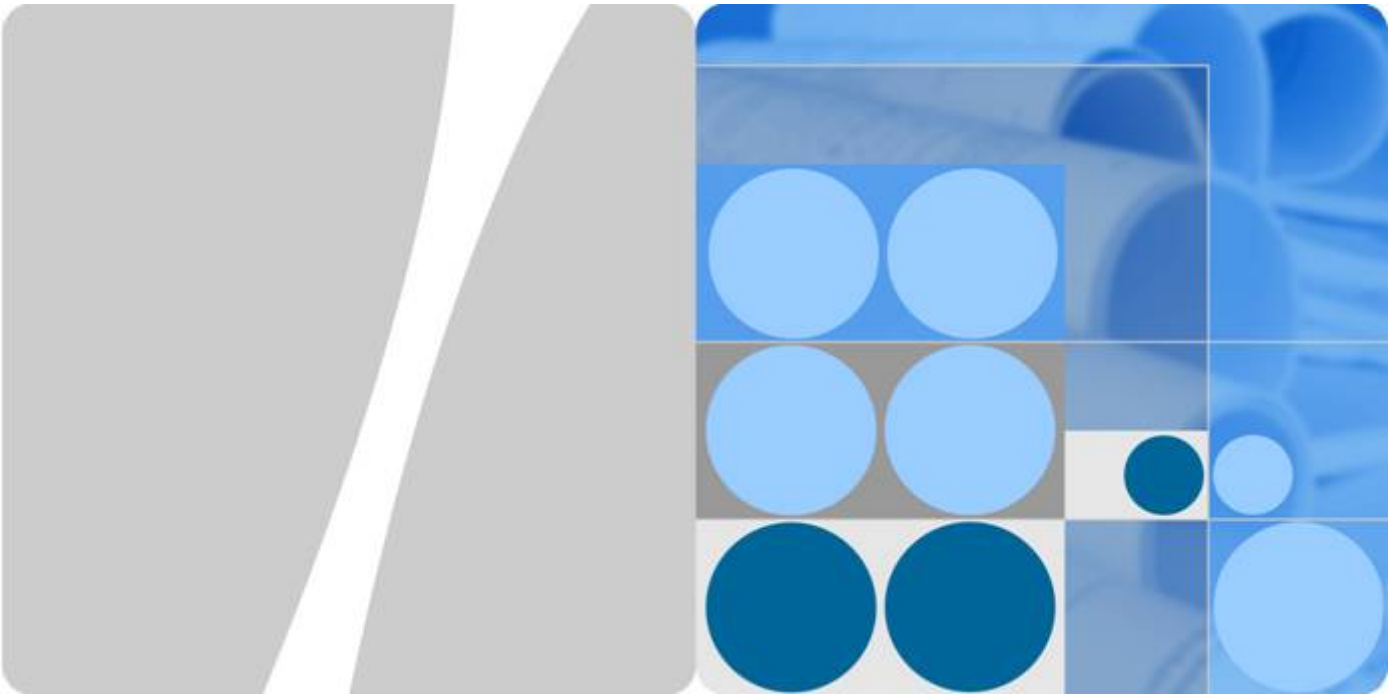


云审计服务

5.0.8

API 参考

发布日期　2024-04-30

目 录

1 使用前必读

1.1 概述

欢迎使用云审计服务（Cloud Trace Service，以下简称CTS），CTS是云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

您可以使用本文档提供API对云审计服务进行相关操作，如创建、删除追踪器等。在调用云审计服务的API之前，请确保已经充分了解云审计服务的相关概念与功能。

1.2 调用说明

云审计服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，请向企业管理员获取区域和终端节点信息。

1.4 基本概念

- 账号

  用户的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。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该用户进行日常管理工作。

- 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）。

  通常在调用API的鉴权过程中，您需要用到账号、用户和密码等信息。

- 区域（Region）

  指云资源所在的物理位置，同一区域内可用区间内网互通，不同区域间内网不互通。通过在不同地区创建云资源，可以将应用程序设计的更接近特定客户的要求，或满足不同地区的法律或其他要求。

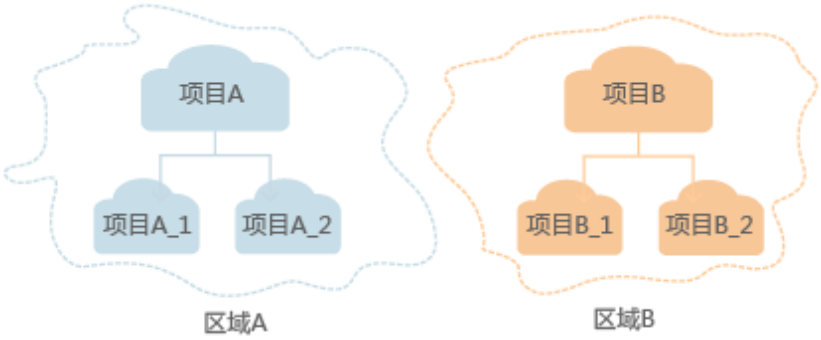
- 可用区（AZ，Availability Zone）

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

- 项目

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

  图 1-1 项目隔离模型

- 企业项目

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

  关于企业项目ID的获取及企业项目特性的详细信息，请参见《企业管理用户指南》。

2 API 概览

云审计服务所提供的接口为扩展接口。通过使用云审计服务所提供的接口，您可以完整的使用云审计服务的所有功能。例如查询事件列表、创建追踪器等。

云审计服务提供的具体API如表2-1所示。

表 2-1 接口说明

子类型	说明
追踪器	CTS API的追踪器管理接口，用来创建、修改、查询以及删除追踪器。
事件	CTS API的事件管理接口，用来查询系统记录的7天内资源操作记录。

3 如何调用 API

3.1 构造请求

本节介绍REST API请求的组成，并以调用IAM服务的获取用户Token说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权

请求 URI

请求URI由如下部分组成。

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

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，您可以从企业管理员处地区和终端点获取。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **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。

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，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

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

```
POST https://{{endpoint}}/v3/auth/tokens
```

请求消息头

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

详细的公共请求消息头字段请参见表3-1。

表 3-1 公共请求消息头

名称	描述	是否必选	示例
Host	请求的服务器信息，从服务API的URL中获取。值为hostname[:port]。端口缺省时使用默认的端口，https的默认端口为443。	否 使用AK/SK认证时该字段必选。	code.test.com or code.test.com:443
Content-Type	消息体的类型（格式）。推荐用户使用默认值application/json，有其他取值时会在具体接口中专门说明。	是	application/json
Content-Length	请求body长度，单位为Byte。	否	3495

名称	描述	是否必选	示例
X-Project-Id	project id，项目编号。请参考**获取账号ID和项目ID**章节获取项目编号。	否	e9993fc787d94b6c886cbaa340f9c0f4
X-Auth-Token	用户Token。 用户Token也就是调用获取用户Token接口的响应值，该接口是唯一不需要认证的接口。 请求响应成功后在响应消息头（Headers）中包含的“X-Subject-Token”的值即为Token值。	否 使用Token认证时该字段必选。	注：以下仅为Token示例片段 MIIPAgYJKoZIhvcNAQcCo...ggg1BBIINPXsidG9rZ

说明

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

AK/SK认证的详细说明请参见**认证鉴权**的“AK/SK认证”。

对于获取用户Token接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://{{endpoint}}/v3/auth/tokens
Content-Type: application/json
```

请求消息体（可选）

该部分可选。请求消息体通常以结构化格式（如JSON或XML）发出，与请求消息头中Content-Type对应，传递除请求消息头之外的内容。若请求消息体中的参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于获取用户Token接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的账号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxx***为project的名称，您可以从企业管理员处获取。

说明

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

```
POST https://{{endpoint}}/v3/auth/tokens
```

```
Content-Type: application/json

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

到这里为止这个请求需要的内容就具备齐全了，您可以使用curl、Postman或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

3.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key)加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

Token 认证

说明

Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

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

Token可通过调用获取用户Token接口获取，调用本服务API需要project级别的Token，即调用获取用户Token接口时，请求body中auth.scope的取值需要选择project，如下所示。

```
{
   "auth": {
      "identity": {
         "methods": [
            "password"
         ],
         "password": {
            "user": {
               "name": "username",
```

```
                "password": "********",
                "domain": {
                    "name": "domainname"
                }
            }
        }
    },
    "scope": {
        "project": {
            "name": "xxxxxxxx"
        }
    }
  }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFJ....”，则调用接口时将“X-Auth-Token: ABCDEFJ....”加到请求消息头即可，如下所示。

```
POST https://{{endpoint}}/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK 认证

说明

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

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

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

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。

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。

以下结合一个Demo来介绍如何对一个请求进行签名，并通过HTTP Client发送一个HTTPS请求的过程。如果您不使用Demo工程，也可以向管理员获取API网关签名工具，并在其他工程中引用。

1. 生成AK/SK。如果已生成过AK/SK，则可跳过此步骤，找到原来已下载的AK/SK文件，文件名一般为：credentials.csv。
   a. 登录管理控制台。
   b. 单击用户名，在下拉列表中单击“我的凭证”。
   c. 单击“访问密钥”。
   d. 单击“新增访问密钥”，进入“新增访问密钥”页面。
   e. 输入描述信息，单击“确定”，下载访问密钥。

