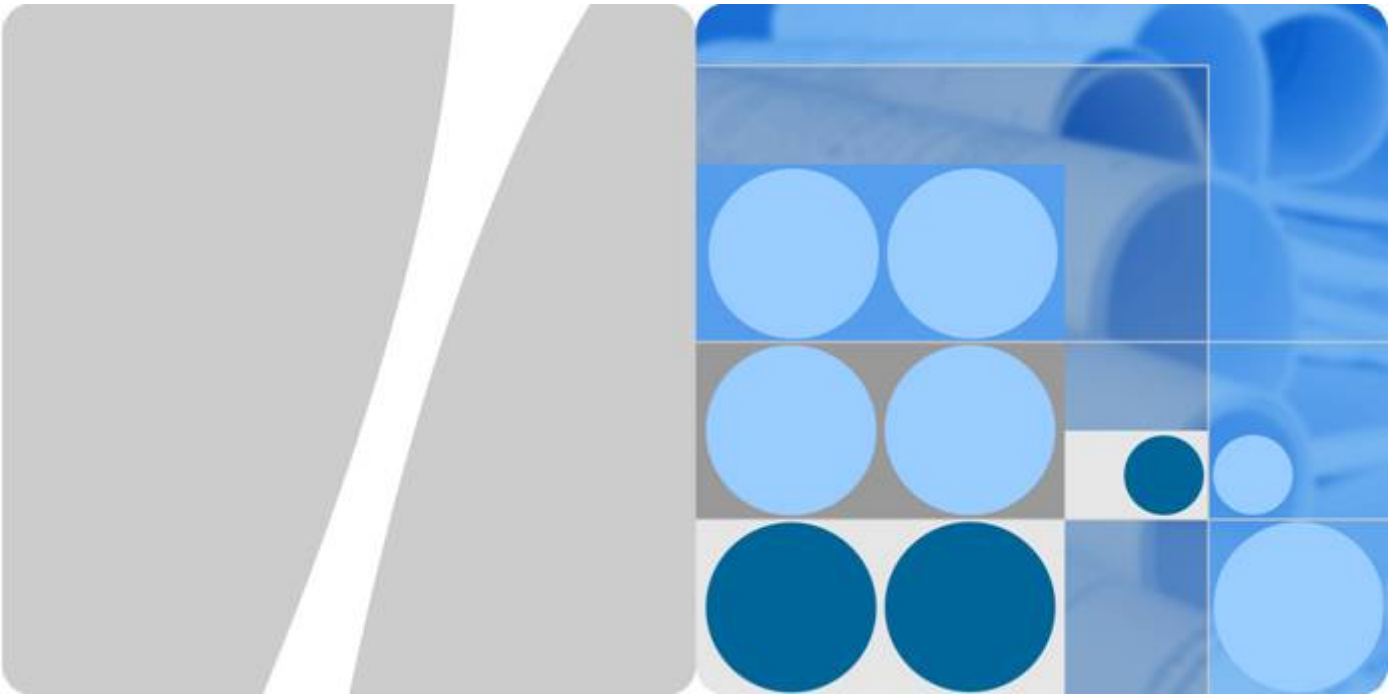


企业主机安全

API 参考（吉隆坡区域）

发布日期　2025-09-23

目 录

1 使用前必读

概述

欢迎使用企业主机安全（Host Security Service，HSS）。企业主机安全是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

您可以使用本文档提供的API对企业主机安全进行相关操作。

在调用企业主机安全API之前，请确保已经充分了解企业主机安全相关概念，详细信息请参见产品介绍。

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。

基本概念

- 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它们进行日常管理工作。

- 用户

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

  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。

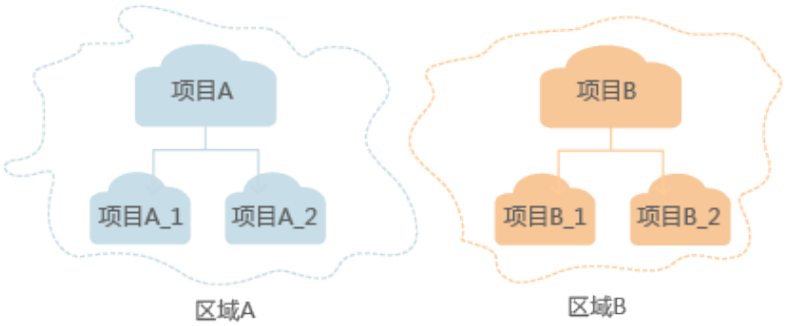
- 可用区（AZ，Availability Zone）

  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。

约束与限制

单API流量每分钟限制访问次数为600次，其中单用户每分钟访问单API次数最大为5次，单IP地址每分钟访问单API次数最大为5次。

更详细的限制请参见具体API的说明。

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。
- **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。

在的URI部分，您可以看到其请求方法为“POST”，则其请求为：

请求消息头

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

如下公共消息头需要添加到请求中。

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

```
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date, Signature=**********
```

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。

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。

- **accountid**为IAM用户所属的账号ID。
- **username**为要创建的IAM用户名。
- **email**为IAM用户的邮箱。
- **********为IAM用户的登录密码。

```
Content-Type: application/json
 X-Sdk-Date: 20240416T095341Z
 Authorization: SDK-HMAC-SHA256 Access=***************, SignedHeaders=content-type;host;x-sdk-date,
Signature=***************

{
    "user": {
        "domain_id": "accountid",
        "name": "username",
        "password": "**********",
        "email": "email",
        "description": "IAM User Description"
    }
 }
```

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。

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。
- 使用Token前请确保Token离过期有足够的时间，防止调用API的过程中Token过期导致调用API失败。

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“ABCDEFG....”，则调用接口时将“X-Auth-Token: ABCDEFG....”加到请求消息头即可，如下所示。

```
GET https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

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既可以使用永久访问密钥中的AK/SK，也可以使用临时访问密钥中的AK/SK，但使用临时访问密钥的AK/SK时需要额外携带“X-Security-Token”字段，字段值为临时访问密钥的security_token。

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2-1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 2-1 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": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

3 API 说明

3.1 基线管理

3.1.1 查询弱口令检测结果列表

功能介绍

查询弱口令检测结果列表

URI

GET /v5/{project_id}/baseline/weak-password-users

表 3-1 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

表 3-2 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
host_name	否	String	服务器名称
host_ip	否	String	服务器IP地址
user_name	否	String	弱口令账号名称
host_id	否	String	主机ID，不赋值时，查租户所有主机

参数	是否必选	参数类型	描述
limit	否	Integer	每页数量
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-3 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）

响应参数

状态码：200

表 3-4 响应 Body 参数

参数	参数类型	描述
total_num	Long	总数
data_list	Array of **WeakPwdListInfoResponseInfo** objects	弱口令列表

表 3-5 WeakPwdListInfoResponseInfo

参数	参数类型	描述
host_id	String	服务器ID
host_name	String	服务器名称
host_ip	String	服务器IP
public_ip	String	服务器公网IP

参数	参数类型	描述
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	弱口令账号列表

表 3-6 WeakPwdAccountInfoResponseInfo

参数	参数类型	描述
user_name	String	弱口令账号名称
service_type	String	账号类型
duration	Integer	弱口令使用时长，单位天

请求示例

查询企业项目id为xxx下的主机弱口令检测结果。默认返回第一页（前10条）数据。

```
GET https://{endpoint}/v5/{project_id}/baseline/weak-password-users?enterprise_project_id=xxx
```

响应示例

状态码：200

弱口令检测结果列表

```
{
  "total_num" : 2,
  "data_list" : [ {
    "host_id" : "caa958adxxxxxxa481",
    "host_name" : "ubuntu1",
    "host_ip" : "192.168.0.8",
    "public_ip" : "100.85.85.85",
    "weak_pwd_accounts" : [ {
      "user_name" : "localhost1",
      "service_type" : "system",
      "duration" : 2147483647
    } ]
  }, {
    "host_id" : "caa958adxxxxxxa482",
    "host_name" : "ubuntu2",
    "host_ip" : "192.168.0.9",
    "public_ip" : "",
    "weak_pwd_accounts" : [ {
      "user_name" : "localhost2",
      "service_type" : "system",
      "duration" : 2147483647
    } ]
  } ]
}
```

状态码

状态码	描述
200	弱口令检测结果列表

错误码

请参见**错误码**。

3.1.2 查询口令复杂度策略检测报告

功能介绍

查询口令复杂度策略检测报告

URI

GET /v5/{project_id}/baseline/password-complexity

表 3-7 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

表 3-8 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
host_name	否	String	服务器名称
host_ip	否	String	服务器IP地址
host_id	否	String	服务器id，不赋值时，查租户所有主机
limit	否	Integer	每页显示数量，默认10
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-9 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）

响应参数

状态码：200

表 3-10 响应 Body 参数

参数	参数类型	描述
total_num	Long	记录总数
data_list	Array of **PwdPolicyInfoResponseInfo** objects	口令复杂度策略检测列表

表 3-11 PwdPolicyInfoResponseInfo

参数	参数类型	描述
host_id	String	服务器id(鼠标在“服务器名称”放置后上浮显示)
host_name	String	服务器名称
host_ip	String	服务器IP
public_ip	String	服务器公网IP
min_length	Boolean	口令最小长度
uppercase_letter	Boolean	大写字母
lowercase_letter	Boolean	小写字母
number	Boolean	数字
special_character	Boolean	特殊字符
suggestion	String	修改建议

请求示例

查询企业项目id为xxx下的主机口令复杂度检测结果。默认返回第一页（前10条）数据。

```
GET https://{endpoint}/v5/{project_id}/baseline/password-complexity?enterprise_project_id=xxx
```

响应示例

状态码：200

口令复杂度策略检测报告

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "76fa440a-5a08-43fa-ac11-d12183ab3a14",
    "host_ip" : "192.168.0.59",
    "public_ip" : "100.85.85.85",
    "host_name" : "ecs-6b96",
    "lowercase_letter" : false,
    "min_length" : true,
    "number" : false,
    "special_character" : false,
    "suggestion" : "The password should contain at least 3 of the following character types: uppercase letters, lowercase letters, digits, and special characters. ",
    "uppercase_letter" : false
  } ]
}
```

状态码

状态码	描述
200	口令复杂度策略检测报告

错误码

请参见**错误码**。

3.1.3 查询租户的服务器安全配置检测结果列表

功能介绍

查询租户的服务器安全配置检测结果列表

URI

GET /v5/{project_id}/baseline/risk-configs

表 3-12 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

表 3-13 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
check_name	否	String	基线名称
group_id	否	String	策略组ID
severity	否	String	风险等级，包含如下: ● Security : 安全 ● Low : 低危 ● Medium : 中危 ● High : 高危
standard	否	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
host_id	否	String	服务器id
limit	否	Integer	每页显示数量，默认10
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-14 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）

响应参数

状态码：200

表 3-15 响应 Body 参数

参数	参数类型	描述
total_num	Long	记录总数
data_list	Array of SecurityCheckInfoResponseInfo objects	服务器配置检测结果列表

表 3-16 SecurityCheckInfoResponseInfo

参数	参数类型	描述
severity	String	风险等级，包含如下: ● Low : 低危 ● Medium : 中危 ● High : 高危
check_name	String	基线名称
check_type	String	基线类型
standard	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
check_rule_num	Integer	检查项数量
failed_rule_num	Integer	风险项数量
host_num	Integer	影响的服务器数量
scan_time	Long	最新检测时间
check_type_desc	String	基线描述信息

请求示例

查询企业项目id为xxx下的主机基线配置检测结果列表。默认返回第一页（前10条）数据。

```
GET https://{endpoint}/v5/{project_id}/baseline/risk-configs?enterprise_project_id=xxx
```

响应示例

状态码：200

服务器安全配置检测结果列表

```
{
  "total_num" : 1,
```

```
 "data_list" : [ {
   "check_name" : "Docker",
   "check_rule_num" : 25,
   "check_type" : "Docker",
   "check_type_desc" : "Configuring security audit of Docker's host configurations and container-running-related contents based on Docker Container Security Specifications V1_0.",
   "failed_rule_num" : 20,
   "host_num" : 0,
   "scan_time" : 1661716860935,
   "severity" : "High",
   "standard" : "hw_standard"
 } ]
}
```

状态码

状态码	描述
200	服务器安全配置检测结果列表

错误码

请参见**错误码**。

3.1.4 查询指定安全配置项的检查结果

功能介绍

查询指定安全配置项的检查结果

URI

GET /v5/{project_id}/baseline/risk-config/{check_name}/detail

表 3-17 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
check_name	是	String	基线名称

表 3-18 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

参数	是否必选	参数类型	描述
standard	是	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
host_id	否	String	主机ID，不赋值时，查租户所有主机
limit	否	Integer	每页数量
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-19 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）

响应参数

状态码：200

表 3-20 响应 Body 参数

参数	参数类型	描述
severity	String	风险等级，包含如下: ● Low : 低危 ● Medium : 中危 ● High : 高危
check_type	String	基线类型
check_type_desc	String	基线描述
check_rule_num	Integer	检查项总数量
failed_rule_num	Integer	未通过的检查项数量
passed_rule_num	Integer	已通过的检查项数量

参数	参数类型	描述
ignored_rule_num	Integer	已忽略的检查项数量
host_num	Long	受影响的服务器的数量

请求示例

查询企业项目id为xxx下的基线名称为SSH、标准类型是“云安全实践”标准的配置检测结果列表。

```
GET https://{endpoint}/v5/{project_id}/baseline/risk-config/SSH/detail?
standard=hw_standard&enterprise_project_id=xxx
```

响应示例

状态码：200

安全配置项的检查结果

```
{
  "check_rule_num" : 17,
  "check_type_desc" : "This policy checks the basic security configuration items of the SSH service to
improve the security of the SSH service.",
  "failed_rule_num" : 15,
  "host_num" : 2,
  "ignored_rule_num" : 1,
  "passed_rule_num" : 14,
  "severity" : "Medium"
}
```

状态码

状态码	描述
200	安全配置项的检查结果

错误码

请参见**错误码**。

3.1.5 查询指定安全配置项的检查项列表

功能介绍

查询指定安全配置项的检查项列表

URI

GET /v5/{project_id}/baseline/risk-config/{check_name}/check-rules

表 3-21 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
check_name	是	String	基线名称

表 3-22 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
standard	是	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
result_type	否	String	结果类型，包含如下: ● safe： 已通过 ● unhandled : 未通过，且未忽略的 ● ignored : 未通过，且已忽略的
check_rule_name	否	String	检查项名称，支持模糊匹配
severity	否	String	风险等级，包含如下: ● Security : 安全 ● Low : 低危 ● Medium : 中危 ● High : 高危 ● Critical : 危急
host_id	否	String	主机ID，不赋值时，查租户所有主机
limit	否	Integer	每页数量
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-23 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）

响应参数

状态码：200

表 3-24 响应 Body 参数

参数	参数类型	描述
total_num	Long	风险总数
data_list	Array of **CheckRuleRiskInfoResponseInfo** objects	数据列表

表 3-25 CheckRuleRiskInfoResponseInfo

参数	参数类型	描述
severity	String	风险等级，包含如下: • Low：低危 • Medium：中危 • High：高危
check_name	String	基线名称
check_type	String	基线类型
standard	String	标准类型，包含如下: • cn_standard：等保合规标准 • hw_standard：云安全实践标准
check_rule_name	String	检查项
check_rule_id	String	检查项ID
host_num	Integer	影响服务器数量

参数	参数类型	描述
scan_result	String	检测结果，包含如下： • pass • failed
status	String	状态，包含如下： • safe：无需处理 • ignored：已忽略 • unhandled：未处理 • fixing：修复中 • fix-failed：修复失败 • verifying：验证中
enable_fix	Integer	是否支持一键修复,1:支持一键修复,0:不支持
enable_click	Boolean	该检查项的修复&忽略&验证按钮是否可点击,true:按钮可点击,false:按钮不可点击
rule_params	Array of **CheckRuleFixParamInfo** objects	支持传递参数修复的检查项可传递参数的范围

表 3-26 CheckRuleFixParamInfo

参数	参数类型	描述
rule_param_id	Integer	检查项参数ID
rule_desc	String	检查项参数描述
default_value	Integer	检查项参数默认值
range_min	Integer	检查项参数可取最小值
range_max	Integer	检查项参数可取最大值

请求示例

查询企业项目id为xxx下的基线名称为SSH、检查标准为“云安全实践”的检查项列表。

```
GET https://{endpoint}/v5/{project_id}/baseline/risk-config/SSH/check-rules?
standard=hw_standard&enterprise_project_id=xxx

{
  "standard" : "hw_standard"
}
```

响应示例

状态码：200

指定安全配置项的检查项列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_rule_id" : "1.1",
    "check_rule_name" : "Rule:Ensure that permissions on /etc/ssh/sshd_config are configured.",
    "check_type" : "SSH",
    "host_num" : 2,
    "standard" : "hw_standard",
    "scan_result" : "failed",
    "severity" : "High",
    "status" : "unhandled",
    "enable_fix" : 1,
    "enable_click" : true,
    "rule_params" : [ {
      "rule_param_id" : 1,
      "rule_desc" : "设置超时时间",
      "default_value" : 5,
      "range_min" : 1,
      "range_max" : 10
    }, {
      "rule_param_id" : 2,
      "rule_desc" : "设置重启次数",
      "default_value" : 10,
      "range_min" : 1,
      "range_max" : 20
    } ]
  } ]
}
```

状态码

状态码	描述
200	指定安全配置项的检查项列表

错误码

请参见**错误码**。

3.1.6 查询指定安全配置项的受影响服务器列表

功能介绍

查询指定安全配置项的受影响服务器列表

URI

GET /v5/{project_id}/baseline/risk-config/{check_name}/hosts

表 3-27 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
check_name	是	String	基线名称

表 3-28 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
standard	是	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
host_name	否	String	服务器名称
host_ip	否	String	服务器IP地址
limit	否	Integer	每页数量
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-29 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）

响应参数

状态码：200

表 3-30 响应 Body 参数

参数	参数类型	描述
total_num	Long	数据总量
data_list	Array of SecurityCheckHostInfoResponseInfo objects	数据列表

表 3-31 SecurityCheckHostInfoResponseInfo

参数	参数类型	描述
host_id	String	服务器ID
host_name	String	服务器名称
host_public_ip	String	服务器公网IP
host_private_ip	String	服务器私网IP
scan_time	Long	扫描时间
failed_num	Integer	风险项数量
passed_num	Integer	通过项数量

请求示例

查询企业项目id为xxx下的基线名称为SSH、检查标准为“云安全实践”的受影响服务器列表。

```
GET https://{endpoint}/v5/{project_id}/baseline/risk-config/SSH/hosts?
standard=hw_standard&enterprise_project_id=xxx
```

响应示例

状态码：200

安全配置项的受影响服务器列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "failed_num" : 6,
    "host_id" : "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    "host_name" : "zhangxiaodong2",
    "host_private_ip" : "192.168.0.129",
    "host_public_ip" : "*.*.*.10",
    "passed_num" : 10,
    "scan_time" : 1661716860935
  } ]
}
```

状态码

状态码	描述
200	安全配置项的受影响服务器列表

错误码

请参见**错误码**。

3.1.7 查询配置检查项检测报告

功能介绍

查询配置检查项检测报告

URI

GET /v5/{project_id}/baseline/check-rule/detail

表 3-32 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

表 3-33 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
check_name	是	String	基线名称
check_type	是	String	基线类型
check_rule_id	是	String	检查项ID
standard	是	String	标准类型，包含如下: • cn_standard：等保合规标准 • hw_standard：云安全实践标准
host_id	否	String	主机ID

请求参数

表 3-34 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）

响应参数

状态码：200

表 3-35 响应 Body 参数

参数	参数类型	描述
description	String	描述
reference	String	根据
audit	String	审计描述
remediation	String	修改建议
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	检测用例信息

表 3-36 CheckRuleCheckCaseResponseInfo

参数	参数类型	描述
check_description	String	检测用例描述
current_value	String	当前结果
suggest_value	String	期待结果

请求示例

查询企业项目id为xxx下的基线名称为SSH、检查项ID为1.12、检查标准为云安全实践标准的配置检查项检测报告。

```
GET https://{endpoint}/v5/{project_id}/baseline/check-rule/detail?
standard=hw_standard&enterprise_project_id=xxx&check_name=SSH&check_type=SSH&check_rule_id=1.12
```

响应示例

状态码：200

配置检查项检测报告

{"audit":"Run the following commands and verify that ClientAliveInterval is smaller than 300 and ClientAliveCountMax is 3 or less:
#grep '^ClientAliveInterval' /etc/ssh/sshd_config
ClientAliveInterval 300(default is 0)
#grep '^ClientAliveCountMax' /etc/ssh/sshd_config
ClientAliveCountMax 0(default is 3)","description":"The two options ClientAliveInterval and ClientAliveCountMax control the timeout of SSH sessions. The ClientAliveInterval parameter sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The ClientAliveCountMax parameter sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. For example, if the ClientAliveInterval is set to 15s and the ClientAliveCountMax is set to 3, unresponsive SSH clients will be disconnected after approximately 45s.","reference":"","remediation":"Edit the /etc/ssh/sshd_config file to set the parameter as follows:
ClientAliveInterval 300
ClientAliveCountMax 0"}

状态码

状态码	描述
200	配置检查项检测报告

错误码

请参见**错误码**。

3.1.8 对未通过的配置检查项进行忽略/取消忽略/修复/验证操作

功能介绍

对未通过的配置检查项进行忽略/取消忽略/修复/验证操作

URI

PUT /v5/{project_id}/baseline/check-rule/action

表 3-37 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-38 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
host_id	否	String	主机ID，不赋值时，查租户所有主机
action	是	String	动作 • "ignore" • "unignore" • "fix" • "verify"

请求参数

表 3-39 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）

表 3-40 请求 Body 参数

参数	是否必选	参数类型	描述
check_rules	否	Array of **CheckRuleKeyInfoRequestInfo** objects	检查项ID列表

表 3-41 CheckRuleKeyInfoRequestInfo

参数	是否必选	参数类型	描述
check_name	否	String	基线名称
check_rule_id	否	String	检查项ID

参数	是否必选	参数类型	描述
standard	否	String	基线标准, 类别包含如下： • cn_standard#等保合规标准 • hw_standard#云安全实践标准
fix_values	否	Array of CheckRuleFixValuesInfo objects	用户键入的检查项修复参数数组

表 3-42 CheckRuleFixValuesInfo

参数	是否必选	参数类型	描述
rule_param_id	否	Integer	检查项的参数ID
fix_value	否	Integer	检查项的参数值

响应参数

状态码：200

执行成功

无

请求示例

- 对企业项目id为xxx下的基线名称为SSH、检查项ID为1.11、检查标准为云安全实践标准的配置检查项进行忽略操作，此操作针对这条检查项的所有受影响主机。

```
PUT https://{endpoint}/v5/{project_id}/baseline/check-rule/action?
enterprise_project_id=xxx&action=ignore

{
  "check_name" : "SSH",
  "check_rule_id" : "1.11",
  "standard" : "hw_standard"
}
```

