态势感知

API 参考

文档版本 07

发布日期 2022-12-28

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。

目 录

1 使用前必读

1.1 概述

欢迎使用态势感知（Situation Awareness，SA）。态势感知是一个可视化威胁检测和分析的平台，利用大数据分析技术，对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

您可以使用本文档提供的API对云上安全态势对进行相关操作，如上报产品数据、检查产品心跳健康等。支持的全部操作请参见**API概览**。

在调用态势感知API之前，请确保已经充分了解态势感知相关概念，详细信息请参见**产品介绍**。

1.2 调用说明

态势感知提供了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，您可以从**地区和终端节点**中查询服务的终端节点。

态势感知的终端节点如下表所示，请您根据业务需要选择对应区域的终端节点。

表 1-1 态势感知的终端节点

区域名称	区域	终端节点（Endpoint）	协议类型
All	All	sa.myhuaweicloud.com	HTTPS

1.4 基本概念

- 账号

  用户注册时的账号，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创建的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）。

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

- 区域（Region）

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

  详情请参见**区域和可用区**。

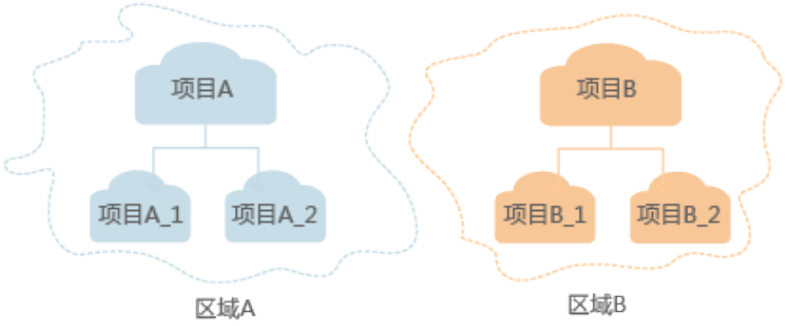
- 可用区（AZ，Availability Zone）

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

- 项目

  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**企业管理服务用户指南**。

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，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。

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}

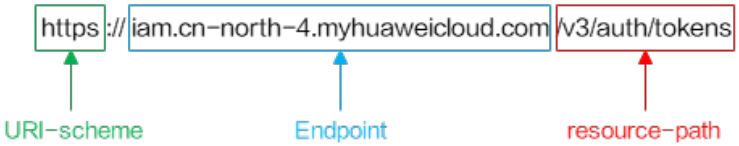
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **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**获取。
  例如IAM服务在“华北-北京四”区域的Endpoint为“iam.cn-north-4.myhuaweicloud.com”。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户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。

例如您需要获取IAM在“华北-北京四”区域的Token，则需使用“华北-北京四”区域的Endpoint（iam.cn-north-4.myhuaweicloud.com），并在**获取用户Token**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
```

图 2-1 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，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://iam.cn-north-4.myhuaweicloud.com/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。

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。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。

  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**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://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

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。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

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

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，***xxxxxxxxxxxxxxxxxx***为project的名称，如“cn-north-4”，您可以从**地区和终端节点**获取，对应地区和终端节点页面的“区域”字段的值。

说明

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

```
POST https://iam.cn-north-4.myhuaweicloud.com/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。

2.2 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。

```
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

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

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。详细的签名方法和SDK使用方法请参见**API签名指南**。

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。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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

对于**获取用户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2-2**所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 2-2 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": "xxxxxxxx",
......
```

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。

3 API 概览

通过使用态势感知提供的接口，您可以完整的使用态势感知的所有功能，包括产品事件接入、健康检查等接口。

类型	API	说明
事件管理	上报安全产品数据	接入安全产品事件的接口。
产品管理	检查心跳健康	检查安全产品接入健康的接口。

4 API

4.1 事件管理

4.1.1 上报安全产品数据

功能介绍

批量数据上报，每批次最多不超过50条。

此接口为继承态势感知 SA的接口。

调试

您可以在**API Explorer**中调试该接口，支持自动认证鉴权。API Explorer可以自动生成SDK代码示例，并提供SDK代码示例调试功能。

URI

POST /v2/{project_id}/events/import

表 4-1 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户项目ID。 最小长度：**32** 最大长度：**36**

请求参数

表 4-2 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
X-Language	否	String	语言。 最小长度：**2** 最大长度：**6**

表 4-3 请求 Body 参数

参数	是否必选	参数类型	描述
events	是	Array of **Event** objects	event 批量导入

表 4-4 Event

参数	是否必选	参数类型	描述
version	是	String	SA数据对象版本号，数据接入时需携带版本号。版本号由SA服务团队负责更新，数据源只可填写SA给定的版本号。目前版本为1.0.0。 最小长度：**5** 最大长度：**5**
environment	是	**Environment** object	环境坐标，DRP。
data_source	是	**DataSource** object	提供数据来源相关信息，必选对象。
first_observed_time	是	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

参数	是否必选	参数类型	描述
last_observed_time	否	String	最新发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
create_time	是	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
arrive_time	否	String	数据接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。 是指事件数据被SA侧接收的时间，由SA接收时填写，产品上报数据时不用填写。
event_id	是	String	事件唯一标识，UUID格式。 最小长度：**32** 最大长度：**36**
title	是	String	事件标题，最大255字符。 最小长度：**1** 最大长度：**255**
description	是	String	事件描述信息，最大1024个字符 最小长度：**1** 最大长度：**1024**
source_url	否	String	事件URL链接，指向数据源产品中有关当前事件说明的页面。 最小长度：**1** 最大长度：**4096**
count	是	Integer	事件发生次数，默认为1，必填。 最小值：**1** 最大值：**9223372036854775807**

参数	是否必选	参数类型	描述
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100%。 最小值：**0** 最大值：**100**
severity	是	**Severity** object	严重性对象。
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。 最小值：**0** 最大值：**100**
type	是	**Type** object	事件分类。
compliance	否	**Compliance** object	扩展信息，用来提供合规检查信息。合规检查相关的数据上报时，必须填充此对象。
network	否	**Network** object	扩展信息，用来提供网络信息。
vulnerability_patch	否	**Vulnerability Patch** object	扩展信息，用来提供漏洞信息。
malware	否	**Malware** object	恶意软件。
threat_intel	否	**ThreatIntel** object	威胁情报。
resource	是	**Resource** object	受影响资源。
remediation	否	**Remediation** object	补救措施。
data_source_fields	否	Object	数据源自定义信息，最多支持50个key/value对，约束条件：1、该对象不能包含冗余数据，并且不能与已定义的SSA事件格式字段冲突。 2、字段名称可以包含字母数字字符、空格和以下符号：_ . / = + \ - @。 示例："data_source_fields": { "key1": "value1", "key2", "value2", }