说明

为防止访问密钥泄露，建议您将其保存到安全的位置。

2. 获取示例代码，并解压缩。
3. 通过import方式将示例工程导入到Eclipse。

图 3-1 选择已存在的工程

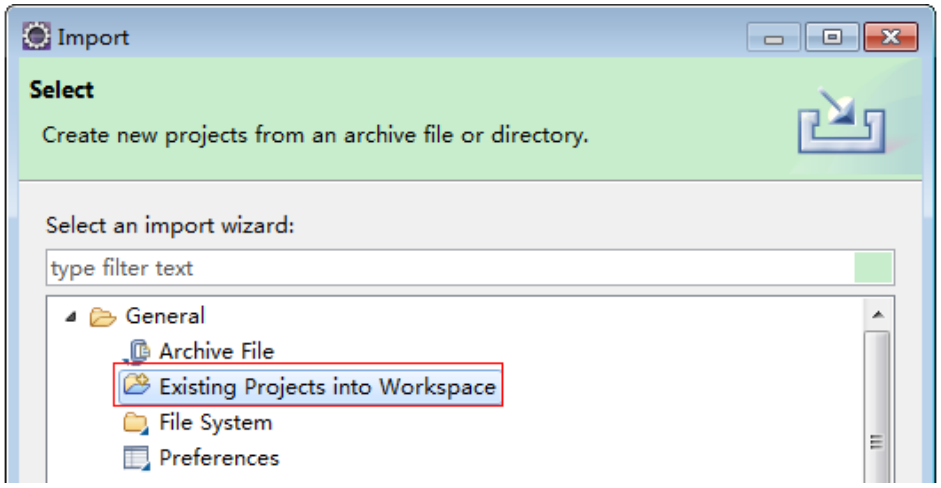


图 3-2 选择解压后的示例代码

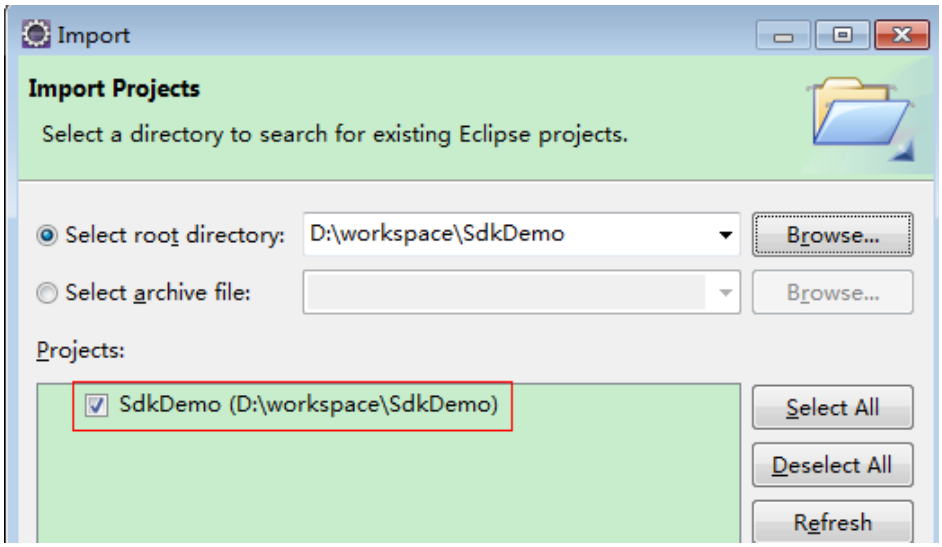
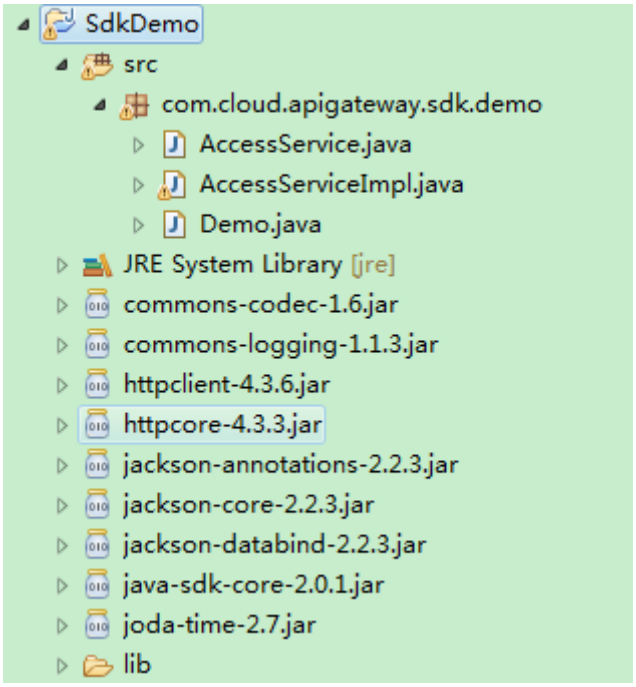


图 3-3 导入成功后工程结构示例



4. 对请求进行签名。

   签名方法集成在3引入的java-sdk-core-x.x.x.jar文件中。发送请求前，需要对请求内容进行签名，得到的签名结果将作为http头部信息一起发送。

   Demo代码分成三个类进行演示：

   - AccessService：抽象类，将GET/POST/PUT/DELETE归一成access方法。
   - Demo：运行入口，模拟用户进行GET/POST/PUT/DELETE请求。
   - AccessServiceImpl：实现access方法，具体与API网关通信的代码都在access方法中。

   a. 编辑“Demo.java”文件中的main方法，将以下内容替换为实际获取到的值。

      如果调用其他方法，如POST，PUT，DELETE等，请参考对应注释方法。

      注意替换 region、serviceName、AK/SK 和 URL，Demo中使用了获取VPC的 URL，请替换为您需要的URL：

      URL中project_id获取请参见“附录 > 获取账号ID和项目ID”。

```
//TODO: Replace region with the name of the region in which the service to be accessed is located.
private static final String region = "";

//TODO: Replace vpc with the name of the service you want to access. For example, ecs, vpc, iam, and elb.
private static final String serviceName = "";

public static void main(String[] args) throws UnsupportedEncodingException
{
//TODO: Replace the AK and SK with those obtained on the My Credential page.
String ak = "ZIRRKMTWP******1WKNKB";
String sk = "Us0mdMNHk******YrRCnW0ecfzl";

//TODO: To specify a project ID (multi-project scenarios), add the X-Project-Id header.
//TODO: To access a global service, such as IAM, DNS, CDN, and TMS, add the X-Domain-Id header to specify an account ID.
//TODO: To add a header, find "Add special headers" in the AccessServiceImple.java file.
```

```
//TODO: Test the API
String url = "https://{Endpoint}/v1/{project_id}/vpcs";
get(ak, sk, url);

//TODO: When creating a VPC, replace {project_id} in postUrl with the actual value.
//String postUrl = "https://serviceEndpoint/v1/{project_id}/cloudservers";
//String postbody ="{\"vpc\": {\"name\": \"vpc\",\"cidr\": \"192.168.0.0/16\"}}";
//post(ak, sk, postUrl, postbody);

//TODO: When querying a VPC, replace {project_id} in url with the actual value.
//String url = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//get(ak, sk, url);

//TODO: When updating a VPC, replace {project_id} and {vpc_id} in putUrl with the actual values.
//String putUrl = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//String putbody ="{\"vpc\":{\"name\": \"vpc1\",\"cidr\": \"192.168.0.0/16\"}}";
//put(ak, sk, putUrl, putbody);

//TODO: When deleting a VPC, replace {project_id} and {vpc_id} in deleteUrl with the actual values.
//String deleteUrl = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//delete(ak, sk, deleteUrl);
}
```

b. 编译与运行接口调用。

在左侧“Package Explorer”中找到“Demo.java”，右键选择“Run AS > Java Application”并单击“运行”。

可在控制台查看调用日志。

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。

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

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于“获取用户Token”接口，返回如图3-4所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 3-4 获取用户 Token 响应消息头

响应消息体（可选）

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

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

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

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

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

4 API

4.1 关键操作通知管理

4.1.1 创建关键操作通知

功能介绍

配置关键操作通知，可在发生特定操作时，使用预先创建好的SMN主题，向用户手机、邮箱发送消息，也可直接发送http/https消息。常用于实时感知高危操作、触发特定操作或对接用户自有审计分析系统。

URI

POST /v3/{project_id}/notifications

表 4-1 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

请求参数

表 4-2 请求 Body 参数

参数	是否必选	参数类型	描述
notification_name	是	String	标识关键操作名称。
operation_type	是	String	标识操作类型。 目前支持的操作类型有完整类型(complete)和自定义类型(customized)。 完整类型下，CTS发送通知的对象为已对接服务的所有事件，此时不用指定operations和notify_user_list字段。 自定义类型下，CTS发送通知的对象是在operations列表中指定的事件。 枚举值： • **complete** • **customized**
operations	否	Array of **Operations** objects	操作事件列表。
notify_user_list	否	Array of **NotificationUsers** objects	通知用户列表，目前最多支持对10个用户组和50个用户发起的操作进行配置。
topic_id	否	String	消息通知服务的topic_urn或者函数工作流的func_urn。- 消息通知服务的topic_urn可以通过消息通知服务的查询主题列表API获取，示例：urn:smn:regionId:f96188c7ccaf4ffba0c9aa149ab2bd57:test_topic_v2。- 函数工作流的func_urn可以通过函数工作流的获取函数列表API获取，示例：urn:fss:xxxxxxxxx:7aad83af3e8d42e99ac194e8419e2c9b:function:default:test。
filter	否	**Filter** object	关键操作通知高级过滤条件。

表 4-3 Operations

参数	是否必选	参数类型	描述
service_type	是	String	标识云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 已对接的云服务列表参见《云审计服务用户指南》“支持审计的服务及详细操作列表”章节。
resource_type	是	String	标识资源类型。
trace_names	是	Array of strings	标识事件名称。

表 4-4 NotificationUsers

参数	是否必选	参数类型	描述
user_group	是	String	IAM用户组。
user_list	是	Array of strings	IAM用户。

表 4-5 Filter

参数	是否必选	参数类型	描述
condition	是	String	多条件关系。 ● AND(默认值) 表示所有过滤条件满足后生效。 ● OR 表示有任意一个条件满足时生效。 枚举值： ● **AND(默认值)** ● **OR**
is_support_filter	是	Boolean	是否打开高级筛选开关。