- 对企业项目id为xxx下的基线名称为SSH、检查项ID为1.11、检查标准为云安全实践标准的配置检查项进行修复操作，此操作只针对主机id为xxx的主机，修复参数为：将ID为1的修复项值设置为5，将ID为2的修复项值设置为20。

```
PUT https://{endpoint}/v5/{project_id}/baseline/check-rule/action?
enterprise_project_id=xxx&host_id=xxx&action=fix

{
  "check_name" : "SSH",
  "check_rule_id" : "1.11",
  "standard" : "hw_standard",
  "fix_values" : [ {
    "rule_param_id" : 1,
    "fix_value" : 5
  }, {
```

```
    "rule_param_id" : 2,
    "fix_value" : 20
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	执行成功

错误码

请参见**错误码**。

3.2 入侵检测

3.2.1 处理告警事件

功能介绍

处理告警事件

URI

POST /v5/{project_id}/event/operate

表 3-43 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

表 3-44 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
container_name	否	String	容器实例名称
container_id	否	String	容器Id

请求参数

表 3-45 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）

表 3-46 请求 Body 参数

参数	是否必选	参数类型	描述
operate_type	是	String	处理方式，包含如下: • mark_as_handled : 手动处理 • ignore : 忽略 • add_to_alarm_whitelist : 加入告警白名单 • add_to_login_whitelist : 加入登录白名单 • isolate_and_kill : 隔离查杀 • unhandle : 取消手动处理 • do_not_ignore : 取消忽略 • remove_from_alarm_whitelist : 删除告警白名单 • remove_from_login_whitelist : 删除登录白名单 • do_not_isolate_or_kill : 取消隔离查杀
handler	否	String	备注信息
operate_event_list	是	Array of **OperateEventRequestInfo** objects	操作的事件列表
event_white_rule_list	否	Array of **EventWhiteRuleListRequestInfo** objects	用户自定义告警白名单规则列表

表 3-47 OperateEventRequestInfo

参数	是否必选	参数类型	描述
event_class_id	是	String	事件分类，包含如下: ● container_1001：容器命名空间 ● container_1002：容器开放端口 ● container_1003：容器安全选项 ● container_1004：容器挂载目录 ● containerescape_0001：容器高危系统调用 ● containerescape_0002：Shocker攻击 ● containerescape_0003：DirtCow攻击 ● containerescape_0004：容器文件逃逸攻击 ● dockerfile_001：用户自定义容器保护文件被修改 ● dockerfile_002：容器文件系统可执行文件被修改 ● dockerproc_001：容器进程异常事件上报 ● fileprotect_0001：文件提权 ● fileprotect_0002：关键文件变更 ● fileprotect_0003：关键文件路径变更 ● fileprotect_0004：文件/目录变更 ● av_1002：病毒 ● av_1003：蠕虫 ● av_1004：木马 ● av_1005：僵尸网络 ● av_1006：后门 ● av_1007：间谍软件 ● av_1008：恶意广告软件 ● av_1009：钓鱼 ● av_1010：Rootkit ● av_1011：勒索软件

参数	是否必选	参数类型	描述
			• av_1012：黑客工具 • av_1013：灰色软件 • av_1015：Webshell • av_1016：挖矿软件 • login_0001：尝试暴力破解 • login_0002：爆破成功 • login_1001：登录成功 • login_1002：异地登录 • login_1003：弱口令 • malware_0001：shell变更事件上报 • malware_0002：反弹shell事件上报 • malware_1001：恶意程序 • procdet_0001：进程异常行为检测 • procdet_0002：进程提权 • procreport_0001：危险命令 • user_1001：账号变更 • user_1002：风险账号 • vmescape_0001：虚拟机敏感命令执行 • vmescape_0002：虚拟化进程访问敏感文件 • vmescape_0003：虚拟机异常端口访问 • webshell_0001：网站后门 • network_1001：恶意挖矿 • network_1002：对外DDoS攻击 • network_1003：恶意扫描 • network_1004：敏感区域攻击 • ransomware_0001：勒索攻击 • ransomware_0002：勒索攻击 • ransomware_0003：勒索攻击 • fileless_0001：进程注入

参数	是否必选	参数类型	描述
			• fileless_0002：动态库注入进程 • fileless_0003：关键配置变更 • fileless_0004：环境变量变更 • fileless_0005：内存文件进程 • fileless_0006：vdso劫持 • crontab_1001：Crontab可疑任务 • vul_exploit_0001：Redis漏洞利用攻击 • vul_exploit_0002：Hadoop漏洞利用攻击 • vul_exploit_0003：MySQL漏洞利用攻击 • rootkit_0001：可疑rootkit文件 • rootkit_0002：可疑内核模块 • RASP_0004：上传Webshell • RASP_0018：无文件Webshell • blockexec_001：已知勒索攻击 • hips_0001：Windows Defender防护被禁用 • hips_0002：可疑的黑客工具 • hips_0003：可疑的勒索加密行为 • hips_0004：隐藏账号创建 • hips_0005：读取用户密码凭据 • hips_0006：可疑的SAM文件导出 • hips_0007：可疑shadow copy删除操作 • hips_0008：备份文件删除 • hips_0009：可疑勒索病毒操作注册表 • hips_0010：可疑的异常进程行为 • hips_0011：可疑的扫描探测

参数	是否必选	参数类型	描述
			• hips_0012 : 可疑的勒索病毒脚本运行 • hips_0013 : 可疑的挖矿命令执行 • hips_0014 : 可疑的禁用windows安全中心 • hips_0015 : 可疑的停止防火墙服务行为 • hips_0016 : 可疑的系统自动恢复禁用 • hips_0017 : Offies 创建可执行文件 • hips_0018 : 带宏Offies文件异常创建 • hips_0019 : 可疑的注册表操作 • hips_0020 : Confluence远程代码执行 • hips_0021 : MSDT远程代码执行 • portscan_0001 : 通用端口扫描 • portscan_0002 : 秘密端口扫描 • k8s_1001 : Kubernetes事件删除 • k8s_1002 : 创建特权Pod • k8s_1003 : Pod中使用交互式shell • k8s_1004 : 创建敏感目录Pod • k8s_1005 : 创建主机网络的Pod • k8s_1006 : 创建主机Pid空间的Pod • k8s_1007 : 普通pod访问APIserver认证失败 • k8s_1008 : 普通Pod通过Curl访问APIServer • k8s_1009 : 系统管理空间执行exec • k8s_1010 : 系统管理空间创建Pod

参数	是否必选	参数类型	描述
			• k8s_1011：创建静态Pod • k8s_1012：创建DaemonSet • k8s_1013：创建集群计划任务 • k8s_1014：Secrets操作 • k8s_1015：枚举用户可执行的操作 • k8s_1016：高权限RoleBinding或ClusterRoleBinding • k8s_1017：ServiceAccount创建 • k8s_1018：创建Cronjob • k8s_1019：Pod中exec使用交互式shell • k8s_1020：无权限访问Apiserver • k8s_1021：使用curl访问APIServer • k8s_1022：Ingress漏洞 • k8s_1023：中间人攻击 • k8s_1024：蠕虫挖矿木马 • k8s_1025：K8s事件删除 • k8s_1026：SelfSubjectRulesReview场景 • imgblock_0001：镜像白名单阻断 • imgblock_0002：镜像黑名单阻断 • imgblock_0003：镜像标签白名单阻断 • imgblock_0004：镜像标签黑名单阻断 • imgblock_0005：创建容器白名单阻断 • imgblock_0006：创建容器黑名单阻断 • imgblock_0007：容器mount proc阻断 • imgblock_0008：容器seccomp unconfined阻断

参数	是否必选	参数类型	描述
			• imgblock_0009：容器特权阻断 • imgblock_0010：容器capabilities阻断
event_id	是	String	事件编号

参数	是否必选	参数类型	描述
event_type	是	Integer	事件类型，包含如下: ● 1001 : 通用恶意软件 ● 1002 : 病毒 ● 1003 : 蠕虫 ● 1004 : 木马 ● 1005 : 僵尸网络 ● 1006 : 后门 ● 1010 : Rootkit ● 1011 : 勒索软件 ● 1012 : 黑客工具 ● 1015 : Webshell ● 1016 : 挖矿 ● 1017 : 反弹Shell ● 2001 : 一般漏洞利用 ● 2012 : 远程代码执行 ● 2047 : Redis漏洞利用 ● 2048 : Hadoop漏洞利用 ● 2049 : MySQL漏洞利用 ● 3002 : 文件提权 ● 3003 : 进程提权 ● 3004 : 关键文件变更 ● 3005 : 文件/目录变更 ● 3007 : 进程异常行为 ● 3015 : 高危命令执行 ● 3018 : 异常Shell ● 3027 : Crontab可疑任务 ● 3029 : 系统安全防护被禁用 ● 3030 : 备份删除 ● 3031 : 异常注册表操作 ● 3036 : 容器镜像阻断 ● 4002 : 暴力破解 ● 4004 : 异常登录 ● 4006 : 非法系统账号 ● 4014 : 用户账号添加 ● 4020 : 用户密码窃取 ● 6002 : 端口扫描 ● 6003 : 主机扫描

参数	是否必选	参数类型	描述
			• 13001：Kubernetes事件删除 • 13002：Pod异常行为 • 13003：枚举用户信息 • 13004：绑定集群用户角色
occur_time	是	Integer	发生时间，毫秒
operate_detail_list	是	Array of **EventDetailRequestInfo** objects	操作详情信息列表，当operate_type 为add_to_alarm_whitelist 或remove_from_alarm_whitelist时，必传 keyword 和 hash；当operate_type 为add_to_login_whitelist 或remove_from_login_whitelist时，必传 login_ip， private_ip和 login_user_name；当operate_type 为isolate_and_kill 或do_not_isolate_or_kill 时，必传agent_id，file_hash，file_path，process_pid；其余情况可不填写内容。

表 3-48 EventDetailRequestInfo

参数	是否必选	参数类型	描述
agent_id	否	String	Agent ID
process_pid	否	Integer	进程id
file_hash	否	String	文件哈希
file_path	否	String	文件路径
file_attr	否	String	文件属性
keyword	否	String	告警事件关键字，仅用于告警白名单
hash	否	String	告警事件hash，仅用于告警白名单
private_ip	否	String	服务器私有IP
login_ip	否	String	登录源IP
login_user_name	否	String	登录用户名

参数	是否必选	参数类型	描述
container_id	否	String	容器ID
container_name	否	String	容器名称

表 3-49 EventWhiteRuleListRequestInfo

参数	是否必选	参数类型	描述
event_type	是	Integer	事件类型，包含如下: ● 1001 : 通用恶意软件 ● 1002 : 病毒 ● 1003 : 蠕虫 ● 1004 : 木马 ● 1005 : 僵尸网络 ● 1006 : 后门 ● 1010 : Rootkit ● 1011 : 勒索软件 ● 1012 ： 黑客工具 ● 1015 : Webshell ● 1016 : 挖矿 ● 1017 : 反弹Shell ● 2001 : 一般漏洞利用 ● 2012 : 远程代码执行 ● 2047 : Redis漏洞利用 ● 2048 : Hadoop漏洞利用 ● 2049 : MySQL漏洞利用 ● 3002 : 文件提权 ● 3003 : 进程提权 ● 3004 : 关键文件变更 ● 3005 : 文件/目录变更 ● 3007 : 进程异常行为 ● 3015 : 高危命令执行 ● 3018 : 异常Shell ● 3027 : Crontab可疑任务 ● 3029 ： 系统安全防护被禁用 ● 3030 ： 备份删除 ● 3031 ： 异常注册表操作 ● 3036 : 容器镜像阻断 ● 4002 : 暴力破解 ● 4004 : 异常登录 ● 4006 : 非法系统账号 ● 4014 : 用户账号添加 ● 4020 : 用户密码窃取 ● 6002 : 端口扫描

参数	是否必选	参数类型	描述
			• 6003：主机扫描 • 13001：Kubernetes事件删除 • 13002：Pod异常行为 • 13003：枚举用户信息 • 13004：绑定集群用户角色
field_key	是	String	加白字段，包含如下: • "file/process hash" # 进程/文件hash • "file_path" # 文件路径 • "process_path" # 进程路径 • "login_ip" # 登录ip • "reg_key" #注册表key • "process_cmdline" # 进程命令行 • "username" # 用户名
field_value	是	String	加白字段值
judge_type	是	String	通配符，包含如下: • "equal" # 相等 • "contain" # 包含

响应参数

状态码：200

success

无

请求示例

手动处理告警事件类型为Rootkit、告警事件编号为2a71e1e2-60f4-4d56-b314-2038fdc39de6的入侵告警事件。

```
POST https://{endpoint}/v5/{project_id}/event/operate?enterprise_project_id=xxx

{
  "operate_type" : "mark_as_handled",
  "handler" : "test",
  "operate_event_list" : [ {
    "event_class_id" : "rootkit_0001",
    "event_id" : "2a71e1e2-60f4-4d56-b314-2038fdc39de6",
    "occur_time" : 1672046760353,
    "event_type" : 1010,
    "operate_detail_list" : [ {
      "agent_id" : "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
```

```
    "file_hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "file_path" : "/usr/test",
    "process_pid" : 3123,
    "file_attr" : 33261,
    "keyword" : "file_path=/usr/test",
    "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "login_ip" : "127.0.0.1",
    "private_ip" : "127.0.0.2",
    "login_user_name" : "root",
    "container_id" : "containerid",
    "container_name" : "/test"
   } ]
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.2.2 查入侵事件列表

功能介绍

查入侵事件列表

URI

GET /v5/{project_id}/event/events

表 3-50 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

表 3-51 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
last_days	否	Integer	查询时间范围天数，与自定义查询时间begin_time，end_time互斥
host_name	否	String	服务器名称
host_id	否	String	服务器ID
private_ip	否	String	服务器私有IP
public_ip	否	String	服务器公网IP
container_name	否	String	容器实例名称
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

参数	是否必选	参数类型	描述
event_types	否	Array of integers	事件类型，包含如下: ● 1001 : 通用恶意软件 ● 1002 : 病毒 ● 1003 : 蠕虫 ● 1004 : 木马 ● 1005 : 僵尸网络 ● 1006 : 后门 ● 1010 : Rootkit ● 1011 : 勒索软件 ● 1012 : 黑客工具 ● 1015 : Webshell ● 1016 : 挖矿 ● 1017 : 反弹Shell ● 2001 : 一般漏洞利用 ● 2012 : 远程代码执行 ● 2047 : Redis漏洞利用 ● 2048 : Hadoop漏洞利用 ● 2049 : MySQL漏洞利用 ● 3002 : 文件提权 ● 3003 : 进程提权 ● 3004 : 关键文件变更 ● 3005 : 文件/目录变更 ● 3007 : 进程异常行为 ● 3015 : 高危命令执行 ● 3018 : 异常Shell ● 3026 : crontab提权 ● 3027 : Crontab可疑任务 ● 3029 : 系统安全防护被禁用 ● 3030 : 备份删除 ● 3031 : 异常注册表操作 ● 3036 : 容器镜像阻断 ● 4002 : 暴力破解 ● 4004 : 异常登录 ● 4006 : 非法系统账号 ● 4014 : 用户账号添加 ● 4020 : 用户密码窃取 ● 6002 : 端口扫描

参数	是否必选	参数类型	描述
			• 6003 : 主机扫描 • 13001 : Kubernetes事件删除 • 13002 : Pod异常行为 • 13003 : 枚举用户信息 • 13004 : 绑定集群用户角色
handle_status	否	String	处置状态，包含如下: • unhandled ： 未处理 • handled : 已处理
severity	否	String	威胁等级，包含如下: • Security ： 安全 • Low : 低危 • Medium : 中危 • High : 高危 • Critical : 危急
category	是	String	事件类别，包含如下: • host : 主机安全事件 • container : 容器安全事件
begin_time	否	String	自定义查询时间，与查询时间范围天数互斥，查询时间段的起始时间，毫秒级时间戳，end_time减去begin_time小于等于2天，与查询时间范围天数互斥
end_time	否	String	自定义时间，查询时间段的终止时间，毫秒级时间戳，end_time减去begin_time小于等于2天，与查询时间范围天数互斥

参数	是否必选	参数类型	描述
event_class_ids	否	Array of strings	事件标识，包含如下: ● container_1001：容器命名空间 ● container_1002：容器开放端口 ● container_1003：容器安全选项 ● container_1004：容器挂载目录 ● containerescape_0001：容器高危系统调用 ● containerescape_0002：Shocker攻击 ● containerescape_0003：DirtCow攻击 ● containerescape_0004：容器文件逃逸攻击 ● dockerfile_001：用户自定义容器保护文件被修改 ● dockerfile_002：容器文件系统可执行文件被修改 ● dockerproc_001：容器进程异常事件上报 ● fileprotect_0001：文件提权 ● fileprotect_0002：关键文件变更 ● fileprotect_0003：关键文件路径变更 ● fileprotect_0004：文件/目录变更 ● av_1002：病毒 ● av_1003：蠕虫 ● av_1004：木马 ● av_1005：僵尸网络 ● av_1006：后门 ● av_1007：间谍软件 ● av_1008：恶意广告软件 ● av_1009：钓鱼 ● av_1010：Rootkit ● av_1011：勒索软件 ● av_1012：黑客工具

参数	是否必选	参数类型	描述
			• av_1013：灰色软件 • av_1015：Webshell • av_1016：挖矿软件 • login_0001：尝试暴力破解 • login_0002：爆破成功 • login_1001：登录成功 • login_1002：异地登录 • login_1003：弱口令 • malware_0001：shell变更事件上报 • malware_0002：反弹shell事件上报 • malware_1001：恶意程序 • procdet_0001：进程异常行为检测 • procdet_0002：进程提权 • crontab_0001：crontab脚本提权 • crontab_0002：恶意路径提权 • procreport_0001：危险命令 • user_1001：账号变更 • user_1002：风险账号 • vmescape_0001：虚拟机敏感命令执行 • vmescape_0002：虚拟化进程访问敏感文件 • vmescape_0003：虚拟机异常端口访问 • webshell_0001：网站后门 • network_1001：恶意挖矿 • network_1002：对外DDoS攻击 • network_1003：恶意扫描 • network_1004：敏感区域攻击 • ransomware_0001：勒索攻击 • ransomware_0002：勒索攻击

参数	是否必选	参数类型	描述
			• ransomware_0003：勒索攻击 • fileless_0001：进程注入 • fileless_0002：动态库注入进程 • fileless_0003：关键配置变更 • fileless_0004：环境变量变更 • fileless_0005：内存文件进程 • fileless_0006：vdso劫持 • crontab_1001：Crontab可疑任务 • vul_exploit_0001：Redis漏洞利用攻击 • vul_exploit_0002：Hadoop漏洞利用攻击 • vul_exploit_0003：MySQL漏洞利用攻击 • rootkit_0001：可疑rootkit文件 • rootkit_0002：可疑内核模块 • RASP_0004：上传Webshell • RASP_0018：无文件Webshell • blockexec_001：已知勒索攻击 • hips_0001：Windows Defender防护被禁用 • hips_0002：可疑的黑客工具 • hips_0003：可疑的勒索加密行为 • hips_0004：隐藏账号创建 • hips_0005：读取用户密码凭据 • hips_0006：可疑的SAM文件导出 • hips_0007：可疑shadow copy删除操作 • hips_0008：备份文件删除 • hips_0009：可疑勒索病毒操作注册表

参数	是否必选	参数类型	描述
			• hips_0010 : 可疑的异常进程行为 • hips_0011 : 可疑的扫描探测 • hips_0012 : 可疑的勒索病毒脚本运行 • hips_0013 : 可疑的挖矿命令执行 • hips_0014 : 可疑的禁用windows安全中心 • hips_0015 : 可疑的停止防火墙服务行为 • hips_0016 : 可疑的系统自动恢复禁用 • hips_0017 : Offies 创建可执行文件 • hips_0018 : 带宏Offies文件异常创建 • hips_0019 : 可疑的注册表操作 • hips_0020 : Confluence远程代码执行 • hips_0021 : MSDT远程代码执行 • portscan_0001 : 通用端口扫描 • portscan_0002 : 秘密端口扫描 • k8s_1001 : Kubernetes事件删除 • k8s_1002 : 创建特权Pod • k8s_1003 : Pod中使用交互式shell • k8s_1004 : 创建敏感目录Pod • k8s_1005 : 创建主机网络的Pod • k8s_1006 : 创建主机Pid空间的Pod • k8s_1007 : 普通pod访问APIserver认证失败 • k8s_1008 : 普通Pod通过Curl访问APIServer

参数	是否必选	参数类型	描述
			• k8s_1009：系统管理空间执行exec • k8s_1010：系统管理空间创建Pod • k8s_1011：创建静态Pod • k8s_1012：创建DaemonSet • k8s_1013：创建集群计划任务 • k8s_1014：Secrets操作 • k8s_1015：枚举用户可执行的操作 • k8s_1016：高权限RoleBinding或ClusterRoleBinding • k8s_1017：ServiceAccount创建 • k8s_1018：创建Cronjob • k8s_1019：Pod中exec使用交互式shell • k8s_1020：无权限访问Apiserver • k8s_1021：使用curl访问APIServer • k8s_1022：Ingress漏洞 • k8s_1023：中间人攻击 • k8s_1024：蠕虫挖矿木马 • k8s_1025：K8s事件删除 • k8s_1026：SelfSubjectRulesReview场景 • imgblock_0001：镜像白名单阻断 • imgblock_0002：镜像黑名单阻断 • imgblock_0003：镜像标签白名单阻断 • imgblock_0004：镜像标签黑名单阻断 • imgblock_0005：创建容器白名单阻断 • imgblock_0006：创建容器黑名单阻断

参数	是否必选	参数类型	描述
			• imgblock_0007 : 容器mount proc阻断 • imgblock_0008 : 容器 seccomp unconfined阻断 • imgblock_0009 : 容器特权阻断 • imgblock_0010 : 容器 capabilities阻断
severity_list	否	Array of strings	威胁等级，包含如下: • Security： 安全 • Low : 低危 • Medium : 中危 • High : 高危 • Critical : 危急
attack_tag	否	String	攻击标识，包含如下: • attack_success : 攻击成功 • attack_attempt : 攻击尝试 • attack_blocked : 攻击被阻断 • abnormal_behavior : 异常行为 • collapsible_host : 主机失陷 • system_vulnerability : 系统脆弱性
asset_value	否	String	资产重要性，包含如下3种 • important： 重要资产 • common： 一般资产 • test： 测试资产
tag_list	否	Array of strings	事件标签列表，例如:["热点事件"]

参数	是否必选	参数类型	描述
att_ck	否	String	ATT&CK攻击阶，包含如下： • Reconnaissance：侦察 • Initial Access：初始访问 • Execution：执行 • Persistence：持久化 • Privilege Escalation：权限提升 • Defense Evasion：防御绕过 • Credential Access：凭据访问 • Command and Control：命令与控制 • Impact：影响破坏
event_name	否	String	告警名称
auto_block	否	Boolean	是否自动阻断告警

请求参数

表 3-52 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）

响应参数

状态码：200

表 3-53 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **EventManagementResponseInfo** objects	事件列表详情

