的唯一标识符。
configurations	**Configuration** object	访问预览配置。
created_at	String	访问预览创建时间。
status	String	访问预览的状态。 • creating：创建中 • completed：创建成功 • failed：创建失败
status_reason	**PreviewStatusReason** object	提供有关访问预览当前状态的更多详细信息。

表 4-518 Configuration

参数	参数类型	描述
iam_agency	**IAMAgency** object	IAM信任委托。
obs_bucket	**OBSBucket** object	OBS桶。
kms_cmk	**KMSCmk** object	KMS密钥。

表 4-519 IAMAgency

参数	参数类型	描述
trust_policy	String	该策略JSON格式策略文档。

表 4-520 OBSBucket

参数	参数类型	描述
bucket_acl	String	桶ACL xml文件的string格式。
bucket_policy	String	该策略JSON格式策略文档。

表 4-521 KMSCmk

参数	参数类型	描述
grants	String	用于加密密钥的授权。

表 4-522 PreviewStatusReason

参数	参数类型	描述
code	String	访问预览当前状态的原因。

请求示例

获取相关访问预览的信息。

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}
```

响应示例

状态码：200

OK

```
{
  "access_preview" : {
    "analyzer_id" : "{analyzer_id}",
    "configurations" : {
      "iam_agency" : {
        "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Condition\":{\"StringMatch\":{\"g:PrincipalOrgId
\":[\"org_id\"]}},\"Action\":[\"sts:agencies:assume\",\"sts::tagSession\",\"sts::setSourceIdentity\"],\"Effect
\":\"Allow\",\"Principal\":{\"IAM\":[\"dd...\"]}}]}"
      }
    },
    "created_at" : "2023-09-07T07:26:23.440Z",
    "access_preview_id" : "{access_preview_id}",
    "status" : "completed"
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.4.4 获取相关预览生成的分析结果

功能介绍

获取相关预览生成的分析结果。

URI

POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings

表 4-523 路径参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。 最小长度：**1** 最大长度：**36**
access_preview_id	是	String	访问预览的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-524 请求 Body 参数

参数	是否必选	参数类型	描述
filters	否	Array of **FindingFilter** objects	匹配要返回的分析结果的筛选项。 数组长度：**1 - 20**
limit	否	Integer	单页最大结果数。
marker	否	String	页面标记。

表 4-525 FindingFilter

参数	是否必选	参数类型	描述
criterion	是	**Criterion** object	要在查找筛选器中使用的条件。最多只能有一个运算符。

参数	是否必选	参数类型	描述
key	是	String	过滤键。 ● resource：资源URN ● resource_type：资源类型 ● resource_owner_account：资源所有者账号 ● is_public：公共访问权限 ● id：分析结果ID ● status：分析结果类型 ● principal_type：主体类型 ● principal_identifier：主体Identifier ● change_type：分析结果状态的变化 ● existing_finding_id：已有分析结果ID ● existing_finding_status：已有分析结果状态 ● condition.g:PrincipalUrn：主体URN ● condition.g:PrincipalId：主体ID ● condition.g:PrincipalAccount：主体账号 ● condition.g:PrincipalOrgId：主体OrgID ● condition.g:PrincipalOrgPath：主体组织路径 ● condition.g:PrincipalOrgManagementAccountId：主体组织管理账号ID ● condition.g:SourceIp：源IP ● condition.g:SourceVpc：源VPC ● condition.g:SourceVpce：源VPCE ● finding_type：分析结果类型

表 4-526 Criterion

参数	是否必选	参数类型	描述
contains	否	Array of strings	要匹配筛选器的“包含”运算符。 数组长度：**1 - 20**
eq	否	Array of strings	要匹配筛选器的“等于”运算符。 数组长度：**1 - 20**
exists	否	Boolean	要匹配筛选器的“存在”运算符。
neq	否	Array of strings	要匹配筛选器的“不等于”运算符。 数组长度：**1 - 20**

响应参数

状态码：200

表 4-527 响应 Body 参数

参数	参数类型	描述
findings	Array of **PreviewFinding** objects	访问预览生成的分析结果列表。
page_info	**PageInfo** object	页面的信息。

表 4-528 PreviewFinding

参数	参数类型	描述
action	Array of strings	允许外部主体使用的操作。
change_type	String	结果状态的变化。 • unchanged：没有变化 • new：新增 • changed：有变化
condition	Array of **FindingCondition** objects	分析的策略语句中导致访问预览分析结果的条件。
created_at	String	生成访问预览分析结果的时间。

参数	参数类型	描述
existing_finding_id	String	访问分析结果的唯一标识符。
existing_finding_status	String	访问分析结果当前状态。 • active：活跃 • archived：已解决 • resolved：已存档
id	String	访问分析结果的唯一标识符。
is_public	Boolean	表示生成访问分析结果的策略是否允许公共访问资源。
principal	**FindingPrincipal** object	访问信任区内资源的外部主体。
resource	String	资源的唯一资源标识符。
resource_owner_account	String	拥有资源的账号ID。
resource_type	String	资源的类型。 • iam:agency：IAM委托 • iam:user：IAM用户 • kms:cmk：DEW共享密钥 • obs:bucket：OBS桶 • swr:repo：SWR镜像仓库 • cbr:backup：CBR备份 • ims:image：IMS镜像
sources	Array of strings	访问分析结果的来源，这指示如何授予生成访问分析结果的访问权限。
status	String	变化后的状态。 • active：活跃 • archived：已解决 • resolved：已存档

表 4-529 FindingCondition

参数	参数类型	描述
key	String	条件"键"的标识符或名称。
value	String	条件"键"对应的"值"。

表 4-530 FindingPrincipal

参数	参数类型	描述
identifier	String	主体身份的标识符。
type	String	主体身份的类型。 ● all_principal：所有主体 ● account：账号 ● all_user_in_account： 账号下所有用户 ● all_agency_in_account： 账号下所有委托 ● all_identity_provider_in_account：账号下所有身份提供商 ● specific_user：特定用户 ● specific_agency：特定委托 ● specific_group：特定用户组 ● specific_identity_provider：特定身份提供商

表 4-531 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

获取相关预览生成的分析结果。

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ]
}
```

响应示例

状态码：200

OK


```
{
  "findings" : [ {
    "action" : [ "sts::setSourceIdentity", "sts::tagSession", "sts:agencies:assume" ],
    "change_type" : "new",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
    } ],
    "created_at" : "2023-09-07T07:26:23.440Z",
    "existing_finding_status" : null,
    "existing_finding_id" : null,
    "is_public" : false,
    "id" : "{finding_id}",
    "principal" : {
      "identifier" : "{domain_id}",
      "type" : "account"
    },
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "resource_owner_account" : "{domain_id}",
    "resource_type" : "iam:agency",
    "status" : "active"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.5 标签

4.3.5.1 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 /v5/{resource_type}/{resource_id}/tags/delete

表 4-532 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	资源类型。 ● analyzers：分析器
resource_id	是	String	资源的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-533 请求 Body 参数

参数	是否必选	参数类型	描述
tag_keys	是	Array of strings	待删除的标签键列表。 数组长度：**1 - 20**

响应参数

状态码：200

OK

无

请求示例

从指定资源中删除标签。

```
POST https://{hostname}/v5/{resource_type}/{resource_id}/tags/delete

{
  "tag_keys" : [ "key-1" ]
}
```

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.5.2 向指定资源添加标签

功能介绍

向指定资源添加标签。

URI

POST /v5/{resource_type}/{resource_id}/tags/create

表 4-534 路径参数

参数	是否必选	参数类型	描述
resource_type	是	String	资源类型。 • analyzers：分析器
resource_id	是	String	资源的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-535 请求 Body 参数