参数	是否必选	参数类型	描述
rule	是	Array of strings	高级过滤条件规则，示例如下："key != value"，格式为：字段 规则 值。-字段取值范围：api_version,code,trace_rating,trace_type,resource_id,resource_name。-规则：!= 或 =。- 值：api_version正则约束：^(a-zA-Z0-9_-.){1,64}$；code：最小长度1，最大长度256；trace_rating枚举值："normal", "warning", "incident"；trace_type枚举值："ConsoleAction", "ApiCall", "SystemAction"；resource_id：最小长度1，最大长度350；resource_name：最小长度1，最大长度256

响应参数

状态码： 201

表 4-6 响应 Body 参数

参数	参数类型	描述
notification_name	String	通知名称。
operation_type	String	操作类型。和自定义。 • complete：完整类型，对所有已对接云审计服务的所有操作发送SMN通知。 • customized：自定义类型，对指定云服务的指定操作发送SMN通知。 枚举值： • **customized** • **complete**
operations	Array of **Operations** objects	操作事件列表。
notify_user_list	Array of **NotificationUsers** objects	通知用户列表，目前最多支持对10个用户组和50个用户发起的操作进行配置。

参数	参数类型	描述
status	String	通知状态。启用和停用。 • disabled：停用关键操作通知。 • enabled：启用关键操作通知。 枚举值： • **enabled** • **disabled**
topic_id	String	消息通知服务(SMN)主题的唯一的资源标识，可通过查询主题列表获取该标识。
notification_id	String	通知的唯一标识ID。
notification_type	String	通知类型。 -smn：消息通知服务。 -fun：函数工作流。 枚举值： • **smn** • **fun**
project_id	String	项目ID。
create_time	Long	通知规则创建时间。
filter	**Filter** object	关键操作通知高级筛选条件。

表 4-7 Operations

参数	参数类型	描述
service_type	String	标识云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 已对接的云服务列表参见《 云审计服务用户指南 》“支持审计的服务及详细操作列表”章节。
resource_type	String	标识资源类型。
trace_names	Array of strings	标识事件名称。

表 4-8 NotificationUsers

参数	参数类型	描述
user_group	String	IAM用户组。
user_list	Array of strings	IAM用户。

表 4-9 Filter

参数	参数类型	描述
condition	String	多条件关系。 ● AND(默认值) 表示所有过滤条件满足后生效。 ● OR 表示有任意一个条件满足时生效。 枚举值： ● **AND(默认值)** ● **OR**
is_support_filter	Boolean	是否打开高级筛选开关。
rule	Array of strings	高级过滤条件规则，示例如下："key != value"，格式为：字段 规则 值。-字段取值范围：api_version,code,trace_rating,trace_type,resource_id,resource_name。-规则：!= 或 =。- 值：api_version正则约束：^(a-zA-Z0-9_-.){1,64}$；code：最小长度1，最大长度256；trace_rating枚举值："normal", "warning", "incident"；trace_type枚举值："ConsoleAction", "ApiCall", "SystemAction"；resource_id：最小长度1，最大长度350；resource_name：最小长度1，最大长度256

状态码： 400

表 4-10 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-11 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-12 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-13 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-14 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-15 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

- 创建自定义类型关键操作通知请求样例。

```
POST  https://{endpoint}/v3/{project_id}/notifications

{
  "notification_name" : "keyOperate_info_cfwy",
  "operation_type" : "customized",
  "filter" : {
    "is_support_filter" : true,
    "rule" : [ "code != 200", "api_version = v1.0", "trace_rating = normal", "trace_type != ApiCall",
"resource_id = xxx", "resource_name = xxx" ],
```

```
    "condition" : "OR"
  },
  "operations" : [ {
    "service_type" : "CTS",
    "resource_type" : "tracker",
    "trace_names" : [ "createTracker", "deleteTracker" ]
  }, {
    "service_type" : "CTS",
    "resource_type" : "notification",
    "trace_names" : [ "deleteNotification", "updateNotification" ]
  }, {
    "service_type" : "AOM",
    "resource_type" : "pe",
    "trace_names" : [ "deletePolicyGroup", "updatePolicyGroup", "createPolicyGroup" ]
  } ],
  "notify_user_list" : [ {
    "user_group" : "admin",
    "user_list" : [ "test1", "test2" ]
  }, {
    "user_group" : "CTS view",
    "user_list" : [ "test3", "test4" ]
  } ],
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:test"
}
```

- 创建完整类型关键操作通知请求样例。

```
POST  https://{endpoint}/v3/{project_id}/notifications

{
  "notification_name" : "test",
  "filter" : {
    "is_support_filter" : true,
    "rule" : [ "code != 200", "api_version = v1.0", "trace_rating = normal", "trace_type != ApiCall",
"resource_id = xxx", "resource_name = xxx" ],
    "condition" : "OR"
  },
  "operation_type" : "complete",
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:test"
}
```

响应示例

状态码： 201

创建成功。

```
{
  "create_time" : 1634001495876,
  "notification_id" : "cda8fd83-d08c-46f0-b914-1453a6a85c00",
  "notification_name" : "keyOperate_info_cfwy",
  "notification_type" : "smn",
  "notify_user_list" : [ {
    "user_group" : "admin",
    "user_list" : [ "test1", "test2" ]
  }, {
    "user_group" : "CTS view",
    "user_list" : [ "test3", "test4" ]
  } ],
  "operation_type" : "customized",
  "operations" : [ {
    "resource_type" : "tracker",
    "service_type" : "CTS",
    "trace_names" : [ "createTracker", "deleteTracker" ]
  }, {
    "resource_type" : "notification",
    "service_type" : "CTS",
    "trace_names" : [ "deleteNotification", "updateNotification" ]
  }, {
    "resource_type" : "pe",
```

```
    "service_type" : "AOM",
    "trace_names" : [ "deletePolicyGroup", "updatePolicyGroup", "createPolicyGroup" ]
  } ],
  "project_id" : "24edf66e79d04187acb99a463e610764",
  "status" : "enabled",
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:test"
}
```

状态码

状态码	描述
201	创建成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源或部分关键操作通知删除失败。
500	服务内部异常，请求未完成；或部分追踪器删除失败。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.1.2 修改关键操作通知

功能介绍

云审计服务支持修改已创建关键操作通知配置项，通过notification_id的字段匹配修改对象，notification_id必须已经存在。

URI

PUT /v3/{project_id}/notifications

表 4-16 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

请求参数

表 4-17 请求 Body 参数

参数	是否必选	参数类型	描述
notification_name	是	String	标识关键操作名称。
operation_type	是	String	标识操作类型。 目前支持的操作类型有完整类型(complete)和自定义类型(customized)。 完整类型下，CTS发送通知的对象为已对接服务的所有事件。 自定义类型下，CTS发送通知的对象是在operations列表中指定的事件。 枚举值： • **customized** • **complete**
operations	否	Array of **Operations** objects	操作事件列表。
notify_user_list	否	Array of **NotificationUsers** objects	通知用户列表，目前最多支持对10个用户组和50个用户发起的操作进行配置。
status	是	String	标识关键操作通知状态，包括正常(enabled)，停止(disabled)两种状态。 枚举值： • **enabled** • **disabled**
topic_id	否	String	消息通知服务的topic_urn或者函数工作流的func_urn，当“status”字段为enabled时，该字段必填。- 消息通知服务的topic_urn可以通过消息通知服务的查询主题列表API获取，示例：urn:smn:regionId:f96188c7ccaf4ffba0c9aa149ab2bd57:test_topic_v2。- 函数工作流的func_urn可以通过函数工作流的获取函数列表API获取，示例：urn:fss:xxxxxxxxx:7aad83af3e8d42e99ac194e8419e2c9b:function:default:test。

参数	是否必选	参数类型	描述
notification_id	是	String	关键操作通知id。
filter	否	**Filter** object	关键操作通知高级筛选条件。

表 4-18 Operations

参数	是否必选	参数类型	描述
service_type	是	String	标识云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 已对接的云服务列表参见《云审计服务用户指南》“支持审计的服务及详细操作列表”章节。
resource_type	是	String	标识资源类型。
trace_names	是	Array of strings	标识事件名称。

表 4-19 NotificationUsers

参数	是否必选	参数类型	描述
user_group	是	String	IAM用户组。
user_list	是	Array of strings	IAM用户。

表 4-20 Filter

参数	是否必选	参数类型	描述
condition	是	String	多条件关系。 • AND(默认值) 表示所有过滤条件满足后生效。 • OR 表示有任意一个条件满足时生效。 枚举值： • **AND(默认值)** • **OR**
is_support_filter	是	Boolean	是否打开高级筛选开关。

参数	是否必选	参数类型	描述
rule	是	Array of strings	高级过滤条件规则，示例如下："key != value"，格式为：字段 规则 值。-字段取值范围：api_version,code,trace_rating,trace_type,resource_id,resource_name。-规则：!= 或 =。- 值：api_version正则约束：^(a-zA-Z0-9_-.){1,64}$；code：最小长度1，最大长度256；trace_rating枚举值："normal", "warning", "incident"；trace_type枚举值："ConsoleAction", "ApiCall", "SystemAction"；resource_id：最小长度1，最大长度350；resource_name：最小长度1，最大长度256

响应参数

状态码： 200

表 4-21 响应 Body 参数

参数	参数类型	描述
notification_name	String	标识关键操作名称。
operation_type	String	标识操作类型。 目前支持的操作类型有完整类型(complete)和自定义类型(customized)。 完整类型下，CTS发送通知的对象为已对接服务的所有事件。 自定义类型下，CTS发送通知的对象是在operations列表中指定的事件。 枚举值： • **customized** • **complete**
operations	Array of **Operations** objects	操作事件列表。
notify_user_list	Array of **NotificationUsers** objects	通知用户列表，目前最多支持对10个用户组和50个用户发起的操作进行配置。