表 3-54 EventManagementResponseInfo

参数	参数类型	描述
event_id	String	事件编号

参数	参数类型	描述
event_class_id	String	事件分类，包含如下: ● container_1001：容器命名空间 ● container_1002：容器开放端口 ● container_1003：容器安全选项 ● container_1004：容器挂载目录 ● containerescape_0001：容器高危系统调用 ● containerescape_0002：Shocker攻击 ● containerescape_0003：DirtCow攻击 ● containerescape_0004：容器文件逃逸攻击 ● dockerfile_001：用户自定义容器保护文件被修改 ● dockerfile_002：容器文件系统可执行文件被修改 ● dockerproc_001：容器进程异常事件上报 ● fileprotect_0001：文件提权 ● fileprotect_0002：关键文件变更 ● fileprotect_0003：关键文件路径变更 ● fileprotect_0004：文件/目录变更 ● av_1002：病毒 ● av_1003：蠕虫 ● av_1004：木马 ● av_1005：僵尸网络 ● av_1006：后门 ● av_1007：间谍软件 ● av_1008：恶意广告软件 ● av_1009：钓鱼 ● av_1010：Rootkit ● av_1011：勒索软件 ● av_1012：黑客工具 ● av_1013：灰色软件 ● av_1015：Webshell ● av_1016：挖矿软件 ● login_0001：尝试暴力破解 ● login_0002：爆破成功 ● login_1001：登录成功

参数	参数类型	描述
		• login_1002：异地登录 • login_1003：弱口令 • malware_0001：shell变更事件上报 • malware_0002：反弹shell事件上报 • malware_1001：恶意程序 • procdet_0001：进程异常行为检测 • procdet_0002：进程提权 • procreport_0001：危险命令 • user_1001：账号变更 • user_1002：风险账号 • vmescape_0001：虚拟机敏感命令执行 • vmescape_0002：虚拟化进程访问敏感文件 • vmescape_0003：虚拟机异常端口访问 • webshell_0001：网站后门 • network_1001：恶意挖矿 • network_1002：对外DDoS攻击 • network_1003：恶意扫描 • network_1004：敏感区域攻击 • ransomware_0001：勒索攻击 • ransomware_0002：勒索攻击 • ransomware_0003：勒索攻击 • fileless_0001：进程注入 • fileless_0002：动态库注入进程 • fileless_0003：关键配置变更 • fileless_0004：环境变量变更 • fileless_0005：内存文件进程 • fileless_0006：vdso劫持 • crontab_1001：Crontab可疑任务 • vul_exploit_0001：Redis漏洞利用攻击 • vul_exploit_0002：Hadoop漏洞利用攻击 • vul_exploit_0003：MySQL漏洞利用攻击 • rootkit_0001：可疑rootkit文件 • rootkit_0002：可疑内核模块

参数	参数类型	描述
		• RASP_0004：上传Webshell • RASP_0018：无文件Webshell • blockexec_001：已知勒索攻击 • hips_0001：Windows Defender防护被禁用 • hips_0002：可疑的黑客工具 • hips_0003：可疑的勒索加密行为 • hips_0004：隐藏账号创建 • hips_0005：读取用户密码凭据 • hips_0006：可疑的SAM文件导出 • hips_0007：可疑shadow copy删除操作 • hips_0008：备份文件删除 • hips_0009：可疑勒索病毒操作注册表 • hips_0010：可疑的异常进程行为 • hips_0011：可疑的扫描探测 • hips_0012：可疑的勒索病毒脚本运行 • hips_0013：可疑的挖矿命令执行 • hips_0014：可疑的禁用windows安全中心 • hips_0015：可疑的停止防火墙服务行为 • hips_0016：可疑的系统自动恢复禁用 • hips_0017：Offies 创建可执行文件 • hips_0018：带宏Offies文件异常创建 • hips_0019：可疑的注册表操作 • hips_0020：Confluence远程代码执行 • hips_0021：MSDT远程代码执行 • portscan_0001：通用端口扫描 • portscan_0002：秘密端口扫描 • k8s_1001：Kubernetes事件删除 • k8s_1002：创建特权Pod • k8s_1003：Pod中使用交互式shell • k8s_1004：创建敏感目录Pod • k8s_1005：创建主机网络的Pod • k8s_1006：创建主机Pid空间的Pod • k8s_1007：普通pod访问APIserver认证失败

参数	参数类型	描述
		• k8s_1008：普通Pod通过Curl访问APIServer • k8s_1009：系统管理空间执行exec • k8s_1010：系统管理空间创建Pod • k8s_1011：创建静态Pod • k8s_1012：创建DaemonSet • k8s_1013：创建集群计划任务 • k8s_1014：Secrets操作 • k8s_1015：枚举用户可执行的操作 • k8s_1016：高权限RoleBinding或ClusterRoleBinding • k8s_1017：ServiceAccount创建 • k8s_1018：创建Cronjob • k8s_1019：Pod中exec使用交互式shell • k8s_1020：无权限访问Apiserver • k8s_1021：使用curl访问APIServer • k8s_1022：Ingress漏洞 • k8s_1023：中间人攻击 • k8s_1024：蠕虫挖矿木马 • k8s_1025：K8s事件删除 • k8s_1026：SelfSubjectRulesReview场景 • imgblock_0001：镜像白名单阻断 • imgblock_0002：镜像黑名单阻断 • imgblock_0003：镜像标签白名单阻断 • imgblock_0004：镜像标签黑名单阻断 • imgblock_0005：创建容器白名单阻断 • imgblock_0006：创建容器黑名单阻断 • imgblock_0007：容器mount proc阻断 • imgblock_0008：容器seccomp unconfined阻断 • imgblock_0009：容器特权阻断 • imgblock_0010：容器capabilities阻断

参数	参数类型	描述
event_type	Integer	事件类型，包含如下: ● 1001 : 通用恶意软件 ● 1002 : 病毒 ● 1003 : 蠕虫 ● 1004 : 木马 ● 1005 : 僵尸网络 ● 1006 : 后门 ● 1010 : Rootkit ● 1011 : 勒索软件 ● 1012 ： 黑客工具 ● 1015 : Webshell ● 1016 : 挖矿 ● 1017 : 反弹Shell ● 2001 : 一般漏洞利用 ● 2012 : 远程代码执行 ● 2047 : Redis漏洞利用 ● 2048 : Hadoop漏洞利用 ● 2049 : MySQL漏洞利用 ● 3002 : 文件提权 ● 3003 : 进程提权 ● 3004 : 关键文件变更 ● 3005 : 文件/目录变更 ● 3007 : 进程异常行为 ● 3015 : 高危命令执行 ● 3018 : 异常Shell ● 3027 : Crontab可疑任务 ● 3029 ： 系统安全防护被禁用 ● 3030 ： 备份删除 ● 3031 ： 异常注册表操作 ● 3036 : 容器镜像阻断 ● 4002 : 暴力破解 ● 4004 : 异常登录 ● 4006 : 非法系统账号 ● 4014 : 用户账号添加 ● 4020 : 用户密码窃取 ● 6002 : 端口扫描 ● 6003 : 主机扫描

参数	参数类型	描述
		● 13001 : Kubernetes事件删除 ● 13002 : Pod异常行为 ● 13003 : 枚举用户信息 ● 13004 : 绑定集群用户角色
event_name	String	事件名称
severity	String	威胁等级，包含如下: ● Security : 安全 ● Low : 低危 ● Medium : 中危 ● High : 高危 ● Critical : 危急
container_name	String	容器实例名称
image_name	String	镜像名称
host_name	String	服务器名称
host_id	String	服务器ID
private_ip	String	服务器私有IP
public_ip	String	弹性公网IP地址
os_type	String	操作系统类型，包含如下2种。 ● Linux： Linux。 ● Windows： Windows。
host_status	String	服务器状态，包含如下4种。 ● ACTIVE： 运行中。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。
agent_status	String	Agent状态，包含如下5种。 ● installed： 已安装。 ● not_installed： 未安装。 ● online： 在线。 ● offline： 离线。 ● install_failed： 安装失败。 ● installing： 安装中。

参数	参数类型	描述
protect_status	String	防护状态，包含如下2种。 ● closed： 未防护。 ● opened： 防护中。
asset_value	String	资产重要性，包含如下4种 ● important： 重要资产 ● common： 一般资产 ● test： 测试资产
attack_phase	String	攻击阶段，包含如下： ● reconnaissance : 侦查跟踪 ● weaponization : 武器构建 ● delivery : 载荷投递 ● exploit : 漏洞利用 ● installation : 安装植入 ● command_and_control : 命令与控制 ● actions : 目标达成
attack_tag	String	攻击标识，包含如下： ● attack_success : 攻击成功 ● attack_attempt : 攻击尝试 ● attack_blocked : 攻击被阻断 ● abnormal_behavior : 异常行为 ● collapsible_host : 主机失陷 ● system_vulnerability : 系统脆弱性
occur_time	Integer	发生时间，毫秒
handle_time	Integer	处理时间，毫秒
handle_status	String	处理状态，包含如下: ● unhandled： 未处理 ● handled : 已处理
handle_method	String	处理方式，包含如下: ● mark_as_handled : 手动处理 ● ignore : 忽略 ● add_to_alarm_whitelist : 加入告警白名单 ● add_to_login_whitelist : 加入登录白名单 ● isolate_and_kill : 隔离查杀

参数	参数类型	描述
handler	String	备注信息
operate_accept_list	Array of strings	支持的处理操作
operate_detail_list	Array of **EventDetailResponseInfo** objects	操作详情信息列表（页面不展示）
forensic_info	Object	取证信息，json格式
resource_info	**EventResourceResponseInfo** object	资源信息
geo_info	Object	地理位置信息，json格式
malware_info	Object	恶意软件信息，json格式
network_info	Object	网络信息，json格式
app_info	Object	应用信息，json格式
system_info	Object	系统信息，json格式
extend_info	Object	事件扩展信息，json格式
recommendation	String	处置建议
description	String	告警说明
event_abstract	String	告警摘要
process_info_list	Array of **EventProcessResponseInfo** objects	进程信息列表
user_info_list	Array of **EventUserResponseInfo** objects	用户信息列表
file_info_list	Array of **EventFileResponseInfo** objects	文件信息列表
event_details	String	事件信息的简述
tag_list	Array of strings	标签列表
event_count	Integer	事件发生次数

表 3-55 EventDetailResponseInfo

参数	参数类型	描述
agent_id	String	Agent ID

参数	参数类型	描述
process_pid	Integer	进程id
is_parent	Boolean	是否是父进程
file_hash	String	文件哈希
file_path	String	文件路径
file_attr	String	文件属性
private_ip	String	服务器私有IP
login_ip	String	登录源IP
login_user_name	String	登录用户名
keyword	String	告警事件关键字，仅用于告警白名单
hash	String	告警事件hash，仅用于告警白名单

表 3-56 EventResourceResponseInfo

参数	参数类型	描述
domain_id	String	租户账号ID
project_id	String	项目ID
enterprise_project_id	String	企业项目ID
region_name	String	Region名称
vpc_id	String	VPC ID
cloud_id	String	云主机ID
vm_name	String	虚拟机名称
vm_uuid	String	虚拟机UUID
container_id	String	容器ID
container_status	String	容器状态
pod_uid	String	pod uid
pod_name	String	pod name
namespace	String	namespace
cluster_id	String	集群id
cluster_name	String	集群名称
image_id	String	镜像ID

参数	参数类型	描述
image_name	String	镜像名称
host_attr	String	主机属性
service	String	业务服务
micro_service	String	微服务
sys_arch	String	系统CPU架构
os_bit	String	操作系统位数
os_type	String	操作系统类型
os_name	String	操作系统名称
os_version	String	操作系统版本

表 3-57 EventProcessResponseInfo

参数	参数类型	描述
process_name	String	进程名称
process_path	String	进程文件路径
process_pid	Integer	进程id
process_uid	Integer	进程用户id
process_username	String	运行进程的用户名
process_cmdline	String	进程文件命令行
process_filename	String	进程文件名
process_start_time	Long	进程启动时间
process_gid	Integer	进程组ID
process_egid	Integer	进程有效组ID
process_euid	Integer	进程有效用户ID
parent_process_name	String	父进程名称
parent_process_path	String	父进程文件路径
parent_process_pid	Integer	父进程id
parent_process_uid	Integer	父进程用户id

参数	参数类型	描述
parent_process_cmdline	String	父进程文件命令行
parent_process_filename	String	父进程文件名
parent_process_start_time	Long	父进程启动时间
parent_process_gid	Integer	父进程组ID
parent_process_egid	Integer	父进程有效组ID
parent_process_euid	Integer	父进程有效用户ID
child_process_name	String	子进程名称
child_process_path	String	子进程文件路径
child_process_pid	Integer	子进程id
child_process_uid	Integer	子进程用户id
child_process_cmdline	String	子进程文件命令行
child_process_filename	String	子进程文件名
child_process_start_time	Long	子进程启动时间
child_process_gid	Integer	子进程组ID
child_process_egid	Integer	子进程有效组ID
child_process_euid	Integer	子进程有效用户ID
virt_cmd	String	虚拟化命令
virt_process_name	String	虚拟化进程名称
escape_mode	String	逃逸方式
escape_cmd	String	逃逸后后执行的命令
process_hash	String	进程启动文件hash

表 3-58 EventUserResponseInfo

参数	参数类型	描述
user_id	Integer	用户uid
user_gid	Integer	用户gid
user_name	String	用户名称
user_group_name	String	用户组名称
user_home_dir	String	用户home目录
login_ip	String	用户登录ip
service_type	String	登录的服务类型
service_port	Integer	登录服务端口
login_mode	Integer	登录方式
login_last_time	Long	用户最后一次登录时间
login_fail_count	Integer	用户登录失败次数
pwd_hash	String	口令hash
pwd_with_fuzzing	String	匿名化处理后的口令
pwd_used_days	Integer	密码使用的天数
pwd_min_days	Integer	口令的最短有效期限
pwd_max_days	Integer	口令的最长有效期限
pwd_warn_left_days	Integer	口令无效时提前告警天数

表 3-59 EventFileResponseInfo

参数	参数类型	描述
file_path	String	文件路径
file_alias	String	文件别名
file_size	Integer	文件大小
file_mtime	Long	文件最后一次修改时间
file_atime	Long	文件最后一次访问时间
file_ctime	Long	文件最后一次状态改变时间
file_hash	String	文件hash
file_md5	String	文件md5

参数	参数类型	描述
file_sha256	String	文件sha256
file_type	String	文件类型
file_content	String	文件内容
file_attr	String	文件属性
file_operation	Integer	文件操作类型
file_action	String	文件动作
file_change_attr	String	变更前后的属性
file_new_path	String	新文件路径
file_desc	String	文件描述
file_key_word	String	文件关键字
is_dir	Boolean	是否目录
fd_info	String	文件句柄信息
fd_count	Integer	文件句柄数量

请求示例

查询前50条企业项目为xxx下未处理的主机事件信息

```
GET https://{endpoint}/v5/{project_id}/event/events?
offset=0&limit=50&handle_status=unhandled&category=host&enterprise_project_id=xxx
```

响应示例

状态码：200

入侵事件列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "attack_phase" : "exploit",
    "attack_tag" : "abnormal_behavior",
    "event_class_id" : "lgin_1002",
    "event_id" : "d8a12cf7-6a43-4cd6-92b4-aabf1e917",
    "event_name" : "different locations",
    "event_type" : 4004,
    "forensic_info" : {
      "country" : "中国",
      "city" : "兰州市",
      "ip" : "127.0.0.1",
      "user" : "zhangsan",
      "sub_division" : "甘肃省",
      "city_id" : 3110
    },
    "handle_status" : "unhandled",
    "host_name" : "xxx",
    "occur_time" : 1661593036627,
```

```
  "operate_accept_list" : [ "ignore" ],
  "operate_detail_list" : [ {
    "agent_id" : "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
    "file_hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "file_path" : "/usr/test",
    "process_pid" : 3123,
    "file_attr" : 33261,
    "keyword" : "file_path=/usr/test",
    "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "login_ip" : "127.0.0.1",
    "private_ip" : "127.0.0.2",
    "login_user_name" : "root",
    "is_parent" : false
  } ],
  "private_ip" : "127.0.0.1",
  "resource_info" : {
    "region_name" : "",
    "project_id" : "",
    "enterprise_project_id" : "0",
    "os_type" : "Linux",
    "os_version" : "2.5",
    "vm_name" : "",
    "vm_uuid" : "71a15ecc",
    "cloud_id" : "",
    "container_id" : "",
    "container_status" : "running / terminated",
    "image_id" : "",
    "pod_uid" : "",
    "pod_name" : "",
    "namespace" : "",
    "cluster_id" : "",
    "cluster_name" : ""
  },
  "severity" : "Medium",
  "extend_info" : "",
  "os_type" : "Linux",
  "agent_status" : "online",
  "asset_value" : "common",
  "protect_status" : "opened",
  "host_status" : "ACTIVE",
  "event_details" : "file_path:/root/test",
  "user_info_list" : [ {
    "login_ip" : "",
    "service_port" : 22,
    "service_type" : "ssh",
    "user_name" : "zhangsan",
    "login_mode" : 0,
    "login_last_time" : 1661593024,
    "login_fail_count" : 0
  } ],
  "description" : "",
  "event_abstract" : "",
  "tag_list" : [ "热点事件" ]
 } ]
}
```


状态码

状态码	描述
200	入侵事件列表

错误码

请参见**错误码**。

3.2.3 查询告警白名单列表

功能介绍

查询告警白名单列表

URI

GET /v5/{project_id}/event/white-list/alarm

表 3-60 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

表 3-61 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
hash	否	String	SHA256

参数	是否必选	参数类型	描述
event_type	否	Integer	事件类型，包含如下: ● 1001：通用恶意软件 ● 1002：病毒 ● 1003：蠕虫 ● 1004：木马 ● 1005：僵尸网络 ● 1006：后门 ● 1010：Rootkit ● 1011：勒索软件 ● 1012： 黑客工具 ● 1015：Webshell ● 1016：挖矿 ● 1017：反弹Shell ● 2001：一般漏洞利用 ● 2012：远程代码执行 ● 2047：Redis漏洞利用 ● 2048：Hadoop漏洞利用 ● 2049：MySQL漏洞利用 ● 3002：文件提权 ● 3003：进程提权 ● 3004：关键文件变更 ● 3005：文件/目录变更 ● 3007：进程异常行为 ● 3015：高危命令执行 ● 3018：异常Shell ● 3027：Crontab可疑任务 ● 3029： 系统安全防护被禁用 ● 3030： 备份删除 ● 3031： 异常注册表操作 ● 3036：容器镜像阻断 ● 4002：暴力破解 ● 4004：异常登录 ● 4006：非法系统账号 ● 4014：用户账号添加 ● 4020：用户密码窃取 ● 6002：端口扫描 ● 6003：主机扫描

参数	是否必选	参数类型	描述
			• 13001：Kubernetes事件删除 • 13002：Pod异常行为 • 13003：枚举用户信息 • 13004：绑定集群用户角色
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

请求参数

表 3-62 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）

响应参数

状态码：200

表 3-63 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
event_type_list	Array of integers	支持筛选的事件类型
data_list	Array of **AlarmWhiteListResponseInfo** objects	告警白名单详情

表 3-64 AlarmWhiteListResponseInfo

参数	参数类型	描述
enterprise_project_name	String	企业项目名称
hash	String	SHA256
description	String	描述信息

参数	参数类型	描述
event_type	Integer	事件类型，包含如下: ● 1001 : 通用恶意软件 ● 1002 : 病毒 ● 1003 : 蠕虫 ● 1004 : 木马 ● 1005 : 僵尸网络 ● 1006 : 后门 ● 1010 : Rootkit ● 1011 : 勒索软件 ● 1012 ： 黑客工具 ● 1015 : Webshell ● 1016 : 挖矿 ● 1017 : 反弹Shell ● 2001 : 一般漏洞利用 ● 2012 : 远程代码执行 ● 2047 : Redis漏洞利用 ● 2048 : Hadoop漏洞利用 ● 2049 : MySQL漏洞利用 ● 3002 : 文件提权 ● 3003 : 进程提权 ● 3004 : 关键文件变更 ● 3005 : 文件/目录变更 ● 3007 : 进程异常行为 ● 3015 : 高危命令执行 ● 3018 : 异常Shell ● 3027 : Crontab可疑任务 ● 3029 ： 系统安全防护被禁用 ● 3030 ： 备份删除 ● 3031 ： 异常注册表操作 ● 3036 : 容器镜像阻断 ● 4002 : 暴力破解 ● 4004 : 异常登录 ● 4006 : 非法系统账号 ● 4014 : 用户账号添加 ● 4020 : 用户密码窃取 ● 6002 : 端口扫描 ● 6003 : 主机扫描

参数	参数类型	描述
		● 13001 : Kubernetes事件删除 ● 13002 : Pod异常行为 ● 13003 : 枚举用户信息 ● 13004 : 绑定集群用户角色
white_field	String	加白字段，包含如下: ● "file/process hash" # 进程/文件hash ● "file_path" # 文件路径 ● "process_path" # 进程路径 ● "login_ip" # 登录ip ● "reg_key" #注册表key ● "process_cmdline" # 进程命令行 ● "username" # 用户名
field_value	String	加白字段值
judge_type	String	通配符，包含如下: ● "equal" # 相等 ● "contain" # 包含
update_time	Integer	更新时间，毫秒

请求示例

查询前10条企业项目为xxx下的告警白名单列表

```
GET https://{endpoint}/v5/{project_id}/event/white-list/alarm?limit=10&offset=0&enterprise_project_id=xxx
```

响应示例

状态码：200

告警白名单列表

```
{
  "data_list" : [ {
    "enterprise_project_name" : "所有项目",
    "event_type" : 1001,
    "hash" : "9ab079e5398cba3a368ccffbd478f54c5ec3edadf6284ec049a73c36419f1178",
    "description" : "/opt/cloud/3rdComponent/install/jre-8u201/bin/java",
    "update_time" : 1665715677307,
    "white_field" : "process/file hash",
    "judge_type" : "contain",
    "field_value" : "abcd12345612311112212323"
  } ],
  "event_type_list" : [ 1001 ],
  "total_num" : 1
}
```

状态码

状态码	描述
200	告警白名单列表

错误码

请参见**错误码**。

3.3 资产管理

3.3.1 统计资产信息，账号、端口、进程等

功能介绍

资产统计信息，账号、端口、进程等

URI

GET /v5/{project_id}/asset/statistics

表 3-65 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id

表 3-66 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_id	否	String	host id
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-67 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-68 响应 Body 参数

参数	参数类型	描述
account_num	Long	账号数量
port_num	Long	开放端口数量
process_num	Long	进程数量
app_num	Long	软件数量
auto_launch_num	Long	自启动数量
web_framework_num	Long	web框架数量
web_site_num	Long	Web站点数量
jar_package_num	Long	Jar包数量
kernel_module_num	Long	内核模块数量
web_service_num	Long	web服务数量
web_app_num	Long	web应用数量
database_num	Long	数据库数量

请求示例

查询主机的指纹信息，账号、端口、进程等的统计数量

```
GET https://{endpoint}/v5/{project_id}/asset/statistics?category=host
```

响应示例

状态码：200

Asset statistic info