参数	是否必选	参数类型	描述
verification_state	否	String	事件验证状态，标识事件的准确性。 Unknown – 未知，默认 True_positive – 确认 False_positive – 误报。 最小长度：**1** 最大长度：**512**
handle_status	是	String	事件处理状态，New/Ignored/Resolved；默认New。 最小长度：**1** 最大长度：**512**
phase	否	String	阶段：Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity。 最小长度：**1** 最大长度：**32**
sla	否	Integer	约束闭环时间：单位：天。 最小值：**1** 最大值：**90**

表 4-5 Environment

参数	是否必选	参数类型	描述
type	是	String	环境供应商，HWCP/HWC/AWS/Azure/GCP等。 最小长度：**1** 最大长度：**36**
domain_id	是	String	租户账号ID，用来标识事件所属租户。 最小长度：**32** 最大长度：**36**
project_id	否	String	租户项目ID，用来标识事件所属项目区域。 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义。 最小长度：**1** 最大长度：**512**

表 4-6 DataSource

参数	是否必选	参数类型	描述
type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3**
domain_id	否	String	数据源产品所属管理账号的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
project_id	否	String	数据源产品所属项目的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义。 最小长度：**1** 最大长度：**512**
company_name	是	String	数据源产品所属公司的名称。 最小长度：**1** 最大长度：**512**
product_name	是	String	数据源产品的名称。 最小长度：**1** 最大长度：**512**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性。 最小长度：**1** 最大长度：**512**

表 4-7 Severity

参数	是否必选	参数类型	描述
label	是	String	严重性等级取值范围：TIPS、LOW、MEDIUM、HIGH、FATAL。 TIPS：未发现任何问题。 LOW：无需针对问题执行任何操作。 MEDIUM：问题需要处理，但不紧急。 HIGH：问题必须优先处理。 FATAL：问题必须立即处理，以防止产生进一步的损害。 最小长度：**1** 最大长度：**512**
normalize_score	否	Integer	严重性评分取值范围：0-100；与严重性等级的对应关系：TIPS 0； LOW 1-39； MEDIUM 40-69； HIGH 70-89； FATAL 90-100。 最小值：**0** 最大值：**100**
original_score	否	Integer	严重性原始评分，指在数据源产品中的评分。 最小值：**0** 最大值：**9223372036854775807**

表 4-8 Type

参数	是否必选	参数类型	描述
business	是	String	事件所属业务领域标签，可选类别如下： attack – 攻击 vulnerability – 漏洞 compliance check – 合规检查 risk - 风险 public opinion - 舆情 illegal&violation - 违法违规 security bulletin - 公告 最小长度：**1** 最大长度：**512**
category	否	String	类别，推荐使用预定义的类型分类。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
classifier	否	String	分类器，推荐使用预定义的分类器。 如果指定了分类器，则必须指定类别。 最小长度：**1** 最大长度：**512**
tech_domain	否	String	技术领域标签： OS：主机 APP：应用 NET：网络 OPS：运维 CS：云服务 CSP：平台云服务 最小长度：**1** 最大长度：**512**
properties	否	**TypeProperties** object	属性信息。

表 4-9 TypeProperties

参数	是否必选	参数类型	描述
killchain	否	String	Kill chain事件分类，仅当business为attack有效 最小长度：**1** 最大长度：**512**
ttps	否	String	Mitre Array 事件分类，仅当business为attack有效 最小长度：**1** 最大长度：**512**
effects	否	String	影响，适用全部类型 最小长度：**1** 最大长度：**512**

表 4-10 Compliance

参数	是否必选	参数类型	描述
checkitem_id	是	String	检查项（检查规则）编号 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
checkpoint_id	是	String	检查点（检查结果）编号，检查项对同一个资源的检查结果 最小长度：**1** 最大长度：**512**
spec_id	是	String	检查规范编号，默认选第一个 最小长度：**1** 最大长度：**512**
status	是	String	合规检查结果，取值定义：PASSED、WARNING、FAILED、NOT_AVAILABLE。 说明： PASSED - 接受评估的所有资源都已通过安全检查。 WARNING - 某些信息缺失或配置不支持此检查。 FAILED - 至少有一个接受评估的资源未能通过安全检查。 NOT_AVAILABLE - 由于服务中断或 API 错误，无法执行检查。 最小长度：**1** 最大长度：**512**
properties	否	String	属性信息 最小长度：**1** 最大长度：**512**

表 4-11 Network

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN、OUT。 最小长度：**2** 最大长度：**3**
protocol	否	String	协议。 最小长度：**0** 最大长度：**512**
src_ip	否	String	源IP地址。 最小长度：**7** 最大长度：**15**
src_port	否	Integer	源端口，0–65535。 最小值：**0** 最大值：**65535**

参数	是否必选	参数类型	描述
src_domain	否	String	源域名，最大128个字符。 最小长度：**1** 最大长度：**128**
src_geo	否	**Geo** object	源IP的地理位置信息。
dest_ip	否	String	目标IP地址。 最小长度：**7** 最大长度：**15**
dest_port	否	Integer	目标端口，0–65535。 最小值：**0** 最大值：**65535**
dest_domain	否	String	目标域名，最大128个字符。 最小长度：**1** 最大长度：**128**
dest_geo	否	**Geo** object	目标IP的地理位置信息。

表 4-12 Geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度。 最小值：**-90.0** 最大值：**90.0**
longitude	否	Number	经度。 最小值：**-180.0** 最大值：**180.0**
city_code	否	String	城市编码。 最小长度：**1** 最大长度：**128**
country_code	否	String	国家简码ISO 3166-1 alpha-2，例如：CN、US、DE、IT、SG。 最小长度：**1** 最大长度：**128**