参数	参数类型	描述
status	String	标识关键操作通知状态，包括正常(enabled)，停止(disabled)两种状态。 枚举值： • **enabled** • **disabled**
topic_id	String	消息通知服务的topic_urn或者函数工作流的func_urn。- 消息通知服务的topic_urn可以通过消息通知服务的查询主题列表API获取，示例：urn:smn:regionId:f96188c7ccaf4ffba0c9aa149ab2bd57:test_topic_v2。- 函数工作流的func_urn可以通过函数工作流的获取函数列表API获取，示例：urn:fss:xxxxxxxxx:7aad83af3e8d42e99ac194e8419e2c9b:function:default:test。
notification_id	String	关键操作通知的唯一标识。
notification_type	String	关键操作通知类型，根据topic_id区分为消息通知服务(smn)和函数工作流(fun)。 枚举值： • **smn** • **fun**
project_id	String	项目ID。
create_time	Long	关键操作通知创建时间戳。
filter	**Filter** object	关键操作通知高级筛选条件。

表 4-22 Operations

参数	参数类型	描述
service_type	String	标识云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 已对接的云服务列表参见《 云审计服务用户指南 》“支持审计的服务及详细操作列表”章节。
resource_type	String	标识资源类型。
trace_names	Array of strings	标识事件名称。

表 4-23 NotificationUsers

参数	参数类型	描述
user_group	String	IAM用户组。
user_list	Array of strings	IAM用户。

表 4-24 Filter

参数	参数类型	描述
condition	String	多条件关系。 ● AND(默认值) 表示所有过滤条件满足后生效。 ● OR 表示有任意一个条件满足时生效。 枚举值： ● **AND(默认值)** ● **OR**
is_support_filter	Boolean	是否打开高级筛选开关。
rule	Array of strings	高级过滤条件规则，示例如下："key != value"，格式为：字段 规则 值。-字段取值范围：api_version,code,trace_rating,trace_type,resource_id,resource_name。-规则：!= 或 =。- 值：api_version正则约束：^(a-zA-Z0-9_-.){1,64}$；code：最小长度1，最大长度256；trace_rating枚举值："normal", "warning", "incident"；trace_type枚举值："ConsoleAction", "ApiCall", "SystemAction"；resource_id：最小长度1，最大长度350；resource_name：最小长度1，最大长度256

状态码： 400

表 4-25 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-26 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-27 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-28 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-29 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-30 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

修改关键操作通知请求样例。

```
PUT https://{endpoint}/v3/{project_id}/notifications

{
  "notification_id" : "6d4a09bb-aa8e-40db-9e87-0d5e203823a8",
  "notification_name" : "keyOperate_info_cfwy",
  "operation_type" : "customized",
  "operations" : [ {
    "service_type" : "CTS",
    "resource_type" : "tracker",
    "trace_names" : [ "createTracker", "deleteTracker" ]
  }, {
    "service_type" : "CTS",
    "resource_type" : "notification",
    "trace_names" : [ "deleteNotification", "updateNotification" ]
  }, {
    "service_type" : "AOM",
    "resource_type" : "pe",
    "trace_names" : [ "deletePolicyGroup", "updatePolicyGroup", "createPolicyGroup" ]
  } ],
  "notify_user_list" : [ {
    "user_group" : "admin",
    "user_list" : [ "test", "test1" ]
  }, {
    "user_group" : "CTS view",
    "user_list" : [ "test2", "test3" ]
  } ],
  "status" : "enabled",
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:foo"
}
```

响应示例

状态码： 200

修改关键操作通知成功。

```
{
  "notification_id" : "6d4a09bb-aa8e-40db-9e87-0d5e203823a8",
  "notification_name" : "keyOperate_info_cfwy",
  "operation_type" : "customized",
  "operations" : [ {
    "service_type" : "CTS",
    "resource_type" : "tracker",
    "trace_names" : [ "createTracker", "deleteTracker" ]
  }, {
    "service_type" : "CTS",
    "resource_type" : "notification",
    "trace_names" : [ "deleteNotification", "updateNotification" ]
  }, {
    "service_type" : "AOM",
    "resource_type" : "pe",
    "trace_names" : [ "deletePolicyGroup", "updatePolicyGroup", "createPolicyGroup" ]
  } ],
  "notify_user_list" : [ {
    "user_group" : "admin",
    "user_list" : [ "test", "test1" ]
  }, {
    "user_group" : "CTS view",
    "user_list" : [ "test2", "test3" ]
  } ],
  "status" : "enabled",
  "project_id" : "24edf66e79d04187acb99a463e610764",
  "notification_type" : "smn",
  "create_time" : 1634001495876,
```

```
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:foo"
}
```

状态码

状态码	描述
200	修改关键操作通知成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源或部分关键操作通知删除失败。
500	服务内部异常，请求未完成；或部分追踪器删除失败。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.1.3 删除关键操作通知

功能介绍

云审计服务支持删除已创建的关键操作通知。

URI

DELETE /v3/{project_id}/notifications

表 4-31 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

表 4-32 Query 参数

参数	是否必选	参数类型	描述
notification_id	是	String	标识关键操作通知id。 批量删除请使用逗号隔开，notification_id="xxx1,cccc2"

请求参数

无

响应参数

状态码： 400

表 4-33 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-34 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-35 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-36 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-37 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-38 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

无

响应示例

无

状态码

状态码	描述
204	删除成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源或部分关键操作通知删除失败。
500	服务内部异常，请求未完成；或部分追踪器删除失败。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.1.4 查询关键操作通知

功能介绍

查询创建的关键操作通知规则。

URI

GET /v3/{project_id}/notifications/{notification_type}

表 4-39 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。
notification_type	是	String	通知类型。 -smn：消息通知服务。 -fun：函数工作流。 枚举值： • **smn** • **fun**

表 4-40 Query 参数

参数	是否必选	参数类型	描述
notification_name	否	String	标识关键操作通知名称。 在不传入该字段的情况下，将查询当前租户所有的关键操作通知。

请求参数

无

响应参数

状态码： 200

表 4-41 响应 Body 参数

参数	参数类型	描述
notifications	Array of **NotificationsResponseBody** objects	关键操作通知列表。

表 4-42 NotificationsResponseBody

参数	参数类型	描述
notification_name	String	标识关键操作名称。
operation_type	String	标识操作类型。 目前支持的操作类型有完整类型(complete)和自定义类型(customized)。 完整类型下，CTS发送通知的对象为已对接服务的所有事件。 自定义类型下，CTS发送通知的对象是在operations列表中指定的事件。 枚举值： • **customized** • **complete**
operations	Array of **Operations** objects	操作事件列表。
notify_user_list	Array of **NotificationUsers** objects	通知用户列表，目前最多支持对10个用户组和50个用户发起的操作进行配置。
status	String	标识关键操作通知状态，包括正常(enabled)，停止(disabled)两种状态。 枚举值： • **enabled** • **disabled**
topic_id	String	消息通知服务的topic_urn或者函数工作流的func_urn。- 消息通知服务的topic_urn可以通过消息通知服务的查询主题列表API获取，示例：urn:smn:regionId:f96188c7ccaf4ffba0c9aa149ab2bd57:test_topic_v2。- 函数工作流的func_urn可以通过函数工作流的获取函数列表API获取，示例：urn:fss:xxxxxxxxx:7aad83af3e8d42e99ac194e8419e2c9b:function:default:test。
notification_id	String	关键操作通知的唯一标识。
notification_type	String	关键操作通知类型，根据topic_id区分为消息通知服务(smn)和函数工作流(fun)。 枚举值： • **smn** • **fun**
project_id	String	项目ID。
create_time	Long	关键操作通知创建时间戳。
filter	**Filter** object	关键操作通知高级筛选条件。

表 4-43 Operations

参数	参数类型	描述
service_type	String	标识云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 已对接的云服务列表参见《 云审计服务用户指南 》“支持审计的服务及详细操作列表”章节。
resource_type	String	标识资源类型。
trace_names	Array of strings	标识事件名称。

表 4-44 NotificationUsers

参数	参数类型	描述
user_group	String	IAM用户组。
user_list	Array of strings	IAM用户。

表 4-45 Filter

参数	参数类型	描述
condition	String	多条件关系。 ● AND(默认值) 表示所有过滤条件满足后生效。 ● OR 表示有任意一个条件满足时生效。 枚举值： ● **AND(默认值)** ● **OR**
is_support_filter	Boolean	是否打开高级筛选开关。

参数	参数类型	描述
rule	Array of strings	高级过滤条件规则，示例如下："key != value"，格式为：字段 规则 值。-字段取值范围：api_version,code,trace_rating,trace_type,resource_id,resource_name。-规则：!= 或 =。- 值：api_version正则约束：^(a-zA-Z0-9_-.){1,64}$；code：最小长度1，最大长度256；trace_rating枚举值："normal", "warning", "incident"；trace_type枚举值："ConsoleAction", "ApiCall", "SystemAction"；resource_id：最小长度1，最大长度350；resource_name：最小长度1，最大长度256

状态码： 400

表 4-46 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-47 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-48 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-49 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-50 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-51 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

无

响应示例

状态码： 200

查询成功。

```
{
  "notifications" : [ {
    "create_time" : 1633933167385,
    "notify_user_list" : [ {
      "user_group" : "admin",
      "user_list" : [ "test1", "test2" ]
    }, {
      "user_group" : "CTS view",
      "user_list" : [ "test3", "test4" ]
    } ],
    "notification_id" : "0b98e1c2-2fd6-4e33-a355-f9e12eaab88a",
    "notification_name" : "test2",
    "notification_type" : "smn",
    "operation_type" : "customized",
    "operations" : [ {
      "resource_type" : "tracker",
```

```
    "service_type" : "CTS",
    "trace_names" : [ "createTracker" ]
  }, {
    "resource_type" : "notification",
    "service_type" : "CTS",
    "trace_names" : [ "deleteNotification", "updateNotification" ]
  }, {
    "resource_type" : "pe",
    "service_type" : "AOM",
    "trace_names" : [ "createPolicyGroup", "updatePolicyGroup", "deletePolicyGroup" ]
  } ],
  "project_id" : "24edf66e79d04187acb99a463e610764",
  "status" : "enabled",
  "topic_id" : "urn:smn:{regionid}:24edf66e79d04187acb99a463e610764:test"
 }, {
  "create_time" : 1633924057706,
  "notify_user_list" : [ {
    "user_group" : "admin",
    "user_list" : [ "test1", "test2" ]
  }, {
    "user_group" : "CTS view",
    "user_list" : [ "test3", "test4" ]
  } ],
  "notification_id" : "6d4a09bb-aa8e-40db-9e87-0d5e203823a8",
  "notification_name" : "test1",
  "notification_type" : "smn",
  "operation_type" : "complete",
  "operations" : [ ],
  "project_id" : "24edf66e79d04187acb99a463e610764",
  "status" : "disabled"
 } ]
}
```