```
{
  "account_num" : 5,
```

```
  "port_num" : 5,
  "process_num" : 5,
  "app_num" : 5,
  "auto_launch_num" : 5,
  "web_framework_num" : 5,
  "web_site_num" : 5,
  "jar_package_num" : 5,
  "kernel_module_num" : 5,
  "core_conf_file_num" : 1,
  "database_num" : 1,
  "environment_num" : 0,
  "web_app_num" : 8,
  "web_service_num" : 2
}
```


状态码

状态码	描述
200	Asset statistic info

错误码

请参见**错误码**。

3.3.2 查询账号信息列表

功能介绍

查询账号信息列表，支持通过传入账号名称参数查询对应的服务器数

URI

GET /v5/{project_id}/asset/user/statistics

表 3-69 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id

表 3-70 Query 参数

参数	是否必选	参数类型	描述
user_name	否	String	账号名称，参考windows文件命名规则，支持字母、数字、下划线、中文，特殊字符!@.-等，不包括中文标点符号
enterprise_project_id	否	String	企业项目

参数	是否必选	参数类型	描述
limit	否	Integer	默认10
offset	否	Integer	默认是0
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-71 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-72 响应 Body 参数

参数	参数类型	描述
total_num	Integer	账号总数
data_list	Array of **UserStatisticInfoResponseInfo** objects	账户统计信息列表

表 3-73 UserStatisticInfoResponseInfo

参数	参数类型	描述
user_name	String	账号名称
num	Integer	账号数量

请求示例

默认查询前10条账号信息列表

```
GET https://{endpoint}/v5/{project_id}/asset/user/statistics
```

响应示例

状态码：200

具备该账号的主机数量

```
{
  "total_num" : 1,
  "data_list" : [ {
    "user_name" : "bin",
    "num" : 5
  } ]
}
```

状态码

状态码	描述
200	具备该账号的主机数量

错误码

请参见**错误码**。

3.3.3 查询开放端口统计信息

功能介绍

查询开放端口列表，支持通过传入端口或协议类型查询服务器数

URI

GET /v5/{project_id}/asset/port/statistics

表 3-74 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id

表 3-75 Query 参数

参数	是否必选	参数类型	描述
port	否	Integer	端口号，精确匹配
port_string	否	String	端口字符串，用来进行模糊匹配
type	否	String	端口类型
enterprise_project_id	否	String	企业项目

参数	是否必选	参数类型	描述
sort_key	否	String	排序的key值，目前支持按照端口号port排序
sort_dir	否	String	升序还是降序，默认升序，asc
limit	否	Integer	默认10
offset	否	Integer	默认是0
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-76 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-77 响应 Body 参数

参数	参数类型	描述
total_num	Integer	开放端口总数
data_list	Array of **PortStatisticResponseInfo** objects	开放端口统计信息列表

表 3-78 PortStatisticResponseInfo

参数	参数类型	描述
port	Integer	端口号
type	String	类型
num	Integer	端口数量
status	String	危险类型:danger/unknown

请求示例

默认查询前10条端口为123，类别为主机的开放端口列表

```
GET https://{endpoint}/v5/{project_id}/asset/port/statistics?port=123&category=host
```

响应示例

状态码：200

返回端口信息，端口号、类型、数量、危险状态

```
{
  "total_num" : 1,
  "data_list" : [ {
    "num" : 4,
    "port" : 123,
    "type" : "UDP",
    "status" : "danger"
  } ]
}
```

状态码

状态码	描述
200	返回端口信息，端口号、类型、数量、危险状态

错误码

请参见**错误码**。

3.3.4 查询进程列表

功能介绍

查询进程列表，通过传入进程路径参数查询对应的服务器数

URI

GET /v5/{project_id}/asset/process/statistics

表 3-79 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-80 Query 参数

参数	是否必选	参数类型	描述
path	否	String	路径
enterprise_project_id	否	String	企业项目
limit	否	Integer	默认10
offset	否	Integer	默认是0
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-81 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-82 响应 Body 参数

参数	参数类型	描述
total_num	Integer	进程统计信息总数,
data_list	Array of **ProcessStatisticResponseInfo** objects	进程统计信息列表

表 3-83 ProcessStatisticResponseInfo

参数	参数类型	描述
path	String	进程名称
num	Integer	进程数量

请求示例

默认查询前10条类别为主机的进程列表

```
GET https://{endpoint}/v5/{project_id}/asset/process/statistics?category=host
```

响应示例

状态码：200

具备该进程的主机数量

```
{
  "total_num" : 1,
  "data_list" : [ {
    "num" : 13,
    "path" : "/usr/lib/systemd/systemd-journald"
  } ]
}
```

状态码

状态码	描述
200	具备该进程的主机数量

错误码

请参见**错误码**。

3.3.5 查询软件列表

功能介绍

查询软件列表，支持通过软件名称查询对应的服务器数

URI

GET /v5/{project_id}/asset/app/statistics

表 3-84 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-85 Query 参数

参数	是否必选	参数类型	描述
app_name	否	String	软件名称

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
limit	否	Integer	默认10
offset	否	Integer	偏移量，为页数*每页显示条数
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-86 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-87 响应 Body 参数

参数	参数类型	描述
total_num	Integer	进程统计信息总数,
data_list	Array of **AppStatisticResponseInfo** objects	进程统计信息列表

表 3-88 AppStatisticResponseInfo

参数	参数类型	描述
app_name	String	软件名称
num	Integer	进程数量

请求示例

默认查询前10条类别为主机的软件列表

```
GET https://{endpoint}/v5/{project_id}/asset/app/statistics?category=host
```

响应示例

状态码：200

具备该软件的主机数量

```
{
  "total_num" : 1,
  "data_list" : [ {
    "app_name" : "kernel",
    "num" : 13
  } ]
}
```

状态码

状态码	描述
200	具备该软件的主机数量

错误码

请参见**错误码**。

3.3.6 查询自启动项信息

功能介绍

查询自启动信息，支持通过传入自启动名称查询启动类型和服务器数

URI

GET /v5/{project_id}/asset/auto-launch/statistics

表 3-89 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-90 Query 参数

参数	是否必选	参数类型	描述
name	否	String	自启动项名称
type	否	String	自启动项类型
enterprise_project_id	否	String	企业项目

参数	是否必选	参数类型	描述
limit	否	Integer	默认10
offset	否	Integer	默认是0

请求参数

表 3-91 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-92 响应 Body 参数

参数	参数类型	描述
total_num	Integer	自启动项统计信息总数,
data_list	Array of **AutoLaunchStatisticsResponseInfo** objects	自启动项统计信息列表

表 3-93 AutoLaunchStatisticsResponseInfo

参数	参数类型	描述
name	String	自启动项名称
type	String	自启动项类型
num	Integer	数量

请求示例

默认查询前10条自启动项列表

```
GET https://{endpoint}/v5/{project_id}/asset/auto-launch/statistics
```

响应示例

状态码：200

具备该进程的主机数量

```
{
  "total_num" : 1,
  "data_list" : [ {
    "name" : "S12hostguard",
    "type" : "0",
    "num" : 5
  } ]
}
```

状态码

状态码	描述
200	具备该进程的主机数量

错误码

请参见**错误码**。

3.3.7 查询账号的服务器列表

功能介绍

查询账号的服务器列表

URI

GET /v5/{project_id}/asset/users

表 3-94 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

表 3-95 Query 参数

参数	是否必选	参数类型	描述
host_id	否	String	服务器ID
user_name	否	String	账号名称
host_name	否	String	服务器名称
private_ip	否	String	服务器私有IP
login_permission	否	Boolean	是否允许登录

参数	是否必选	参数类型	描述
root_permission	否	Boolean	是否有root权限
user_group	否	String	用户组
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
limit	否	Integer	默认10
offset	否	Integer	默认是0
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器
part_match	否	Boolean	是否模糊匹配，默认false表示精确匹配

请求参数

表 3-96 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）

响应参数

状态码：200

表 3-97 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数,
data_list	Array of **UserResponseInfo** objects	账号信息列表

表 3-98 UserResponseInfo

参数	参数类型	描述
agent_id	String	agent_id
host_id	String	服务器ID
host_name	String	服务器名称
host_ip	String	服务器ip
user_name	String	用户名
login_permission	Boolean	是否有登录权限
root_permission	Boolean	是否有root权限
user_group_name	String	用户组
user_home_dir	String	用户目录
shell	String	用户启动shell
expire_time	Long	到期时间，采用时间戳，默认毫秒，
recent_scan_time	Long	最近扫描时间
container_id	String	容器id
container_name	String	容器名称

请求示例

默认查询账号为daemon的服务器列表

```
GET https://{endpoint}/v5/{project_id}/asset/users?user_name=daemon
```

响应示例

状态码：200

账号信息列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxece69",
    "host_ip" : "192.168.0.1",
    "host_name" : "test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_home_dir" : "/bin",
    "user_name" : "bin",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6"
```

```
 }]
}
```

状态码

状态码	描述
200	账号信息列表

错误码

请参见**错误码**。

3.3.8 查询单服务器的开放端口列表

功能介绍

查询单服务器的开放端口列表

URI

GET /v5/{project_id}/asset/ports

表 3-99 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-100 Query 参数

参数	是否必选	参数类型	描述
host_id	是	String	主机id
host_name	否	String	主机名称
host_ip	否	String	主机ip
port	否	Integer	端口号
type	否	String	端口类型
enterprise_project_id	否	String	企业项目
limit	否	Integer	默认10
offset	否	Integer	默认是0

参数	是否必选	参数类型	描述
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器

请求参数

表 3-101 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-102 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of PortResponseInfo objects	端口信息列表

表 3-103 PortResponseInfo

参数	参数类型	描述
host_id	String	主机id
laddr	String	监听ip
status	String	port status, normal, danger or unknow • "normal" : 正常 • "danger" : 危险 • "unknow" : 未知
port	Integer	端口号
type	String	类型
pid	Integer	进程ID

参数	参数类型	描述
path	String	程序文件

请求示例

默认查询前10条host_id为dd91cd32-a238-4c0e-bc01-3b11653714ac的开放端口列表

```
GET https://{endpoint}/v5/{project_id}/asset/ports?hlimit=10&offset=0&host_id=dd91cd32-a238-4c0e-bc01-3b11653714ac
```

响应示例

状态码：200

端口信息列表

```
{
  "data_list" : [ {
    "agent_id" : "eb5d03f02fffd85aaf5d0ba5c992d97713244f420e0b076dcf6ae0574c78aa4b",
    "container_id" : "",
    "host_id" : "dd91cd32-a238-4c0e-bc01-3b11653714ac",
    "laddr" : "0.0.0.0",
    "path" : "/usr/sbin/dhclient",
    "pid" : 1507,
    "port" : 68,
    "status" : "unknow",
    "type" : "UDP"
  }, {
    "agent_id" : "eb5d03f02fffd85aaf5d0ba5c992d97713244f420e0b076dcf6ae0574c78aa4b",
    "container_id" : "",
    "host_id" : "dd91cd32-a238-4c0e-bc01-3b11653714ac",
    "laddr" : "127.0.0.1",
    "path" : "/usr/sbin/chronyd",
    "pid" : 493,
    "port" : 323,
    "status" : "unknow",
    "type" : "UDP"
  } ],
  "total_num" : 2
}
```

状态码

状态码	描述
200	端口信息列表

错误码

请参见**错误码**。

3.3.9 查询软件的服务器列表

功能介绍

查询软件的服务器列表

URI

GET /v5/{project_id}/asset/apps

表 3-104 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-105 Query 参数

参数	是否必选	参数类型	描述
host_id	否	String	主机id
host_name	否	String	主机名称
app_name	否	String	软件名称
host_ip	否	String	主机ip
version	否	String	版本号
install_dir	否	String	安装目录
enterprise_project_id	否	String	企业项目
limit	否	Integer	默认10
offset	否	Integer	默认是0
category	否	String	类别，默认为host，包含如下： ● host：主机 ● container：容器
part_match	否	Boolean	是否模糊匹配，默认false表示精确匹配

请求参数

表 3-106 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-107 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of AppResponseInfo objects	软件列表

表 3-108 AppResponseInfo

参数	参数类型	描述
agent_id	String	agent_id
host_id	String	主机id
host_name	String	服务器名称
host_ip	String	服务器ip
app_name	String	软件名称
version	String	版本号
update_time	Long	更新时间
recent_scan_time	Long	最近扫描时间
container_id	String	容器id
container_name	String	容器名称

请求示例

默认查询前10条软件名称为acl的服务器列表

```
GET https://{endpoint}/v5/{project_id}/asset/apps?app_name=acl
```

响应示例

状态码：200

单台主机安装的app

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
    "host_id" : "55dac7fe-d81b-43bc-a4a7-4710fe673972",
    "host_name" : "xxxx",
    "host_ip" : "192.168.0.126",
    "app_name" : "acl",
    "version" : "2.2.51-14.eulerosv2r7",
    "update_time" : 1668150671981,
    "recent_scan_time" : 1668506044147,
```

```
    "container_id" : "ce794b8a6071f5fd7e4d142dab7b36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6"
  } ]
}
```

状态码

状态码	描述
200	单台主机安装的app

错误码

请参见**错误码**。

3.3.10 查询自启动项的服务列表

功能介绍

查询自启动项的服务列表

URI

GET /v5/{project_id}/asset/auto-launchs

表 3-109 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id

表 3-110 Query 参数

参数	是否必选	参数类型	描述
host_id	否	String	主机id
host_name	否	String	主机名称
name	否	String	自启动项名称
host_ip	否	String	主机ip
type	否	String	自启动项类型
enterprise_project_id	否	String	企业项目
limit	否	Integer	默认10
offset	否	Integer	默认是0

参数	是否必选	参数类型	描述
part_match	否	Boolean	是否模糊匹配，默认false表示精确匹配

请求参数

表 3-111 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-112 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **AutoLauchResponseInfo** objects	自启动项列表

表 3-113 AutoLauchResponseInfo

参数	参数类型	描述
agent_id	String	agent_id
host_id	String	主机id
host_name	String	服务器名称
host_ip	String	服务器ip
name	String	自启动项名称
type	Integer	自启动项类型
path	String	路径
hash	String	文件hash
run_user	String	运行用户
recent_scan_time	Long	最近扫描时间

请求示例

默认查询前10条自启动项名称为S50multi-queue的服务列表

```
GET https://{endpoint}/v5/{project_id}/asset/auto-launchs?name=S50multi-queue
```

响应示例

状态码：200

auto launch list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "9e742932bff2894e3d0869d03989b05cefb27a6cbc201d98c4465296xxxxxxxx",
    "host_id" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "host_name" : "name",
    "host_ip" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "name" : "S12hostguard",
    "type" : 0,
    "path" : "/etc/hostguard",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxx",
    "run_user" : "user",
    "recent_scan_time" : 1668240858425
  } ]
}
```

状态码

状态码	描述
200	auto launch list

错误码

请参见**错误码**。

3.3.11 获取账户变动历史信息

功能介绍

获取账户变动历史记录信息

URI

GET /v5/{project_id}/asset/user/change-history

表 3-114 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-115 Query 参数

参数	是否必选	参数类型	描述
user_name	否	String	账号名
host_id	否	String	主机id
root_permission	否	Boolean	是否有root权限
host_name	否	String	主机名称
private_ip	否	String	服务器私有IP
change_type	否	String	变更类型: ● ADD： 添加 ● DELETE： 删除 ● MODIFY： 修改
limit	否	Integer	默认10
offset	否	Integer	默认是0
enterprise_project_id	否	String	企业项目
start_time	否	Long	变更开始时间，13位时间戳
end_time	否	Long	变更结束时间，13位时间戳

请求参数

表 3-116 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-117 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数

参数	参数类型	描述
data_list	Array of **UserChangeHistoryResponseInfo** objects	账号历史变动记录列表

表 3-118 UserChangeHistoryResponseInfo

参数	参数类型	描述
agent_id	String	Agent ID
change_type	String	变更类型 • ADD： 添加 • DELETE： 删除 • MODIFY： 修改
host_id	String	服务器ID
host_name	String	服务器名称
private_ip	String	服务器私有IP
login_permission	Boolean	是否有登录权限
root_permission	Boolean	是否有root权限
user_group_name	String	用户组
user_home_dir	String	用户目录
shell	String	用户启动shell
user_name	String	账号名称
expire_time	Long	到期时间，采用时间戳，默认毫秒，
recent_scan_time	Long	变更时间

请求示例

默认查询前10条开始时间为1700446129130，结束时间为1701050929130的账户变动历史记录信息

```
GET https://{endpoint}/v5/{project_id}/asset/user/change-history?
start_time=1700446129130&end_time=1701050929130
```

响应示例

状态码：200

账号历史变动记录列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxxece69",
    "private_ip" : "192.168.0.1",
    "host_name" : "test",
    "user_home_dir" : "/test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_name" : "bin",
    "change_type" : "test"
  } ]
}
```

状态码

状态码	描述
200	账号历史变动记录列表

错误码

请参见**错误码**。

3.3.12 获取软件信息的历史变动记录

功能介绍

获取软件信息的历史变动记录

URI

GET /v5/{project_id}/asset/app/change-history

表 3-119 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-120 Query 参数

参数	是否必选	参数类型	描述
host_id	否	String	主机id
host_ip	否	String	主机ip
host_name	否	String	主机名称

参数	是否必选	参数类型	描述
app_name	否	String	软件名称
variation_type	否	String	变更类型: • add： 新建 • delete： 删除 • modify： 修改
enterprise_project_id	否	String	企业项目
sort_key	否	String	排序的key值
sort_dir	否	String	升序还是降序，默认升序，asc
limit	否	Integer	默认10
offset	否	Integer	默认是0
start_time	否	Long	变更开始时间，13位时间戳
end_time	否	Long	变更结束时间，13位时间戳

请求参数

表 3-121 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-122 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数,
data_list	Array of **AppChangeResponseInfo** objects	软件历史变动记录列表

表 3-123 AppChangeResponseInfo

参数	参数类型	描述
agent_id	String	agent_id
variation_type	String	the type of change ● add： 新建 ● delete： 删除 ● modify： 修改
host_id	String	host_id
app_name	String	软件名称
host_name	String	弹性服务器名称
host_ip	String	服务器ip
version	String	版本号
update_time	Long	更新时间
recent_scan_time	Long	变更时间

请求示例

默认查询前10条开始时间为1700446175490，结束时间为1701050975490的软件信息的历史变动记录

```
GET https://{endpoint}/v5/{project_id}/asset/app/change-history?
start_time=1700446175490&end_time=1701050975490
```

响应示例

状态码：200

App change history info list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxxx",
    "variation_type" : "abnormal_behavior",
    "host_id" : "f4aaca51-xxxx-xxxx-xxxx-891c9e84d885",
    "app_name" : "hostguard",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "version" : "3.2.3",
    "update_time" : 1668246126302,
    "recent_scan_time" : 1668246126302
  } ]
}
```

状态码

状态码	描述
200	App change history info list

错误码

请参见**错误码**。

3.3.13 获取自启动项的历史变动记录

功能介绍

获取自启动项的历史变动记录

URI

GET /v5/{project_id}/asset/auto-launch/change-history

表 3-124 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-125 Query 参数

参数	是否必选	参数类型	描述
host_id	否	String	主机id
host_ip	否	String	主机ip
host_name	否	String	主机名称
auto_launch_name	否	String	自启动项名称
type	否	Integer	自启动项类型 • 0： 自启动服务 • 1： 定时任务 • 2： 预加载动态库 • 3： Run注册表键 • 4： 开机启动文件夹

参数	是否必选	参数类型	描述
variation_type	否	String	变更类型: • add： 新建 • delete： 删除 • modify： 修改
enterprise_project_id	否	String	企业项目
sort_key	否	String	排序的key值
sort_dir	否	String	升序还是降序，默认升序，asc
limit	否	Integer	默认10
offset	否	Integer	默认是0
start_time	否	Long	变更开始时间，13位时间戳
end_time	否	Long	变更结束时间，13位时间戳

请求参数

表 3-126 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-127 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **AutoLaunchChangeResponseInfo** objects	软件历史变动记录列表

表 3-128 AutoLaunchChangeResponseInfo

参数	参数类型	描述
agent_id	String	agent_id
variation_type	String	the type of change ● add： 新建 ● delete： 删除 ● modify： 修改
type	Integer	自启动项类型
host_id	String	host_id
host_name	String	弹性服务器名称
host_ip	String	主机IP
path	String	路径
hash	String	文件hash
run_user	String	运行用户
name	String	自启动项名称
recent_scan_time	Long	最近更新时间

请求示例

默认查询前10条开始时间为1693101881568，结束时间为1701050681569的自启动项的历史变动记录

```
GET https://{endpoint}/v5/{project_id}/asset/auto-launch/change-history?
start_time=1693101881568&end_time=1701050681569
```

响应示例

状态码：200

App change history info list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxxx",
    "variation_type" : "abnormal_behavior",
    "type" : 0,
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "path" : "/path",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxx",
    "run_user" : 1668246126302,
    "name" : 1668246126302,
    "recent_scan_time" : 1668246126302
  } ]
}
```

状态码

状态码	描述
200	App change history info list

错误码

请参见错误码。

3.3.14 资产指纹-进程-服务器列表

功能介绍

具备该进程的主机/容器信息

URI

GET /v5/{project_id}/asset/processes/detail

表 3-129 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-130 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_name	否	String	主机名称
host_ip	否	String	主机ip
path	否	String	进程路径
category	否	String	类型，默认为host，包含如下： • host：主机 • container：容器
limit	否	Integer	默认10
offset	否	Integer	默认是0

请求参数

表 3-131 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-132 响应 Body 参数

参数	参数类型	描述
total_num	Integer	主机统计信息总数,
data_list	Array of **ProcessesHostResponseInfo** objects	主机统计信息列表

表 3-133 ProcessesHostResponseInfo

参数	参数类型	描述
hash	String	文件hash
host_ip	String	主机ip
host_name	String	主机名称
launch_params	String	启动参数
launch_time	Long	启动时间
process_path	String	进程路径
process_pid	Integer	进程pid
run_permission	String	文件权限
container_id	String	容器id
container_name	String	容器名称

请求示例

默认查询前10条进程路径为/usr/bin/bash的主机列表

```
GET https://{endpoint}/v5/{project_id}/asset/processes/detail?path=/usr/bin/bash
```

响应示例

状态码：200

具备该进程的主机信息

```
{
  "total_num" : 1,
  "data_list" : [ {
    "hash" : "xxxxxx96a7ceb67731c0158xxxxxxff8456914d8275d221671d1190e888xxxxx",
    "host_ip" : "192.168.0.1",
    "host_name" : "ecs-euler-z00800211",
    "launch_params" : "",
    "launch_time" : 1673504622000,
    "process_path" : "/CloudResetPwdUpdateAgent/bin/wrapper",
    "process_pid" : 888,
    "run_permission" : "rwx------",
    "container_id" : "ce794b8a6071f5fd7e4d142dab7b36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6"
  } ]
}
```

状态码

状态码	描述
200	具备该进程的主机信息

错误码

请参见**错误码**。

3.3.15 资产指纹-端口-服务器列表

功能介绍

具备该端口的主机/容器信息

URI

GET /v5/{project_id}/asset/ports/detail

表 3-134 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-135 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_name	否	String	主机名称
host_ip	否	String	主机ip
port	是	Integer	端口号
type	否	String	端口类型
category	否	String	类别，默认为host，包含如下： • host：主机 • container：容器
limit	否	Integer	默认10
offset	否	Integer	默认是0

请求参数

表 3-136 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

响应参数

状态码：200

表 3-137 响应 Body 参数

参数	参数类型	描述
total_num	Integer	机器总数
data_list	Array of **PortHostResponseInfo** objects	机器信息列表

表 3-138 PortHostResponseInfo

参数	参数类型	描述
container_id	String	镜像id
host_id	String	主机id
host_ip	String	主机ip
host_name	String	主机名称
laddr	String	监听ip
path	String	程序文件路径
pid	Integer	pid
port	Integer	端口
status	String	状态
type	String	类型
container_name	String	容器名称
agent_id	String	agent id

请求示例

默认查询前10条端口为22的主机列表

