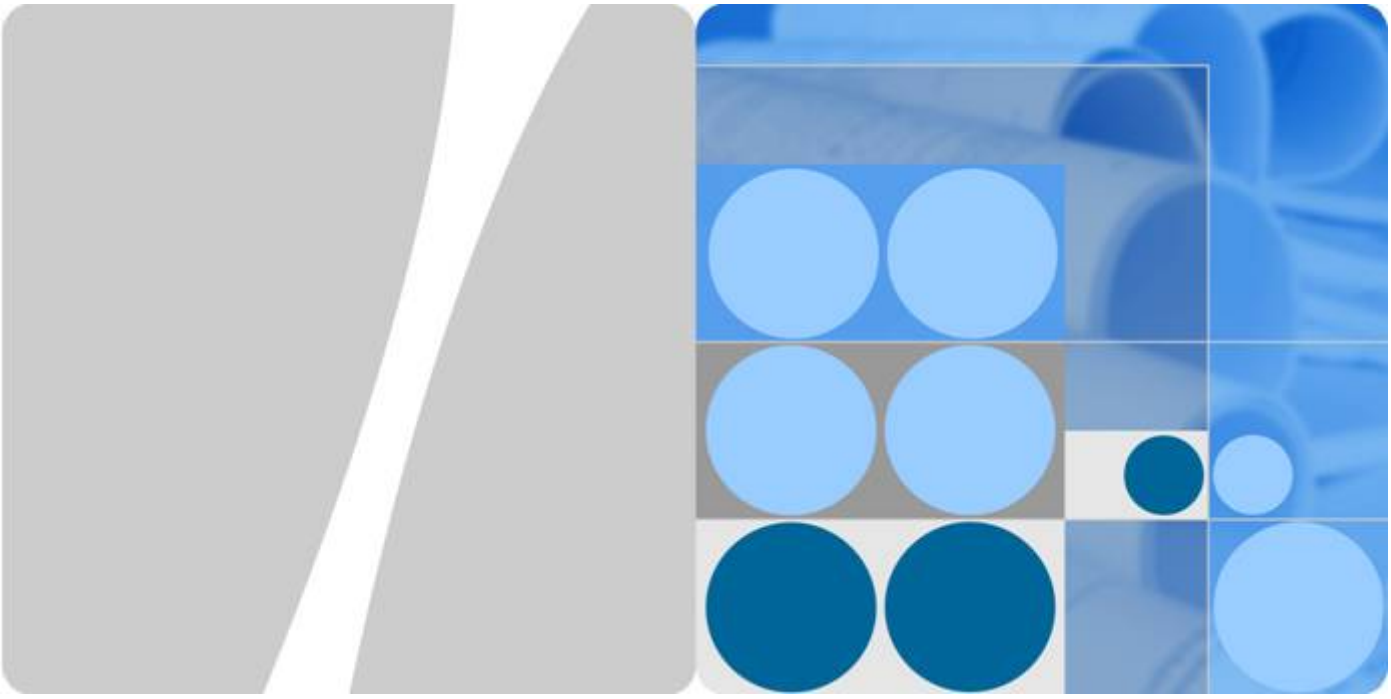

云审计服务

接口参考

文档版本　01

发布日期　2017-08-07

华为技术有限公司

商标声明


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

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 接口调用方法

1.1 服务使用方法

云服务API符合RESTful API的设计理论。

REST从资源的角度来观察整个网络，分布在各处的资源由URI（Uniform Resource Identifier）确定，而客户端的应用通过URL（Unified Resource Locator）来获取资源。

URL的一般格式为：https://***Endpoint*/*uri***

说明

URL中传递的参数对大小写敏感，请在调用时额外关注。

URL中的参数说明如表1-1所示。

表 1-1 URL 中的参数说明

参数	描述
Endpoint	Web服务入口点的URL，请向企业管理员获取。
uri	资源路径，也即API访问路径。从具体接口的URI模块获取，例如“v3/auth/tokens”。

1.2 请求方法

在HTTP协议中，请求可以使用多种请求方法例如GET、 PUT、 POST、 DELETE、 PATCH，用于指明以何种方式来访问指定的资源，目前提供的REST接口支持的请求方法如下表所示。

表 1-2 请求方法一览表

方法	说明
GET	请求服务器返回指定资源。
PUT	请求服务器更新指定资源。

方法	说明
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。
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。