参数	是否必选	参数类型	描述
tags	是	Array of **Tag** objects	自定义标签列表。 数组长度：**1 - 20**

表 4-536 Tag

参数	是否必选	参数类型	描述
key	是	String	标签键。
value	是	String	与标签键关联的字符串值。

响应参数

状态码：200

OK

无

请求示例

向指定资源添加标签。

```
POST https://{hostname}/v5/{resource_type}/{resource_id}/tags/create

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

响应示例

无

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.6 策略校验

4.3.6.1 校验策略

功能介绍

校验策略并返回结果列表。

URI

POST /v5/policies/validate

表 4-537 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	单页最大结果数。 最小值：**1** 最大值：**200** 缺省值：**100**

参数	是否必选	参数类型	描述
marker	否	String	页面标记。 最小长度：**4** 最大长度：**400**

请求参数

表 4-538 请求 Header 参数

参数	是否必选	参数类型	描述
X-Language	否	String	返回消息的语言，默认值为'zh-cn'。 ● zh-cn：中文 ● en-us：英文 缺省值：**zh-cn**

表 4-539 请求 Body 参数

参数	是否必选	参数类型	描述
policy_document	是	String	该策略JSON格式策略文档。
policy_type	是	String	要校验的策略类型。 ● identity_policy：身份策略 ● resource_policy：资源策略 ● service_control_policy：服务控制策略
validate_policy_resource_type	否	String	要附加到资源策略的资源类型。 ● iam:agency： IAM委托

响应参数

状态码：200

表 4-540 响应 Body 参数

参数	参数类型	描述
findings	Array of **ValidatePolicyFinding** objects	可用于改进策略的可操作建议。
page_info	**PageInfo** object	页面的信息。

表 4-541 ValidatePolicyFinding

参数	参数类型	描述
finding_details	String	一条本地化消息提供了如何解决该问题的指导。
finding_type	String	影响级别。 • security_warning 安全：策略存在安全风险，可能是允许访问的权限过于宽松等导致。 • error 错误：存在策略无法运行的错误，如语法错误、参数错误等。存在错误的情况下策略无法创建。 • warning 警告：存在策略无法运行的警告，如参数取值类型不匹配等。存在警告的情况下策略可以创建。 • suggestion 建议：不影响策略运行，但策略可能不能达到预期的效果。如存在空数组、空对象条件等。
issue_code	String	问题码提供了与此校验结果关联的问题的标识符。
learn_more_link	String	指向与此校验结果关联的相关文档的链接。
locations	Array of **Location** objects	策略文档中与校验结果相关的位置列表。

表 4-542 Location

参数	参数类型	描述
path	Array of **PathElement** objects	策略中的路径，表示为路径元素的有序序列。
span	**Span** object	光标在策略文本中的范围。范围由开始位置（含）和结束位置（不含）组成。

表 4-543 PathElement

参数	参数类型	描述
index	Integer	数组中的索引，从0开始。
key	String	对象中的键。
substring	**Substring** object	JSON反序列化后的字符串的子串。
value	String	与对象中给定键关联的值。

表 4-544 Substring

参数	参数类型	描述
start	Integer	子字符串的起始索引，从0开始。0表示第一个字符。
length	Integer	子字符串的长度。

表 4-545 Span

参数	参数类型	描述
start	**Position** object	策略中的位置。
end	**Position** object	策略中的位置。

表 4-546 Position

参数	参数类型	描述
line	Integer	位置的行号，从1开始。
column	Integer	位置的列号，从0开始。
offset	Integer	策略中与位置对应的偏移量，从0开始。

表 4-547 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。

参数	参数类型	描述
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

请求示例

校验策略并返回结果列表。

```
POST https://{hostname}/v5/policies/validate

{
  "policy_document" : "",
  "policy_type" : "identity_policy"
}
```

响应示例

状态码：200

OK

```
{
  "findings" : [ {
    "finding_details" : "修复索引 0 第 1 行第 0 列的 JSON 语法错误。",
    "finding_type" : "error",
    "issue_code" : "JSON_SYNTAX_ERROR",
    "learn_more_link" : "https://{endpoint}/section0",
    "locations" : [ {
      "path" : [ ],
      "span" : {
        "start" : {
          "line" : 1,
          "column" : 0,
          "offset" : 0
        },
        "end" : {
          "line" : 1,
          "column" : 1,
          "offset" : 1
        }
      }
    } ]
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.6.2 校验策略是否有新访问权限

功能介绍

校验策略是否有新访问权限。

URI

POST /v5/policies/check-no-new-access

请求参数

表 4-548 请求 Body 参数

参数	是否必选	参数类型	描述
existing_policy_document	是	String	该策略JSON格式策略文档。
new_policy_document	是	String	该策略JSON格式策略文档。
policy_type	是	String	要校验的策略类型。 • identity_policy：身份策略 • agency_trust_policy：委托信任策略 • bucket_policy：桶策略

响应参数

状态码：200

表 4-549 响应 Body 参数

参数	参数类型	描述
message	String	更新后的策略是否允许新访问权限的消息。
check_result	String	检查新访问权限的结果。 • pass：无新增访问权限 • fail：有新增访问权限
reasons	Array of **CheckNoNewAccessReason** objects	新增action的statement描述。

表 4-550 CheckNoNewAccessReason

参数	参数类型	描述
description	String	对访问权限检查结果的推理的描述。
statement_id	String	新增权限statement的sid标识符。
statement_index	Integer	新增权限statement的index，从0开始。 最小值：**0**

请求示例

校验策略是否有新访问权限。

```
POST https://{hostname}/v5/policies/check-no-new-access

{
  "existing_policy_document" : "{\\\"Version\\\":\\\"5.0\\\",\\\"Statement\\\":[{\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\\":[\\\"iam:users:createUserV5\\\"]}]}",
  "new_policy_document" : "{\\\"Version\\\":\\\"5.0\\\",\\\"Statement\\\":[{\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\\":[\\\"iam:users:createUserV5\\\",\\\"obs:bucket:createBucket\\\"]}]}",
  "policy_type" : "identity_policy"
}
```

响应示例

状态码：200

OK

```
{
  "check_result" : "fail",
  "message" : "The modified permissions grant new access compared to your existing policy.",
  "reasons" : [ {
    "description" : "New access in the statement with sid: {statement_sid}.",
    "statement_index" : 0,
    "statement_id" : "{statement_sid}"
  } ]
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

4.3.7 消息通知配置

4.3.7.1 获取消息通知配置列表

功能介绍

获取消息通知配置列表。

URI

GET /v5/notification-settings

表 4-551 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	单页最大结果数。 最小值：**1** 最大值：**200** 缺省值：**100**
marker	否	String	页面标记。 最小长度：**4** 最大长度：**400**

请求参数

无

响应参数

状态码：200

表 4-552 响应 Body 参数

参数	参数类型	描述
notification_settings	Array of **NotificationSettingSummary** objects	消息通知配置列表。
page_info	**PageInfo** object	页面的信息。

表 4-553 NotificationSettingSummary

参数	参数类型	描述
id	String	消息通知配置的唯一标识符。

参数	参数类型	描述
urn	String	消息通知配置的唯一资源标识符。
analyzer_id	String	分析器的唯一标识符。
analyzer_name	String	分析器的名称。
analyzer_type	String	分析器的类型。 ● account: 账号级外部访问分析器 ● organization：组织级外部访问分析器 ● account_unused_access：账号级未使用访问分析器 ● organization_unused_access：组织级未使用访问分析器 ● account_iam_best_practice：账号级IAM最佳实践分析器
mc_switch	Boolean	是否开启消息中心通知开关。
smn_topic_urns	Array of strings	消息通知配置的SMN主题URN列表。
created_at	String	创建消息通知配置的时间。
updated_at	String	上次更新消息通知配置的时间。

表 4-554 PageInfo

参数	参数类型	描述
current_count	Integer	当前页中的项数。
next_marker	String	如果存在更多可用的输出，那么该值表示可用输出比当前响应中包含的更多。在后续调用此操作时，您可以在标记请求参数中使用此值，以获取输出的下一部分。您应该重复这个过程，直到next_marker返回为null。

状态码：400

表 4-555 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。

参数	参数类型	描述
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：403

表 4-556 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

请求示例

获取消息通知配置列表。

```
GET https://{hostname}/v5/notification-settings
```

响应示例

状态码：200

OK

```
{
  "notification_settings" : [ {
    "id" : "{notification_setting_id}",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
    "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
    "analyzer_type" : "account",
    "analyzer_name" : "external_analyzer_1",
    "mc_switch" : true,
    "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  }, {
    "id" : "{notification_setting_id}",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
    "analyzer_id" : "7d866d909fda4e32b1fc2aae45c34a97",
    "analyzer_type" : "account",
    "analyzer_name" : "external_analyzer_2",
    "mc_switch" : true,
    "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  } ],
  "page_info" : {
    "current_count" : 2,
```



```
  "next_marker" : null
 }
}
```

状态码

状态码	描述
200	OK
400	Bad request
403	Forbidden

错误码

请参见**错误码**。

4.3.7.2 创建消息通知配置

功能介绍

创建消息通知配置。

URI

POST /v5/notification-settings

请求参数

表 4-557 请求 Body 参数

参数	是否必选	参数类型	描述
analyzer_id	是	String	分析器的唯一标识符。
mc_switch	是	Boolean	是否开启消息中心通知开关。
smn_topic_urns	是	Array of strings	消息通知配置的SMN主题URN列表。

响应参数

状态码：201

表 4-558 响应 Body 参数

参数	参数类型	描述
id	String	消息通知配置的唯一标识符。

参数	参数类型	描述
urn	String	消息通知配置的唯一资源标识符。

状态码：400

表 4-559 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：403

表 4-560 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：404

表 4-561 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

请求示例

创建消息通知配置。

```
POST https://{hostname}/v5/notification-settings

{
  "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ]
}
```

响应示例

状态码：201

Created