表 4-13 VulnerabilityPatch

参数	是否必选	参数类型	描述
patch_id	是	String	补丁编号。 最小长度：**1** 最大长度：**256**
patch_name	否	String	补丁名称。 最小长度：**1** 最大长度：**256**
type	否	String	补丁类型（0：linux，1：windows，2：web-cms）。 最小长度：**1** 最大长度：**32**
major_level	否	String	重要等级。 最小长度：**1** 最大长度：**32**
status	否	String	补丁状态。 最小长度：**1** 最大长度：**32**
repair_cmd	否	String	修复命令。 最小长度：**0** 最大长度：**512**
repair_necessity	否	String	修复必要程度（1：需立刻修复，2：可延后修复，3：暂可以不修复）。 最小长度：**0** 最大长度：**512**
release_time	否	String	发布时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息 为事件发生时区，无法解析时区的时间，默认时区填东八区。
reference_url	否	String	参考链接。 最小长度：**0** 最大长度：**512**
vendor_name	否	String	漏洞报告提供者信息。 最小长度：**1** 最大长度：**32**

参数	是否必选	参数类型	描述
vulnerable_package	否	String	受影响软件版本。 最小长度：**1** 最大长度：**32**
cve_ids	否	String	CVE编号列表。 最小长度：**1** 最大长度：**256**

表 4-14 Malware

参数	是否必选	参数类型	描述
name	是	String	恶意软件名称，最大64个字符。 最小长度：**1** 最大长度：**64**
sha256	否	String	恶意软件sha256 最小长度：**1** 最大长度：**1024**
type	是	String	恶意软件类型，遵循STIX规范：adware、backdoor、bot、bootkit、ddos、downloader、dropper、exploit-kit、keylogger、ransomware、remote-access-trojan、resource-exploitation、rogue-security-software、rootkit、screen-capture、spyware、trojan、unknown、virus、webshell、wiper、worm 最小长度：**1** 最大长度：**512**
path	否	String	恶意软件在系统中的路径，最大512个字符。 最小长度：**0** 最大长度：**512**
state	否	String	恶意软件状态，取值范围：OBSERVED、REMOVAL_FAILED、REMOVED。 最小长度：**0** 最大长度：**512**

参数	是否必选	参数类型	描述
properties	否	**MalwareProperties** object	属性信息。

表 4-15 MalwareProperties

参数	是否必选	参数类型	描述
pid	否	String	进程ID。 最小长度：**1** 最大长度：**64**
user	否	String	系统角色（例如:root，service）。 最小长度：**1** 最大长度：**64**
mod	否	String	系统权限（例如：777，755）。 最小长度：**1** 最大长度：**64**
start_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。

表 4-16 ThreatIntel

参数	是否必选	参数类型	描述
id	是	String	情报Id。 最小长度：**0** 最大长度：**32**
indicator_type	否	String	威胁情报类型，Domain、Email_Address、Hash_MD5、Hash_SHA1、Hash_SHA256、Hash_SHA512、IPv4_Address、IPv6_Address、URL。 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
labels	否	String	标签，如'矿池','外联'等，"Directory Scan|Directory Traversal"。 最小长度：**0** 最大长度：**512**
confidence	否	Integer	置信度，不同来源目前置信度分值定义不一样（分数）。 最小值：**0** 最大值：**9223372036854775807**
information_source	是	String	威胁情报源，最大64个字符。 最小长度：**0** 最大长度：**64**
severity	否	Integer	严重程度，不同渠道定义值不一样（分数）。 最小值：**0** 最大值：**9223372036854775807**
description	是	String	威胁情报描述。 最小长度：**0** 最大长度：**4096**
modified	否	String	威胁情报的更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
valid_from	否	String	有效期开始（可读字符串）。 最小长度：**0** 最大长度：**32**
valid_until	否	String	有效期结束（可读字符串）。 最小长度：**0** 最大长度：**32**
properties	否	**ThreatIntelProperties** object	威胁情报属性信息。

表 4-17 ThreatIntelProperties

参数	是否必选	参数类型	描述
file_md5	否	String	恶意软件Md5。 最小长度：**1** 最大长度：**64**
file_sha1	否	String	恶意软件Sha1。 最小长度：**1** 最大长度：**255**
file_sha256	否	String	恶意软件Sha256值。 最小长度：**1** 最大长度：**255**
file_name	否	String	文件名称。 最小长度：**1** 最大长度：**255**
create_time	否	String	编译时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
file_class	否	String	文件类别，TEXT|XCODE。 最小长度：**1** 最大长度：**255**
file_family	否	String	家族，例如：wannacry（勒索软件）。 最小长度：**1** 最大长度：**255**
file_maltype	否	String	类别，例如：trojan（特洛伊）。 最小长度：**1** 最大长度：**255**
ip_resolves_to_refs	否	String	mac地址。 最小长度：**1** 最大长度：**255**
belongs_to_refs	否	String	IP AS 自治系统。 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
ip_location	否	String	地区 格式：country/provice/city/lngwgs/latwgs。 最小长度：**1** 最大长度：**255**
domain_family	否	String	例如：banjori|iodine。 最小长度：**1** 最大长度：**255**
domain_resolves_to_refs	否	String	解析的IP地址。 最小长度：**1** 最大长度：**255**
domain_dns_type	否	String	DNS类别。A|NS|CNAME|TXT。 最小长度：**1** 最大长度：**255**
url_host	否	String	例：3ms.huawei.com。 最小长度：**1** 最大长度：**255**
url_resolves_to_refs	否	String	IP地址。 最小长度：**1** 最大长度：**255**
display_name	否	String	显示名称。 最小长度：**1** 最大长度：**128**
url_belongs_to_ref	否	String	邮箱账户，@之前部分。 最小长度：**1** 最大长度：**128**

表 4-18 Resource

参数	是否必选	参数类型	描述
id	是	String	资源ID。 最小长度：**32** 最大长度：**36**
name	是	String	资源名称；最大长度255个字符。 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
type	是	String	资源类型。 最小长度：**1** 最大长度：**128**
provider	是	String	云服务名称。 最小长度：**1** 最大长度：**128**
region_id	否	String	区域。 最小长度：**1** 最大长度：**128**
domain_id	是	String	资源所属租户账号ID。 最小长度：**32** 最大长度：**36**
project_id	否	String	资源所属项目ID。 最小长度：**32** 最大长度：**36**
ep_id	否	String	企业项目ID。 最小长度：**32** 最大长度：**36**
ep_name	否	String	企业项目名称。 最小长度：**32** 最大长度：**36**
tags	否	Object	资源标签 1、最多50个key/values对。 2、values：最大255字符。 3、取值范围：字母数字、空格、“+”、“-”、“=”、“.”、“_”、“:”、“/”、“@”。