1.3 请求认证方式

调用接口的方式如下：

Token认证：通过Token认证调用请求。

1.4 Token 认证

应用场景

当您使用Token认证方式完成认证鉴权时，需要获取用户Token并在调用接口时增加“X-Auth-Token”到业务接口请求消息头中。

本节介绍如何调用接口完成Token认证。

调用接口步骤

1. 发送“POST https://***IAM的Endpoint***/v3/auth/tokens”，获取IAM的Endpoint及消息体中的区域名称。

   请向企业管理员获取区域和终端节点信息。

   请求内容示例如下：

   说明

   下面示例代码中的斜体字需要替换为实际内容，详情请参考《CloudSOP *X.X* IAM服务 API参考》。

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "password",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "aaa" //假设区域名称是“aaa”

      }
```

```
    }
  }
}
```

2. 获取Token，请参考《CloudSOP *X.X* IAM服务 API参考》。
3. 调用业务接口，在请求消息头中增加“X-Auth-Token”，“X-Auth-Token”的取值为2中获取的Token。

1.5 获取项目编号

在调用接口的时候，部分URL中需要填入项目编号(project_id或者tenant_id，本文中project_id和tenant_id含义一样)，所以需要先在管理控制台上获取到项目编号。项目编号获取步骤如下：

1. 注册并登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的账号”。
   在“我的账号”页面的项目列表中查看项目ID。

图 1-1 查看项目 ID

2 公共消息头

2.1 公共请求消息头

表 2-1 公共请求消息头

名称	描述	是否必选	示例
Content-type	发送的实体的MIME类型。	是	application/json
Content-Length	请求body长度，单位为Byte。	POST/PUT请求必填。 GET不能包含。	3495
X-Project-Id	project id，用于不同project取token。	否	e9993fc787d94b6c886cbaa340f9c0f4
X-Auth-Token	用户Token。	否 使用Token认证时必选。	-

说明

其它header属性，请遵照http协议。

2.2 公共响应消息头

表 2-2 公共响应消息头

名称	描述
Content-Length	响应消息体的字节长度，单位为Byte。
Date	系统响应的时间。
Content-type	响应消息体的MIME类型。

3 追踪器管理

3.1 创建追踪器

功能介绍

使用云审计服务前需要开通服务，开通云审计服务系统会自动创建一个追踪器，系统记录的所有操作将关联在该追踪器中。目前，一个云账户在一个Region下仅支持创建一个追踪器。为了保存更长时间段的操作记录，需要将操作记录实时同步保存至对象存储服务（OBS）桶，所以使用云审计服务之前，您需要开通OBS服务并指定OBS桶。桶（Bucket）是OBS中存储对象的容器。

URI

- URI格式

  POST /v1.0/{project_id}/tracker

- 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	项目ID

请求

- 要素说明

名称	是否必选	参数类型	说明
bucket_name	是	String	标识OBS桶名称，来自于OBS服务真实存在的桶，桶名称包含数字、字母、'-'和'.'（非数字、字母类字符最多存在1个），长度为3～64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。

- 请求样例

```
{
  "bucket_name" : "defaultbucket",
  "file_prefix_name" : "mytracker1"
}
```

响应

- 要素说明

名称	参数类型	说明
bucket_name	String	标识OBS桶名称，来自于OBS服务真实存在的桶。
file_prefix_name	String	标识需要存储于OBS的日志文件前缀。
status	String	标识追踪器状态，该接口返回正常（enabled）状态。
tracker_name	String	标识追踪器名称，默认值为“system”。

- 响应样例

```
{
  "bucket_name" : "defaultbucket",
  "tracker_name" : "system",
  "file_prefix_name" : "mytracker1",
  "status" : "enabled"
}
```

返回值

- 正常

返回值	说明
201	请求成功。

- 异常

返回值	说明
400	服务器未能处理请求。
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。
401	请求鉴权校验失败，访问被拒绝。
404	请求中的OBS桶不存在，请求未完成。

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OBS桶，操作事件文件前缀以及追踪器的状态，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

- URI格式

  PUT /v1.0/{project_id}/tracker/{tracker_name}

- 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	项目ID
tracker_name	是	String	标识追踪器名称，目前单租户仅支持一个追踪器，默认为“system”。

请求

- 要素说明

名称	是否必选	参数类型	说明
bucket_name	是	String	标识OBS桶名称，来自于OBS服务真实存在的桶，桶名称包含数字、字母、'-'和'.'（非数字、字母类字符最多存在1个），长度为3～64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。
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。

- 请求样例

```
PUT /v1.0/{project_id}/tracker/system
{
  "bucket_name" : "my_created_bucket",
```

```
  "file_prefix_name" : "some_folder",
  "status" : "disabled"
}
```

响应

- 要素说明

名称	参数类型	说明
tracker_name	String	标识追踪器名称。默认为“system”。
bucket_name	String	标识OBS桶名称，来自于OBS服务真实存在的桶。
file_prefix_name	String	标识需要存储于OBS的日志文件前缀。
status	String	标识追踪器状态，该接口返回正常（enabled）和 停止（disabled）两种状态。

- 响应样例