```
{
  "id" : "1c8b66cc466943ad9f6238a19f6f6679"
}
```

状态码

状态码	描述
201	Created
400	Bad request
403	Forbidden
404	NotFound

错误码

请参见**错误码**。

4.3.7.3 获取消息通知配置

功能介绍

获取消息通知配置。

URI

GET /v5/notification-settings/{notification_setting_id}

表 4-562 路径参数

参数	是否必选	参数类型	描述
notification_setting_id	是	String	消息通知配置的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：200

表 4-563 响应 Body 参数

参数	参数类型	描述
id	String	消息通知配置的唯一标识符。
urn	String	消息通知配置的唯一资源标识符。
analyzer_id	String	分析器的唯一标识符。
analyzer_name	String	分析器的名称。
analyzer_type	String	分析器的类型。 ● account: 账号级外部访问分析器 ● organization：组织级外部访问分析器 ● account_unused_access：账号级未使用访问分析器 ● organization_unused_access：组织级未使用访问分析器 ● account_iam_best_practice：账号级IAM最佳实践分析器
mc_switch	Boolean	是否开启消息中心通知开关。
smn_topic_urns	Array of strings	消息通知配置的SMN主题URN列表。
created_at	String	创建消息通知配置的时间。
updated_at	String	上次更新消息通知配置的时间。

状态码：400

表 4-564 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：403

表 4-565 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：404

表 4-566 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

请求示例

获取消息通知配置。

```
GET https://{hostname}/v5/notification-settings/{notification_setting_id}
```

响应示例

状态码：200

OK

```
{
  "id" : "{notification_setting_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
  "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
  "analyzer_type" : "account",
  "analyzer_name" : "external_analyzer_1",
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
  "created_at" : "2023-09-07T08:04:41.698Z",
  "updated_at" : "2023-09-07T08:04:41.698Z"
}
```

状态码

状态码	描述
200	OK
400	Bad request
403	Forbidden
404	NotFound

错误码

请参见**错误码**。

4.3.7.4 更新消息通知配置

功能介绍

更新消息通知配置。

URI

PUT /v5/notification-settings/{notification_setting_id}

表 4-567 路径参数

参数	是否必选	参数类型	描述
notification_setting_id	是	String	消息通知配置的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

表 4-568 请求 Body 参数

参数	是否必选	参数类型	描述
mc_switch	是	Boolean	是否开启消息中心通知开关。
smn_topic_urns	是	Array of strings	消息通知配置的SMN主题URN列表。

响应参数

状态码：200

OK

状态码：400

表 4-569 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：403

表 4-570 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：404

表 4-571 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

请求示例

更新消息通知配置。

```
POST https://{hostname}/v5/notification-settings/{notification_setting_id}

{
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ]
}
```

响应示例

无

状态码

状态码	描述
200	OK
400	Bad request
403	Forbidden
404	NotFound

错误码

请参见**错误码**。

4.3.7.5 删除消息通知配置

功能介绍

删除消息通知配置。

URI

DELETE /v5/notification-settings/{notification_setting_id}

表 4-572 路径参数

参数	是否必选	参数类型	描述
notification_setting_id	是	String	消息通知配置的唯一标识符。 最小长度：**1** 最大长度：**36**

请求参数

无

响应参数

状态码：204

Deleted

状态码：400

表 4-573 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

状态码：403

表 4-574 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误信息。
request_id	String	请求 ID。
encoded_authorization_message	String	鉴权信息。

请求示例

删除消息通知配置。

```
POST https://{hostname}/v5/notification-settings/{notification_setting_id}
```

响应示例

无

状态码

状态码	描述
204	Deleted
400	Bad request
403	Forbidden

错误码

请参见**错误码**。

5 应用示例

5.1 密钥定期自动化轮换

场景描述

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

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

总体思路

定期轮换访问密钥（AK/SK）时，步骤如下：

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

涉及的接口如下：

- **创建永久访问密钥**
- **查询所有永久访问密钥**
- **删除指定永久访问密钥**

步骤 1：创建永久 AK/SK

URI：POST /v5/users/{user_id}/access-keys

API文档详情请参见：**创建永久访问密钥**

- 请求示例


```
POST https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys
```

- 响应示例

```
{
  "access_key" : {
    "user_id" : "07609fb9358010e21f7bc003751...",
    "access_key_id" : "P83EVBZJMXCYTMUII...",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "secret_access_key" : "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
    "status" : "active"
  }
}
```

步骤 2：查询 AK/SK 的创建时间

URI：GET /v5/users/{user_id}/access-keys

API文档详情请参见：**查询所有永久访问密钥**

- 请求示例

```
GET https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys
```

- 响应示例

```
{
  "access_keys" : [ {
    "user_id" : "07609fb9358010e21f7bc003751...",
    "access_key_id" : "P83EVBZJMXCYTMUII...",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  } ],
  "page_info" : {
    "current_count" : 1
  }
}
```

步骤 3：更换新的 AK/SK

更换新的AK/SK，请重复**步骤1：创建永久AK/SK**。

步骤 4：删除需要轮换的 AK/SK

URI：DELETE /v5/users/{user_id}/access-keys/{access_key_id}

API文档详情请参见：**删除指定永久访问密钥**

- 请求示例

```
DELETE https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys/
P83EVBZJMXCYTMUII...
```

- 响应示例

  该接口无返回体，状态码为204表示删除成功。

5.2 对 IAM 用户的权限进行安全审计

场景描述

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

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

总体思路

对IAM用户的权限进行安全审计，包含审计IAM用户自身附加的身份策略，以及IAM用户组附加的身份策略。对IAM用户自身附加的身份策略进行权限审计，只需要将待审计的权限与附加的身份策略内容进行对比即可。因此，接下来只以IAM用户组附加的身份策略权限审计为例进行详细说明，操作对步骤如下：

1. 查询用户组列表；
2. 查询用户组权限；
3. 查询身份策略内容；
4. 确定需要审计的权限，查询用户组中的IAM用户，进行安全审计。

涉及的接口如下：

- **查询用户组列表**
- **查询指定用户组附加的所有身份策略**
- **查询指定身份策略的所有版本**
- **查询IAM用户列表**

步骤 1：查询用户组列表

URI：GET /v5/groups

API文档详情请参见：**查询用户组列表**

- 请求示例
```
GET https://{endpoint}/v5/groups
```
- 响应示例
```
{
  "groups" : [ {
    "group_id" : "5b050baea9db472c88cbae67e8d6....",
    "group_name" : "IAMGroupA",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::d78cbac186b744899480f25bd022....:group:IAMGroupA",
    "description" : "IAMdescription"
  }, {
    "group_id" : "07609e7eb200250a3f7dc003cb7a....",
    "group_name" : "IAMGroupB",
    "created_at" : "2023-09-11T10:13:40.016Z",
    "urn" : "iam::d78cbac186b744899480f25bd022....:group:IAMGroupB",
    "description" : "IAMdescription"
  } ],
  "page_info" : {
    "current_count" : 2
  }
}
```

步骤 2：查询用户组权限

URI：GET /v5/groups/{group_id}/attached-policies

API文档详情请参见：**查询指定用户组附加的所有身份策略**

- 请求示例


```
GET https://{endpoint}/v5/groups/5b050baea9db472c88cbae67e8d6..../attached-policies
```

- 响应示例

```
{
 "attached_policies" : [ {
  "policy_name" : "ReadPolicy",
  "policy_id" : "75cfe22af2b3498d82b655fbb39d....",
  "urn" : "iam::d78cbac186b744899480f25bd022.....:policy:ReadPolicy",
  "attached_at" : "2023-09-25T09:31:44.935Z"
 } ],
 "page_info" : {
  "current_count" : 1
 }
}
```

步骤 3：查询身份策略内容

URI：GET /v5/policies/{policy_id}/versions

API文档详情请参见：**查询指定身份策略的所有版本**

- 请求示例

```
GET https://{endpoint}/v5/policies/75cfe22af2b3498d82b655fbb39d..../versions
```

- 响应示例

```
{
 "versions" : [ {
  "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"iam:*:get*
\",\"iam:*:list*\"]}]}",
  "version_id" : "v1",
  "is_default" : true,
  "created_at" : "2023-09-25T09:03:24.786Z"
 } ],
 "page_info" : {
  "current_count" : 1
 }
}
```

步骤 4：确定需要审计的权限，查询用户组中的 IAM 用户，进行安全审计

URI：GET /v5/users

API文档详情请参见：**查询IAM用户列表**

- 请求示例

```
GET https://{endpoint}/v5/users?group_id=5b050baea9db472c88cbae67e8d6....
```

- 响应示例

```
{
 "users" : [ {
  "description" : "description",
  "user_name" : "IAMUserA",
  "is_root_user" : false,
  "created_at" : "2023-04-26T03:49:42Z",
  "user_id" : "07609fb9358010e21f7bc003751c....",
  "urn" : "iam::d78cbac186b744899480f25bd022.....:user:IAMUserA",
  "enabled" : true
 }, {
  "description" : "description",
  "user_name" : "IAMUserB",
  "is_root_user" : false,
  "created_at" : "2023-04-26T03:52:27Z",
  "user_id" : "076837351e80251c1f0fc003afe4....",
  "urn" : "iam::d78cbac186b744899480f25bd022.....:user:IAMUserB",
  "enabled" : true
 } ],
```