表 4-19 Remediation

参数	是否必选	参数类型	描述
recommendation	是	String	处理建议，最长512个字符。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证。 最小长度：**1** 最大长度：**128**

响应参数

状态码： 400

表 4-20 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效请求提示信息 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 401

表 4-21 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 500

表 4-22 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

请求示例

```
POST https://{endpoint}/v2/{project_id}/events/import

{
  "events" : [ {
    "version" : "1.1.0",
    "environment" : {
      "type" : "xxx",
      "domain_id" : "dfaf9864b95c448797b5dc0f0xxxxxxx",
      "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
      "region_id" : "xx-xx-1"
    },
    "data_source" : {
      "type" : 1,
      "domain_id" : "dfaf9864b95c448797b5dc0f0xxxxxxx",
      "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
      "region_id" : "xx-xx-1",
      "company_name" : "xxx",
      "product_name" : "xxx",
      "product_feature" : "xxx"
    },
    "first_observed_time" : "2020-10-10T13:10:40.436+0800",
    "last_observed_time" : "2020-10-10T13:10:40.436+0800",
    "create_time" : "2020-10-10T13:10:40.436+0800",
    "arrive_time" : "2020-10-21T01:20:31.343+0800",
    "event_id" : "1683fbf6-01fd-49f4-8222-0fe33d3f2d2e",
    "title" : "TCP Malformed",
    "description" : "TCP Malformed",
    "count" : 1,
    "severity" : {
      "original_score" : 1,
      "label" : "TIPS"
    },
    "type" : [ {
      "business" : "attack",
      "category" : "Brute Force",
      "classifier" : "ssh"
    } ],
    "network" : {
      "direction" : "IN",
      "dest_ip" : "xxx.xxx.xxx.xxx",
      "dest_port" : 80,
      "dest_geo" : {
        "latitude" : 1.352083,
        "longitude" : 103.81984
      }
    },
    "resource" : [ {
      "id" : "f1f4076a-9d12-497f-aac4-a9dcb5462fcc",
      "name" : "ecs-s3_large_2_win-20200828214727",
```

```
    "type" : "cloudservers",
    "provider" : "ecs",
    "region_id" : "xx-xx-1",
    "domain_id" : "dfaf9864b95c448797b5dc0f00709a55",
    "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
    "ep_id" : "7e998f85-xxxx-xxxx-xxxx-xxxxxxxx",
    "ep_name" : "test001"
   } ],
   "verification_state" : "Unknown",
   "handle_status" : "New"
 } ]
}
```

响应示例

无

状态码

状态码	描述
201	Succeeded
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

错误码

请参见**错误码**。

4.2 产品管理

4.2.1 检查心跳健康

功能介绍

SA提供心跳接口，集成产品定时（每五分钟）发送心跳报文到态势感知，用来确认集成产品与态势感知之间的通路是否健康。

此接口为继承态势感知 SA的接口。

调试

您可以在**API Explorer**中调试该接口，支持自动认证鉴权。API Explorer可以自动生成SDK代码示例，并提供SDK代码示例调试功能。

URI

POST /v1/{project_id}/products/health-check

表 4-23 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户项目ID。 最小长度：**32** 最大长度：**36**

请求参数

表 4-24 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
X-Language	否	String	语言 最小长度：**2** 最大长度：**6**

表 4-25 请求 Body 参数

参数	是否必选	参数类型	描述
domain_id	是	String	数据源产品所属账号的ID。 最小长度：**32** 最大长度：**36**
project_id	是	String	数据源产品所属项目的ID。 最小长度：**32** 最大长度：**36**
region	是	String	数据源产品所在区域。 最小长度：**1** 最大长度：**512**
company_name	是	String	数据源产品所属公司的名称。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
product_name	是	String	数据源产品的名称。 最小长度：**1** 最大长度：**512**

响应参数

状态码： 400

表 4-26 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效数据的描述信息。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 401

表 4-27 响应 Body 参数

参数	参数类型	描述
error_msg	String	token认证错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 403

表 4-28 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 500

表 4-29 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

请求示例

```
POST https://{endpoint}/v1/{project_id}/products/health-check

{
  domain_id: "dfaf9864b95c448797b5dc0f0xxxxxxx",
  project_id: "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  region: "xx-xx-1",
  company_name: "xxx",
  product_name: "xxx"
}
```

响应示例

无

状态码

状态码	描述
201	Succeeded
400	Bad Request

状态码	描述
401	Unauthorized
403	Forbidden
500	Internal Server Error

错误码

请参见**错误码**。

5 历史 API

5.1 上报安全产品数据(V1)

功能介绍

批量数据上报，每批次最多不超过50条。

URI

POST /v1/{project_id}/events/import

表 5-1 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户项目ID。 最小长度：**32** 最大长度：**36**

请求参数

表 5-2 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**

参数	是否必选	参数类型	描述
X-Language	否	String	最小长度：**2** 最大长度：**6**

表 5-3 请求 Body 参数

参数	是否必选	参数类型	描述
events	否	Array of **Event** objects	event 批量导入

表 5-4 Event

参数	是否必选	参数类型	描述
version	是	String	SA数据对象版本号，数据接入时需携带版本号。版本号由SA服务团队负责更新，数据源只可填写SA给定的版本号。目前版本为1.0.0。 最小长度：**5** 最大长度：**5**
domain_id	是	String	租户账号ID，用来标识事件所属租户。 最小长度：**32** 最大长度：**36**
project_id	否	String	租户项目ID，用来标识事件所属项目区域。 最小长度：**32** 最大长度：**36**
data_source	是	**DataSource** object	提供数据来源相关信息，必选对象。
first_observed_time	是	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
last_observed_time	否	String	最新发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

参数	是否必选	参数类型	描述
create_time	是	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
arrive_time	是	String	数据接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。 是指事件数据被SA侧接收的时间，由SA接收时填写，产品上报数据时不用填写。
event_id	是	String	事件唯一标识，UUID格式。 最小长度：**32** 最大长度：**36**
title	是	String	事件标题，最大255字符。 最小长度：**1** 最大长度：**255**
description	是	String	事件描述信息，最大1024个字符 最小长度：**1** 最大长度：**1024**
source_url	否	String	事件URL链接，指向数据源产品中有关当前事件说明的页面。 最小长度：**1** 最大长度：**4096**
count	是	Integer	事件发生次数，默认为1，必填。 最小值：**1** 最大值：**9223372036854775807**
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100%。 最小值：**0** 最大值：**100**
severity	是	**Severity** object	严重性对象。