状态码

状态码	描述
200	查询成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源或部分关键操作通知删除失败。
500	服务内部异常，请求未完成；或部分追踪器删除失败。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.2 事件管理

4.2.1 查询事件列表

功能介绍

通过事件列表查询接口，可以查出系统记录的7天内资源操作记录。

URI

GET /v3/{project_id}/traces

表 4-52 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

表 4-53 Query 参数

参数	是否必选	参数类型	描述
trace_type	是	String	标识审计事件类型。 目前支持管理类事件（system）和数据类事件（data）。 默认值为"system"。 枚举值： • **system** • **data**
limit	否	Integer	标示查询事件列表中限定返回的事件条数。不传时默认10条，最大值200条。
from	否	Long	标识查询事件列表的起始时间戳（timestamp，为标准UTC时间，毫秒级，13位数字，不包括传入时间）默认为上一小时的时间戳。查询条件from与to配套使用。
next	否	String	取值为响应中中marker的值，用于标识查询事件的起始时间（自此条事件的记录时间起，向更早时间查询）。 可以与“from”、“to”结合使用。最终的查询条件取两组时间条件的交集。

参数	是否必选	参数类型	描述
to	否	Long	标识查询事件列表的结束时间戳（timestamp，为标准UTC时间，毫秒级，13位数字，不包括传入时间）默认为当前时间戳。查询条件to与from配套使用。
tracker_name	否	String	当"trace_type"字段值为"system"时，该字段值默认为"system"。 当"trace_type"字段值为"data"时，该字段值可以传入数据类追踪器名称，达到筛选某个数据类追踪器下的数据事件目的。
service_type	否	String	标识查询事件列表对应的云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。 当"trace_type"字段值为"system"时，该字段筛选有效"。 已对接的云服务列表参见《云审计服务用户指南》“支持审计的服务及详细操作列表”章节。
user	否	String	标识特定用户名称，用以查询该用户下的所有事件。 当"trace_type"字段值为"system"时，该字段筛选有效"。
resource_id	否	String	标示查询事件列表对应的云服务资源ID。 当"trace_type"字段值为"system"时，该字段筛选有效"。
resource_name	否	String	标示查询事件列表对应的的资源名称。 当"trace_type"字段值为"system"时，该字段筛选有效"。 说明：该字段可能包含大写字母。
resource_type	否	String	标示查询事件列表对应的资源类型。 当"trace_type"字段值为"system"时，该字段筛选有效"。
trace_id	否	String	标示某一条事件的事件ID。当传入这个查询条件时，其他查询条件自动不生效。 当"trace_type"字段值为"system"时，该字段筛选有效"。

参数	是否必选	参数类型	描述
trace_name	否	String	标示查询事件列表对应的事件名称。 当"trace_type"字段值为"system"时，该字段筛选有效"。 说明：该字段可能包含大写字母。
trace_rating	否	String	标示查询事件列表对应的事件等级目前有三种：正常(normal)，警告(warning),事故(incident)。 当"trace_type"字段值为"system"时，该字段筛选有效"。 枚举值： • **normal** • **warning** • **incident**

请求参数

无

响应参数

状态码： 200

表 4-54 响应 Body 参数

参数	参数类型	描述
traces	Array of **Traces** objects	本次查询事件列表返回事件数组。
meta_data	**MetaData** object	本次查询事件条数和标记位。

表 4-55 Traces

参数	参数类型	描述
resource_id	String	标识事件对应的云服务资源ID。
trace_name	String	标识查询事件列表对应的事件名称。由0-9,a-z,A-Z,'-','.','_',组成，长度为1～64个字符，且以首字符必须为字母。

参数	参数类型	描述
trace_rating	String	标识事件等级，目前有三种：正常（normal），警告（warning），事故（incident）。 枚举值： • **normal** • **warning** • **incident**
trace_type	String	标识事件发生源头类型，管理类事件主要包括API调用（ApiCall），Console页面调用（ConsoleAction）和系统间调用（SystemAction）。数据类事件主要包括ObsSDK，ObsAPI。
request	String	标识事件对应接口请求内容，即资源操作请求体。
response	String	记录用户请求的响应，标识事件对应接口响应内容，即资源操作结果返回体。
code	String	记录用户请求的响应，标识事件对应接口返回的HTTP状态码。
api_version	String	标识事件对应的云服务接口版本。
message	String	标识其他云服务为此条事件添加的备注信息。
record_time	Long	标识云审计服务记录本次事件的时间戳。
trace_id	String	标识事件的ID，由系统生成的UUID。
time	Long	标识事件产生的时间戳。
user	**UserInfo** object	标识触发事件的用户信息。
service_type	String	标识查询事件列表对应的云服务类型。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。
resource_type	String	查询事件列表对应的资源类型。
source_ip	String	标识触发事件的租户IP。
resource_name	String	标识事件对应的资源名称。
request_id	String	记录本次请求的request id
location_info	String	记录本次请求出错后，问题定位所需要的辅助信息。
endpoint	String	云资源的详情页面
resource_url	String	云资源的详情页面的访问链接（不含endpoint）

表 4-56 UserInfo

参数	参数类型	描述
id	String	账号ID，参见《云审计服务API参考》“获取账号ID和项目ID”章节。
name	String	账号名称。
domain	**BaseUser** object	标识触发事件的用户domain信息。

表 4-57 BaseUser

参数	参数类型	描述
id	String	账号ID，参见《云审计服务API参考》“获取账号ID和项目ID”章节。
name	String	账号名称。

表 4-58 MetaData

参数	参数类型	描述
count	Integer	标识本次查询事件列表返回的事件记录的总条数。
marker	String	标识本次查询事件列表返回的最后一个事件ID。可以使用这个参数返回值作为分页请求参数next的值，如果marker返回为null，则表示当前请求条件下查询事件列表已经全部返回没有下一页。

状态码： 400

表 4-59 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-60 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-61 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-62 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-63 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-64 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

- 查询管理类事件请求样例。
  ```
  GET https://{endpoint}/v3/{project_id}/traces?
  limit=11&to=1479095278000&from=1478490478000&trace_name=createTracker&resource_type=tracke
  r&service_type=CTS&trace_type=system
  ```
- 查询数据类事件请求样例。
  ```
  GET https://{endpoint}/v3/{project_id}/traces?
  limit=11&to=1479095278000&from=1478490478000&trace_type=data
  ```

响应示例

状态码： 200

请求正常。

```
{
  "meta_data" : {
    "count" : 2,
    "marker" : "e001ccb8-bc09-11e6-b2cc-2640a43cc6e8"
  },
  "traces" : [ {
    "time" : 1472148708232,
    "user" : {
      "name" : "xxx",
      "domain" : {
        "name" : "xxx",
        "id" : "ded649d814464428ba89d04d7955c93e"
      }
    },
    "response" : {
      "code" : "VPC.0514",
      "message" : "Update port fail."
    },
    "code" : 200,
    "service_type" : "VPC",
    "resource_type" : "eip",
    "resource_name" : "192.144.163.1",
    "resource_id" : "d502809d-0d1d-41ce-9690-784282142ccc",
    "trace_name" : "deleteEip",
    "trace_rating" : "warning",
    "trace_type" : "ConsoleAction",
    "api_version" : "2.0",
    "record_time" : 1481066128032,
    "trace_id" : "e001ccb9-bc09-11e6-b00b-4b2a61338db6"
  }, {
    "time" : 1472148708232,
    "user" : {
      "name" : "xxx",
      "domain" : {
        "name" : "xxx",
        "id" : "ded649d814464428ba89d04d7955c93e"
      }
    },
    "response" : {
      "code" : "VPC.0514",
      "message" : "Update port fail."
    },
    "code" : 200,
    "service_type" : "VPC",
    "resource_type" : "eip",
    "resource_name" : "192.144.163.1",
    "resource_id" : "d502809d-0d1d-41ce-9690-784282142ccc",
    "trace_name" : "deleteEip",
    "trace_rating" : "warning",
    "trace_type" : "ConsoleAction",
    "api_version" : "2.0",
```

```
    "record_time" : 1481066128032,
    "trace_id" : "e001ccb8-bc09-11e6-b2cc-2640a43cc6e8"
  } ]
}
```

状态码

状态码	描述
200	请求正常。
400	查询参数异常，请求未完成。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	查询事件不存在，请求未完成。
500	服务内部异常，请求未完成。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.3 追踪器管理

4.3.1 创建追踪器

功能介绍

云审计服务开通后系统会自动创建一个追踪器，用来关联系统记录的所有操作。目前，一个云账户在一个Region下支持创建一个管理类追踪器和多个数据类追踪器。云审计服务支持在管理控制台查询近7天内的操作记录。如需保存更长时间的操作记录，您可以在创建追踪器之后通过对象存储服务（Object Storage Service，以下简称OBS）将操作记录实时保存至OBS桶中。