```
  "page_info" : {
    "current_count" : 2
  }
}
```


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IAM进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），如果华为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IAM服务的其他功能。

通过IAM，您可以通过授权控制主体（IAM用户、委托、信任委托）对华为云资源的访问范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 6-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	• 系统角色 • 系统策略 • 自定义策略	为IAM身份授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	• 系统身份策略 • 自定义身份策略	• 为IAM身份授予身份策略 • 身份策略附加至IAM身份	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。

帐号下的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。

6.2 IAM 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）。

- 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IAM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IAM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IAM的相关操作。

表 6-2 IAM 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
iam::listAccessKeys	授予列举永久访问密钥的权限。	List	-	-	• iam:credentials:listCredentials
iam::createAccessKey	授予创建永久访问密钥的权限。	Write	-	-	• iam:credentials:createCredential
iam::getAccessKey	授予查询永久访问密钥的权限。	Read	-	-	• iam:credentials:getCredential
iam::updateAccessKey	授予修改永久访问密钥的权限。	Write	-	-	• iam:credentials:updateCredential
iam::deleteAccessKey	授予删除永久访问密钥的权限。	Write	-	-	• iam:credentials:deleteCredential
iam:projects:list	授予列举项目的权限。	List	-	-	• iam:projects:listProjects
iam:projects:create	授予创建项目的权限。	Write	-	-	• iam:projects:createProject

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:projects:listForUser	授予列举指定用户项目的权限。	List	-	-	• iam:projects:listProjectsForUser
iam:projects:update	授予修改项目的权限。	Write	-	-	• iam:projects:updateProject
iam:groups:list	授予列举用户组的权限。	List	-	-	• iam:groups:listGroups
iam:groups:create	授予创建用户组的权限。	Write	-	-	• iam:groups:createGroup
iam:groups:get	授予查询用户组的权限。	Read	-	-	• iam:groups:getGroup
iam:groups:delete	授予删除用户组的权限。	Write	-	-	• iam:groups:deleteGroup
iam:groups:update	授予修改用户组的权限。	Write	-	-	• iam:groups:updateGroup
iam:groups:removeUser	授予从用户组中移除用户的权限。	Write	-	-	• iam:permissions:removeUserFromGroup
iam:groups:listUsers	授予列举指定用户组中用户的权限。	List	-	-	• iam:users:listUsersForGroup
iam:groups:checkUser	授予查询用户是否在用户组中的权限。	Read	-	-	• iam:permissions:checkUserInGroup
iam:groups:addUser	授予添加用户到用户组的权限。	Write	-	-	• iam:permissions:addUserToGroup
iam:users:create	授予创建用户的权限。	Write	-	-	• iam:users:createUser

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:users:get	授予查询用户的权限。	Read	-	-	• iam:users:getUser
iam:users:update	授予修改用户的权限。	Write	-	-	• iam:users:updateUser
iam:users:list	授予列举用户的权限。	List	-	-	• iam:users:listUsers
iam:users:delete	授予删除用户的权限。	Write	-	-	• iam:users:deleteUser
iam:users:listGroups	授予列举指定用户所属用户组的权限。	List	-	-	• iam:groups:listGroupsForUser
iam:users:listVirtualMFADevices	授予列举指定用户所属虚拟MFA设备的权限。	List	-	-	• iam:mfa:listVirtualMFADevices
iam:users:createVirtualMFADevice	授予创建虚拟MFA设备密钥的权限。	Write	-	-	• iam:mfa:createVirtualMFADevice
iam:users:deleteVirtualMFADevice	授予删除虚拟MFA设备的权限。	Write	-	-	• iam:mfa:deleteVirtualMFADevice
iam:users:getVirtualMFADevice	授予查询虚拟MFA设备的权限。	Read	-	-	• iam:mfa:getVirtualMFADevice
iam:users:bindVirtualMFADevice	授予绑定虚拟MFA设备的权限。	Write	-	-	• iam:mfa:bindMFADevice
iam:users:unbindVirtualMFADevice	授予解绑虚拟MFA设备的权限。	Write	-	-	• iam:mfa:unbindMFADevice
iam:identityProviders:list	授予列举身份提供商的权限。	List	-	-	• iam:identityProviders:listIdentityProviders

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:identityProviders:get	授予查询身份提供商的权限。	Read	-	-	• iam:identityProviders:getIdentityProvider
iam:identityProviders:create	授予创建身份提供商的权限。	Write	-	-	• iam:identityProviders:createIdentityProvider
iam:identityProviders:delete	授予删除身份提供商的权限。	Write	-	-	• iam:identityProviders:deleteIdentityProvider
iam:identityProviders:update	授予修改身份提供商的权限。	Write	-	-	• iam:identityProviders:updateIdentityProvider
iam:identityProviders:listMappings	授予列举身份提供商映射关系的权限。	List	-	-	-
iam:identityProviders:getMapping	授予查询身份提供商映射关系的权限。	Read	-	-	-
iam:identityProviders:createMapping	授予创建身份提供商映射关系的权限。	Write	-	-	-
iam:identityProviders:deleteMapping	授予删除身份提供商映射关系的权限。	Write	-	-	-
iam:identityProviders:updateMapping	授予修改身份提供商映射关系的权限。	Write	-	-	-
iam:identityProviders:listProtocols	授予列举身份提供商协议的权限。	List	-	-	-
iam:identityProviders:getProtocol	授予查询身份提供商协议的权限。	Read	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:identityProviders:createProtocol	授予创建身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:deleteProtocol	授予删除身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:updateProtocol	授予修改身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:getSAMLMetadata	授予查询身份提供商SAML metadata文件的权限。	Read	-	-	• iam:identityProviders:getIDPMetadata
iam:identityProviders:createSAMLMetadata	授予创建身份提供商SAML metadata文件的权限。	Write	-	-	• iam:identityProviders:createIDPMetadata
iam:identityProviders:getOIDCConfig	授予查询身份提供商OIDC配置的权限。	Read	-	-	• iam:identityProviders:getOpenIDConnectConfig
iam:identityProviders:createOIDCConfig	授予创建身份提供商OIDC配置的权限。	Write	-	-	• iam:identityProviders:createOpenIDConnectConfig
iam:identityProviders:updateOIDCConfig	授予修改身份提供商OIDC配置的权限。	Write	-	-	• iam:identityProviders:updateOpenIDConnectConfig
iam:securityPolicies:getProtectPolicy	授予查询操作保护策略的权限。	Read	-	-	-
iam:securityPolicies:updateProtectPolicy	授予修改操作保护策略的权限。	Write	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:securityPolicies:getPasswordPolicy	授予查询密码策略的权限。	Read	-	-	-
iam:securityPolicies:updatePasswordPolicy	授予修改密码策略的权限。	Write	-	-	-
iam:securityPolicies:getLoginPolicy	授予查询登录策略的权限。	Read	-	-	-
iam:securityPolicies:updateLoginPolicy	授予修改登录策略的权限。	Write	-	-	-
iam:securityPolicies:getConsoleAclPolicy	授予查询控制台访问策略的权限。	Read	-	-	-
iam:securityPolicies:updateConsoleAclPolicy	授予修改控制台访问策略的权限。	Write	-	-	-
iam:securityPolicies:getApiAclPolicy	授予查询接口访问策略的权限。	Read	-	-	-
iam:securityPolicies:updateApiAclPolicy	授予修改接口访问策略的权限。	Write	-	-	-
iam:securityPolicies:getPrivacyTransferPolicy	授予查询账号信息跨境传输策略的权限。	Read	-	-	-
iam:securityPolicies:updatePrivacyTransferPolicy	授予修改账号信息跨境传输策略的权限。	Write	-	-	-
iam:users:listLoginProtectSettings	授予列举租户下用户登录保护设置的权限。	List	-	-	• iam:users:listUserLoginProtects

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:users:getLoginProtectSetting	授予查询登录保护设置的权限。	Read	-	-	• iam:users:getUserLoginProtect
iam:users:updateLoginProtectSetting	授予修改登录保护设置的权限。	Write	-	-	• iam:users:setUserLoginProtect
iam:quotas:list	授予列举配额的权限。	List	-	-	• iam:quotas:listQuotas
iam:quotas:listForProject	授予查询项目配额的权限。	List	-	-	• iam:quotas:listQuotasForProject
iam:agencies:pass	授予向云服务传递委托的权限。	Permission_management	agency *	-	-
iam:roles:list	授予查询权限列表的权限。	List	-	-	• iam:roles:listRoles
iam:roles:get	授予查询权限详情的权限。	Read	-	-	• iam:roles:getRole
iam::listRoleAssignments	授予查询租户授权记录的权限。	List	-	-	• iam:permissions:listRoleAssignments
iam:groups:listRolesOnDomain	授予查询全局服务中用户组权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnDomain
iam:groups:listRolesOnProject	授予查询项目服务中用户组权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnProject
iam:groups:grantRoleOnDomain	授予为用户组授予全局服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToGroupOnDomain

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:groups:grantRoleOnProject	授予为用户组授予项目级服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToGroupOnProject
iam:groups:checkRoleOnDomain	授予查询用户组是否拥有全局服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroupOnDomain
iam:groups:checkRoleOnProject	授予查询用户组是否拥有项目服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroupOnProject
iam:groups:listRoles	授予查询用户组的所有权限的权限。	List	-	-	• iam:permissions:listRolesForGroup
iam:groups:checkRole	授予查询用户组是否拥有指定权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroup
iam:groups:revokeRole	授予移除用户组指定权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroup
iam:groups:revokeRoleOnDomain	授予移除用户组的全局服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnDomain
iam:groups:revokeRoleOnProject	授予移除用户组的项目服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnProject

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:groups:grantRole	授予为用户组授予指定权限的权限。	Write	-	-	• iam:permissions:grantRoleToGroup
iam:roles:create	授予创建自定义策略的权限。	Write	-	-	• iam:roles:createRole
iam:roles:update	授予修改自定义策略的权限。	Write	-	-	• iam:roles:updateRole
iam:roles:delete	授予删除自定义策略的权限。	Write	-	-	• iam:roles:deleteRole
iam:agencies:list	授予列出委托的权限。	List	-	-	• iam:agencies:listAgencies
iam:agencies:listSwitchAgencyHistories	授予列出切换委托历史的权限。	List	-	-	-
iam:agencies:get	授予查询指定委托详情的权限。	Read	-	-	• iam:agencies:getAgency
iam:agencies:create	授予创建委托的权限。	Write	-	-	• iam:agencies:createAgency
iam:agencies:update	授予修改委托的权限。	Write	-	-	• iam:agencies:updateAgency
iam:agencies:delete	授予删除委托的权限。	Write	-	-	• iam:agencies:deleteAgency
iam:agencies:listRolesOnDomain	授予查询委托拥有的全局服务权限的权限。	List	-	-	• iam:permissions:listRolesForAgencyOnDomain

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:agencies:listRolesOnProject	授予查询委托拥有的指定项目权限的权限。	List	-	-	• iam:permissions:listRolesForAgencyOnProject
iam:agencies:grantRoleOnDomain	授予为委托授予全局服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnDomain
iam:agencies:grantRoleOnProject	授予为委托授予项目服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnProject
iam:agencies:checkRoleOnDomain	授予查询委托是否拥有全局服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgencyOnDomain
iam:agencies:checkRoleOnProject	授予查询委托是否拥有项目服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgencyOnProject
iam:agencies:revokeRoleOnDomain	授予移除委托的全局服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnDomain
iam:agencies:revokeRoleOnProject	授予移除委托的项目服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnProject
iam:agencies:listRoles	授予查询委托的所有权限的权限。	List	-	-	• iam:permissions:listRolesForAgency

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:agencies:grantRole	授予为委托授予指定权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgency
iam:agencies:checkRole	授予查询委托是否拥有指定权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgency
iam:agencies:revokeRole	授予移除委托的指定权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgency
iam::listGroupsAssignedEnterpriseProject	授予查询企业项目关联的用户组的权限。	List	-	-	• iam:permissions:listGroupsOnEnterpriseProject
iam:groups:listRolesOnEnterpriseProject	授予查询企业项目已关联用户组的权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnEnterpriseProject
iam:groups:grantRoleOnEnterpriseProject	授予基于用户组为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToGroupOnEnterpriseProject
iam:groups:revokeRoleOnEnterpriseProject	授予删除企业项目关联的用户组权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnEnterpriseProject
iam:groups:listAssignedEnterpriseProjects	授予查询用户组直接关联的企业项目的权限。	List	-	-	• iam:permissions:listEnterpriseProjectsForGroup

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:users:listAssignedEnterpriseProjects	授予查询用户直接关联的企业项目的权限。	List	-	-	• iam:permissions:listEnterpriseProjectsForUser
iam::listUsersAssignedEnterpriseProject	授予查询企业项目直接关联用户的权限。	List	-	-	• iam:permissions:listUsersForEnterpriseProject
iam:users:listRolesOnEnterpriseProject	授予查询企业项目直接关联用户权限的权限。	List	-	-	• iam:permissions:listRolesForUserOnEnterpriseProject
iam:users:grantRoleOnEnterpriseProject	授予基于用户为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToUserOnEnterpriseProject
iam:users:revokeRoleOnEnterpriseProject	授予删除企业项目直接关联用户的权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromUserOnEnterpriseProject
iam:agencies:grantRoleOnEnterpriseProject	授予基于委托为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnEnterpriseProject
iam:agencies:revokeRoleOnEnterpriseProject	授予删除企业项目关联的委托的权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnEnterpriseProject
iam:mfa:listMFADevicesV5	授予列举MFA设备的权限。	List	mfa *	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:mfa:createVirtualMFADeviceV5	授予创建虚拟MFA设备的权限。	Write	mfa *	-	-
iam:mfa:deleteVirtualMFADeviceV5	授予删除虚拟MFA设备的权限。	Write	mfa *	-	-
iam:mfa:enableV5	授予启用MFA设备的权限。	Write	mfa *	-	-
iam:mfa:disableV5	授予禁用MFA设备的权限。	Write	mfa *	-	-
iam:securitypolicies:getPasswordPolicyV5	授予获取密码策略信息的权限。	Read	-	-	-
iam:securitypolicies:updatePasswordPolicyV5	授予修改密码策略的权限。	Write	-	-	-
iam:securitypolicies:getLoginPolicyV5	授予获取登录策略信息的权限。	Read	-	-	-
iam:securitypolicies:updateLoginPolicyV5	授予修改登录策略的权限。	Write	-	-	-
iam:credentials:listCredentialsV5	授予权限以列举IAM用户的永久访问密钥。	List	user *	**g:ResourceTag/<tag-key>**	-
iam:credentials:showAccessKeyLastUsedV5	授予获取指定永久访问密钥最后一次使用时间的权限。	Read	user *	**g:ResourceTag/<tag-key>**	-
iam:credentials:createCredentialV5	授予为IAM用户创建永久访问密钥的权限。	Write	user *	**g:ResourceTag/<tag-key>**	-
iam:credentials:updateCredentialV5	授予为IAM用户修改永久访问密钥的权限。	Write	user *	**g:ResourceTag/<tag-key>**	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:credentials:deleteCredentialV5	授予为IAM用户删除永久访问密钥的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:changePasswordV5	授予IAM用户修改自己密码的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:showLoginProfileV5	授予获取IAM用户登录信息的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:createLoginProfileV5	授予为IAM用户创建登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:updateLoginProfileV5	授予为IAM用户修改登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:deleteLoginProfileV5	授予为IAM用户删除登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:listUsersV5	授予列举IAM用户的权限。	List	user *	-	-