```
GET https://{endpoint}/v5/{project_id}/asset/ports/detail?port=22
```

响应示例

状态码：200

具备该端口的主机信息

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "03117200-xxxx-xxxx-xxxx-a89a10e66dbe",
    "host_ip" : "192.168.0.1",
    "host_name" : "ecs-eule",
    "laddr" : "0.0.0.0",
    "path" : "C:\\Windows\\system32\\svchost.exe",
    "process_path" : "/CloudResetPwdUpdateAgent/bin/wrapper",
    "port" : 888,
    "status" : "unknow",
    "type" : "UDP",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6",
    "agent_id" : "03jjj-xxxx-xxxx-wwwsedf"
  } ]
}
```

状态码

状态码	描述
200	具备该端口的主机信息

错误码

请参见**错误码**。

3.3.16 查询中间件列表

功能介绍

查询中间件列表，支持通过中间件名称查询对应的服务器树

URI

GET /v5/{project_id}/asset/midwares

表 3-139 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-140 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID
file_name	否	String	jar包名称
category	否	String	类别，包含如下: • host : 主机 • container : 容器
limit	否	Integer	默认10
offset	否	Integer	默认是0

请求参数

表 3-141 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）

响应参数

状态码：200

表 3-142 响应 Body 参数

参数	参数类型	描述
total_num	Integer	Jar包统计信息总数
data_list	Array of **JarPackageStatisticsResponseInfo** objects	Jar包统计信息列表

表 3-143 JarPackageStatisticsResponseInfo

参数	参数类型	描述
file_name	String	Jar包名称
num	Integer	Jar包统计信息总数

请求示例

默认查询前10条中间件名称为rt.jar，类别为主机的中间件列表

```
GET https://{endpoint}/v5/{project_id}/asset/midwares?file_name=rt.jar&category=host
```

响应示例

状态码：200

JarPackage statistics

```
{
  "data_list" : [ {
    "file_name" : "rt.jar",
    "num" : 18
  } ],
```

```
  "total_num" : 1
}
```

状态码

状态码	描述
200	JarPackage statistics

错误码

请参见**错误码**。

3.3.17 查询指定中间件的服务器列表

功能介绍

查询指定中间件的服务器列表，通过传入中间件名称参数，返回对应的中间件服务器列表

URI

GET /v5/{project_id}/asset/midwares/detail

表 3-144 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-145 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID
file_name	是	String	文件名称
category	否	String	类别，包含如下: • host : 主机 • container : 容器
host_name	否	String	服务器名称
host_ip	否	String	服务器IP
limit	否	Integer	默认10
offset	否	Integer	默认是0

参数	是否必选	参数类型	描述
part_match	否	Boolean	是否模糊匹配，默认false表示精确匹配

请求参数

表 3-146 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）

响应参数

状态码：200

表 3-147 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **JarPackageHostInfo** objects	服务器列表

表 3-148 JarPackageHostInfo

参数	参数类型	描述
agent_id	String	agent_id
host_id	String	主机id
host_name	String	服务器名称
host_ip	String	服务器ip
file_name	String	Jar包名称
name	String	Jar包名称(不带后缀)
catalogue	String	Jar包类型
file_type	String	Jar包后缀

参数	参数类型	描述
version	String	Jar包版本
path	String	Jar包路径
hash	String	Jar包hash
size	Integer	Jar包大小
uid	Integer	uid
gid	Integer	gid
mode	String	文件权限
pid	Integer	进程id
proc_path	String	进程可执行文件路径
container_id	String	容器实例id
container_name	String	容器名称
package_path	String	包路径
is_embedded	Integer	显示的是否是嵌套包
record_time	Long	扫描时间

请求示例

默认查询前10条中间件名称为log4j-core-2.8.2.jar，类别为主机的服务器列表

```
GET https://{endpoint}/v5/{project_id}/asset/midwares/detail?file_name=log4j-core-2.8.2.jar&category=host
```

响应示例

状态码：200

ListJarPackageHostInfo

```
{
  "data_list" : [ {
    "agent_id" : "2d0fe7824005bf001220ad9d892e86f8af44a7d3608dab11165008ce439d3583",
    "catalogue" : "util",
    "container_id" : "",
    "file_name" : "rt.jar",
    "file_type" : "jar",
    "gid" : 0,
    "hash" : "04bf14e3b1da55d95561ca78cb29caa909410051dbe047e91ad6f5c1dedb8d6d",
    "host_id" : "103ed820-62e5-4754-b0f8-3e47b6dd49d2",
    "host_ip" : "192.168.1.76",
    "host_name" : "正在测试勿删",
    "mode" : "-rw-------",
    "name" : "Java Runtime Environment",
    "path" : "/CloudResetPwdUpdateAgent/depend/jre/lib/rt.jar",
    "pid" : 1614,
    "proc_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
    "record_time" : 1690513169986,
    "uid" : 0,
```

```
    "version" : "1.8.0_252",
    "size" : 128,
    "container_name" : "aaaa",
    "package_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
    "is_embedded" : 0
  } ],
  "total_num" : 1
}
```


状态码

状态码	描述
200	ListJarPackageHostInfo

错误码

请参见**错误码**。

3.4 主机管理

3.4.1 查询云服务器列表

功能介绍

查询云服务器列表

URI

GET /v5/{project_id}/host-management/hosts

表 3-149 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

表 3-150 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

参数	是否必选	参数类型	描述
version	否	String	主机开通的版本，包含如下7种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.advanced： 专业版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。 ● hss.version.container.enterprise：容器版。
agent_status	否	String	Agent状态，包含如下6种。 ● installed： 已安装。 ● not_installed： 未安装。 ● online： 在线。 ● offline： 离线。 ● install_failed： 安装失败。 ● installing： 安装中。 ● not_online： 不在线的（除了在线以外的所有状态，仅作为查询条件）。
detect_result	否	String	检测结果，包含如下4种。 ● undetected： 未检测。 ● clean： 无风险。 ● risk： 有风险。 ● scanning： 检测中。
host_name	否	String	服务器名称
host_id	否	String	服务器ID
host_status	否	String	主机状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。

参数	是否必选	参数类型	描述
os_type	否	String	操作系统类型，包含如下2种。 ● Linux： Linux。 ● Windows： Windows。
private_ip	否	String	服务器私有IP
public_ip	否	String	服务器公网IP
ip_addr	否	String	公网或私网IP
protect_status	否	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
group_id	否	String	服务器组ID
group_name	否	String	服务器组名称
has_intrusion	否	Boolean	存在告警事件
policy_group_id	否	String	策略组ID
policy_group_name	否	String	策略组名称
charging_mode	否	String	收费模式，包含如下: ● on_demand： 按需。
refresh	否	Boolean	是否强制从ECS同步主机
above_version	否	Boolean	是否返回比当前版本高的所有版本
outside_host	否	Boolean	是否为云主机
asset_value	否	String	资产重要性，包含如下4种 ● important： 重要资产 ● common： 一般资产 ● test： 测试资产
label	否	String	资产标签
server_group	否	String	资产服务器组
agent_upgradable	否	Boolean	agent是否可升级
protect_interrupt	否	Boolean	是否防护中断
protect_degradation	否	Boolean	是否防护降级

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示个数，默认10
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-151 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）

响应参数

状态码：200

表 3-152 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **Host** objects	查询弹性云服务器状态列表

表 3-153 Host

参数	参数类型	描述
host_name	String	服务器名称
host_id	String	服务器ID
agent_id	String	Agent ID
private_ip	String	私有IP地址
public_ip	String	弹性公网IP地址
enterprise_project_id	String	企业项目ID

参数	参数类型	描述
enterprise_project_name	String	所属企业项目名称
host_status	String	服务器状态，包含如下4种。 ● ACTIVE： 运行中。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。
agent_status	String	Agent状态，包含如下5种。 ● installed： 已安装。 ● not_installed： 未安装。 ● online： 在线。 ● offline： 离线。 ● install_failed： 安装失败。 ● installing： 安装中。
install_result_code	String	安装结果，包含如下12种。 ● install_succeed： 安装成功。 ● network_access_timeout： 网络不通，访问超时。 ● invalid_port： 无效端口。 ● auth_failed： 认证错误，口令不正确。 ● permission_denied： 权限错误，被拒绝。 ● no_available_vpc： 没有相同VPC的agent在线虚拟机。 ● install_exception： 安装异常。 ● invalid_param： 参数错误。 ● install_failed： 安装失败。 ● package_unavailable： 安装包失效。 ● os_type_not_support： 系统类型错误。 ● os_arch_not_support： 架构类型错误。

参数	参数类型	描述
version	String	主机开通的版本，包含如下7种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.advanced： 专业版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。 ● hss.version.container.enterprise： 容器版。
protect_status	String	防护状态，包含如下2种。 ● closed： 未防护。 ● opened： 防护中。
os_image	String	系统镜像
os_type	String	操作系统类型，包含如下2种。 ● Linux： Linux。 ● Windows： Windows。
os_bit	String	操作系统位数
detect_result	String	云主机安全检测结果，包含如下4种。 ● undetected： 未检测。 ● clean： 无风险。 ● risk： 有风险。 ● scanning： 检测中。
expire_time	Long	试用版到期时间（-1表示非试用版配额，当值不为-1时为试用版本过期时间）
charging_mode	String	收费模式，包含如下: ● on_demand： 按需。
resource_id	String	主机安全配额ID（UUID）
outside_host	Boolean	是否非云机器
group_id	String	服务器组ID
group_name	String	服务器组名称
policy_group_id	String	策略组ID
policy_group_name	String	策略组名称
asset	Integer	资产风险

参数	参数类型	描述
vulnerability	Integer	漏洞风险
baseline	Integer	基线风险
intrusion	Integer	入侵风险
asset_value	String	资产重要性，包含如下4种 ● important： 重要资产 ● common： 一般资产 ● test： 测试资产
labels	Array of strings	标签列表
agent_create_time	Long	agent安装时间，采用时间戳，默认毫秒，
agent_update_time	Long	agent状态修改时间，采用时间戳，默认毫秒，
agent_version	String	agent版本
upgrade_status	String	升级状态，包含如下4种。 ● not_upgrade： 未升级，也就是默认状态，客户还没有给这台机器下发过升级。 ● upgrading： 正在升级中。 ● upgrade_failed： 升级失败。 ● upgrade_succeed： 升级成功。
upgrade_result_code	String	升级失败原因，只有当 upgrade_status 为 upgrade_failed 时才显示，包含如下6种。 ● package_unavailable： 升级包解析失败，升级文件有错误。 ● network_access_timeout： 下载升级包失败，网络异常。 ● agent_offline： agent离线。 ● hostguard_abnormal： agent工作进程异常。 ● insufficient_disk_space： 磁盘空间不足。 ● failed_to_replace_file： 替换文件失败。
upgradable	Boolean	该服务器agent是否可升级
open_time	Long	开启防护时间，采用时间戳，默认毫秒，

参数	参数类型	描述
protect_interrupt	Boolean	防护是否中断
protect_degradation	Boolean	防护是否降级
degradation_reason	String	防护降级原因

请求示例

查询agent状态为在线的所有企业项目下的10台linux主机。

```
GET https://{endpoint}/v5/{project_id}/host-management/hosts?
limit=10&offset=0&agent_status=online&os_type=Linux&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

云服务器列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "agent_status" : "online",
    "asset" : 0,
    "asset_value" : "common",
    "baseline" : 0,
    "charging_mode" : "on_demand",
    "detect_result" : "risk",
    "enterprise_project_id" : "all_granted_eps",
    "enterprise_project_name" : "default",
    "group_id" : "7c659ea3-006f-4687-9f1c-6d975d955f37",
    "group_name" : "default",
    "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
    "host_name" : "ecs-r00431580-ubuntu",
    "host_status" : "ACTIVE",
    "intrusion" : 0,
    "expire_time" : -1,
    "os_bit" : "64",
    "os_type" : "Linux",
    "outside_host" : false,
    "policy_group_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "policy_group_name" : "wtp_ecs-r00431580-ubuntu(default)",
    "private_ip" : "192.168.0.182",
    "protect_status" : "opened",
    "protect_interrupt" : false,
    "public_ip" : "100.85.123.9",
    "resource_id" : "60f08ea4-c74e-4a45-be1c-3c057e373af2",
    "version" : "hss.version.wtp",
    "vulnerability" : 97,
    "labels" : [ "" ],
    "agent_create_time" : 0,
    "agent_update_time" : 0,
    "open_time" : 0
  } ]
}
```

状态码

状态码	描述
200	云服务器列表

错误码

请参见**错误码**。

3.4.2 切换防护状态

功能介绍

切换防护状态

URI

POST /v5/{project_id}/host-management/protection

表 3-154 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

表 3-155 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-156 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）

表 3-157 请求 Body 参数

参数	是否必选	参数类型	描述
version	是	String	主机开通的版本，包含如下: • hss.version.null ： 无，代表关闭防护。 • hss.version.basic ： 基础版。 • hss.version.advanced ： 专业版。 • hss.version.enterprise ： 企业版。 • hss.version.premium ： 旗舰版。 • hss.version.wtp ： 网页防篡改版。
charging_mode	否	String	付费模式，当version不为“hss.version.null”时，则需必填该参数 • on_demand : 按需
resource_id	否	String	HSS配额ID，不填该参数时，则随机选择对应版本配额
host_id_list	是	Array of strings	服务器列表
tags	否	Array of **TagInfo** objects	资源标签列表

表 3-158 TagInfo

参数	是否必选	参数类型	描述
key	否	String	键。最大长度128个unicode字符。 key不能为空
value	否	String	值。最大长度255个unicode字符。

响应参数

状态码：200

successful response

无

请求示例

切换ID为71a15ecc-049f-4cca-bd28-5e90aca1817f的服务器防护版本为基础版。

```
{
  "version" : "hss.version.basic",
  "charging_mode" : "on_demand",
  "resource_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
  "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
  "tags" : [ {
    "key" : "服务",
    "value" : "hss"
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.4.3 查询服务器组列表

功能介绍

查询服务器组列表

URI

GET /v5/{project_id}/host-management/groups

表 3-159 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

表 3-160 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数
group_name	否	String	服务器组名称

请求参数

表 3-161 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）

响应参数

状态码：200

表 3-162 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **HostGroupItem** objects	服务器组列表

表 3-163 HostGroupItem

参数	参数类型	描述
group_id	String	服务器组ID
group_name	String	服务器组名称
host_num	Integer	关联服务器数
risk_host_num	Integer	有风险服务器数
unprotect_host_num	Integer	未防护服务器数

参数	参数类型	描述
host_id_list	Array of strings	服务器ID列表
is_outside	Boolean	是否是线下数据中心服务器组

请求示例

查询服务器组名称为test的服务器组。

```
GET https://{endpoint}/v5/{project_id}/host-management/groups?
offset=0&limit=200&enterprise_project_id=all_granted_eps&&group_name=test
```

响应示例

状态码：200

服务器组列表

```
{
  "data_list" : [ {
    "group_id" : "36e59701-e2e7-4d56-b229-0db3bcf4e6e8",
    "group_name" : "test",
    "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
    "host_num" : 1,
    "risk_host_num" : 1,
    "unprotect_host_num" : 0
  } ],
  "total_num" : 1
}
```

状态码

状态码	描述
200	服务器组列表

错误码

请参见**错误码**。

3.4.4 创建服务器组

功能介绍

创建服务器组

URI

POST /v5/{project_id}/host-management/groups

表 3-164 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

表 3-165 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-166 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）

表 3-167 请求 Body 参数

参数	是否必选	参数类型	描述
group_name	是	String	服务器组名称
host_id_list	是	Array of strings	服务器ID列表

响应参数

状态码：200

success

无

请求示例

创建名称为test的服务器组，服务器组中包含的服务器ID为15dac7fe-d81b-43bc-a4a7-4710fe673972。

```
POST https://{endpoint}/v5/{project_id}/host-management/groups
```

```
{
  "group_name" : "test",
  "host_id_list" : [ "15dac7fe-d81b-43bc-a4a7-4710fe673972" ]
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.4.5 编辑服务器组

功能介绍

编辑服务器组

URI

PUT /v5/{project_id}/host-management/groups

表 3-168 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

表 3-169 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-170 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）

表 3-171 请求 Body 参数

参数	是否必选	参数类型	描述
group_name	否	String	服务器组名称
group_id	是	String	服务器组ID
host_id_list	否	Array of strings	服务器ID列表

响应参数

状态码：200

success

无

请求示例

编辑名称为test的服务器组，服务器组ID为eca40dbe-27f7-4229-8f9d-a58213129fdc，服务器组包含的服务器ID为15dac7fe-d81b-43bc-a4a7-4710fe673972、21303c5b-36ad-4510-a1b0-cb4ac4c2875c。

```
PUT https://{endpoint}/v5/{project_id}/host-management/groups

{
  "group_id" : "eca40dbe-27f7-4229-8f9d-a58213129fdc",
  "group_name" : "test",
  "host_id_list" : [ "15dac7fe-d81b-43bc-a4a7-4710fe673972", "21303c5b-36ad-4510-a1b0-cb4ac4c2875c" ]
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.4.6 删除服务器组

功能介绍

删除服务器组

URI

DELETE /v5/{project_id}/host-management/groups

表 3-172 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

表 3-173 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
group_id	是	String	服务器组ID

请求参数

表 3-174 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）

响应参数

状态码：200

success

无

请求示例

删除组id为34fcf861-402b-45c6-9b6a-13087791aae3的服务器组。

```
DELETE https://{endpoint}/v5/{project_id}/host-management/groups

{
  "group_id" : "34fcf861-402b-45c6-9b6a-13087791aae3"
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.5 网页防篡改

3.5.1 查询防护列表

功能介绍

查询防护列表：查询网页防篡改主机防护状态列表信息

URI

GET /v5/{project_id}/webtamper/hosts

表 3-175 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-176 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_name	否	String	服务器名称
host_id	否	String	云服务器ID
public_ip	否	String	弹性公网IP
private_ip	否	String	私有IP
group_name	否	String	服务器组名称
os_type	否	String	操作系统类别（linux，windows） ● linux : linux操作系统 ● windows : windows操作系统
protect_status	否	String	防护状态 ● closed : 未开启 ● opened : 防护中

参数	是否必选	参数类型	描述
agent_status	否	String	客户端状态 • not_installed : agent未安装 • online : agent在线 • offline : agent不在线
limit	否	Integer	默认10
offset	否	Integer	默认是0

请求参数

表 3-177 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM token

响应参数

状态码：200

表 3-178 响应 Body 参数

参数	参数类型	描述
data_list	Array of **WtpProtectHostResponseInfo** objects	data list
total_num	Integer	total number

表 3-179 WtpProtectHostResponseInfo

参数	参数类型	描述
host_name	String	服务器名称
host_id	String	云服务器ID
public_ip	String	弹性公网IP
private_ip	String	私有IP
group_name	String	服务器组名称

参数	参数类型	描述
os_bit	String	操作系统位数
os_type	String	操作系统（linux，windows）
protect_status	String	防护状态 ● closed：未开启 ● opened：防护中
rasp_protect_status	String	动态网页防篡改状态 ● closed：未开启 ● opened：防护中
anti_tampering_times	Long	已防御篡改攻击次数
detect_tampering_times	Long	已发现篡改攻击
last_detect_time	Long	最近检测时间
scheduled_shutdown_status	String	定时关闭防护开关状态 ● opened：开启 ● closed：未开启
agent_status	String	Agent状态 ● not_installed：agent未安装 ● online：agent在线 ● offline：agent不在线

请求示例

查询防护状态为开启，企业项目为XX的网页防篡改主机防护状态列表信息，默认查询第一页10条

```
GET https://{endpoint}/v5/{project_id}/webtamper/hosts?
offset=XX&limit=XX&protect_status=opened&enterprise_project_id=XX

{
  "protect_status" : "opened"
}
```

响应示例

状态码：200

OK

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_name" : "test",
    "host_id" : "000411f9-42a7-4acd-80e6-f7b9d3db895f",
```

```
    "public_ip" : "",
    "private_ip" : "192.168.0.70",
    "group_name" : "UNINSTALL",
    "os_bit" : "64",
    "os_type" : "Linux",
    "protect_status" : "opened",
    "rasp_protect_status" : "opened",
    "anti_tampering_times" : 0,
    "detect_tampering_times" : 0,
    "last_detect_time" : 0,
    "agent_status" : "not_installed"
  } ]
}
```

状态码

状态码	描述
200	OK

错误码

请参见**错误码**。

3.5.2 开启关闭网页防篡改防护

功能介绍

开启/关闭网页防篡改功能防护，下发/清空网页防篡改策略

URI

POST /v5/{project_id}/webtamper/static/status

表 3-180 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-181 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目

请求参数

表 3-182 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM token

表 3-183 请求 Body 参数

参数	是否必选	参数类型	描述
status	否	Boolean	开启关闭状态
host_id_list	否	Array of strings	HostId list
resource_id	否	String	资源ID
charging_mode	否	String	计费模式 • on_demand: 按需

响应参数

状态码：200

successful response

无

请求示例

开启网页防篡改防护，目标服务器ID为a、b，按需计费。

```
POST https://{endpoint}/v5/{project_id}/webtamper/static/status

{
  "status" : true,
  "host_id_list" : [ "a", "b" ],
  "resource_id" : "aaxxx",
  "charging_mode" : "on_demand"
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.5.3 开启/关闭动态网页防篡改防护

功能介绍

开启/关闭动态网页防篡改防护，下发/清空动态网页防篡改策略

URI

POST /v5/{project_id}/webtamper/rasp/status

表 3-184 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-185 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目

请求参数

表 3-186 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM token

表 3-187 请求 Body 参数

参数	是否必选	参数类型	描述
host_id_list	否	Array of strings	HostId list
status	否	Boolean	动态网页防篡改状态

响应参数

状态码：200

successful response

无

请求示例

开启动态网页防篡改防护，目标服务器为a、b。

```
POST https://{endpoint}/v5/{project_id}/webtamper/rasp/status

{
  "host_id_list" : [ "a", "b" ],
  "status" : true
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.5.4 查询主机静态网页防篡改防护动态

功能介绍

查询主机静态网页防篡改防护动态：展示服务器名称、服务器ip、防护策略、检测时间、防护文件、事件描述信息

URI

GET /v5/{project_id}/webtamper/static/protect-history

表 3-188 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-189 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_id	是	String	Host Id
start_time	是	Long	起始时间
end_time	是	Long	终止时间
limit	是	Integer	limit
offset	是	Integer	offset
host_name	否	String	服务器名称
host_ip	否	String	服务器ip
file_path	否	String	防护文件
file_operation	否	String	文件操作类型 • add: 新增 • delete: 删除 • modify: 修改内容 • attribute: 修改属性

请求参数

表 3-190 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM token

响应参数

状态码：200

表 3-191 响应 Body 参数

参数	参数类型	描述
host_name	String	服务器名称
protect_status	String	防护状态 • close : 未开启 • opened : 防护中

参数	参数类型	描述
total_num	Long	total number
data_list	Array of HostProtectHistoryResponseInfo objects	data list

表 3-192 HostProtectHistoryResponseInfo

参数	参数类型	描述
occr_time	Long	检测时间
file_path	String	被篡改文件路径
file_operation	String	文件操作类型 • add: 新增 • delete: 删除 • modify: 修改内容 • attribute: 修改属性 • unknown: 未知
host_name	String	服务器名称
host_ip	String	服务器ip
process_id	String	进程ID
process_name	String	进程名称
process_cmd	String	进程命令行

请求示例

查询主机静态网页防篡改防护动态，目标主机ID为caa958ad-a481-4d46-b51e-6861b8864515，查询起始时间为1668563099000，查询终止时间1668563199000。