```
{
  "bucket_name" : "my_created_bucket",
  "tracker_name" : "system",
  "file_prefix_name" : "some_folder",
  "status" : "disabled"
}
```

返回值

- 正常

返回值	说明
200	请求成功。

- 异常

返回值	说明
400	服务器未能处理请求。
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。
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。

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系统自动创建的追踪器的详细信息。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

- URI格式

  GET /v1.0/{project_id}/tracker{?tracker_name}

- 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	项目ID
tracker_name	否	String	标识追踪器名称。 在不传入该字段的情况下，将查询租户所有的追踪器。 目前单租户仅支持一个追踪器，名称默认为“system”。

说明

因CTS后期可能会支持多tracker，因此查询请求不包含tracker_name参数时（GET /v1.0/{project_id}/tracker），接口响应类型为数组格式，反之接口响应则为对象格式。

请求

- 要素说明

  无

- 请求样例

```
GET /v1.0/{project_id}/tracker?tracker_name=system
```

响应

- 要素说明

名称	参数类型	说明
tracker_name	String	标识追踪器名称，默认为“system”。

名称	参数类型	说明
bucket_name	String	标识OBS桶名称，来自于OBS服务真实存在的桶。
file_prefix_name	String	标识需要存储于OBS的日志文件前缀。
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。
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。

- 响应样例

```
{
  "bucket_name" : "my_created_bucket",
  "tracker_name" : "system",
  "detail" : "noBucket",
  "file_prefix_name" : "some_folder",
  "status" : "disabled"
}
```

返回值

- 正常

返回值	说明
200	请求成功，返回查询结果。

- 异常

返回值	说明
400	服务器未能处理请求。
500	服务内部异常，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。

3.4 删除追踪器

功能介绍

云审计服务管理控制台支持删除已创建的追踪器。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

- URI格式

  DELETE /v1.0/{project_id}/tracker{?tracker_name}

- 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	项目ID
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追踪器。 目前单租户仅支持一个追踪器，名称默认为“system”。

请求

- 要素说明

  无

- 请求样例

```
DELETE /v1.0/{project_id}/tracker?tracker_name=system
```

响应

- 要素说明

  无

- 响应样例

  无

返回值

- 正常

返回值	说明
204	删除成功

- 异常

返回值	说明
400	服务器未能处理请求。
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。
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。

4 事件管理

4.1 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天内的资源操作记录。

URI

- URI格式

  GET /v2.0/{project_id}/{tracker_name}/trace{?trace_id,service_type,resource_type,resource_id,resource_name,trace_name,trace_status,user,limit,from,to,next}

- 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	项目ID
tracker_name	是	String	追踪器名称，默认值为“system”。

请求

- 要素说明

名称	是否必选	参数类型	说明
service_type	否	String	标识查询事件列表对应的云服务类型。 **说明** 服务类型一般为大写字母。
resource_type	否	String	标识查询事件列表对应的资源类型。 **说明** 该字段可能包含大写字母。

名称	是否必选	参数类型	说明
resource_id	否	String	标识查询事件列表对应的云服务资源ID。
resource_name	否	String	标识查询事件列表对应的资源名称。 **说明** 该字段可能包含大写字母。
trace_name	否	String	标识查询事件列表对应的事件名称。 **说明** 该字段可能包含大写字母。
limit	否	String	标识查询事件列表中限定返回的事件条数。不传时默认50条，最大值200条。
next	否	String	标识查询事件列表截止于这个事件ID(不包括这个事件)。如果与from、to混合使用，当next对应时间小于to时，to不生效。
from	否	String	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）。查询条件from与to配套使用。
to	否	String	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）。查询条件to与from配套使用。
trace_id	否	String	标识某一条事件的事件ID。 当trace_id作为查询条件时具有排他性，不能再传入其他查询条件。
trace_status	否	String	标识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）。
user	否	String	标识特定用户，用以查询该用户下的所有事件。 **说明** 该字段可能包含大写字母。

- 请求样例