iam:users:getUserV5	授予获取IAM用户信息的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:showUserLastLoginV5	授予获取IAM用户最后一次登录时间的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:createUserV5	授予创建IAM用户的权限。	Write	user *	-	-
iam:users:updateUserV5	授予修改IAM用户的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:deleteUserV5	授予删除IAM用户的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:groups:listGroupsV5	授予列举用户组的权限。	List	group *	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:groups:getGroupV5	授予获取用户组信息的权限。	Read	group *	-	-
iam:groups:createGroupV5	授予创建用户组的权限。	Write	group *	-	-
iam:groups:updateGroupV5	授予修改用户组的权限。	Write	group *	-	-
iam:groups:deleteGroupV5	授予删除用户组的权限。	Write	group *	-	-
iam:permissions:addUserToGroupV5	授予添加IAM用户到用户组的权限。	Write	group *	-	-
iam:permissions:removeUserFromGroupV5	授予从用户组中移除IAM用户的权限。	Write	group *	-	-
iam:policies:listV5	授予列举身份策略的权限。	List	policy *	-	-
iam:policies:getV5	授予获取身份策略信息的权限。	Read	policy *	-	-
iam:policies:createV5	授予创建自定义身份策略的权限。	Permission_management	policy *	-	-
iam:policies:deleteV5	授予删除自定义身份策略的权限。	Permission_management	policy *	-	-
iam:policies:listVersionsV5	授予列举身份策略版本的权限。	List	policy *	-	-
iam:policies:getVersionV5	授予获取身份策略版本信息的权限。	Read	policy *	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:policies:createVersionV5	授予为自定义身份策略创建新版本的权限。	Permission_management	policy *	-	-
iam:policies:deleteVersionV5	授予为自定义身份策略删除版本的权限。	Permission_management	policy *	-	-
iam:policies:setDefaultVersionV5	授予设置自定义身份策略默认版本的权限。	Permission_management	policy *	-	-
iam:agencies:attachPolicyV5	授予为委托或信任委托附加身份策略的权限。	Permission_management	agency *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:groups:attachPolicyV5	授予为用户组附加身份策略的权限。	Permission_management	group *	-	-
			-	iam:PolicyURN	
iam:users:attachPolicyV5	授予为IAM用户附加身份策略的权限。	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:agencies:detachPolicyV5	授予为委托或信任委托分离身份策略的权限。	Permission_management	agency *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:groups:detachPolicyV5	授予为用户组分离身份策略的权限。	Permission_management	group *	-	-
			-	iam:PolicyURN	

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:users:detachPolicyV5	授予为IAM用户分离身份策略的权限。	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:policies:listEntitiesV5	授予权限以列举附加在身份策略上的所有实体。	List	policy *	-	-
iam:agencies:listAttachedPoliciesV5	授予权限以列举委托或信任委托附加的身份策略。	List	agency *	g:ResourceTag/<tag-key>	-
iam:groups:listAttachedPoliciesV5	授予权限以列举用户组附加的身份策略。	List	group *	-	-
iam:users:listAttachedPoliciesV5	授予权限以列举IAM用户附加的身份策略。	List	user *	g:ResourceTag/<tag-key>	-
iam:agencies:createServiceLinkedAgencyV5	授予创建服务关联委托的权限以允许云服务代表您执行操作。	Write	agency *	-	-
			-	iam:ServicePrincipal	
iam:agencies:deleteServiceLinkedAgencyV5	授予删除服务关联委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	iam:ServicePrincipal	
iam:agencies:getServiceLinkedAgencyDeletionStatusV5	授予获取服务关联委托删除状态的权限。	Read	agency *	-	-
iam:agencies:listV5	授予列举委托及信任委托的权限。	List	agency *	-	-
iam:agencies:getV5	授予获取委托或信任委托信息的权限。	Read	agency *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:agencies:createV5	授予创建信任委托的权限。	Write	agency *	-	-
iam:agencies:updateV5	授予修改信任委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:deleteV5	授予删除信任委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:updateTrustPolicyV5	授予修改信任委托信任策略的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam::listTagsForResourceV5	授予列举资源标签的权限。	List	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
iam::tagForResourceV5	授予设置资源标签的权限。	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
iam::untagForResourceV5	授予删除资源标签的权限。	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
iam::getAccountSummaryV5	授予获取此账号中IAM实体使用情况和IAM配额的摘要信息的权限。	List	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam::getAsymmetricSignatureSwitchV5	授予获取临时令牌非对称签名开关状态的权限。	Read	-	-	-
iam::setAsymmetricSignatureSwitchV5	授予设置临时令牌非对称签名开关状态的权限。	Write	-	-	-

IAM的API通常对应着一个或多个授权项。表6-3展示了API与授权项的关系，以及该API需要依赖的授权项。

表 6-3 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3.0/OS-CREDENTIAL/credentials	iam::listAccessKeys	-
POST /v3.0/OS-CREDENTIAL/credentials	iam::createAccessKey	-
GET /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::getAccessKey	-
PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::updateAccessKey	-
DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::deleteAccessKey	-
GET /v3.0/OS-QUOTA/domains/{domain_id}	iam:quotas:list	-
GET /v3.0/OS-QUOTA/projects/{project_id}	iam:quotas:listForProject	-
GET /v3/projects	iam:projects:list	-
POST /v3/projects	iam:projects:create	-
GET /v3/users/{user_id}/projects	iam:projects:listForUser	-
PATCH /v3/projects/{project_id}	iam:projects:update	-

API	对应的授权项	依赖的授权项
PUT /v3-ext/projects/{project_id}	iam:projects:update	-
GET /v3/groups	iam:groups:list	-
POST /v3/groups	iam:groups:create	-
GET /v3/groups/{group_id}	iam:groups:get	-
DELETE /v3/groups/{group_id}	iam:groups:delete	-
PATCH /v3/groups/{group_id}	iam:groups:update	-
GET /v3/groups/{group_id}/users	iam:groups:listUsers	-
HEAD /v3/groups/{group_id}/users/{user_id}	iam:groups:checkUser	-
PUT /v3/groups/{group_id}/users/{user_id}	iam:groups:addUser	-
DELETE /v3/groups/{group_id}/users/{user_id}	iam:groups:removeUser	-
POST /v3.0/OS-USER/users	iam:users:create	-
GET /v3.0/OS-USER/users/{user_id}	iam:users:get	-
PUT /v3.0/OS-USER/users/{user_id}	iam:users:update	-
PUT /v3.0/OS-USER/users/{user_id}/info	iam:users:update	-
GET /v3/users	iam:users:list	-
POST /v3/users	iam:users:create	-
GET /v3/users/{user_id}	iam:users:get	-
DELETE /v3/users/{user_id}	iam:users:delete	-
PATCH /v3/users/{user_id}	iam:users:update	-
GET /v3/users/{user_id}/groups	iam:users:listGroups	-
GET /v3.0/OS-MFA/virtual-mfa-devices	iam:users:listVirtualMFADevices	-
POST /v3.0/OS-MFA/virtual-mfa-devices	iam:users:createVirtualMFADevice	-
DELETE /v3.0/OS-MFA/virtual-mfa-devices	iam:users:deleteVirtualMFADevice	-

API	对应的授权项	依赖的授权项
GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device	iam:users:getVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/bind	iam:users:bindVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/unbind	iam:users:unbindVirtualMFADevice	-
GET /v3.0/OS-USER/login-protects	iam:users:listLoginProtectSettings	-
GET /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:getLoginProtectSetting	-
PUT /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:updateLoginProtectSetting	-
GET /v3/OS-FEDERATION/identity_providers	iam:identityProviders:list	-
GET /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:get	-
PUT /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:create	-
DELETE /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:delete	-
PATCH /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:update	-
GET /v3/OS-FEDERATION/mappings	iam:identityProviders:listMappings	-
GET /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:getMapping	-
PUT /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:createMapping	-
DELETE /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:deleteMapping	-
PATCH /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:updateMapping	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols	iam:identityProviders:listProtocols	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-

API	对应的授权项	依赖的授权项
PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:createProtocol	-
DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:deleteProtocol	-
PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:updateProtocol	-
GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:getSAMLMetadata	-
POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:createSAMLMetadata	-
GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:getOIDCConfig	-
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:createOIDCConfig	-
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:updateOIDCConfig	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:getProtectPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:updateProtectPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:getPasswordPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:updatePasswordPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:getLoginPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:updateLoginPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:getConsoleAclPolicy	-

API	对应的授权项	依赖的授权项
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:updateConsoleAclPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:getApiAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:updateApiAclPolicy	-
GET /v3/roles	iam:roles:list	-
GET /v3/roles/{role_id}	iam:roles:get	-
GET /v3.0/OS-PERMISSION/role-assignments	iam::listRoleAssignments	-
GET /v3/domains/{domain_id}/groups/{group_id}/roles	iam:groups:listRolesOnDomain	-
GET /v3/projects/{project_id}/groups/{group_id}/roles	iam:groups:listRolesOnProject	-
PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnDomain	-
PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnProject	-
HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnDomain	-
HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnProject	-
GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects	iam:groups:listRoles	-
HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:checkRole	-
DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:revokeRole	-
DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnDomain	-
DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnProject	-

API	对应的授权项	依赖的授权项
PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:grantRole	-
GET /v3.0/OS-ROLE/roles	iam:roles:list	-
GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:get	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
DELETE /v3.0/OS-ROLE/roles/{role_id}	iam:roles:delete	-
GET /v3.0/OS-AGENCY/agencies	iam:agencies:list	-
GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:get	-
POST /v3.0/OS-AGENCY/agencies	iam:agencies:create	-
PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:update	-
DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:delete	-
GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnDomain	-
GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnProject	-
PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnDomain	-
PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnProject	-
HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnDomain	-
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnProject	-

API	对应的授权项	依赖的授权项
DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnDomain	-
DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnProject	-
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:agencies:listRoles	-
PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:grantRole	-
HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:checkRole	-
DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:revokeRole	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups	iam::listGroupsAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles	iam:groups:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnEnterpriseProject	-
GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects	iam:groups:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects	iam:users:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users	iam::listUsersAssignedEnterpriseProject	-

API	对应的授权项	依赖的授权项
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles	iam:users:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:revokeRoleOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:revokeRoleOnEnterpriseProject	-
GET /v5/asymmetric-signature-switch	iam::getAsymmetricSignatureSwitchV5	-
PUT /v5/asymmetric-signature-switch	iam::setAsymmetricSignatureSwitchV5	-
GET /v5/mfa-devices	iam:mfa:listMFADevicesV5	-
POST /v5/virtual-mfa-devices	iam:mfa:createVirtualMFADeviceV5	-
DELETE /v5/virtual-mfa-devices	iam:mfa:deleteVirtualMFADeviceV5	-
POST /v5/mfa-devices/enable	iam:mfa:enableV5	-
POST /v5/mfa-devices/disable	iam:mfa:disableV5	-
GET /v5/password-policy	iam:securitypolicies:getPasswordPolicyV5	-
PUT /v5/password-policy	iam:securitypolicies:updatePasswordPolicyV5	-
GET /v5/login-policy	iam:securitypolicies:getLoginPolicyV5	-

API	对应的授权项	依赖的授权项
PUT /v5/login-policy	iam:securitypolicies:updateLoginPolicyV5	-
GET /v5/users/{user_id}/access-keys	iam:credentials:listCredentialsV5	-
GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used	iam:credentials:showAccessKeyLastUsedV5	-
POST /v5/users/{user_id}/access-keys	iam:credentials:createCredentialV5	-
PUT /v5/users/{user_id}/access-keys/{access_key_id}	iam:credentials:updateCredentialV5	-
DELETE /v5/users/{user_id}/access-keys/{access_key_id}	iam:credentials:deleteCredentialV5	-
POST /v5/caller-password	iam:users:changePasswordV5	-