```
GET https://{endpoint}/v5/{project_id}/webtamper/static/protect-history

{
  "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
  "start_time" : 1668563099000,
  "end_time" : 1668563199000,
  "limit" : 10,
  "offset" : 0
}
```

响应示例

状态码：200

successful response

```
{
  "host_name" : "ecs-ubuntu",
  "protect_status" : "opened",
  "total_num" : 1,
  "data_list" : [ {
    "occr_time" : 1668156691000,
    "file_path" : "/root/test/tamper/test.xml",
    "host_name" : "hss-test",
    "host_ip" : "192.168.5.98",
    "file_operation" : "add",
    "process_id" : "18672",
    "process_name" : "program1",
    "process_cmd" : "del test.xml"
  } ]
}
```

状态码

状态码	描述
200	successful response

错误码

请参见错误码。

3.5.5 查询主机动态网页防篡改防护动态

功能介绍

查询主机动态网页防篡改防护动态：包含告警级别、服务器ip、服务器名称、威胁类型、告警时间、攻击源ip、攻击源url信息

URI

GET /v5/{project_id}/webtamper/rasp/protect-history

表 3-193 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-194 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目
host_id	是	String	Host Id

参数	是否必选	参数类型	描述
start_time	是	Long	起始时间
end_time	是	Long	终止时间
limit	是	Integer	limit
offset	是	Integer	offset
alarm_level	否	Integer	告警级别
severity	否	String	威胁等级 • Security : 安全 • Low : 低危 • Medium : 中危 • High : 高危 • Critical : 危急
protect_status	否	String	防护状态 • closed : 未开启 • opened : 防护中

请求参数

表 3-195 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	IAM token

响应参数

状态码：200

表 3-196 响应 Body 参数

参数	参数类型	描述
total_num	Long	total number
data_list	Array of **HostRaspProtectHistoryResponseInfo** objects	data list

表 3-197 HostRaspProtectHistoryResponseInfo

参数	参数类型	描述
host_ip	String	服务器ip
host_name	String	服务器名称
alarm_time	Long	告警时间
threat_type	String	威胁类型
alarm_level	Integer	告警级别
source_ip	String	源IP
attacked_url	String	攻击URL

请求示例

查询主机动态网页防篡改防护动态，目标主机ID为caa958ad-a481-4d46-b51e-6861b8864515，查询起始时间为1668563099000，查询终止时间为1668563199000。

```
GET https://{endpoint}/v5/{project_id}/webtamper/rasp/protect-history

{
  "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
  "start_time" : 1668563099000,
  "end_time" : 1668563199000,
  "limit" : 10,
  "offset" : 0
}
```

响应示例

状态码：200

successful response

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_ip" : "192.168.5.98",
    "host_name" : "hss-test",
    "alarm_level" : 2,
    "alarm_time" : 1668394634000,
    "attacked_url" : "/vulns/001-dir-1.jsp",
    "source_ip" : "10.100.30.200",
    "threat_type" : "Path Traversal"
  } ]
}
```

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.6 容器镜像

3.6.1 查询 swr 镜像仓库镜像列表

功能介绍

查询swr镜像仓库镜像列表,如果需要从swr同步最新镜像，需要先调用“从swr同步镜像”接口

URI

GET /v5/{project_id}/image/swr-repository

表 3-198 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

表 3-199 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
namespace	否	String	组织名称
image_name	否	String	镜像名称 id
image_version	否	String	镜像版本
latest_version	否	Boolean	仅关注最新版本镜像
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

参数	是否必选	参数类型	描述
image_type	是	String	镜像类型，包含如下: ● private_image : 私有镜像仓库 ● shared_image : 共享镜像仓库 ● local_image : 本地镜像 ● instance_image : 企业镜像
scan_status	否	String	扫描状态，包含如下: ● unscan : 未扫描 ● success : 扫描完成 ● scanning : 扫描中 ● failed : 扫描失败 ● download_failed : 下载失败 ● image_oversized : 镜像超大
instance_name	否	String	企业镜像实例名称
image_size	否	Long	镜像大小
start_latest_update_time	否	Long	创建时间开始日期
end_latest_update_time	否	Long	创建时间结束日期
start_latest_scan_time	否	Long	最近一次扫描完成时间开始日期
end_latest_scan_time	否	Long	最近一次扫描完成时间结束日期
has_malicious_file	否	Boolean	是否存在恶意文件
has_unsafe_setting	否	Boolean	是否存在基线检查
has_vul	否	Boolean	是否存在软件漏洞
instance_id	否	String	企业仓库实例ID，swr共享版无需使用该参数

请求参数

表 3-200 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）

响应参数

状态码：200

表 3-201 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **PrivateImageRepositoryInfo** objects	查询swr镜像仓库镜像列表

表 3-202 PrivateImageRepositoryInfo

参数	参数类型	描述
id	Long	id
namespace	String	命名空间
image_name	String	镜像名称
image_id	String	镜像id
image_digest	String	镜像digest
image_version	String	镜像版本
image_type	String	镜像类型，包含如下2种。 • private_image： 私有镜像。 • shared_image： 共享镜像。
latest_version	Boolean	是否是最新版本

参数	参数类型	描述
scan_status	String	扫描状态，包含如下2种。 ● unscan： 未扫描。 ● success： 扫描完成。 ● scanning： 正在扫描。 ● failed： 扫描失败。 ● download_failed： 下载失败。 ● image_oversized： 镜像超大。 ● waiting_for_scan： 等待扫描。
scan_failed_desc	String	扫描失败原因，包含如下14种。 ● "unknown_error" :未知错误 ● "authentication_failed":认证失败 ● "download_failed":镜像下载失败 ● "image_over_sized":镜像大小超限 ● "image_oversized":镜像超大 ● "failed_to_scan_vulnerability":漏洞扫描失败 ● "failed_to_scan_file":文件扫描失败 ● "failed_to_scan_software":软件扫描失败 ● "failed_to_check_sensitive_information":敏感信息核查失败 ● "failed_to_check_baseline":基线检查失败 ● "failed_to_check_software_compliance":软件合规检查失败 ● "failed_to_query_basic_image_information":基础镜像信息查询失败 ● "response_timed_out":响应超时 ● "database_error" : 数据库错误 ● "failed_to_send_the_scan_request" : 发送扫描请求失败
image_size	Long	镜像大小
latest_update_time	Long	镜像版本最后更新时间
latest_scan_time	Long	最近扫描时间
vul_num	Integer	漏洞个数
unsafe_setting_num	Integer	基线扫描未通过数

参数	参数类型	描述
malicious_file_num	Integer	恶意文件数
domain_name	String	拥有者（共享镜像参数）
shared_status	String	共享镜像状态，包含如下2种。 ● expired： 已过期。 ● effective： 有效。
scannable	Boolean	是否可扫描
association_images	Array of **AssociateImages** objects	多架构关联镜像信息

表 3-203 AssociateImages

参数	参数类型	描述
image_name	String	镜像名称
image_version	String	镜像版本
image_type	String	镜像类型
namespace	String	命名空间
image_digest	String	镜像digest
scan_status	String	扫描状态，包含如下2种。 ● unscan： 未扫描。 ● success： 扫描完成。 ● scanning： 正在扫描。 ● failed： 扫描失败。 ● download_failed： 下载失败。 ● image_oversized： 镜像超大。 ● waiting_for_scan： 等待扫描。

请求示例

查询镜像类型为私有镜像的swr镜像仓库镜像列表。

```
GET https://{endpoint}/v5/{project_id}/image/swr-repository?
offset=0&limit=50&image_type=private_image&latest_version=false&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

查询swr镜像仓库镜像列表,包括私有镜像列表和共享镜像列表（通过传参image_type控制）


```
{
  "total_num" : 3,
  "data_list" : [ {
    "id" : "111(私有镜像举例)",
    "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_name" : "centos7",
    "image_size" : "1000 单位（Bytes）",
    "image_type" : "private_image",
    "image_version" : "common",
    "latest_scan_time" : 1691748641788,
    "latest_update_time" : 1687664346000,
    "latest_version" : false,
    "malicious_file_num" : 0,
    "namespace" : "aaa",
    "scan_status" : "success",
    "scannable" : true,
    "unsafe_setting_num" : 1,
    "vul_num" : 111,
    "instance_name" : "",
    "instance_id" : "",
    "instance_url" : ""
  }, {
    "id" : "222(共享镜像举例)",
    "domain_name" : "scc_cgs_XXX",
    "shared_status" : "effective",
    "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_name" : "mysql",
    "image_size" : "1000 单位（Bytes）",
    "image_type" : "shared_image",
    "image_version" : "5.5",
    "latest_scan_time" : 1691748641788,
    "latest_update_time" : 1687664346000,
    "latest_version" : false,
    "malicious_file_num" : 0,
    "namespace" : "aaa",
    "scan_status" : "success",
    "scannable" : true,
    "unsafe_setting_num" : 1,
    "vul_num" : 111,
    "instance_name" : "",
    "instance_id" : "",
    "instance_url" : ""
  }, {
    "id" : "333(企业镜像举例)",
    "domain_name" : "scc_cgs_XXX",
    "shared_status" : "effective",
    "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_name" : "mysql",
    "image_size" : "1000 单位（Bytes）",
    "image_type" : "shared_image",
    "image_version" : "5.5",
    "latest_scan_time" : 1691748641788,
    "latest_update_time" : 1687664346000,
    "latest_version" : false,
    "malicious_file_num" : 0,
    "namespace" : "aaa",
    "scan_status" : "success",
    "scannable" : true,
    "unsafe_setting_num" : 1,
    "vul_num" : 111,
    "instance_name" : "企业实例名称",
    "instance_id" : "",
    "instance_url" : ""
```

```
 }]
}
```

状态码

状态码	描述
200	查询swr镜像仓库镜像列表,包括私有镜像列表和共享镜像列表（通过传参image_type控制）

错误码

请参见**错误码**。

3.6.2 镜像仓库镜像批量扫描

功能介绍

镜像仓库镜像批量扫描

URI

POST /v5/{project_id}/image/batch-scan

表 3-204 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

表 3-205 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-206 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）

表 3-207 请求 Body 参数

参数	是否必选	参数类型	描述
repo_type	否	String	仓库类型，现阶段接入了swr镜像仓库，包含如下: • SWR : SWR镜像仓库
image_info_list	否	Array of BatchScanSwrImageInfo objects	要扫描的镜像信息列表，operate_all参数为false时为必填
operate_all	否	Boolean	若为true全量查询，可筛选条件全部查询，若image_info_list为空，则必填
namespace	否	String	组织名称
image_name	否	String	镜像名称
image_version	否	String	镜像版本
image_type	是	String	镜像类型，包含如下: • private_image : 私有镜像仓库 • shared_image : 共享镜像仓库
scan_status	否	String	扫描状态，包含如下: • unscan : 未扫描 • success : 扫描完成 • scanning : 扫描中 • failed : 扫描失败 • download_failed : 下载失败 • image_oversized : 镜像超大
latest_version	否	Boolean	仅关注最新版本镜像
image_size	否	Long	镜像大小
start_latest_update_time	否	Long	创建时间开始日期
end_latest_update_time	否	Long	创建时间结束日期
start_latest_scan_time	否	Long	最近一次扫描完成时间开始日期
end_latest_scan_time	否	Long	最近一次扫描完成时间结束日期

表 3-208 BatchScanSwrImageInfo

参数	是否必选	参数类型	描述
namespace	否	String	命名空间
image_name	否	String	镜像名称
image_version	否	String	镜像版本
instance_id	否	String	企业实例ID
instance_url	否	String	下载企业镜像URL

响应参数

状态码：200

successful response

无

请求示例

- 类型为私有镜像的镜像进行批量扫描，body体传参镜像列表，operate_all没有传参，说明需要镜像列表批量扫描。

```
POST https://{endpoint}/v5/{project_id}/image/batch-scan

{
  "image_type" : "private_image",
  "image_info_list" : [ {
    "image_name" : "openjdk",
    "image_version" : "v8.8",
    "namespace" : "test"
  }, {
    "image_name" : "openjdk1",
    "image_version" : "v1.0",
    "namespace" : "test1"
  } ]
}
```

- 类型为私有镜像的镜像进行全量扫描，body体没有传参镜像列表，operate_all=true，说明需要镜像列表全量扫描。

```
POST https://{endpoint}/v5/{project_id}/image/batch-scan

{
  "image_type" : "private_image",
  "operate_all" : true
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见错误码。

3.6.3 查询镜像的漏洞信息

功能介绍

查询镜像的漏洞信息

URI

GET /v5/{project_id}/image/{image_id}/vulnerabilities

表 3-209 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
image_id	是	String	镜像id

表 3-210 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
image_type	是	String	镜像类型，包含如下: • private_image : 私有镜像仓库 • shared_image : 共享镜像仓库 • local_image : 本地镜像 • instance_image : 企业镜像
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

参数	是否必选	参数类型	描述
instance_id	否	String	企业仓库实例ID，swr共享版无需使用该参数
namespace	是	String	组织名称
image_name	是	String	镜像名称
tag_name	是	String	镜像版本
repair_necessity	否	String	危险程度，包含如下3种。 • immediate_repair： 高危。 • delay_repair： 中危。 • not_needed_repair： 低危。
vul_id	否	String	漏洞ID（支持模糊查询）
app_name	否	String	软件名
type	否	String	漏洞类型，包含如下： -linux_vul : linux漏洞 -app_vul : 应用漏洞

请求参数

表 3-211 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）

响应参数

状态码：200

表 3-212 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **ImageVulInfo** objects	镜像的漏洞列表

表 3-213 ImageVulInfo

参数	参数类型	描述
vul_id	String	漏洞id
repair_necessity	String	修复紧急度，包含如下3种。 ● immediate_repair： 高危。 ● delay_repair： 中危。 ● not_needed_repair： 低危。
description	String	漏洞描述
position	String	漏洞所在镜像层
app_name	String	漏洞的软件名称
app_path	String	应用软件的路径（只有应用漏洞有该字段）
version	String	软件版本
solution	String	解决方案
url	String	补丁地址

请求示例

查询私有镜像中命名空间为scc_hss_container，镜像名称为apptest，镜像版本为V1的漏洞信息。

```
GET https://{endpoint}/v5/{project_id}/image/{image_id}/vulnerabilities?
limit=10&offset=0&namespace=scc_hss_container&tag_name=v1&image_name=apptest&image_type=private
_image&type=linux_vul&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

镜像漏洞信息列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "app_name" : "xz-lib",
    "description" : "online",
    "position" : "sha256:74ddd0ec08fa43dXXXX",
    "repair_necessity" : "delay_repair",
    "solution" : "To upgrade the affected software",
    "url" : "https://access.redhat.com/errata/RHSAXXX",
    "version" : "5.2.4-3.el8",
    "vul_id" : "RHSA-2022:49XX"
  } ]
}
```

状态码

状态码	描述
200	镜像漏洞信息列表

错误码

请参见**错误码**。

3.6.4 漏洞对应 cve 信息

功能介绍

漏洞对应cve信息

URI

GET /v5/{project_id}/image/vulnerability/{vul_id}/cve

表 3-214 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
vul_id	是	String	漏洞ID

表 3-215 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

请求参数

表 3-216 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）

响应参数

状态码：200

表 3-217 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of ImageVulCveInfo objects	列表

表 3-218 ImageVulCveInfo

参数	参数类型	描述
cve_id	String	cve id
cvss_score	Float	CVSS分数
publish_time	Long	公布时间
description	String	cve描述

请求示例

查询漏洞id为vul_id的漏洞对应cve信息。

```
GET https://{endpoint}/v5/{project_id}/image/vulnerability/{vul_id}/cve?
offset=0&limit=200&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

漏洞对应cve信息列表请求成功

```
{
  "total_num" : 1,
```

```
 "data_list" : [ {
   "cve_id" : "CVE-2021-45960",
   "cvss_score" : 8.8,
   "description" : "In Expat (aka libexpat) XXXX",
   "publish_time" : 1641035700000
 } ]
}
```

状态码

状态码	描述
200	漏洞对应cve信息列表请求成功

错误码

请参见**错误码**。

3.6.5 从 SWR 服务同步镜像列表

功能介绍

从SWR服务同步镜像列表

URI

POST /v5/{project_id}/image/synchronize

表 3-219 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

表 3-220 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-221 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）

表 3-222 请求 Body 参数

参数	是否必选	参数类型	描述
image_type	是	String	镜像类型，包含如下: • private_image : 私有镜像仓库 • shared_image : 共享镜像仓库

响应参数

状态码：200

表 3-223 响应 Body 参数

参数	参数类型	描述
error_code	Integer	错误编码
error_description	String	错误描述

请求示例

从swr服务同步镜像，类型为私有镜像或者共享镜像。

```
POST https://{endpoint}/v5/{project_id}/image/synchronize

{
  "image_type" : "private_image"
}
```

响应示例

状态码：200

请求成功

```
{
  "error_code" : 0,
```

```
  "error_description" : "success"
}
```

状态码

状态码	描述
200	请求成功

错误码

请参见**错误码**。

3.6.6 查询镜像安全配置检测结果列表

功能介绍

查询镜像安全配置检测结果列表,当前支持检测CentOS 7、Debian 10、EulerOS和Ubuntu16镜像的系统配置项、SSH应用配置项。

URI

GET /v5/{project_id}/image/baseline/risk-configs

表 3-224 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

表 3-225 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
image_type	是	String	镜像类型，包含如下: • private_image : 私有镜像仓库 • shared_image : 共享镜像仓库 • local_image : 本地镜像 • instance_image : 企业镜像
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示个数
namespace	否	String	组织名称
image_name	否	String	镜像名称
image_version	否	String	镜像版本名称
check_name	否	String	基线名称
severity	否	String	风险等级，包含如下: • Security : 安全 • Low : 低危 • Medium : 中危 • High : 高危
standard	否	String	标准类型，包含如下: • cn_standard : 等保合规标准 • hw_standard : 云安全实践标准
instance_id	否	String	企业仓库实例ID，swr共享版无需使用该参数

请求参数

表 3-226 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）

响应参数

状态码：200

表 3-227 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数

参数	参数类型	描述
data_list	Array of ImageRiskConfigsInfoResponseInfo objects	配置检测列表

表 3-228 ImageRiskConfigsInfoResponseInfo

参数	参数类型	描述
severity	String	风险等级，包含如下: • Security：安全 • Low：低危 • Medium：中危 • High：高危
check_name	String	基线名称
check_type	String	基线类型
standard	String	标准类型，包含如下: • cn_standard：等保合规标准 • hw_standard：云安全实践标准
check_rule_num	Integer	检查项数量
failed_rule_num	Integer	风险项数量
check_type_desc	String	基线描述信息

请求示例

查询私有镜像中命名空间为scc_hss_container，镜像名称为euleros，镜像版本为2.2的镜像安全配置检测结果列表。

```
GET https://{endpoint}/v5/{project_id}/image/baseline/risk-configs?
offset=0&limit=200&image_type=private_image&namespace=scc_hss_container&image_name=euleros/
test&image_version=2.2.6&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

镜像配置检测结果列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_name" : "CentOS 7",
    "check_rule_num" : 3,
    "check_type" : 3,
    "check_type_desc" : "本规范着重于从XXX",
```

```
    "failed_rule_num" : 0,
    "severity" : "Low",
    "standard" : "cn_standard"
  } ]
}
```

状态码

状态码	描述
200	镜像配置检测结果列表

错误码

请参见**错误码**。

3.6.7 查询镜像指定安全配置项的检查项列表

功能介绍

查询镜像指定安全配置项的检查项列表

URI

GET /v5/{project_id}/image/baseline/risk-configs/{check_name}/rules

表 3-229 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
check_name	是	String	基线名称

表 3-230 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
image_type	是	String	镜像类型，包含如下: • private_image：私有镜像仓库 • shared_image：共享镜像仓库 • local_image：本地镜像 • instance_image：企业镜像

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数
namespace	否	String	组织名称（没有镜像相关信息时，表示查询所有镜像）
image_name	否	String	镜像名称
image_version	否	String	镜像版本名称
standard	是	String	标准类型，包含如下: ● cn_standard : 等保合规标准 ● hw_standard : 云安全实践标准
result_type	否	String	结果类型，包含如下: ● pass： 已通过 ● failed : 未通过
check_rule_name	否	String	检查项名称，支持模糊匹配
severity	否	String	风险等级，包含如下: ● Security : 安全 ● Low : 低危 ● Medium : 中危 ● High : 高危 ● Critical : 危急
instance_id	否	String	企业仓库实例ID，swr共享版无需使用该参数

请求参数

表 3-231 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）

响应参数

状态码：200

表 3-232 响应 Body 参数

参数	参数类型	描述
total_num	Integer	风险总数
data_list	Array of ImageRiskConfigsCheckRulesResponseInfo objects	数据列表

表 3-233 ImageRiskConfigsCheckRulesResponseInfo

参数	参数类型	描述
severity	String	风险等级，包含如下: • Security : 安全 • Low : 低危 • Medium : 中危 • High : 高危
check_name	String	基线名称
check_type	String	基线类型
standard	String	标准类型，包含如下: • cn_standard : 等保合规标准 • hw_standard : 云安全实践标准
check_rule_name	String	检查项
check_rule_id	String	检查项ID
scan_result	String	检测结果，包含如下： • pass 通过 • failed 未通过

请求示例

查询所属组织为aaa，镜像名称为centos7，镜像版本为common的私有镜像并且标准类型为云规范的指定安全配置项的检查项列表。

```
GET https://{endpoint}/v5/{project_id}/image/baseline/risk-configs/{check_name}/rules?
offset=0&limit=200&image_type=private_image&namespace=aaa&image_name=centos7/
test&image_version=common&standard=hw_standard&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

指定安全配置项的检查项列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_rule_id" : "1.1",
    "check_rule_name" : "规则：口令锁定策略.",
    "check_name" : "CentOS 7",
    "check_type" : "CentOS 7",
    "standard" : "hw_standard",
    "scan_result" : "failed",
    "severity" : "High"
  } ]
}
```

状态码

状态码	描述
200	指定安全配置项的检查项列表

错误码

请参见**错误码**。

3.6.8 查询镜像配置检查项检测报告

功能介绍

查询镜像配置检查项检测报告

URI

GET /v5/{project_id}/image/baseline/check-rule/detail

表 3-234 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

表 3-235 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

参数	是否必选	参数类型	描述
image_type	是	String	镜像类型，包含如下: • private_image : 私有镜像仓库 • shared_image : 共享镜像仓库 • local_image : 本地镜像 • instance_image : 企业镜像
namespace	否	String	组织名称（没有镜像相关信息时，表示查询所有镜像）
image_name	否	String	镜像名称
image_version	否	String	镜像版本名称
check_name	是	String	基线名称
check_type	是	String	基线类型
check_rule_id	是	String	检查项id
standard	是	String	标准类型，包含如下: • cn_standard : 等保合规标准 • hw_standard : 云安全实践标准
instance_id	否	String	企业仓库实例ID，swr共享版无需使用该参数

请求参数

表 3-236 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）

响应参数

状态码：200

表 3-237 响应 Body 参数

参数	参数类型	描述
description	String	检查项描述
reference	String	参考
audit	String	审计描述
remediation	String	修改建议
check_info_list	Array of **ImageCheckRuleCheckCaseResponseInfo** objects	检测用例信息

表 3-238 ImageCheckRuleCheckCaseResponseInfo

参数	参数类型	描述
check_description	String	检测用例描述
current_value	String	当前结果
suggest_value	String	期待结果

请求示例

查询所属组织为aaa，镜像名称为centos7，镜像版本为common的私有镜像、基线名称为SSH、检测项id为1.12并且标准类型为云规范的配置检查项检测报告。