```
GET
/v2.0/{project_id}/{tracker_name}/trace?
limit=11&to=1479095278000&from=1478490478000&trace_name=createTracker&resource_type=tracker&service_type=CTS
```

响应

- 要素说明

名称	参数类型	说明
traces	traces	本次查询事件列表返回事件数组。

- traces字段数据结构说明

名称	参数类型	说明
resource_id	String	标识事件对应的云服务资源ID。
trace_name	String	标识事件名称。
trace_status	String	标识事件等级，目前有三种：正常（normal），警告（warning），事故（incident）。
trace_type	String	标识事件发生源头类型，主要包括API调用（ApiCall），Console页面调用（ConsoleAction）和系统间调用（SystemAction）。
request	Structure	标识事件对应接口请求内容，即资源操作请求体。
response	Structure	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。
meta_data	meta_data	标识为扩展字段，包括count（当前响应中事件记录的个数）和marker（本次查询返回事件列表最后一个事件ID）。
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	Structure	标识触发事件的租户信息。
service_type	String	标识事件对应的云服务英文缩写
resource_type	String	标识事件对应的资源类型
source_ip	String	标识触发事件的租户IP。

名称	参数类型	说明
resource_name	String	标识事件对应的资源名称。

- meta_data 字段数据结构说明

名称	参数类型	说明
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。

- 响应样例

```
{
  "traces" : [ {
    "time" : 1472148708232,
    "user" : {"name":"xxx","id":"a2e899190fcd444084a68fc0ac2sc1e9","domain":
{"name":"xxx","id":"05b2598d69bc4a209f9ac5eeeb1f91ad"}},
    "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_status " : "warning",
    "trace_type" : "ConsoleAction",
    "api_version" : "2.0",
    "record_time" : 1481066128032,
    "trace_id" : "e001ccb9-bc09-11e6-b00b-4b2a61338db6"
  }, {
    "time" : 1472148708232,
    "user" : {"name":"xxx","id":"a2e899190fcd444084a68fc0ac2sc1e9","domain":
{"name":"xxx","id":"05b2598d69bc4a209f9ac5eeeb1f91ad"}},
"request": {"servers":[{"id":"3045f042-9a7c-436d-a944-
ff76ceb7b477"}],"delete_volume":false,"delete_publicip":false},
    "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_status" : "warning",
    "trace_type" : "ConsoleAction",
    "api_version" : "2.0",
    "record_time" : 1481066128032,
    "trace_id" : "e001ccb8-bc09-11e6-b2cc-2640a43cc6e8"
  } ],
  "meta_data" : {
    "count" : 2,
    "marker" : "e001ccb8-bc09-11e6-b2cc-2640a43cc6e8"
  }
}
```

返回值

- 正常

返回值	说明
200	请求成功，返回查询结果。

- 异常

返回值	说明
400	查询参数异常，请求未完成。
500	服务内部异常，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。

A 附录

A.1 返回错误码说明

功能说明

所有云审计服务的接口，有自定义错误信息返回，本小节介绍云审计服务的错误码的含义。

返回体格式

{"details":{"details":"Message body or context format is not valid","code":"cts.0006"}}

错误码说明

错误码	说明
cts.0001	URL中API版本信息为空，请确认API版本信息是否填写。
cts.0002	URL中API版本信息非法，请核对API版本信息是否正确。
cts.0003	URL中project ID为空，请确认project ID是否填写。
cts.0004	URL中project ID非法，请核对project ID参数是否正确。
cts.0005	URL中查询条件非法，请核查传入参数是否正确：****参数不存在。
cts.0006	URL不存在，请核对URL是否符合要求。
cts.0007	消息体非法，具体提示存在5种： OBS桶名只能包含数字、字母、'-'和'.'，长度3～64字符。 追踪器前缀只能包含数字、字母、'-'、'_'和'.'，长度0~64字符。 追踪器状态只能是“enabled”或“disabled”。 消息体格式或内容错误。 消息体格式并非JSON格式。
cts.0008	读取数据异常，请联系运维人员。

错误码	说明
cts.0009	写入数据异常，请联系运维人员。
cts.0011	用户认证失败或没有权限进行该操作。
cts.0012	追踪器不存在，请确认追踪器名称是否正确。
cts.0013	该事件不存在，请核对事件ID是否正确。
cts.0015	服务内部错误，请联系运维人员。
cts.0016	缓存写入失败，请联系运维人员。
cts.0017	token不存在或不合法，请核对token信息是否正确。
cts.0018	当前环境不支持运维侧接口调用，请核对URL信息是否正确。
cts.0019	获取当前用户AK SK失败。
cts.0020	当前用户AK SK不合法。
cts.0021	当前用户OBS桶不存在，请确认OBS桶是否被删除。
cts.0022	校验OBS桶失败，请联系运维人员。
cts.0023	请求中的OBS桶不存在，请核实该OBS桶是否被删除。
cts.0024	云审计服务未获得当前用户OBS桶授权，请确认是否已经授权成功。
cts.0029	创建用户OBS桶策略失败，请联系运维人员。
cts.0030	删除用户OBS桶策略失败，请联系运维人员。
cts.0031	查询用户OBS桶列表失败，请联系运维人员。

B 修订记录

发布日期	修订记录
2017-06-26	第一次正式发布。