GET /v5/users/{user_id}/login-profile	iam:users:showLoginProfileV5	-
POST /v5/users/{user_id}/login-profile	iam:users:createLoginProfileV5	-
PUT /v5/users/{user_id}/login-profile	iam:users:updateLoginProfileV5	-
DELETE /v5/users/{user_id}/login-profile	iam:users:deleteLoginProfileV5	-
GET /v5/users	iam:users:listUsersV5	-
GET /v5/users/{user_id}	iam:users:getUserV5	-
GET /v5/users/{user_id}/last-login	iam:users:showUserLastLoginV5	-
POST /v5/users	iam:users:createUserV5	-
PUT /v5/users/{user_id}	iam:users:updateUserV5	-
DELETE /v5/users/{user_id}	iam:users:deleteUserV5	-
GET /v5/groups	iam:groups:listGroupsV5	-

API	对应的授权项	依赖的授权项
GET /v5/groups/{group_id}	iam:groups:getGroupV5	-
POST /v5/groups	iam:groups:createGroupV5	-
PUT /v5/groups/{group_id}	iam:groups:updateGroupV5	-
DELETE /v5/groups/{group_id}	iam:groups:deleteGroupV5	-
POST /v5/groups/{group_id}/add-user	iam:permissions:addUserToGroupV5	-
POST /v5/groups/{group_id}/remove-user	iam:permissions:removeUserFromGroupV5	-
GET /v5/policies	iam:policies:listV5	-
GET /v5/policies/{policy_id}	iam:policies:getV5	-
POST /v5/policies	iam:policies:createV5	-
DELETE /v5/policies/{policy_id}	iam:policies:deleteV5	-
GET /v5/policies/{policy_id}/versions	iam:policies:listVersionsV5	-
GET /v5/policies/{policy_id}/versions/{version_id}	iam:policies:getVersionV5	-
POST /v5/policies/{policy_id}/versions	iam:policies:createVersionV5	-
DELETE /v5/policies/{policy_id}/versions/{version_id}	iam:policies:deleteVersionV5	-
POST /v5/policies/{policy_id}/versions/{version_id}/set-default	iam:policies:setDefaultVersionV5	-
POST /v5/policies/{policy_id}/attach-agency	iam:agencies:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-group	iam:groups:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-user	iam:users:attachPolicyV5	-
POST /v5/policies/{policy_id}/detach-agency	iam:agencies:detachPolicyV5	-

API	对应的授权项	依赖的授权项
POST /v5/policies/{policy_id}/detach-group	iam:groups:detachPolicyV5	-
POST /v5/policies/{policy_id}/detach-user	iam:users:detachPolicyV5	-
GET /v5/policies/{policy_id}/attached-entities	iam:policies:listEntitiesV5	-
GET /v5/agencies/{agency_id}/attached-policies	iam:agencies:listAttachedPoliciesV5	-
GET /v5/groups/{group_id}/attached-policies	iam:groups:listAttachedPoliciesV5	-
GET /v5/users/{user_id}/attached-policies	iam:users:listAttachedPoliciesV5	-
PUT /v5/service-linked-agencies	iam:agencies:createServiceLinkedAgencyV5	-
DELETE /v5/service-linked-agencies/{agency_id}	iam:agencies:deleteServiceLinkedAgencyV5	-
GET /v5/service-linked-agencies/deletion-task/{deletion_task_id}	iam:agencies:getServiceLinkedAgencyDeletionStatusV5	-
GET /v5/agencies	iam:agencies:listV5	-
GET /v5/agencies/{agency_id}	iam:agencies:getV5	-
POST /v5/agencies	iam:agencies:createV5	-
PUT /v5/agencies/{agency_id}	iam:agencies:updateV5	-
DELETE /v5/agencies/{agency_id}	iam:agencies:deleteV5	-
PUT /v5/agencies/{agency_id}/trust-policy	iam:agencies:updateTrustPolicyV5	-
GET /v5/{resource_type}/{resource_id}/tags	iam::listTagsForResourceV5	-
POST /v5/{resource_type}/{resource_id}/tags/create	iam::tagForResourceV5	-
DELETE /v5/{resource_type}/{resource_id}/tags/delete	iam::untagForResourceV5	-

API	对应的授权项	依赖的授权项
GET /v5/account-summary	iam::getAccountSummaryV5	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表6-4中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

IAM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 6-4 IAM 支持的资源类型

资源类型	URN
agency	iam::<account-id>:agency:<agency-name-with-path>
policy	iam::<account-id>:policy:<policy-name-with-path>
mfa	iam::<account-id>:mfa:<mfa-name>
user	iam::<account-id>:user:<user-name>
group	iam::<account-id>:group:<group-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iam:）仅适用于对应服务的操作，详情请参见表6-5。
  - 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。

IAM支持的服务级条件键

IAM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 6-5 IAM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
iam:PolicyURN	string	单值	按照身份策略的URN筛选访问权限。
iam:ServicePrincipal	string	单值	按照服务关联委托传递的云服务对应的服务标识筛选访问权限。

6.3 STS 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）。

- 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STS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STS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STS的相关操作。

表 6-6 STS 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
sts:agencies:assume	授予权限以获取一组可用来访问您通常无法访问的资源的临时安全凭证。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:ExternalId • sts:SourceIdentity • sts:TransitiveTagKeys • sts:AgencySessionName • g:RequestTag/<tag-key> • g:TagKeys • g:SourceAccount • g:SourceUrn	
sts::decodeAuthorizationMessage	授予权限以从为响应请求而返回的编码消息中解码有关请求授权状态的其他信息。	Write	-	-	-
sts::setSourceIdentity	授予在 STS 会话上设置源身份的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	sts:SourceIdentity	

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sts::tagSession	授予权限以将标签添加至 STS 会话。	Tagging	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:TransitiveTagKeys • g:RequestTag/<tag-key> • g:TagKeys	
sts::createServiceBearerToken	授予权限获取一个绑定至某服务的 Bearer Token。	Write	-	• sts:DurationTime • sts:ServiceName	-

STS的API通常对应着一个或多个授权项。表6-7展示了API与授权项的关系，以及该API需要依赖的授权项。

表 6-7 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/agencies/assume	sts:agencies:assume	• sts::tagSession • sts::setSourceIdentity
POST /v5/decode-authorization-message	sts::decodeAuthorizationMessage	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表6-8中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

STS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 6-8 STS 支持的资源类型

资源类型	URN
agency	iam::<account-id>:agency:<agency-name-with-path>

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sts:）仅适用于对应服务的操作，详情请参见**表6-9**。
  - 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**。

STS支持的服务级条件键

STS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 6-9 STS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
sts:ExternalId	string	单值	按您代入另一个账号中的委托时所需的唯一标识符筛选访问权限。
sts:SourceIdentity	string	单值	按照在请求中传递的源身份筛选访问权限。
sts:TransitiveTagKeys	string	多值	按照在请求中传递的可传递标签键筛选访问权限。
sts:AgencySessionName	string	单值	按您代入委托时所需的委托会话名称筛选访问权限。

服务级条件键	类型	单值/多值	说明
sts:DurationTime	numeric	单值	按照创建 Bearer Token 的持续时间筛选访问权限。
sts:ServiceName	string	单值	按照创建 Bearer Token 的服务名筛选访问权限。

6.4 IAM Access Analyzer 身份策略授权参考

云服务在IAM预置了常用授权项，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）。

- 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IAM Access Analyzer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IAM Access Analyzer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IAM Access Analyzer的相关操作。

表 6-10 IAM Access Analyzer 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
AccessAnalyzer:analyzer:create	授予创建分析器的权限。	Write	analyzer *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
AccessAnalyzer:analyzer:get	授予查询分析器的权限。	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:list	授予查询分析器列表的权限。	List	analyzer *	-	-
AccessAnalyzer:analyzer:delete	授予删除分析器的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:scan	授予启动分析器扫描的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:getFinding	授予查询分析结果的权限。	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listFindings	授予查询分析结果列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:updateFindings	授予更新分析结果的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::tagResource	授予给资源添加标签的权限。	Tagging	analyzer *	g:ResourceTag/<tag-key>	-

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	
AccessAnalyzer::untagResource	授予给资源删除标签的权限。	Tagging	analyzer *	g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
AccessAnalyzer:archiveRule:create	授予创建存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:get	授予查询存档规则的权限。	Read	archiveRule *	-	-
AccessAnalyzer:archiveRule:list	授予查询存档规则列表的权限。	List	archiveRule *	-	-
AccessAnalyzer:archiveRule:update	授予更新存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:delete	授予删除存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:apply	授予应用存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:analyzer:createPreview	授予创建访问分析预览的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:getPreview	授予查询访问分析预览的权限。	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviews	授予查询访问分析预览列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviewFindings	授予查询访问分析预览分析结果列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
AccessAnalyzer:analyzer:createResourceConfigurations	授予创建资源配置的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listResourceConfigurations	授予查询资源配置列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:deleteResourceConfigurations	授予删除资源配置的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::validatePolicy	授予验证策略的权限。	Read	-	-	-
AccessAnalyzer::checkNoNewAccess	授予检查更新后的策略是否有新的访问权限。	Read	-	-	-
AccessAnalyzer:notificationSetting:list	授予查询消息通知配置列表的权限。	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:create	授予创建消息通知配置的权限。	Write	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:get	授予查询消息通知配置的权限。	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:update	授予更新消息通知配置的权限。	Write	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:delete	授予删除消息通知配置的权限。	Write	notificationSetting *	-	-

IAM Access Analyzer的API通常对应着一个或多个授权项。表6-11展示了API与授权项的关系，以及该API需要依赖的授权项。

表 6-11 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/analyzers	AccessAnalyzer:analyzer:create	iam:agencies:createServiceLinkedAgencyV5
GET /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:get	-
GET /v5/analyzers	AccessAnalyzer:analyzer:list	-
DELETE /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:delete	-
POST /v5/analyzers/{analyzer_id}/scan	AccessAnalyzer:analyzer:scan	-
GET /v5/analyzers/{analyzer_id}/findings/{finding_id}	AccessAnalyzer:analyzer:getFinding	-
POST /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:listFindings	-
PUT /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:updateFindings	-
POST /v5/{resource_type}/{resource_id}/tags/create	AccessAnalyzer::tagResource	-
POST /v5/{resource_type}/{resource_id}/tags/delete	AccessAnalyzer::untagResource	-
POST /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:create	-
GET /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:get	-

API	对应的授权项	依赖的授权项
GET /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:list	-
PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:update	-
DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:delete	-
POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply	AccessAnalyzer:archiveRule:apply	-
POST /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:createPreview	-
GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}	AccessAnalyzer:analyzer:getPreview	-
GET /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:listPreviews	-
POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings	AccessAnalyzer:analyzer:listPreviewFindings	-
POST /v5/analyzers/{analyzer_id}/resource-configurations/create	AccessAnalyzer:analyzer:createResourceConfigurations	-

API	对应的授权项	依赖的授权项
GET /v5/analyzers/{analyzer_id}/resource-configurations	AccessAnalyzer:analyzer:listResourceConfigurations	-
POST /v5/analyzers/{analyzer_id}/resource-configurations/delete	AccessAnalyzer:analyzer:deleteResourceConfigurations	-
POST /v5/policies/validate	AccessAnalyzer::validatePolicy	-
POST /v5/policies/check-no-new-access	AccessAnalyzer::checkNoNewAccess	-
GET /v5/notification-settings	AccessAnalyzer:notificationSetting:list	-
POST /v5/notification-settings	AccessAnalyzer:notificationSetting:create	-
GET /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:get	-
PUT /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:update	-
DELETE /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:delete	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如**表6-12**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

IAM Access Analyzer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 6-12 IAM Access Analyzer 支持的资源类型

资源类型	URN
analyzer	AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>
notificationSetting	AccessAnalyzer:<region>:<account-id>:notificationSetting:<notification-setting-id>
archiveRule	AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>

条件（Condition）

IAM Access Analyzer服务不支持在身份策略中的条件键中配置服务级的条件键。IAM Access Analyzer可以使用适用于所有服务的全局条件键，请参考**全局条件键**。

7 附录

7.1 状态码

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。
201	Created	创建类的请求完全成功。
202	Accepted	已经接受请求，但未处理完成。
203	Non-Authoritative Information	非授权信息，请求成功。
204	NoContent	请求完全成功，同时HTTP响应不包含响应体。 在响应OPTIONS方法的HTTP请求时返回此状态码。
205	Reset Content	重置内容，服务器处理成功。
206	Partial Content	服务器成功处理了部分GET请求。
300	Multiple Choices	多种选择。请求的资源可包括多个位置，相应可返回一个资源特征与地址的列表用于用户终端（例如：浏览器）选择。

状态码	编码	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。

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_msg": "attached policies per agency limit exceeded",
    "error_code": "PAP5.0003",
    "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，错误相应地Body体格式如下所示。