参数	是否必选	参数类型	描述
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。 最小值：**0** 最大值：**100**
business_code	是	String	业务类型。 attack：攻击；vulnerability：漏洞；compliance check：合规检查；risk：风险；public opinion：舆情；illegal&violation：违法违规；security bulletin：公告。 最小长度：**1** 最大长度：**1024**
types	是	Array of **Type** objects	事件分类，最多50个。
compliance	否	**Compliance** object	扩展信息，用来提供合规检查信息。合规检查相关的数据上报时，必须填充此对象。
network	否	**Network** object	扩展信息，用来提供网络信息。
process	否	**Process** object	扩展信息，用来提供进程信息。
vulnerabilities	否	**Vulnerabilities** object	扩展信息，用来提供漏洞信息。
malware	否	Array of **Malware** objects	恶意软件，最多5个。
threat_intel	否	Array of **ThreatIntel** objects	威胁情报，最多5个。
resources	是	Array of **Resource** objects	受影响资源，最多10个。
remediation	否	**remediation** object	补救措施。
related_events	否	Array of **RelatedEvent** objects	相关事件。

参数	是否必选	参数类型	描述
data_source_fields	否	Object	数据源自定义信息，最多支持50个key/value对，约束条件：1、该对象不能包含冗余数据，并且不能与已定义的SSA事件格式字段冲突。 2、字段名称可以包含字母数字字符、空格和以下符号：_ . / = + \ - @。 示例："data_source_fields": { "key1": "value1", "key2", "value2", }
verification_state	是	String	事件验证状态，标识事件的准确性。 Unknown – 未知，默认 True_positive – 确认 False_positive – 误报。 最小长度：**1** 最大长度：**512**
handle_status	是	String	事件处理状态，New/Ignored/Resolved；默认New。 最小长度：**1** 最大长度：**512**

表 5-5 DataSource

参数	是否必选	参数类型	描述
type	是	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3**
domain_id	是	String	数据源产品所属管理账号的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
project_id	否	String	数据源产品所属项目的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
region	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
company_name	是	String	数据源产品所属公司的名称。 最小长度：**1** 最大长度：**512**
product_name	是	String	数据源产品的名称。 最小长度：**1** 最大长度：**512**
product_feature	是	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性。 最小长度：**1** 最大长度：**512**

表 5-6 Severity

参数	是否必选	参数类型	描述
label	是	String	严重性等级取值范围：TIPS、LOW、MEDIUM、HIGH、FATAL。 TIPS：未发现任何问题。 LOW：无需针对问题执行任何操作。 MEDIUM：问题需要处理，但不紧急。 HIGH：问题必须优先处理。 FATAL：问题必须立即处理，以防止产生进一步的损害。 最小长度：**1** 最大长度：**512**
normalize_score	否	Integer	严重性评分取值范围：0-100；与严重性等级的对应关系：TIPS 0； LOW 1-39； MEDIUM 40-69； HIGH 70-89； FATAL 90-100。 最小值：**0** 最大值：**100**
original_score	否	Integer	严重性原始评分，指在数据源产品中的评分。 最小值：**0** 最大值：**9223372036854775807**

表 5-7 Type

参数	是否必选	参数类型	描述
namespace	是	String	命名空间，只能使用预定义的命名空间值，有效取值如下：Compliance Checks、Vulnerabilities、Attack、Illegal and Violation、Risk、Public Opinion、TTPs、Killchain、Effects、Sensitive Data Identifications、Unusual Behaviors 最小长度：**1** 最大长度：**512**
category	否	String	类别，推荐使用预定义的类型分类。 最小长度：**1** 最大长度：**512**
classifier	否	String	分类器，推荐使用预定义的分类器。 如果指定了分类器，则必须指定类别。 最小长度：**1** 最大长度：**512**

表 5-8 Compliance

参数	是否必选	参数类型	描述
status	是	String	合规检查结果，取值定义：PASSED、WARNING、FAILED、NOT_AVAILABLE。 说明： PASSED - 接受评估的所有资源都已通过安全检查。 WARNING - 某些信息缺失或配置不支持此检查。 FAILED - 至少有一个接受评估的资源未能通过安全检查。 NOT_AVAILABLE - 由于服务中断或 API 错误，无法执行检查。 最小长度：**1** 最大长度：**512**
related_requirements	是	Array of strings	与该合规检查相关的行业或监管要求，最多可以提供32个相关的要求。用规范要求的识别码来标识。

参数	是否必选	参数类型	描述
status_reasons	否	Array of strings	与该合规检查相关的原因。

表 5-9 Network

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN、OUT。 最小长度：**2** 最大长度：**3**
protocol	否	String	协议。 最小长度：**0** 最大长度：**512**
src_ip	否	String	源IP地址。 最小长度：**7** 最大长度：**15**
src_port	否	Integer	源端口，0–65535。 最小值：**0** 最大值：**65535**
src_domain	否	String	源域名，最大128个字符。 最小长度：**1** 最大长度：**128**
src_geo	否	**Geo** object	源IP的地理位置信息。
destc_ip	否	String	目标IP地址。 最小长度：**7** 最大长度：**15**
dest_port	否	Integer	目标端口，0–65535。 最小值：**0** 最大值：**65535**
dest_domain	否	String	目标域名，最大128个字符。 最小长度：**1** 最大长度：**128**
dest_geo	否	**Geo** object	目标IP的地理位置信息。

表 5-10 Geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度。 最小值：**-180.0** 最大值：**180.0**
longitude	否	Number	经度。 最小值：**-180.0** 最大值：**180.0**
city_code	否	String	城市编码。 最小长度：**1** 最大长度：**128**
country_code	否	String	国家简码ISO 3166-1 alpha-2，例如：CN、US、DE、IT、SG。 最小长度：**1** 最大长度：**128**

表 5-11 Process

参数	是否必选	参数类型	描述
name	是	String	进程名，最大64个字符。 最小长度：**1** 最大长度：**64**
path	是	String	进程执行文件路径，最大512个字符。 最小长度：**1** 最大长度：**512**
pid	是	Integer	进程ID。 最小值：**0** 最大值：**65535**
parent_pid	否	Integer	父进程ID。 最小值：**0** 最大值：**65535**
launche_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