URI

POST /v3/{project_id}/tracker

表 4-65 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

请求参数

表 4-66 请求 Body 参数

参数	是否必选	参数类型	描述
tracker_type	是	String	标识追踪器类型。 目前支持系统追踪器类型有管理类追踪器(system)和数据类追踪器(data)。 数据类追踪器和管理类追踪器共同参数有：is_lts_enabled, obs_info, is_support_validate; 管理类追踪器参数：is_support_trace_files_encryption, kms_id; 数据类追踪器参数：tracker_name, data_bucket。 枚举值： • **system** • **data**
tracker_name	是	String	标识追踪器名称。 当"tracker_type"参数值为"system"时该参数为默认值"system"。 当"tracker_type"参数值为"data"时该参数需要指定追踪器名称"。
is_lts_enabled	否	Boolean	是否打开事件分析。
obs_info	否	**TrackerObsInfo** object	转储桶配置
is_support_trace_files_encryption	否	Boolean	事件文件转储加密功能开关。 当"tracker_type"参数值为"system"时该参数值有效。 该参数必须与kms_id参数同时使用。
kms_id	否	String	事件文件转储加密所采用的秘钥id（从KMS获取）。 当"tracker_type"参数值为"system"时该参数值有效。 当"is_support_trace_files_encryption"参数值为“是”时，此参数为必选项。
is_support_validate	否	Boolean	事件文件转储时是否打开事件文件校验。
data_bucket	否	**DataBucket** object	追踪桶配置信息。 当"tracker_type"参数值为"data"时该参数值有效。

表 4-67 TrackerObsInfo

参数	是否必选	参数类型	描述
bucket_name	否	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。
file_prefix_name	否	String	标识需要存储于OBS的日志文件前缀，0-9，a-z，A-Z，'-'，'.'，'_'长度为0～64字符。
is_obs_created	否	Boolean	是否支持新建OBS桶。 值为“true”时，表示新创建OBS桶存储事件文件； 值为“false”时，选择已存在的OBS桶存储事件文件。
bucket_lifecycle	否	Integer	标识配置桶内对象存储周期。当"tracker_type"参数值为"data"时该参数值有效。 枚举值： • **30** • **60** • **90** • **180** • **1095**
compress_type	否	String	压缩类型。包括不压缩（json），压缩（gzip）两种状态。默认为gzip格式。 枚举值： • **gzip** • **json**
is_sort_by_service	否	Boolean	路径按云服务划分，打开后转储文件路径中将增加云服务名。默认为true。

表 4-68 DataBucket

参数	是否必选	参数类型	描述
data_bucket_name	否	String	数据类追踪器追踪对象的桶名。 ● 当启用或者停用数据类追踪器时，该参数为必选。 ● 管理类追踪器无此参数。 ● 追踪器一旦创建追踪桶无法修改。
data_event	否	Array of strings	数据类追踪器追踪的操作类型。 ● 当启用或者停用数据类追踪器时，该参数为必选。 ● 管理类追踪器无此参数。 ● READ OBS对象读取操作；WRITE OBS对象写操作。 枚举值： ● **WRITE** ● **READ**

响应参数

状态码： 201

表 4-69 响应 Body 参数

参数	参数类型	描述
id	String	追踪器唯一标识。
create_time	Long	追踪器创建时间戳。
kms_id	String	事件文件转储加密所采用的秘钥id（从KMS获取）。当"tracker_type"参数值为"system"和"is_support_trace_files_encryption"参数值为“是”时，此参数为必选项。
is_support_validate	Boolean	是否打开事件文件校验。
lts	**Lts** object	事件分析
tracker_type	String	标识追踪器类型。 目前支持系统追踪器类型有管理类追踪器（system）和数据类追踪器（data）。 枚举值： ● **system** ● **data**

参数	参数类型	描述
domain_id	String	账号ID，参见《云审计服务API参考》“获取账号ID和项目ID”章节。
project_id	String	项目ID。
tracker_name	String	标识追踪器名称，当前版本默认为“system”。
status	String	标识追踪器状态，包括正常（enabled），停止（disabled）和异常（error）三种状态，状态为异常时需通过明细（detail）字段说明错误来源。 枚举值： • **enabled** • **disabled**
detail	String	该参数仅在追踪器状态异常时返回，用于标识追踪器异常的原因，包括桶策略异常（bucketPolicyError），桶不存在（noBucket）和欠费或冻结（arrears）三种原因。
is_support_trace_files_encryption	Boolean	事件文件转储加密功能开关。 该参数必须与kms_id参数同时使用。 当前环境仅"tracker_type"参数值为"system"时支持该功能。
obs_info	**ObsInfo** object	事件转储桶信息。
data_bucket	**DataBucketQuery** object	数据类事件追踪桶信息。 当"tracker_type"参数值为"data"时有效。

表 4-70 Lts

参数	参数类型	描述
is_lts_enabled	Boolean	是否启用日志服务检索功能。
log_group_name	String	云审计服务在日志服务中创建的日志组名称。
log_topic_name	String	云审计服务在日志服务中创建的日志主题名称。

表 4-71 ObsInfo

参数	参数类型	描述
bucket_name	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。

参数	参数类型	描述
file_prefix_name	String	标识需要存储于OBS的日志文件前缀，0-9，a-z，A-Z，'-'，'.'，'_'长度为0～64字符。
is_obs_created	Boolean	标识配置桶是否由追踪器自动创建。
is_authorized_bucket	Boolean	标识配置桶是否已经授权给CTS服务账号。
bucket_lifecycle	Long	标识配置桶内对象存储周期。 当"tracker_type"参数值为"data"时该参数值有效。
compress_type	String	压缩类型。包括不压缩（json），压缩（gzip）两种状态。默认为gzip格式。 枚举值： ● **gzip** ● **json**
is_sort_by_service	Boolean	路径按云服务划分，打开后转储文件路径中将增加云服务名。默认为true。

表 4-72 DataBucketQuery

参数	参数类型	描述
data_bucket_name	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。
search_enabled	Boolean	追踪桶日志是否支持搜索。
data_event	Array of strings	数据类追踪器追踪对象的桶名。 ● 当启用或者停用数据类追踪器时，该参数为必选。 ● 管理类追踪器无此参数。 ● 追踪器一旦创建追踪桶无法修改。 ● READ OBS对象读取操作；WRITE OBS对象写操作。 枚举值： ● **WRITE** ● **READ**

状态码： 400

表 4-73 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-74 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-75 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-76 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-77 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-78 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

- 管理类追踪器创建样例。

```
POST https://{endpoint}/v3/{project_id}/tracker

{
  "tracker_type" : "system",
  "tracker_name" : "system",
  "obs_info" : {
    "is_obs_created" : false,
    "bucket_name" : "test-data-tracker",
    "file_prefix_name" : "11"
  },
  "is_lts_enabled" : true,
  "is_support_trace_files_encryption" : true,
  "kms_id" : "13a4207c-7abe-4b68-8510-16b84c3b5504",
  "is_support_validate" : true
}
```

- 数据类追踪器创建样例。

```
{
  "tracker_type" : "data",
  "tracker_name" : "data-tracker-name",
  "obs_info" : {
    "is_obs_created" : false,
    "bucket_name" : "saveTraceBucket",
    "file_prefix_name" : "11",
    "bucket_lifecycle" : 30
  },
  "is_lts_enabled" : true,
  "data_bucket" : {
    "data_event" : [ "READ", "WRITE" ],
    "data_bucket_name" : "cstest0423"
  }
}
```

响应示例

状态码： 201

请求成功。

```
{
  "id" : "2e6fa9b8-8c6e-456d-b5d3-77be972d220b",
  "create_time" : 1587958482923,
  "domain_id" : "aexxxxxxxx4d4fb4bexxxxxxx791fbf",
  "is_support_trace_files_encryption" : true,
  "kms_id" : "13a4207c-7abe-4b68-8510-16b84c3b5504",
  "obs_info" : {
    "is_obs_created" : false,
    "bucket_name" : "test-bucket",
    "is_authorized_bucket" : false,
    "file_prefix_name" : "11",
```

```
    "bucket_lifecycle" : 30
  },
  "project_id" : "bb1xxxxxxxxe4f498cbxxxxxxxx35634",
  "lts" : {
    "is_lts_enabled" : true,
    "log_group_name" : "CTS",
    "log_topic_name" : "system-trace"
  },
  "log_file_validate" : {
    "is_support_validate" : true
  },
  "tracker_name" : "system",
  "tracker_type" : "system",
  "status" : "enabled"
}
```

状态码

状态码	描述
201	请求成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	请求中的资源不存在，请求未完成。
500	服务内部异常，请求未完成。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.3.2 修改追踪器

功能介绍

云审计服务支持修改已创建追踪器的配置项，包括OBS桶转储、关键事件通知、事件转储加密、通过LTS对管理类事件进行检索、事件文件完整性校验以及追踪器启停状态等相关参数，修改追踪器对已有的操作记录没有影响。修改追踪器完成后，系统立即以新的规则开始记录操作。

URI

PUT /v3/{project_id}/tracker

表 4-79 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

请求参数

表 4-80 请求 Body 参数

参数	是否必选	参数类型	描述
tracker_type	是	String	标识追踪器类型。 目前支持系统追踪器类型有管理类追踪器(system)和数据类追踪器(data)。 数据类追踪器和管理类追踪器共同参数有：is_lts_enabled, obs_info, is_support_validate; 管理类追踪器参数：is_support_trace_files_encryption, kms_id; 数据类追踪器参数：tracker_name, data_bucket。 枚举值： • **system** • **data**
tracker_name	是	String	标识追踪器名称。 当"tracker_type"参数值为"system"时该参数为默认值"system"。 当"tracker_type"参数值为"data"时该参数需要指定追踪器名称"。
status	否	String	标识追踪器状态，该接口中可修改的状态包括正常（enabled）和停止（disabled）。如果选择修改状态为停止，则修改成功后追踪器停止记录事件。 枚举值： • **enabled** • **disabled**
is_lts_enabled	否	Boolean	是否打开事件分析。
obs_info	否	**TrackerObsInfo** object	转储桶配置

参数	是否必选	参数类型	描述
is_support_trace_files_encryption	否	Boolean	事件文件转储加密功能开关。 当"tracker_type"参数值为"system"时该参数值有效。 该参数必须与kms_id参数同时使用。
kms_id	否	String	事件文件转储加密所采用的秘钥id（从KMS获取）。 当"tracker_type"参数值为"system"时该参数值有效。 当"is_support_trace_files_encryption"参数值为“是”时，此参数为必选项。
is_support_validate	否	Boolean	事件文件转储时是否打开事件文件校验。
data_bucket	否	DataBucket object	追踪桶配置信息。 当"tracker_type"参数值为"data"时该参数值有效。