```
{
    "error_msg": "access denied: xxx...xxx",
    "error_code": "PAP5.0001",
    "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；如果遇到“IAM”开头的错误码，请参见**经典IAM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
400	PAP5.0010	invalid marker	无效的marker。	请检查marker字段的值是否正确。
400	PAP5.0011	malformed policy document	身份策略或信任策略内容错误。	请检查policy document字段的值是否正确。
400	PAP5.0029	invalid agency name	无效的信任委托名。	请检查agency name字段的值是否正确。
400	PAP5.0030	invalid path	无效的path。	请检查path字段的值是否正确。
400	PAP5.0033	duplicate key	重复的键值。	请确认请求或联系技术支持。
400	PAP5.0036	tag non-compliant	标签值不匹配预设规则。	请确认请求或联系技术支持。

状态码	错误码	错误信息	描述	处理措施
400	PAP5.0038	This operation is only supported by v5 agencies	仅信任委托支持此类操作。	请确认请求或联系技术支持。
400	PAP5.0040	invalid caller	无效的调用方。	请确认调用方是否为IAM用户。
400	PAP5.0041	invalid serial number	无效的序列号。	请检查serial number字段的值是否正确。
400	PAP5.0046	missing header `x-user-profile`	请求头中缺少x-user-profile。	请确认请求或联系技术支持。
403	PAP5.0001	access denied: %s	访问受限。	请确认是否允许此操作。
404	PAP5.0012	no such agency	未找到此委托或信任委托。	请确认请求或联系技术支持。
404	PAP5.0014	no such authorization schema	未找到此授权概要。	请确认请求或联系技术支持。
404	PAP5.0015	no such deletion task	未找到此删除任务。	请确认请求或联系技术支持。
404	PAP5.0016	no such group	未找到此用户组。	请确认请求或联系技术支持。
404	PAP5.0018	no such policy	未找到此身份策略。	请确认请求或联系技术支持。
404	PAP5.0019	no such policy attachment	未找到此身份策略附加记录。	请确认请求或联系技术支持。
404	PAP5.0020	no such policy version	未找到此身份策略版本。	请确认请求或联系技术支持。
404	PAP5.0021	no such user	未找到此IAM用户。	请确认请求或联系技术支持。
404	PAP5.0022	no such service linked agency	未找到此服务关联委托。	请确认请求或联系技术支持。
404	PAP5.0023	no such service principal	未找到此服务主体。	请确认请求或联系技术支持。
404	PAP5.0034	no such domain	未找到此租户。	请确认请求或联系技术支持。
404	PAP5.0037	Resource tag not found	未找到此资源标签。	请确认请求或联系技术支持。