```
GET https://{endpoint}/v5/{project_id}/image/baseline/check-rule/detail?image_type=private_image&namespace=aaa&image_name=centos7&image_version=common&check_rule_id=1.12&standard=hw_standard&check_type=SSH&check_name=SSH&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

配置检查项检测报告


```
{"audit":"检查配置文件/etc/pam.d/system","check_info_list":[{"check_description":"检查配置文件/etc/pam.d/system-auth"},{"current_value":""},{"suggest_value":"每个文件都配置auth required "}],"description":"The two options ClientAliveInterval and ClientAliveCountMax control the timeout of SSH sessions. The ClientAliveInterval parameter sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The ClientAliveCountMax parameter sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. For example, if the ClientAliveInterval is set to 15s and the ClientAliveCountMax is set to 3, unresponsive SSH clients will be disconnected after approximately 45s.","reference":"","remediation":"Edit the /etc/ssh/sshd_config file to set the parameter as follows:
ClientAliveInterval 300
ClientAliveCountMax 0"}
```

状态码

状态码	描述
200	配置检查项检测报告

错误码

请参见错误码。

3.7 勒索防护

3.7.1 查询勒索防护服务器列表

功能介绍

查询勒索防护服务器列表，与云备份服务配合使用。因此使用勒索相关接口之前确保该局点有云备份服务

URI

GET /v5/{project_id}/ransomware/server

表 3-239 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

表 3-240 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数
host_name	否	String	服务器名称
os_type	否	String	操作系统类型，包含如下2种。 • Linux： Linux。 • Windows： Windows。

参数	是否必选	参数类型	描述
host_ip	否	String	服务器IP地址
host_status	否	String	主机状态，包含如下3种。 • 不传参默认为全部。 • ACTIVE ： 正在运行。 • SHUTOFF ： 关机。
last_days	否	Integer	查询时间范围天数，最近7天为last_days=7，若不填，则默认查询一天内的防护事件和已有备份数

请求参数

表 3-241 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）

响应参数

状态码：200

表 3-242 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **ProtectionServerInfo** objects	查询勒索防护服务器列表

表 3-243 ProtectionServerInfo

参数	参数类型	描述
host_id	String	服务器ID
agent_id	String	Agent ID

参数	参数类型	描述
host_name	String	服务器名称
host_ip	String	弹性公网IP地址
private_ip	String	私有IP地址
os_type	String	操作系统类型，包含如下2种。 • Linux： Linux。 • Windows： Windows。
os_name	String	系统名称
host_status	String	服务器状态，包含如下2种。 • ACTIVE： 运行中。 • SHUTOFF： 关机。
ransom_protection_status	String	勒索防护状态，包含如下4种。 • closed： 关闭。 • opened： 开启。 • opening： 开启中。 • closing： 关闭中。
agent_version	String	agent版本
protect_status	String	防护状态，包含如下2种。 • closed： 未防护。 • opened： 防护中。
group_id	String	服务器组ID
group_name	String	服务器组名称
protect_policy_id	String	防护策略ID
protect_policy_name	String	防护策略名称
backup_error	backup_error object	备份错误信息
backup_protection_status	String	是否开启备份，包含如下3种。 • failed_to_turn_on_backup: 无法开启备份 • closed： 关闭。 • opened： 开启。
count_protect_event	Integer	防护事件数
count_backuped	Integer	已有备份数

参数	参数类型	描述
agent_status	String	Agent状态
version	String	主机开通的版本，包含如下7种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.advanced： 专业版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。 ● hss.version.container.enterprise： 容器版。
host_source	String	服务器类型，包含如下3种输入。 ● ecs： ecs。 ● outside： 线下主机。 ● workspace： 云桌面。
vault_id	String	存储库ID
vault_name	String	存储库名称
vault_size	Integer	总容量，单位GB
vault_used	Integer	已使用容量，单位MB
vault_allocated	Integer	已分配容量，单位GB，指绑定的服务器大小
vault_charging_mode	String	存储库创建模式，按需：post_paid
vault_status	String	存储库状态。 ● available： 可用。 ● lock： 被锁定。 ● frozen：冻结。 ● deleting：删除中。 ● error：错误。
backup_policy_id	String	备份策略ID，若为空，则为未绑定状态，若不为空，通过backup_policy_enabled字段判断策略是否启用
backup_policy_name	String	备份策略名称
backup_policy_enabled	Boolean	策略是否启用

参数	参数类型	描述
resources_num	Integer	已绑定服务器（个）

表 3-244 backup_error

参数	参数类型	描述
error_code	Integer	错误编码，包含如下2种。 ● 0： 无错误信息。 ● 1： 已綁定至其它存储库，无法开启备份。 ● 2： 备份库已超过最大限额。 ● 3： CBR接口调用异常。
error_description	String	错误描述

请求示例

查询勒索防护服务器列表，不传limit默认返回10条。

```
GET https://{endpoint}/v5/{project_id}/ransomware/server
```

响应示例

状态码：200

勒索病毒防护服务器列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "agent_status" : "online",
    "backup_error" : {
      "error_code" : 1,
      "error_description" : "已綁定至其它存储库，无法开启备份"
    },
    "ransom_protection_status" : "opened",
    "backup_protection_status" : "failed_to_turn_on_backup",
    "count_backuped" : 0,
    "count_protect_event" : 0,
    "group_id" : "7c659ea3-006f-4687-9f1c-6d975d955f37",
    "group_name" : "333",
    "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
    "host_ip" : "100.85.119.68",
    "host_name" : "Euler",
    "host_status" : "ACTIVE",
    "os_name" : "EulerOS",
    "os_type" : "Linux",
    "private_ip" : "100.85.123.9",
    "protect_policy_id" : "0253edfd-30e7-439d-8f3f-17c54c99706",
    "protect_policy_name" : "tst",
    "protect_status" : "opened"
  } ]
}
```

状态码

状态码	描述
200	勒索病毒防护服务器列表

错误码

请参见**错误码**。

3.7.2 查询防护策略列表

功能介绍

查询防护策略列表

URI

GET /v5/{project_id}/ransomware/protection/policy

表 3-245 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

表 3-246 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数
policy_name	否	String	防护策略名称
protect_policy_id	否	String	防护策略id
operating_system	否	String	策略支持的操作系统

请求参数

表 3-247 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）

响应参数

状态码：200

表 3-248 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **ProtectionPolicyInfo** objects	查询防护策略列表

表 3-249 ProtectionPolicyInfo

参数	参数类型	描述
policy_id	String	策略ID
policy_name	String	策略名称
protection_mode	String	防护动作，包含如下2种。 • alarm_and_isolation： 告警并自动隔离。 • alarm_only： 仅告警。
bait_protection_status	String	是否开启诱饵防护，包含如下1种, 默认为开启防护诱饵防护。 • opened： 开启。 • closed： 关闭。
deploy_mode	String	是否开启动态诱饵防护，包含如下2种, 默认为关闭动态诱饵防护。 • opened： 开启。 • closed： 关闭。

参数	参数类型	描述
protection_directory	String	防护目录
protection_type	String	防护文件类型
exclude_directory	String	排除目录，选填
runtime_detection_status	String	是否运行时检测，包含如下2种，暂时只有关闭一种状态，为保留字段。 ● opened： 开启。 ● closed： 关闭。
runtime_detection_directory	String	运行时检测目录，所有目录是/,现在为保留字段
count_associated_server	Integer	关联server个数
operating_system	String	操作系统类型
process_whitelist	Array of TrustProcessInfo objects	进程白名单
default_policy	Integer	是否为默认策略，包含如下2种。 ● 0： 非默认策略。 ● 1： 默认策略

表 3-250 TrustProcessInfo

参数	参数类型	描述
path	String	进程路径
hash	String	进程hash

请求示例

查询防护策略列表，不传limit参数默认返回10条数据。

```
GET https://{endpoint}/v5/{project_id}/ransomware/protection/policy
```

响应示例

状态码：200

防护策略列表

```
{
  "total_num" : 1,
  "data_list" : [ {
```

```
    "bait_protection_status" : "opened",
    "exclude_directory" : "/opt",
    "count_associated_server" : 0,
    "operating_system" : "Linux",
    "protection_mode" : "alarm_only",
    "policy_id" : "4117d16-074b-41ae-b7d7-9cc25ee258",
    "policy_name" : "test",
    "protection_directory" : "/dd",
    "protection_type" : "docx",
    "runtime_detection_status" : "closed"
  } ]
}
```


状态码

状态码	描述
200	防护策略列表

错误码

请参见**错误码**。

3.7.3 修改防护策略

功能介绍

修改防护策略

URI

PUT /v5/{project_id}/ransomware/protection/policy

表 3-251 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

表 3-252 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-253 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）

表 3-254 请求 Body 参数

参数	是否必选	参数类型	描述
policy_id	是	String	策略ID
policy_name	是	String	策略名称
protection_mode	是	String	防护动作，包含如下2种。 ● alarm_and_isolation： 告警并自动隔离。 ● alarm_only： 仅告警。
bait_protection_status	是	String	是否开启诱饵防护，包含如下1种, 默认为开启防护诱饵防护。 ● opened： 开启。 ● closed： 关闭。
protection_directory	是	String	防护目录,多个目录请用英文分号隔开，最多支持填写20个防护目录
protection_type	是	String	防护文件类型
exclude_directory	否	String	排除目录(选填)，多个目录请用英文分号隔开，最多支持填写20个排除目录
agent_id_list	否	Array of strings	关联server
operating_system	是	String	操作系统，包含如下： ● Windows : Windows系统 ● Linux : Linux系统

参数	是否必选	参数类型	描述
runtime_detection_status	否	String	是否运行时检测，包含如下2种，暂时只有关闭一种状态，为保留字段。 • opened： 开启。 • closed： 关闭。
process_whitelist	否	Array of TrustProcessInfo objects	进程白名单

表 3-255 TrustProcessInfo

参数	是否必选	参数类型	描述
path	否	String	进程路径
hash	否	String	进程hash

响应参数

状态码：200

success

无

请求示例

修改勒索病毒防护策略，目标服务器操作系统类型为Linux，防护策略ID为0253edfd-30e7-439d-8f3f-17c54c997064，防护动作为仅告警。

```
PUT https://{endpoint}/v5/{project_id}/ransomware/protection/policy

{
  "bait_protection_status" : "opened",
  "protection_type" : "docx",
  "exclude_directory" : "",
  "operating_system" : "Linux",
  "policy_id" : "0253edfd-30e7-439d-8f3f-17c54c997064",
  "policy_name" : "aaa",
  "protection_mode" : "alarm_only",
  "protection_directory" : "/root",
  "runtime_detection_status" : "closed",
  "agent_id_list" : [ "" ]
}
```

响应示例

无

状态码

状态码	描述
200	success

错误码

请参见错误码。

3.7.4 开启勒索病毒防护

功能介绍

开启勒索病毒防护,请保证该region有cbr云备份服务，勒索服务与云备份服务有关联关系

URI

POST /v5/{project_id}/ransomware/protection/open

表 3-256 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

表 3-257 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-258 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）

表 3-259 请求 Body 参数

参数	是否必选	参数类型	描述
operating_system	是	String	操作系统，包含如下： • Windows : Windows系统 • Linux : Linux系统
ransom_protection_status	是	String	勒索防护是否开启，包含如下： • closed： 关闭。 • opened： 开启。 若选择开启，protection_policy_id或者create_protection_policy必填一项
protection_policy_id	否	String	防护策略ID,若选择已有策略防护,则该字段必选
create_protection_policy	否	**ProtectionProxyInfoRequestInfo** object	创建防护策略。若新建防护策略，则protection_policy_id为空，create_protection_policy必选
backup_protection_status	是	String	是否服务器备份，包含如下： • closed： 关闭。 • opened： 开启。 若选择开启服务器备份，则backup_cycle必填
backup_resources	否	**BackupResources** object	开启备份功能新版参数，必填；若为空代表兼容之前绑定HSS_projectid的存储库
backup_policy_id	否	String	备份策略ID
backup_cycle	否	**UpdateBackupPolicyRequestInfo1** object	备份策略
agent_id_list	是	Array of strings	开启防护的Agent id列表
host_id_list	是	Array of strings	开启防护的host id列表

表 3-260 ProtectionProxyInfoRequestInfo

参数	是否必选	参数类型	描述
policy_id	否	String	策略ID，新建策略可不填
policy_name	否	String	策略名称，新建防护策略则必填
protection_mode	否	String	防护动作，新建防护策略则必填。包含如下： • alarm_and_isolation ： 告警并自动隔离。 • alarm_only ： 仅告警。
bait_protection_status	否	String	是否开启诱饵防护，新建防护策略则必填。包含如下1种, 默认为开启防护诱饵防护。 • opened ： 开启。 • closed ： 关闭。
protection_directory	否	String	防护目录，新建防护策略则必填
protection_type	否	String	防护类型，新建防护策略则必填
exclude_directory	否	String	排除目录，可选填
runtime_detection_status	否	String	是否运行时检测，选填。包含如下2种，暂时只有关闭一种状态，为保留字段。 • opened ： 开启。 • closed ： 关闭。
operating_system	否	String	操作系统，新建防护策略则必填。包含如下： • Windows : Windows系统 • Linux : Linux系统
process_whitelist	否	Array of **TrustProcessInfo** objects	进程白名单

表 3-261 TrustProcessInfo

参数	是否必选	参数类型	描述
path	否	String	进程路径
hash	否	String	进程hash

表 3-262 BackupResources

参数	是否必选	参数类型	描述
vault_id	否	String	选择需要绑定的存储库ID，不为空
resource_list	否	Array of **ResourceInfo** objects	需要开启备份功能的主机情况列表

表 3-263 ResourceInfo

参数	是否必选	参数类型	描述
host_id	否	String	主机id
history_backup_status	否	String	历史开启备份状态，通过筛选可用服务器的error_message或者status判断，如果error_message为空，则没有开启备份，该字段为closed；若不为空，则为opened

表 3-264 UpdateBackupPolicyRequestInfo1

参数	是否必选	参数类型	描述
enabled	否	Boolean	策略是否启用，缺省值：true
policy_id	否	String	策略ID,若开启防护时开启备份防护，该字段必选
operation_definition	否	**OperationDefinitionRequestInfo** object	调度参数
trigger	否	**BackupTriggerRequestInfo1** object	策略时间调度规则

表 3-265 OperationDefinitionRequestInfo

参数	是否必选	参数类型	描述
day_backups	否	Integer	保留日备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0，最大值：100

参数	是否必选	参数类型	描述
max_backups	否	Integer	单个备份对象自动备份的最大备份数。取值为-1或0-99999。-1代表不按备份数清理。若该字段和retention_duration_days字段同时为空，备份会永久保留。最小值：1,最大值：99999,缺省值：-1
month_backups	否	Integer	保留月备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0,最大值：100
retention_duration_days	否	Integer	备份保留时长，单位天。最长支持99999天。-1代表不按时间清理。若该字段和max_backups参数同时为空，备份会永久保留。最小值：1, 最大值：99999, 缺省值：-1
timezone	否	String	用户所在时区,格式形如UTC +08:00,若没有选择年备，月备，周备，日备中任一参数，则不能选择该参数。
week_backups	否	Integer	保留周备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。
year_backups	否	Integer	保留年备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0，最大值：100

表 3-266 BackupTriggerRequestInfo1

参数	是否必选	参数类型	描述
properties	否	**BackupTriggerPropertiesRequestInfo1** object	策略执行时间规则，若开启勒索防护时开启备份功能，则该字段必选

表 3-267 BackupTriggerPropertiesRequestInfo1

参数	是否必选	参数类型	描述
pattern	否	Array of strings	调度规则。若开启勒索防护时开启备份功能，则该字段必选。限制24条规则。调度器的调度规则，可参照iCalendar RFC 2445规范中的事件规则，但仅支持FREQ、BYDAY、BYHOUR、BYMINUTE、INTERVAL等参数，其中FREQ仅支持WEEKLY和DAILY，BYDAY支持一周七天（MO、TU、WE、TH、FR、SA、SU），BYHOUR支持0-23小时，BYMINUTE支持0-59分钟，并且间隔不能小于一小时，一天最大24个时间点。例如，周一到周天，每天14:00调度，其规则为：'FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00'。每天14:00调度，其规则为'FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00'。

响应参数

状态码：200

开启勒索病毒防护成功

无

请求示例

开启服务器勒索病毒防护，目标服务器操作系统类型为Linux，目标服务器ID为71a15ecc-049f-4cca-bd28-5e90aca1817f，目标服务器的Agent ID为c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8，不开启服务器备份。

```
POST https://{endpoint}/v5/{project_id}/ransomware/protection/open

{
  "ransom_protection_status" : "opened",
  "backup_protection_status" : "closed",
  "operating_system" : "Linux",
  "protection_policy_id" : "",
  "agent_id_list" : [ "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8" ],
  "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
  "create_protection_policy" : {
    "bait_protection_status" : "opened",
    "exclude_directory" : "",
    "protection_mode" : "alarm_only",
    "policy_name" : "test111",
```

```
  "protection_directory" : "/etc/test",
  "protection_type" : "docx"
 }
}
```

响应示例

无

状态码

状态码	描述
200	开启勒索病毒防护成功

错误码

请参见**错误码**。

3.7.5 关闭勒索病毒防护

功能介绍

关闭勒索病毒防护

URI

POST /v5/{project_id}/ransomware/protection/close

表 3-268 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

表 3-269 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-270 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）

表 3-271 请求 Body 参数

参数	是否必选	参数类型	描述
host_id_list	是	Array of strings	需要关闭勒索防护的主机ID列表
agent_id_list	是	Array of strings	需要关闭勒索防护的agentID列表
close_protection_type	是	String	关闭防护类型，包含如下： • close_all : 关闭所有防护 • close_anti : 关闭勒索防护 • close_backup : 关闭备份功能

响应参数

状态码：200

关闭勒索病毒防护成功

无

请求示例

关闭服务器勒索病毒防护，目标服务器ID为71a15ecc-049f-4cca-bd28-5e90aca1817f，目标服务器的Agent ID为c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8。

```
POST https://{endpoint}/v5/{project_id}/ransomware/protection/close

{
  "close_protection_type" : "close_anti",
  "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
  "agent_id_list" : [ "c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8" ]
}
```

响应示例

无

状态码

状态码	描述
200	关闭勒索病毒防护成功

错误码

请参见错误码。

3.7.6 查询 HSS 存储库绑定的备份策略信息

功能介绍

查询HSS存储库绑定的备份策略信息,确保已经购买了勒索防护存储库，可以从cbr云备份服务进行验证，确保已经存在HSS_projectid命名的存储库已经购买

URI

GET /v5/{project_id}/backup/policy

表 3-272 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

表 3-273 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-274 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）

响应参数

状态码：200

表 3-275 响应 Body 参数

参数	参数类型	描述
enabled	Boolean	策略是否启用
id	String	策略ID
name	String	策略名称
operation_type	String	备份类型。备份（backup）、复制(replication)，包含如下2种。 • backup： 备份。 • replication： 复制。
operation_definition	**OperationDefinitionInfo** object	策略属性 保留规则
trigger	**BackupTriggerInfo** object	备份:策略时间调度规则

表 3-276 OperationDefinitionInfo

参数	参数类型	描述
day_backups	Integer	保留日备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0,最大值：100
max_backups	Integer	单个备份对象自动备份的最大备份数。取值为-1或0-99999。-1代表不按备份数清理。若该字段和retention_duration_days字段同时为空，备份会永久保留。最小值：1,最大值：99999,缺省值：-1
month_backups	Integer	保留月备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0, 最大值：100
retention_duration_days	Integer	备份保留时长，单位天。最长支持99999天。-1代表不按时间清理。若该字段和max_backups 参数同时为空，备份会永久保留。最小值：1, 最大值：99999, 缺省值：-1

参数	参数类型	描述
timezone	String	用户所在时区,格式形如UTC+08:00,若没有选择年备，月备，周备，日备中任一参数，则不能选择该参数。
week_backups	Integer	保留周备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。
year_backups	Integer	保留年备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0，最大值：100

表 3-277 BackupTriggerInfo

参数	参数类型	描述
id	String	调度器id
name	String	调度器名称
type	String	调度器类型,目前只支持 time,定时调度。
properties	**BackupTriggerPropertiesInfo** object	调度器属性

表 3-278 BackupTriggerPropertiesInfo

参数	参数类型	描述
pattern	Array of strings	调度器的调度策略，长度限制为10240个字符，参照iCalendar RFC 2445规范，但仅支持FREQ、BYDAY、BYHOUR、BYMINUTE四个参数，其中FREQ仅支持WEEKLY和DAILY，BYDAY支持一周七天（MO、TU、WE、TH、FR、SA、SU），BYHOUR支持0-23小时，BYMINUTE支持0-59分钟，并且时间点间隔不能小于一小时，一个备份策略可以同时设置多个备份时间点，一天最多可以设置24个时间点。
start_time	String	调度器开始时间，例如：2020-01-08 09:59:49

请求示例

查询HSS存储库绑定的备份策略信息。

```
GET https://{endpoint}/v5/{project_id}/backup/policy
```

响应示例

状态码：200

备份策略信息