表 4-81 TrackerObsInfo

参数	是否必选	参数类型	描述
bucket_name	否	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。
file_prefix_name	否	String	标识需要存储于OBS的日志文件前缀，0-9，a-z，A-Z，'-'，'.'，'_'长度为0～64字符。
is_obs_created	否	Boolean	是否支持新建OBS桶。 值为“true”时，表示新创建OBS桶存储事件文件； 值为“false”时，选择已存在的OBS桶存储事件文件。

参数	是否必选	参数类型	描述
bucket_lifecycle	否	Integer	标识配置桶内对象存储周期。当"tracker_type"参数值为"data"时该参数值有效。 枚举值： • **30** • **60** • **90** • **180** • **1095**
compress_type	否	String	压缩类型。包括不压缩（json），压缩（gzip）两种状态。默认为gzip格式。 枚举值： • **gzip** • **json**
is_sort_by_service	否	Boolean	路径按云服务划分，打开后转储文件路径中将增加云服务名。默认为true。

表 4-82 DataBucket

参数	是否必选	参数类型	描述
data_bucket_name	否	String	数据类追踪器追踪对象的桶名。 • 当启用或者停用数据类追踪器时，该参数为必选。 • 管理类追踪器无此参数。 • 追踪器一旦创建追踪桶无法修改。
data_event	否	Array of strings	数据类追踪器追踪的操作类型。 • 当启用或者停用数据类追踪器时，该参数为必选。 • 管理类追踪器无此参数。 • READ OBS对象读取操作；WRITE OBS对象写操作。 枚举值： • **WRITE** • **READ**

响应参数

状态码： 400

表 4-83 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-84 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-85 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-86 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-87 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-88 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

- 管理类追踪器修改样例。

```
PUT https://{endpoint}/v3/{project_id}/tracker

{
  "tracker_type" : "system",
  "tracker_name" : "system",
  "obs_info" : {
    "is_obs_created" : false,
    "bucket_name" : "test-data-tracker",
    "file_prefix_name" : "11"
  },
  "is_lts_enabled" : false,
  "is_support_trace_files_encryption" : false,
  "kms_id" : "",
  "is_support_validate" : false,
  "status" : "enabled"
}
```

- 数据类追踪器修改样例。

```
{
  "tracker_type" : "data",
  "tracker_name" : "data-tracker-name",
  "obs_info" : {
    "is_obs_created" : false,
    "bucket_name" : "",
    "file_prefix_name" : "",
    "bucket_lifecycle" : 60
  },
  "is_lts_enabled" : true,
  "data_bucket" : {
    "data_event" : [ "READ", "WRITE" ]
  }
}
```

响应示例

无

状态码

状态码	描述
200	请求正常。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源。
500	服务内部异常，请求未完成。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.3.3 查询追踪器

功能介绍

开通云审计服务成功后，您可以在追踪器信息页面查看追踪器的详细信息。详细信息主要包括追踪器名称，用于存储操作事件的OBS桶名称和OBS桶中的事件文件前缀。

URI

GET /v3/{project_id}/trackers

表 4-89 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

表 4-90 Query 参数

参数	是否必选	参数类型	描述
tracker_name	否	String	标示追踪器名称。 在不传入该字段的情况下，将查询租户所有的追踪器。

参数	是否必选	参数类型	描述
tracker_type	否	String	标识追踪器类型。 目前支持系统追踪器有管理类追踪器（system）和数据类追踪器（data）。 枚举值： • **system** • **data**

请求参数

无

响应参数

状态码： 200

表 4-91 响应 Body 参数

参数	参数类型	描述
trackers	Array of **TrackerResponseBody** objects	本次查询追踪器列表返回的追踪器数组。

表 4-92 TrackerResponseBody

参数	参数类型	描述
id	String	追踪器唯一标识。
create_time	Long	追踪器创建时间戳。
kms_id	String	事件文件转储加密所采用的秘钥id（从KMS获取）。当"tracker_type"参数值为"system"和"is_support_trace_files_encryption"参数值为“是”时，此参数为必选项。
is_support_validate	Boolean	是否打开事件文件校验。
lts	**Lts** object	事件分析

参数	参数类型	描述
tracker_type	String	标识追踪器类型。 目前支持系统追踪器类型有管理类追踪器（system）和数据类追踪器（data）。 枚举值： • **system** • **data**
domain_id	String	账号ID，参见《云审计服务API参考》“获取账号ID和项目ID”章节。
project_id	String	项目ID。
tracker_name	String	标识追踪器名称，当前版本默认为“system”。
status	String	标识追踪器状态，包括正常（enabled），停止（disabled）和异常（error）三种状态，状态为异常时需通过明细（detail）字段说明错误来源。 枚举值： • **enabled** • **disabled**
detail	String	该参数仅在追踪器状态异常时返回，用于标识追踪器异常的原因，包括桶策略异常（bucketPolicyError），桶不存在（noBucket）和欠费或冻结（arrears）三种原因。
is_support_trace_files_encryption	Boolean	事件文件转储加密功能开关。 该参数必须与kms_id参数同时使用。 当前环境仅"tracker_type"参数值为"system"时支持该功能。
obs_info	**ObsInfo** object	事件转储桶信息。
data_bucket	**DataBucketQuery** object	数据类事件追踪桶信息。 当"tracker_type"参数值为"data"时有效。
group_id	String	LTS服务日志组的ID。
stream_id	String	LTS服务日志流的ID。

表 4-93 Lts

参数	参数类型	描述
is_lts_enabled	Boolean	是否启用日志服务检索功能。
log_group_name	String	云审计服务在日志服务中创建的日志组名称。

参数	参数类型	描述
log_topic_name	String	云审计服务在日志服务中创建的日志主题名称。

表 4-94 ObsInfo

参数	参数类型	描述
bucket_name	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。
file_prefix_name	String	标识需要存储于OBS的日志文件前缀，0-9，a-z，A-Z，'-'，'.'，'_'长度为0～64字符。
is_obs_created	Boolean	标识配置桶是否由追踪器自动创建。
is_authorized_bucket	Boolean	标识配置桶是否已经授权给CTS服务账号。
bucket_lifecycle	Long	标识配置桶内对象存储周期。 当"tracker_type"参数值为"data"时该参数值有效。
compress_type	String	压缩类型。包括不压缩（json），压缩（gzip）两种状态。默认为gzip格式。 枚举值： • **gzip** • **json**
is_sort_by_service	Boolean	路径按云服务划分，打开后转储文件路径中将增加云服务名。默认为true。

表 4-95 DataBucketQuery

参数	参数类型	描述
data_bucket_name	String	标识OBS桶名称。由数字或字母开头，支持小写字母、数字、“-”、“.”，长度为3～63个字符。
search_enabled	Boolean	追踪桶日志是否支持搜索。

参数	参数类型	描述
data_event	Array of strings	数据类追踪器追踪对象的桶名。 ● 当启用或者停用数据类追踪器时，该参数为必选。 ● 管理类追踪器无此参数。 ● 追踪器一旦创建追踪桶无法修改。 ● READ OBS对象读取操作；WRITE OBS对象写操作。 枚举值： ● **WRITE** ● **READ**

状态码： 400

表 4-96 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-97 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-98 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-99 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-100 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

```
GET https://{endpoint}/v3/{project_id}/trackers?tracker_name=system
```

响应示例

状态码： 200

请求成功。

```
{
  "trackers" : [ {
    "is_support_trace_files_encryption" : true,
    "create_time" : 1589886034121,
    "stream_id" : "4a1ef2b6-d79a-4dc6-90f0-48151cd5491b",
    "kms_id" : "7dbbb3fa-93e4-4528-bc7b-9beb794b0229",
    "group_id" : "26fa12ac-75f7-42ed-8118-ab9f2263042f",
    "is_support_validate" : false,
    "obs_info" : {
      "is_obs_created" : false,
      "bucket_name" : "",
      "is_authorized_bucket" : false,
      "file_prefix_name" : "",
      "bucket_lifecycle" : 0
    },
    "lts" : {
      "log_group_name" : "CTS",
      "is_lts_enabled" : true,
      "log_topic_name" : "system-trace"
    },
    "tracker_type" : "system",
    "domain_id" : "2306579dc99f4c8690b14b68e734fcd9",
    "project_id" : "24edf66e79d04187acb99a463e610764",
    "tracker_name" : "system",
    "id" : "ebf8d1c3-762b-4ce3-b316-6b1aa32f8be3",
    "status" : "enabled"
  }, {
    "domain_id" : "2306579dc99f4c8690b14b68e734fcd9",
    "is_support_trace_files_encryption" : false,
    "obs_info" : {
      "is_obs_created" : false,
```

```
    "bucket_name" : "",
    "is_authorized_bucket" : false,
    "file_prefix_name" : "",
    "bucket_lifecycle" : 0
   },
   "create_time" : 1589276171198,
   "project_id" : "24edf66e79d04187acb99a463e610764",
   "data_bucket" : {
    "data_event" : [ "READ", "WRITE" ],
    "search_enabled" : false,
    "data_bucket_name" : "cstest0423"
   },
   "tracker_name" : "sdsa",
   "is_support_validate" : false,
   "lts" : {
    "log_group_name" : "CTS",
    "is_lts_enabled" : false,
    "log_topic_name" : "sdsa"
   },
   "id" : "c9a3961d-3aa0-4e60-8e63-dd4ce7f1a88a",
   "status" : "enabled",
   "tracker_type" : "data"
  } ]
}
```


状态码

状态码	描述
200	请求成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
500	服务内部异常，请求未完成。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.3.4 删除追踪器