参数	是否必选	参数类型	描述
terminate_time	否	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

表 5-12 Vulnerabilities

参数	是否必选	参数类型	描述
vulnerability_list	否	Array of **Vulnerability** objects	漏洞信息。
patch_list	否	Array of **Patch** objects	补丁信息。
reference_urls	否	Array of strings	参考链接，提供有关此漏洞更多信息的URL列表。
related_vulnerabilities	否	Array of strings	相关漏洞，提供与此漏洞相关的漏洞ID列表。
vendor_name	否	String	漏洞报告提供者信息。 最小长度：**1** 最大长度：**32**
vulnerable_packages	否	Array of strings	受影响软件及版本列表。

表 5-13 Vulnerability

参数	是否必选	参数类型	描述
vul_id	否	String	漏洞编号。 最小长度：**1** 最大长度：**256**
type	否	String	漏洞类型。 最小长度：**1** 最大长度：**32**
threat_type	否	String	威胁类型。 最小长度：**1** 最大长度：**32**

参数	是否必选	参数类型	描述
severity	否	String	危害等级（超危、高危、中危、低危）。 最小长度：**1** 最大长度：**32**
score	否	Number	CVSS评分。 最小值：**0.0** 最大值：**10.0**
vector	否	String	评分向量。 最小长度：**0** 最大长度：**512**
version	否	String	CVSS版本。 最小长度：**0** 最大长度：**512**
description	否	String	漏洞描述。 最小长度：**0** 最大长度：**512**
created_at	否	String	漏洞报告的创建时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
updated_at	否	String	漏洞报告的更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

表 5-14 Patch

参数	是否必选	参数类型	描述
patch_id	否	String	补丁编号。 最小长度：**1** 最大长度：**256**
patch_name	否	String	补丁名称。 最小长度：**1** 最大长度：**256**

参数	是否必选	参数类型	描述
type	否	String	补丁类型（0：linux，1：windows，2：web-cms）。 最小长度：**1** 最大长度：**32**
major_level	否	String	重要等级。 最小长度：**1** 最大长度：**32**
status	否	String	补丁状态。 最小长度：**1** 最大长度：**32**
repair_cmd	否	String	修复命令。 最小长度：**0** 最大长度：**512**
repair_necessity	否	String	修复必要程度（1：需立刻修复，2：可延后修复，3：暂可以不修复）。 最小长度：**0** 最大长度：**512**
release_time	否	String	发布时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息 为事件发生时区，无法解析时区的时间，默认时区填东八区。

表 5-15 Malware

参数	是否必选	参数类型	描述
name	是	String	恶意软件名称，最大64个字符。 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
type	是	String	恶意软件类型，遵循STIX规范：adware、backdoor、bot、bootkit、ddos、downloader、dropper、exploit-kit、keylogger、ransomware、remote-access-trojan、resource-exploitation、rogue-security-software、rootkit、screen-capture、spyware、trojan、unknown、virus、webshell、wiper、worm 最小长度：**1** 最大长度：**512**
path	否	String	恶意软件在系统中的路径，最大512个字符。 最小长度：**0** 最大长度：**512**
state	否	String	恶意软件状态，取值范围：OBSERVED、REMOVAL_FAILED、REMOVED。 最小长度：**0** 最大长度：**512**

表 5-16 ThreatIntel

参数	是否必选	参数类型	描述
type	否	String	威胁情报类型，Domain、Email_Address、Hash_MD5、Hash_SHA1、Hash_SHA256、Hash_SHA512、IPv4_Address、IPv6_Address、URL。 最小长度：**0** 最大长度：**64**
value	否	String	威胁情报指标值，最大512个字符。 最小长度：**0** 最大长度：**512**

参数	是否必选	参数类型	描述
source	是	String	威胁情报源，最大64个字符。 最小长度：**0** 最大长度：**64**
description	是	String	威胁情报描述。 最小长度：**0** 最大长度：**4096**
update_time	否	String	威胁情报的更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
source_url	否	String	链接，提供有关威胁情报源的更多详细信息。 最小长度：**0** 最大长度：**512**

表 5-17 Resource

参数	是否必选	参数类型	描述
id	是	String	资源ID。 最小长度：**32** 最大长度：**36**
name	是	String	资源名称；最大长度255个字符。 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
type	是	String	资源类型；cloud_servers、vpcs、security_groups、public_ips、volumes、containers、websites、hws_account、iam_user、firewall、security_group_rules、elb_loadbalancers、elb_listeners、cts、obs_buckets、rds_instances、dds_instances、dcs_instances、certificates、anti_ddos_eip、dns、other。 最小长度：**1** 最大长度：**128**
service	否	String	资源所属服务名称。 最小长度：**1** 最大长度：**128**
provider	是	String	资源提供商名称。 最小长度：**1** 最大长度：**128**
region	否	String	区域。 最小长度：**1** 最大长度：**128**
domain_id	是	String	资源所属租户账号ID。 最小长度：**32** 最大长度：**36**
project_id	否	String	资源所属项目ID。 最小长度：**32** 最大长度：**36**
idc_id	否	String	线下机房ID。 最小长度：**32** 最大长度：**36**
tags	否	Object	资源标签 1、最多50个key/values对。 2、values：最大255字符。 3、取值范围：字母数字、空格、“+”、“-”、“=”、“.”、“_”、“:”、“/”、“@”。
details	否	**Detail** object	资源详情。

表 5-18 Detail

参数	是否必选	参数类型	描述
cloud_servers	否	**CloudServers** object	ECS实例详情。
vpcs	否	**Vpcs** object	虚拟私有云。
public_ips	否	**PublicIps** object	弹性公网IP。
volumes	否	**Volumes** object	磁盘。
containers	否	**Container** object	容器。
websites	否	**Websites** object	网站。

表 5-19 CloudServers

参数	是否必选	参数类型	描述
status	是	String	弹性云服务器状态。 取值范围： ACTIVE、BUILD、ERROR、HARD_REBOOT、MIGRATING、REBOOT、REBUILD、RESIZE、REVERT_RESIZE、SHUTOFF、VERIFY_RESIZE 最小长度：**1** 最大长度：**128**
addresses	是	Array of **Addresses** objects	弹性云服务器的网络属性。
flavor	是	**Flavor** object	云服务器规格。
security_groups	是	Array of **SecurityGroups** objects	弹性云服务器所属安全组列表。
metadata	是	**Metadata** object	元数据。