状态码	错误码	错误信息	描述	处理措施
409	PAP5.0003	attached policies per agency limit exceeded	单个委托或信任委托附加的身份策略数超过限制。	请分离多余的身份策略。
409	PAP5.0004	attached policies per group limit exceeded	单个用户组附加的身份策略数超过限制。	请分离多余的身份策略。
409	PAP5.0005	attached policies per user limit exceeded	单个IAM用户附加的身份策略数超过限制。	请分离多余的身份策略。
409	PAP5.0006	concurrent modification	并发修改。	请稍后重试。
409	PAP5.0007	delete conflict: %s	存在冲突，无法删除。	请解决冲突。
409	PAP5.0024	policies limit exceeded	自定义身份策略数超过限制。	请删除多余的自定义身份策略。
409	PAP5.0025	policy already exists	身份策略已存在。	请确认请求或联系技术支持。
409	PAP5.0026	policy attachment already exists	该身份策略已附加。	请确认请求或联系技术支持。
409	PAP5.0027	policy size limit exceeded	身份策略或信任策略内容的字节数超过最大值%d（不包括空白字符）。	请精简身份策略或信任策略的内容。
409	PAP5.0028	versions per policy limit exceeded	单个身份策略的版本数超过限制。	请删除多余的身份策略版本。
409	PAP5.0031	agency already exists	该委托或信任委托已存在。	请确认请求或联系技术支持。
409	PAP5.0035	tags limit exceeded	标签数量超过上限。	请确认请求或联系技术支持。
409	PAP5.0039	mfa device already exists	该MFA设备已存在。	请确认请求或联系技术支持。
409	PAP5.0042	user already exists	该IAM用户已存在。	请确认请求或联系技术支持。
409	PAP5.0043	group already exists	该用户组已存在。	请确认请求或联系技术支持。
409	PAP5.0044	user already in group	该IAM用户已在该用户组中。	请确认请求。

状态码	错误码	错误信息	描述	处理措施
409	PAP5.0045	login profile already exists	登录信息已存在。	请确认请求或联系技术支持。