功能介绍

云审计服务目前仅支持删除已创建的数据类追踪器。删除追踪器对已有的操作记录没有影响，当您重新开通云审计服务后，依旧可以查看已有的操作记录。

URI

DELETE /v3/{project_id}/trackers

表 4-101 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

表 4-102 Query 参数

参数	是否必选	参数类型	描述
tracker_name	否	String	标识追踪器名称。 在不传入该字段的情况下，将删除当前租户所有的数据类追踪器。
tracker_type	否	String	标识追踪器类型。 目前仅支持数据类追踪器（data）的删除，默认值为"data"。 枚举值： • **data**

请求参数

无

响应参数

状态码： 400

表 4-103 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-104 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-105 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-106 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-107 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-108 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

```
DELETE https://{endpoint}/v3/{project_id}/trackers?tracker_name=data-tracker-name
```

响应示例

无

状态码

状态码	描述
204	删除成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	服务器无法找到被请求的资源或部分追踪器删除失败。
500	服务内部异常，请求未完成；或部分追踪器删除失败。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

4.4 其它接口

4.4.1 查询租户追踪器配额信息

功能介绍

查询租户追踪器配额信息。

URI

GET /v3/{project_id}/quotas

表 4-109 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方法请参见**获取项目ID**。

请求参数

无

响应参数

状态码： 200

表 4-110 响应 Body 参数

参数	参数类型	描述
resources	Array of **Quota** objects	本次查询追踪器列表返回的追踪器数组。

表 4-111 Quota

参数	参数类型	描述
type	String	quota资源类型。
used	Long	已使用的资源个数。
quota	Long	总资源个数。

状态码： 400

表 4-112 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 401

表 4-113 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 403

表 4-114 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 404

表 4-115 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 500

表 4-116 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

状态码： 503

表 4-117 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码标识，CTS.XXX。
error_msg	String	错误描述。

请求示例

```
GET https://{endpoint}/v3/{project_id}/quotas
```

响应示例

状态码： 200

请求成功。

```
{
  "resources" : [ {
    "type" : "data_tracker",
    "used" : 9,
    "quota" : 100
  }, {
    "type" : "system_tracker",
    "used" : 1,
    "quota" : 1
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	服务器未能处理请求。
401	请求鉴权校验失败，访问被拒绝。
403	请求权限校验失败，访问被禁止。
404	请求资源不存在，请求未完成。
500	服务内部异常，请求未完成。
503	被请求的服务无效。建议直接修改该请求，不要重试该请求。

错误码

请参见**错误码**。

5 权限和授权项

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

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对CTS进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

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

支持的授权项

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

- 权限：自定义策略中授权项定义的内容即为权限。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项

对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

说明

“√”表示支持，“x”表示暂不支持。

表 5-1 生命周期管理

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
查询事件列表	GET /v3/{project_id}/traces	cts:trace:list	-	√	x
查询事件列表	GET /v2.0/{project_id}/{tracker_name}/trace	cts:trace:list	-	√	x
查询事件列表	GET /v1.0/{project_id}/{tracker_name}/trace	cts:trace:list	-	√	x
查询追踪器	GET /v3/{project_id}/trackers	cts:tracker:list	obs:bucket:GetBucketAcl obs:bucket:ListAllMyBuckets	√	x
查询追踪器	GET /v1.0/{project_id}/tracker	cts:tracker:list	obs:bucket:GetBucketAcl obs:bucket:ListAllMyBuckets	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
创建追踪器	POST /v3/{project_id}/tracker	cts:tracker:create	lts:topics:list lts:topics:create lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAclkms:cmk:list	√	x
创建追踪器	POST /v1.0/{project_id}/tracker	cts:tracker:create	lts:topics:list lts:topics:create lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAclkms:cmk:list	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
修改追踪器	PUT /v3/{project_id}/tracker	cts:tracker:update	lts:topics:list lts:topics:create lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAcl kms:cmk:list	√	x
修改追踪器	PUT /v1.0/{project_id}/tracker/{tracker_name}	cts:tracker:update	lts:topics:list lts:topics:create lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAcl kms:cmk:list	√	x
删除追踪器	DELETE /v3/{project_id}/trackers	cts:tracker:delete	-	√	x

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
删除追踪器	DELETE /v1.0/{project_id}/tracker	cts:tracker:delete	-	√	x
查询租户追踪器配额信息	GET /v3/{project_id}/quotas	cts:quota:get	-	√	x
创建关键操作通知	POST /v3/{project_id}/notifications	cts:notification:create	smn:topic:list	√	x
修改关键操作通知	PUT /v3/{project_id}/notifications	cts:notification:update	smn:topic:list	√	x
删除关键操作通知	DELETE /v3/{project_id}/notifications	cts:notification:delete	-	√	x
查询关键操作通知	GET /v3/{project_id}/notifications/{notification_type}	cts:notification:list	-	√	x

6 附录

6.1 错误码

状态码	错误码	错误信息	描述	处理措施
400	CTS.0001	The IAM or OBS service is abnormal.	IAM或OBS服务异常	请联系技术支持
400	CTS.0003	The message body is empty or invalid.	body体为空或非法	请校验body内容和格式
400	CTS.0200	The number of trackers has reached the upper limit.	追踪器数量已满	请删除或修改不需要的追踪器
400	CTS.0201	A management tracker has been created.	已有管理类追踪器	请检查是否已生效
400	CTS.0202	The value of the tracker_type parameter is incorrect.	tracker_type字段不符合格式	请将对应值改为system或data

状态码	错误码	错误信息	描述	处理措施
400	CTS.0203	The value of tracker_name parameter is in an incorrect format.	tracker_name字段不符合格式	请参考参数描述进行修改
400	CTS.0204	The tracker_name parameter of a management tracker can only be set to system.	管理类追踪器tracker_name字段应为system	请参考参数描述进行修改
400	CTS.0205	The status parameter can only be set to enabled or disabled.	status字段只能为enabled或disabled	请将对应值改为enabled或disabled
400	CTS.0206	The data_bucket parameter cannot be included in the message body for a management tracker.	管理类追踪器body体不能有data_bucket参数	请去掉data_buket参数
400	CTS.0207	The tracker_name parameter in the message body cannot be set to system for a data tracker.	数据类追踪器body体tracker_name不能为system	请将tracker_name改为除system以外的值
400	CTS.0209	A type of operations on an OBS bucket can be tracked by only one tracker.	追踪一个桶的同一个操作类型	请更改追踪项

状态码	错误码	错误信息	描述	处理措施
400	CTS.0210	The OBS bucket to track cannot be empty.	追踪的桶不能为空	请换一个桶或使桶不为空
400	CTS.0211	The tracked OBS bucket does not exist.	被追踪的桶不存在	请检查bucket_name是否填写正确
400	CTS.0212	The tracked OBS bucket cannot be modified.	被追踪的obs桶不可修改	请撤回桶的更改
400	CTS.0213	The OBS bucket used for trace transfer cannot be a tracked OBS bucket.	被追踪的桶与转储的桶相同	请更换转储的桶
400	CTS.0215	The OBS bucket already exists.	桶已经存在	请修改bucket_name
400	CTS.0216	Failed to create a bucket.	创建桶失败	请联系技术支持
400	CTS.0217	Failed to set a lifecycle rule for the OBS bucket.	设置桶生命周期规则失败	请联系技术支持
400	CTS.0218	The value of file_prefix_name is in an incorrect format.	file_prefix_name字段不符合格式	请参考参数描述进行修改
400	CTS.0219	The operation type cannot be empty.	操作类型不能为空	请选择至少一个追踪操作
400	CTS.0220	KMS is not supported.	不支持KMS	请联系技术支持
400	CTS.0221	The KMS ID is empty.	KMS_ID为空	请检查kms_id是否正确

状态码	错误码	错误信息	描述	处理措施
400	CTS.0222	KMS verification failed.	KMS校验失败	请检查kms_id是否正确
400	CTS.0225	Only WRITE and/or READ operations on the OBS bucket can be tracked.	追踪桶操作类型必须为WRITE、READ或WRITE和READ。	检查参数是否传入正确。
400	CTS.0231	Invalid bucket name. A bucket name must be a string of 3 to 63 characters, including only lowercase letters, digits, hyphens (-), or periods (.). It must start with a digit or a lowercase letter.	无效的桶名称。bucket_name是3到63个字符的字符串，以数字或字母开头，支持小写字母，数字，“-”或“.”。	检查桶名称填写是否正确。
400	CTS.0300	Query failed.	query查询失败	请稍后重试或联系技术支持
403	CTS.0002	Authentication failed or you do not have the permissions required.	用户鉴权失败或没有权限	请检查用户权限
403	CTS.0208	The tracker already exists.	已存在该追踪器	请检查该追踪器是否已经存在
404	CTS.0100	API version query is not supported in CTS.	CTS不支持查询接口版本号	请联系技术支持
404	CTS.0214	The tracker does not exist.	追踪器不存在	请检查该追踪器是否已删除
500	CTS.0004	Failed to write data.	写入数据失败	请联系技术支持

状态码	错误码	错误信息	描述	处理措施
500	CTS.0005	Failed to read data.	读取数据失败	请联系技术支持

6.2 获取账号 ID 和项目 ID

从控制台获取账号 ID 和项目 ID

在调用接口的时候，部分URL中需要填入账号ID（ domain-id ）和项目ID，您可以通过控制台获取这些参数，步骤如下：

1. 注册并登录管理控制台。单击用户名，在下拉列表中单击“我的凭证”。
2. 在“我的凭证”页面查看账号ID和项目ID。

多项目时，展开“所属区域”，从“项目ID”列获取子项目ID。

调用 API 获取项目 ID

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180xxxx",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d1xxxx",
            "name": "xx-region-1",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f89xxxx"
            },
            "id": "a4a5d4098fb4474fa22cd0xxxx",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

A 修订记录

发布日期	修订记录
2024-04-30	第四次正式发布。
2023-10-30	第三次正式发布。
2023-07-11	第二次正式发布。 本次变更说明如下： ● 修改关键字 ● 补充获取AK/SK的操作步骤。
2023-01-30	第一次正式发布。