参数	是否必选	参数类型	描述
host_id	是	String	弹性云服务器所在主机的主机ID。 最小长度：**1** 最大长度：**128**
host_status	是	String	云服务器所在主机状态。 UP：服务正常； UNKNOWN：状态未知； DOWN：服务异常； MAINTENANCE：维护状态； 空字符串：弹性云服务器无主机信息。 最小长度：**1** 最大长度：**128**
volumes_attached	是	Array of **VolumesAttached** objects	挂载到弹性云服务器上的磁盘。

表 5-20 Addresses

参数	是否必选	参数类型	描述
version	是	String	IP地址版本。“4”：代表IPv4。“6”：代表IPv6。 最小长度：**1** 最大长度：**1**
addr	是	String	IP地址。 最小长度：**7** 最大长度：**15**
ip_type	是	String	IP地址类型 fixed：代表私有IP地址。floating：代表浮动IP地址。 最小长度：**1** 最大长度：**128**
mac_addr	是	String	MAC地址。 最小长度：**1** 最大长度：**128**

表 5-21 Flavor

参数	是否必选	参数类型	描述
id	是	String	云服务器规格ID。 最小长度：**1** 最大长度：**128**
name	是	String	云服务器规格名称。 最小长度：**1** 最大长度：**128**
disk	是	String	该云服务器规格对应要求系统盘大小，0为不限制。 最小长度：**1** 最大长度：**128**
vcpus	是	String	该云服务器规格对应的CPU核数。 最小长度：**1** 最大长度：**10**
ram	是	String	该云服务器规格对应的内存大小，单位为MB。 最小长度：**1** 最大长度：**10**

表 5-22 SecurityGroups

参数	是否必选	参数类型	描述
id	是	String	安全组ID。 最小长度：**1** 最大长度：**128**
name	是	String	安全组名称。 最小长度：**1** 最大长度：**128**

表 5-23 Metadata

参数	是否必选	参数类型	描述
vpc_id	是	String	云服务器所属的虚拟私有云ID。 最小长度：**1** 最大长度：**128**

参数	是否必选	参数类型	描述
image_id	是	String	云服务器操作系统对应的镜像ID。 最小长度：**1** 最大长度：**128**
image_name	是	String	云服务器操作系统对应的镜像名称。 最小长度：**1** 最大长度：**128**
image_type	是	String	镜像类型，目前支持： 公共镜像（gold）、 私有镜像（private）、 共享镜像（shared）。 最小长度：**1** 最大长度：**128**
os_bit	是	String	操作系统位数，一般取值为“32”或者“64”。 最小长度：**1** 最大长度：**128**
os_type	是	String	操作系统类型，取值为：Linux、Windows。 最小长度：**1** 最大长度：**128**

表 5-24 VolumesAttached

参数	是否必选	参数类型	描述
id	是	String	磁盘ID。 最小长度：**1** 最大长度：**128**
boot_index	是	String	云硬盘启动顺序。0为系统盘，非0为数据盘。 最小长度：**1** 最大长度：**128**
device	是	String	云硬盘挂载盘符，即磁盘挂载点。 最小长度：**1** 最大长度：**128**

表 5-25 Vpcs

参数	是否必选	参数类型	描述
cidr	是	String	虚拟私有云下可用子网的范围。 取值范围： 10.0.0.0/8~10.255.255.240/28 、 172.16.0.0/12 ~ 172.31.255.240/28、 192.168.0.0/16 ~ 192.168.255.240/28。 约束： 必须是cidr格式，例如:192.168.0.0/16。 最小长度：**1** 最大长度：**128**
status	是	String	功能说明：虚拟私有云的状态。 取值范围： CREATING：创建中； OK：创建成功。 最小长度：**1** 最大长度：**128**

表 5-26 PublicIps

参数	是否必选	参数类型	描述
status	是	String	弹性公网IP的状态。 取值范围： FREEZED：冻结； BIND_ERROR：绑定失败； BINDING：绑定中； PENDING_DELETE：释放中； PENDING_CREATE：创建中； PENDING_UPDATE：更新中； DOWN：未绑定； ACTIVE：绑定； ELB：绑定ELB； ERROR：异常失败。 最小长度：**1** 最大长度：**128**
type	是	String	弹性公网IP的类型。 取值范围：5_telcom（电信）、5_union（联通）、5_bgp（全动态BGP）、5_sbgp（静态BGP）。 最小长度：**1** 最大长度：**128**

参数	是否必选	参数类型	描述
ip_version	是	Integer	IP版本信息，取值范围是4和6。4：表示IPv4； 6：表示IPv6。 最小值：**4** 最大值：**6**
public_ipv6_address	否	String	IPv4时无此字段，IPv6时为申请到的弹性公网IP地址。 最小长度：**1** 最大长度：**128**
public_ip_address	是	String	IPv4时是申请到的弹性公网IP地址，IPv6时是IPv6地址对应的IPv4地址。 最小长度：**1** 最大长度：**128**
private_ip_address	是	String	绑定弹性公网IP的私有IP地址。 最小长度：**1** 最大长度：**128**
vpc_id	是	String	弹性公网IP所属虚拟私有云ID。 最小长度：**1** 最大长度：**128**
port_id	否	String	端口id。 约束：只有绑定了的弹性公网IP查询才会返回该参数。 最小长度：**1** 最大长度：**128**
device_id	否	String	端口所属设备ID。 最小长度：**1** 最大长度：**128**
bandwidth_id	是	String	弹性公网IP对应带宽ID。 最小长度：**1** 最大长度：**128**
bandwidth_name	是	String	带宽名称。 最小长度：**1** 最大长度：**128**

表 5-27 Volumes

参数	是否必选	参数类型	描述
status	是	String	云硬盘状态，见EVS服务云硬盘状态描述。 最小长度：**1** 最大长度：**128**
availability_zone	是	String	云硬盘所属的AZ信息。 最小长度：**1** 最大长度：**128**
attachments	是	Array of **Attachment** objects	云硬盘的挂载信息。
size	是	String	云硬盘大小，单位为GB。 最小长度：**1** 最大长度：**10**
volume_type	是	String	云硬盘类型。 目前支持“SSD”，“SAS”和“SATA”三种。 “SSD”为超高IO云硬盘， “SAS”为高IO云硬盘，“SATA”为普通IO云硬盘。 最小长度：**1** 最大长度：**10**
encrypted	是	Boolean	是否加密。
multiattach	是	Boolean	是否为共享云硬盘。 true：表示为共享云硬盘。 false：表示为非共享云硬盘。

表 5-28 Attachment

参数	是否必选	参数类型	描述
server_id	是	String	云硬盘挂载到的云服务器的ID。 最小长度：**1** 最大长度：**128**
attachment_id	是	String	挂载信息对应的ID。 最小长度：**1** 最大长度：**128**
attached_at	是	String	挂载时间。

参数	是否必选	参数类型	描述
device	是	String	挂载点。 最小长度：**1** 最大长度：**128**

表 5-29 Container

参数	是否必选	参数类型	描述
image_id	是	String	镜像ID。 最小长度：**1** 最大长度：**128**
image_name	是	String	镜像名称。 最小长度：**1** 最大长度：**128**
node_id	否	String	容器所在节点ID。 最小长度：**1** 最大长度：**128**
node_name	否	String	容器所在节点名称。 最小长度：**1** 最大长度：**128**
launched_time	否	String	容器启动时间。

表 5-30 Websites

参数	是否必选	参数类型	描述
url	是	String	网站地址，最长128个字符。 最小长度：**1** 最大长度：**128**
port	否	String	端口号。 最小长度：**1** 最大长度：**12**

表 5-31 remediation

参数	是否必选	参数类型	描述
recommendation	否	**Recommendation** object	补救措施。

表 5-32 Recommendation

参数	是否必选	参数类型	描述
text	是	String	处理建议，最长512个字符。 最小长度：**1** 最大长度：**512**
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证。 最小长度：**1** 最大长度：**128**

表 5-33 RelatedEvent

参数	是否必选	参数类型	描述
id	是	String	与当前事件相关的事件的ID，最大36个字符。 最小长度：**1** 最大长度：**36**
company_name	是	String	生成相关事件的产品所属公司名称，最大16个字符。 最小长度：**1** 最大长度：**16**
product_name	是	String	生成相关事件的产品名称，最大24个字符。 最小长度：**1** 最大长度：**24**

响应参数

状态码： 400

表 5-34 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效请求提示信息 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 401

表 5-35 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 500

表 5-36 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

请求示例

```
POST https://{endpoint}/v1/{project_id}/events/import

{
  "events" : [ {
    "version" : "1.0.0",
```

```
  "domain_id" : "dfaf9864b95c448797b5dc0f00709a55",
  "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  "data_source" : {
    "type" : 1,
    "domain_id" : "39d29606d49b483a9914c581ce190d54",
    "project_id" : "86670b7b5c6b41e0a5716c0ed77dfc32",
    "region" : "cn-north-4",
    "company_name" : "Huawei",
    "product_name" : "Anti-DDOS",
    "product_feature" : "Anti-DDOS"
  },
  "first_observed_time" : "2020-10-10T13:10:40.436+0800",
  "last_observed_time" : "2020-10-10T13:10:40.436+0800",
  "create_time" : "2020-10-10T13:10:40.436+0800",
  "arrive_time" : "2020-10-21T01:20:31.343+0800",
  "event_id" : "1683fbf6-01fd-49f4-8222-0fe33d3f2d2e",
  "title" : "TCP Malformed",
  "description" : "TCP Malformed",
  "severity" : {
    "original_score" : 1,
    "label" : "TIPS"
  },
  "business_code" : "attack",
  "types" : [ {
    "namespace" : "Attack",
    "category" : "DDoS",
    "classifier" : "TCP Malformed"
  } ],
  "network" : {
    "direction" : "IN",
    "dest_ip" : "119.8.124.133",
    "dest_port" : 0,
    "dest_geo" : {
      "latitude" : 1.352083,
      "longitude" : 103.81984
    }
  },
  "resources" : [ {
    "id" : "f1f4076a-9d12-497f-aac4-a9dcb5462fcc",
    "name" : "ecs-s3_large_2_win-20200828214727",
    "type" : "CloudServers",
    "service" : "ECS",
    "provider" : "Huawei",
    "region" : "cn-north-4",
    "domain_id" : "dfaf9864b95c448797b5dc0f00709a55",
    "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx"
  } ],
  "verification_state" : "Unknown",
  "handle_status" : "New"
 } ]
}
```


响应示例

无

状态码

状态码	描述
201	Succeeded
400	Bad Request
401	Unauthorized

状态码	描述
403	Forbidden
500	Internal Server Error

错误码

请参见**错误码**。

A 附录

A.1 状态码

- 正常

返回值	说明
201	成功。

- 异常

状态码	编码	说明
400	Bad Request	参数错误。
401	Unauthorized	认证失败。
403	Forbidden	拒绝访问。
500	Internal Server Error	系统内部错误。

A.2 错误码

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。

状态码	错误码	错误信息	描述	处理措施
400	sa.00000001	Bad Request	参数错误	请检查请求参数
401	sa.00000012	Unauthorized	无效的用户TOKEN	重新申请Token
403	sa.00000010	Forbidden	拒绝访问	开通SA权限

状态码	错误码	错误信息	描述	处理措施
403	sa.00100001	Forbidden	接收权限不存在	检查导入权限
403	sa.00100004	Forbidden	不存在产品信息	检查产品信息
500	CSB.10061104	ALERT_RULE_NAME_ALREADY_EXIST	告警名称已存在	
500	CSB.11061001	ALERT_PROCESS_STATUS_ERROR	进程状态有误	
500	CSB.11061002	ALERT_RULE_OUT_OF_RANGE	参数超出范围	
500	CSB.11061003	ALERT_RULE_SCHEDULE_OUT_OF_RANGE	schedule参数超出范围	
500	sa.00000008	Internal Server Error	系统内部错误	联系管理员

A.3 获取项目 ID

操作场景

在调用接口的时候，部分URL中需要填入项目ID，所以需要获取到项目ID。有如下两种获取方式：

- **调用API获取项目ID**
- **从控制台获取项目ID**

调用 API 获取项目 ID

项目ID可以通过调用**查询指定条件下的项目信息**API获取。

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从**地区和终端节点**获取。接口的认证鉴权请参见**认证鉴权**。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
```

```
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```


从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目编号，所以需要获取到项目编号。项目编号获取步骤如下：

1. 登录管理控制台。
2. 鼠标悬停在右上角的用户名，选择下拉列表中的“我的凭证”。
   在“API凭证”页面的项目列表中查看项目ID。

图 A-1 查看项目 ID