```
{
  "enabled" : true,
  "id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
  "name" : "HSS_84b5266c14ae489fa6549827f032dc62",
  "operation_type" : "backup",
  "operation_definition" : {
    "day_backups" : 0,
    "max_backups" : "-1",
    "month_backups" : 0,
    "retention_duration_days" : 5,
    "timezone" : "UTC+08:00",
    "week_backups" : 0,
    "year_backups" : 0
  },
  "trigger" : {
    "properties" : {
      "pattern" : [ "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00" ]
    }
  }
}
```

状态码

状态码	描述
200	备份策略信息

错误码

请参见**错误码**。

3.7.7 修改存储库绑定的备份策略

功能介绍

修改存储库绑定的备份策略

URI

PUT /v5/{project_id}/backup/policy

表 3-279 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

表 3-280 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-281 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）

表 3-282 请求 Body 参数

参数	是否必选	参数类型	描述
enabled	否	Boolean	策略是否启用，缺省值：true
policy_id	是	String	策略ID
operation_definition	否	**OperationDefinitionRequestInfo** object	调度参数
trigger	否	**BackupTriggerRequestInfo** object	策略时间调度规则

表 3-283 OperationDefinitionRequestInfo

参数	是否必选	参数类型	描述
day_backups	否	Integer	保留日备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0,最大值：100
max_backups	否	Integer	单个备份对象自动备份的最大备份数。取值为-1或0-99999。-1代表不按备份数清理。若该字段和retention_duration_days字段同时为空，备份会永久保留。最小值：1,最大值：99999,缺省值：-1
month_backups	否	Integer	保留月备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0,最大值：100
retention_duration_days	否	Integer	备份保留时长，单位天。最长支持99999天。-1代表不按时间清理。若该字段和max_backups参数同时为空，备份会永久保留。最小值：1, 最大值：99999, 缺省值：-1
timezone	否	String	用户所在时区,格式形如UTC+08:00,若没有选择年备，月备，周备，日备中任一参数，则不能选择该参数。
week_backups	否	Integer	保留周备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。
year_backups	否	Integer	保留年备个数，该备份不受保留最大备份数限制。取值为0到100。若选择该参数，则timezone 也必选。最小值：0，最大值：100

表 3-284 BackupTriggerRequestInfo

参数	是否必选	参数类型	描述
properties	是	**BackupTriggerPropertiesRequestInfo** object	策略执行时间规则

表 3-285 BackupTriggerPropertiesRequestInfo

参数	是否必选	参数类型	描述
pattern	是	Array of strings	调度规则。限制24条规则。调度器的调度规则，可参照iCalendar RFC 2445规范中的事件规则，但仅支持FREQ、BYDAY、BYHOUR、BYMINUTE、INTERVAL等参数，其中FREQ仅支持WEEKLY和DAILY，BYDAY支持一周七天（MO、TU、WE、TH、FR、SA、SU），BYHOUR支持0-23小时，BYMINUTE支持0-59分钟，并且间隔不能小于一小时，一天最大24个时间点。例如，周一到周天，每天14:00调度，其规则为：'FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00'。每天14:00调度，其规则为'FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00'。

响应参数

状态码：200

表 3-286 响应 Body 参数

参数	参数类型	描述
error_code	Integer	错误编码,成功返回0
error_description	String	错误描述，成功返回success

请求示例

修改备份策略，目标备份策略ID为af4d08ad-2b60-4916-a5cf-8d6a23956dda。

```
PUT https://{endpoint}/v5/{project_id}/backup/policy

{
  "enabled" : true,
  "policy_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
  "operation_definition" : {
    "day_backups" : 0,
    "max_backups" : -1,
    "month_backups" : 0,
    "retention_duration_days" : 5,
    "timezone" : "UTC+08:00",
    "week_backups" : 0,
    "year_backups" : 0
  },
  "trigger" : {
    "properties" : {
      "pattern" : [ "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00" ]
    }
  }
}
```

响应示例

状态码：200

修改备份策略

```
{
  "error_code" : 0,
  "error_description" : "success"
}
```

状态码

状态码	描述
200	修改备份策略

错误码

请参见**错误码**。

3.8 配额管理

3.8.1 查询配额信息

功能介绍

查询配额信息

URI

GET /v5/{project_id}/billing/quotas

表 3-287 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

表 3-288 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
version	否	String	主机开通的版本，包含如下7种输入。 ● hss.version.null ： 无。 ● hss.version.basic ： 基础版。 ● hss.version.advanced ： 专业版。 ● hss.version.enterprise ： 企业版。 ● hss.version.premium ： 旗舰版。 ● hss.version.wtp ： 网页防篡改版。 ● hss.version.container.enterprise：容器版。
charging_mode	否	String	收费模式，包含如下： ● on_demand ： 按需。

请求参数

表 3-289 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）

响应参数

状态码：200

表 3-290 响应 Body 参数

参数	参数类型	描述
data_list	Array of **ResourceQuotasInfo** objects	配额统计列表

表 3-291 ResourceQuotasInfo

参数	参数类型	描述
version	String	主机开通的版本，包含如下7种输入。 • hss.version.null ： 无。 • hss.version.basic ： 基础版。 • hss.version.advanced ： 专业版。 • hss.version.enterprise ： 企业版。 • hss.version.premium ： 旗舰版。 • hss.version.wtp ： 网页防篡改版。 • hss.version.container.enterprise：容器版。
total_num	Integer	总配额数
used_num	Integer	已使用配额数
available_num	Integer	可用总配额数
available_resources_list	Array of **AvailableResourceIdsInfo** objects	可用资源列表

表 3-292 AvailableResourceIdsInfo

参数	参数类型	描述
resource_id	String	资源ID
current_time	String	当前时间
shared_quota	String	是否共享配额 • shared：共享的 • unshared：非共享的

请求示例

查询所有企业项目下的基础版配额信息

```
GET https://{endpoint}/v5/{project_id}/billing/quotas?
version=hss.version.basic&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

配额统计列表

```
{
  "data_list" : [ {
    "available_num" : 1,
    "available_resources_list" : [ {
      "current_time" : "2022-09-17T17:00:24Z",
      "resource_id" : "9ecb83a7-8b03-4e37-a26d-c3e90ca97eea",
      "shared_quota" : "shared"
    } ],
    "total_num" : 2,
    "used_num" : 1,
    "version" : "hss.version.basic"
  } ]
}
```

状态码

状态码	描述
200	配额统计列表

错误码

请参见**错误码**。

3.8.2 查询配额详情

功能介绍

查询配额详情

URI

GET /v5/{project_id}/billing/quotas-detail

表 3-293 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

表 3-294 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
version	否	String	主机开通的版本，包含如下7种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.advanced： 专业版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。 ● hss.version.container.enterprise：容器版。
category	否	String	类别，包含如下几种： ● host_resource：HOST_RESOURCE ● container_resource：CONTAINER_RESOURCE
quota_status	否	String	配额状态，包含如下几种： ● normal：QUOTA_STATUS_NORMAL ● expired：QUOTA_STATUS_EXPIRED ● freeze：QUOTA_STATUS_FREEZE
used_status	否	String	使用状态，包含如下几种： ● idle： USED_STATUS_IDLE ● used：USED_STATUS_USED
host_name	否	String	服务器名称
resource_id	否	String	资源ID
charging_mode	否	String	收费模式，包含如下： ● on_demand： 按需。
limit	否	Integer	每页数量

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

请求参数

表 3-295 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）

响应参数

状态码：200

表 3-296 响应 Body 参数

参数	参数类型	描述
packet_cycle_num	Integer	配额数
on_demand_num	Integer	按需配额数
used_num	Integer	已使用配额数
idle_num	Integer	空闲配额数
normal_num	Integer	正常配额数
expired_num	Integer	过期配额数
freeze_num	Integer	冻结配额数
quota_statistics_list	Array of **QuotaStatisticsResponseInfo** objects	配额统计列表
total_num	Integer	总数
data_list	Array of **QuotaResourcesResponseInfo** objects	配额列表

表 3-297 QuotaStatisticsResponseInfo

参数	参数类型	描述
version	String	资源规格编码，包含如下: • hss.version.basic : 基础版 • hss.version.advanced : 专业版 • hss.version.enterprise : 企业版 • hss.version.premium : 旗舰版 • hss.version.wtp : 网页防篡改版 • hss.version.container : 容器版
total_num	Integer	总数

表 3-298 QuotaResourcesResponseInfo

参数	参数类型	描述
resource_id	String	主机安全配额的资源ID
version	String	资源规格编码，包含如下: • hss.version.basic : 基础版 • hss.version.advanced : 专业版 • hss.version.enterprise : 企业版 • hss.version.premium : 旗舰版 • hss.version.wtp : 网页防篡改版 • hss.version.container : 容器版
quota_status	String	配额状态 • normal : 正常 • expired : 已过期 • freeze : 已冻结
used_status	String	使用状态 • idle : 空闲 • used : 使用中
host_id	String	服务器ID
host_name	String	服务器名称
charging_mode	String	计费模式 • on_demand : 按需
tags	Array of **TagInfo** objects	标签

参数	参数类型	描述
expire_time	Long	过期时间，-1表示没有到期时间
shared_quota	String	是否共享配额 ● shared：共享的 ● unshared：非共享的
enterprise_project_id	String	企业项目ID
enterprise_project_name	String	所属企业项目名称

表 3-299 TagInfo

参数	参数类型	描述
key	String	键。最大长度128个unicode字符。 key不能为空
value	String	值。最大长度255个unicode字符。

请求示例

查询所有企业项目下的配额详情

```
GET https://{endpoint}/v5/{project_id}/billing/quotas-detail?
offset=0&limit=100&version=hss.version.basic&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

配额详情列表

```
{
  "data_list" : [ {
    "charging_mode" : "on_demand",
    "expire_time" : -1,
    "host_id" : "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    "host_name" : "zhangxiaodong2",
    "quota_status" : "normal",
    "resource_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
    "shared_quota" : "shared",
    "tags" : [ {
      "key" : "服务",
      "value" : "HSS"
    } ],
    "used_status" : "used",
    "version" : "hss.version.wtp"
  } ],
  "expired_num" : 0,
  "freeze_num" : 0,
  "idle_num" : 20,
  "normal_num" : 60,
  "on_demand_num" : 0,
```

```
  "packet_cycle_num" : 60,
  "quota_statistics_list" : [ {
    "total_num" : 8,
    "version" : "hss.version.basic"
  } ],
  "total_num" : 60,
  "used_num" : 40
}
```

状态码

状态码	描述
200	配额详情列表

错误码

请参见**错误码**。

3.9 策略管理

3.9.1 查询策略组列表

功能介绍

查询策略组列表

URI

GET /v5/{project_id}/policy/groups

表 3-300 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

表 3-301 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
group_name	否	String	策略组名
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示个数
container_mode	否	Boolean	是否查询容器版策略
group_id	否	String	策略组id

请求参数

表 3-302 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）

响应参数

状态码：200

表 3-303 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **PolicyGroupResponseInfo** objects	策略组列表

表 3-304 PolicyGroupResponseInfo

参数	参数类型	描述
group_name	String	策略组名
group_id	String	策略组ID
description	String	描述信息
deletable	Boolean	是否允许删除该策略组
host_num	Integer	关联服务器数
default_group	Boolean	是否是默认策略组

参数	参数类型	描述
support_os	String	支持的操作系统，包含如下: ● Linux： 支持Linux系统 ● Windows：支持Windows系统
support_version	String	支持的版本，包含如下: ● hss.version.basic： 基础版策略组 ● hss.version.advanced：专业版策略组 ● hss.version.enterprise：企业版策略组 ● hss.version.premium：旗舰版策略组 ● hss.version.wtp：网页防篡改版策略组 ● hss.version.container.enterprise：容器版策略组

请求示例

查询所有企业项目下的策略组列表。

```
GET https://{endpoint}/v5/{project_id}/policy/groups?
offset=0&limit=100&enterprise_project_id=all_granted_eps
```

响应示例

状态码：200

策略组列表

```
{
  "data_list" : [ {
    "default_group" : true,
    "deletable" : false,
    "description" : "container policy group for linux",
    "group_id" : "c831f177-226d-4b91-be0f-bcf98d04ef5d",
    "group_name" : "tenant_linux_container_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.container.enterprise",
    "support_os" : "Linux"
  }, {
    "default_group" : true,
    "deletable" : false,
    "description" : "enterprise policy group for windows",
    "group_id" : "1ff54b90-1b3e-42a9-a1da-9883a83385ce",
    "group_name" : "tenant_windows_enterprise_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.enterprise",
    "support_os" : "Windows"
  }, {
    "default_group" : true,
    "deletable" : false,
    "description" : "enterprise policy group for linux",
    "group_id" : "1069bcc0-c806-4ccd-a35d-f1f7456805e9",
    "group_name" : "tenant_linux_enterprise_default_policy_group ",
    "host_num" : 1,
    "support_version" : "hss.version.enterprise",
    "support_os" : "Linux"
```

```
 }, {
   "default_group" : true,
   "deletable" : false,
   "description" : "premium policy group for windows",
   "group_id" : "11216d24-9e91-4a05-9212-c4c1d646ee79",
   "group_name" : "tenant_windows_premium_default_policy_group ",
   "host_num" : 0,
   "support_version" : "hss.version.premium",
   "support_os" : "Linux"
 }, {
   "default_group" : true,
   "deletable" : false,
   "description" : "premium policy group for linux",
   "group_id" : "e6e1228a-7bb4-424f-a42b-755162234da7",
   "group_name" : "tenant_linux_premium_default_policy_group ",
   "host_num" : 0,
   "support_version" : "hss.version.premium",
   "support_os" : "Windows"
 } ],
 "total_num" : 5
}
```

状态码

状态码	描述
200	策略组列表

错误码

请参见**错误码**。

3.9.2 部署策略

功能介绍

部署策略

URI

POST /v5/{project_id}/policy/deploy

表 3-305 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

表 3-306 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-307 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）

表 3-308 请求 Body 参数

参数	是否必选	参数类型	描述
target_policy_group_id	是	String	部署的目标策略组ID
operate_all	否	Boolean	是否要对全量主机部署策略，如果为true的话，不需填写host_id_list，如果为false的话，需要填写host_id_list
host_id_list	否	Array of strings	服务器ID列表

响应参数

状态码：200

success

无

请求示例

部署服务器防护策略，目标服务器ID为15462c0e-32c6-4217-a869-bbd131a00ecf，目标策略ID为f671f7-2677-4705-a320-de1a62bff306。

```
POST https://{endpoint}/v5/{project_id}/policy/deploy

{
  "target_policy_group_id" : "1df671f7-2677-4705-a320-de1a62bff306",
  "host_id_list" : [ "15462c0e-32c6-4217-a869-bbd131a00ecf" ],
  "operate_all" : false
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.10 容器管理

3.10.1 查询容器节点列表

功能介绍

查询容器节点列表

URI

GET /v5/{project_id}/container/nodes

表 3-309 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

表 3-310 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业项目ID，查询所有企业项目时填写：all_granted_eps
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

参数	是否必选	参数类型	描述
limit	否	Integer	每页显示个数
host_name	否	String	节点名称
agent_status	否	String	Agent状态，包含如下3种。 • not_installed ： 未安装 • online ： 在线 • offline ： 离线
protect_status	否	String	防护状态，包含如下2种。 • closed ： 关闭 • opened ： 开启
container_tags	否	String	标签：用来识别cce容器节点和自建 • cce：cce节点 • self：自建节点 • other：其他节点

请求参数

表 3-311 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）

响应参数

状态码：200

表 3-312 响应 Body 参数

参数	参数类型	描述
total_num	Integer	容器节点总数
data_list	Array of **ContainerNodeInfo** objects	容器节点列表

表 3-313 ContainerNodeInfo

参数	参数类型	描述
agent_id	String	Agent ID
host_id	String	服务器ID
host_name	String	节点名称
host_status	String	服务器状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。
agent_status	String	Agent状态，包含如下3种。 ● not_installed： 未安装。 ● online： 在线。 ● offline： 离线。
protect_status	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
protect_interrupt	Boolean	防护是否中断
protect_degradation	Boolean	防护是否降级
degradation_reason	String	防护降级原因
container_tags	String	标签：用来识别cce容器节点和自建 ● cce：cce节点 ● self：自建节点 ● other：其他节点
private_ip	String	私有IP地址
public_ip	String	弹性公网IP地址
resource_id	String	主机安全配额ID（UUID）
group_name	String	服务器组名称
enterprise_project_name	String	所属企业项目名称

参数	参数类型	描述
detect_result	String	云主机安全检测结果，包含如下4种。 ● undetected： 未检测。 ● clean： 无风险。 ● risk： 有风险。 ● scanning： 检测中。
asset	Integer	资产风险
vulnerability	Integer	漏洞风险
intrusion	Integer	入侵风险
policy_group_id	String	策略组ID
policy_group_name	String	策略组名称

请求示例

查询容器节点列表，不传limit参数默认返回10条。

```
GET https://{endpoint}/v5/{project_id}/container/nodes
```

响应示例

状态码：200

success response

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2d0fe7824005bf001220ad9d892e86f8af44XXXXXXXXXX",
    "agent_status" : "online",
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_status" : "ACTIVE",
    "protect_status" : "opened",
    "protect_intrrupt" : false,
    "private_ip" : "192.168.0.114",
    "public_ip" : "100.85.218.122",
    "resource_id" : "ef5eb4fd-7376-48ac-886f-16fd057776f3",
    "group_name" : "as(All projects)",
    "enterprise_project_name" : "default",
    "detect_result" : "risk",
    "asset" : 0,
    "vulnerability" : 14,
    "intrusion" : 0,
    "policy_group_id" : "ce4d5e95-0cbf-4102-9c77-ef1bcb6b35aa",
    "policy_group_name" : "tenant_linux_enterprise_default_policy_group (All projects)"
  } ]
}
```

状态码

状态码	描述
200	success response

错误码

请参见**错误码**。

3.11 漏洞管理

3.11.1 查询漏洞列表

功能介绍

查询漏洞列表

URI

GET /v5/{project_id}/vulnerability/vulnerabilities

表 3-314 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

表 3-315 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps
type	否	String	漏洞类型，包含如下： -linux_vul : linux漏洞 -windows_vul : windows漏洞 -web_cms : Web-CMS漏洞 -app_vul : 应用漏洞
vul_id	否	String	漏洞ID
vul_name	否	String	漏洞名称
limit	否	Integer	每页显示个数

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
repair_priority	否	String	修复优先级 Critical 紧急 High 高 Medium 中 Low 低
handle_status	否	String	处置状态，包含如下: ● unhandled ： 未处理 ● handled : 已处理
cve_id	否	String	漏洞编号
label_list	否	String	漏洞标签
status	否	String	漏洞状态
asset_value	否	String	资产重要性 important common test
group_name	否	String	服务器组名称

请求参数

表 3-316 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）

响应参数

状态码：200

表 3-317 响应 Body 参数

参数	参数类型	描述
total_num	Long	总数
data_list	Array of **VulInfo** objects	软件漏洞列表

表 3-318 VulInfo

参数	参数类型	描述
vul_name	String	漏洞名称
vul_id	String	漏洞ID
label_list	Array of strings	漏洞标签
repair_necessity	String	修复必要性
severity_level	String	漏洞级别
host_num	Integer	受影响服务器台数
unhandle_host_num	Integer	未处理服务器台数
scan_time	Long	最近扫描时间
solution_detail	String	解决方案
url	String	URL链接
description	String	漏洞描述
type	String	漏洞类型，包含如下： -linux_vul : linux漏洞 -windows_vul : windows漏洞 -web_cms : Web-CMS漏洞 -app_vul : 应用漏洞
host_id_list	Array of strings	主机列表
cve_list	Array of **cve_list** objects	CVE列表
patch_url	String	补丁地址
repair_priority	String	修复优先级 Critical 紧急 High 高 Medium 中 Low 低

参数	参数类型	描述
hosts_num	VulnerabilityHostNumberInfo object	影响主机
repair_success_num	Integer	修复成功次数
fixed_num	Long	修复数量
ignored_num	Long	忽略数量
verify_num	Integer	验证数量

表 3-319 cve_list

参数	参数类型	描述
cve_id	String	CVE ID
cvss	Float	CVSS分值

表 3-320 VulnerabilityHostNumberInfo

参数	参数类型	描述
important	Integer	重要主机数量
common	Integer	一般主机数量
test	Integer	测试主机数量

请求示例

查询project_id为2b31ed520xxxxxxebedb6e57xxxxxxxx的漏洞列表前10条数据。

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/vulnerabilities?offset=0&limit=10
```

响应示例

状态码：200

漏洞列表

```
{
  "total_num" : 1,
  "data_list" : [ {
    "description" : "It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, or possibly execute arbitrary code.",
    "host_id_list" : [ "caa958ad-a481-4d46-b51e-6861b8864515" ],
    "host_num" : 1,
```

```
  "scan_time" : 1661752185836,
  "severity_level" : "Critical",
  "repair_necessity" : "Critical",
  "solution_detail" : "To upgrade the affected software",
  "type" : "linux_vul",
  "unhandle_host_num" : 0,
  "url" : "https://ubuntu.com/security/CVE-2022-27405",
  "vul_id" : "USN-5528-1",
  "vul_name" : "USN-5528-1: FreeType vulnerabilities"
 } ]
}
```


状态码

状态码	描述
200	漏洞列表

错误码

请参见**错误码**。

3.11.2 查询单个漏洞影响的云服务器信息

功能介绍

查询单个漏洞影响的云服务器信息

URI

GET /v5/{project_id}/vulnerability/hosts

表 3-321 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-322 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps
vul_id	是	String	漏洞ID

参数	是否必选	参数类型	描述
type	是	String	漏洞类型 ● linux_vul : 漏洞类型-linux漏洞 ● windows_vul : 漏洞类型-windows漏洞 ● web_cms : Web-CMS漏洞 ● app_vul : 应用漏洞 ● urgent_vul : 应急漏洞
host_name	否	String	受影响资产名称
host_ip	否	String	受影响资产ip
status	否	String	漏洞状态 ● vul_status_unfix : 未处理 ● vul_status_ignored : 已忽略 ● vul_status_verified : 验证中 ● vul_status_fixing : 修复中 ● vul_status_fixed : 修复成功 ● vul_status_reboot : 修复成功待重启 ● vul_status_failed : 修复失败 ● vul_status_fix_after_reboot : 请重启主机再次修复
limit	否	Integer	每页条数
offset	否	Integer	偏移
asset_value	否	String	资产重要性 important:重要 common：一般 test：测试
group_name	否	String	服务器组名称
handle_status	否	String	处置状态，包含如下: ● unhandled ： 未处理 ● handled : 已处理
severity_level	否	String	危险程度 ，Critical，High，Medium，Low
is_affect_business	否	Boolean	是否影响业务

请求参数

表 3-323 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）

响应参数

状态码：200

表 3-324 响应 Body 参数

参数	参数类型	描述
total_num	Integer	受影响的云服务器台数
data_list	Array of **VulHostInfo** objects	受影响的云服务器台数信息

表 3-325 VulHostInfo

参数	参数类型	描述
host_id	String	主机id
severity_level	String	危险程度 • Critical : 漏洞cvss评分大于等于9；对应控制台页面的高危 • High : 漏洞cvss评分大于等于7，小于9；对应控制台页面的中危 • Medium : 漏洞cvss评分大于等于4，小于7；对应控制台页面的中危 • Low : 漏洞cvss评分小于4；对应控制台页面的低危
host_name	String	受影响资产名称
host_ip	String	受影响资产ip
agent_id	String	主机对应的agent id
cve_num	Integer	漏洞cve数
cve_id_list	Array of strings	cve列表

参数	参数类型	描述
status	String	漏洞状态 ● vul_status_unfix：未处理 ● vul_status_ignored：已忽略 ● vul_status_verified：验证中 ● vul_status_fixing：修复中 ● vul_status_fixed：修复成功 ● vul_status_reboot：修复成功待重启 ● vul_status_failed：修复失败 ● vul_status_fix_after_reboot：请重启主机再次修复
repair_cmd	String	修复命令行
app_path	String	应用软件的路径（只有应用漏洞有该字段）
region_name	String	地域
public_ip	String	服务器公网ip
private_ip	String	服务器私网ip
group_id	String	服务器组id
group_name	String	服务器组名称
os_type	String	操作系统
asset_value	String	资产重要性，包含如下3种 important： 重要资产 common： 一般资产 test： 测试资产
is_affect_business	Boolean	是否影响业务
first_scan_time	Long	首次扫描时间
scan_time	Long	扫描时间
support_restore	Boolean	是否可以回滚到修复漏洞时创建的备份

请求示例

查询具有漏洞EulerOS-SA-2021-1894的服务器列表的前10条数据

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/hosts?vul_id=EulerOS-SA-2021-1894&offset=0&limit=10
```

响应示例

状态码：200

Vul host info list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "severity_level" : "Low",
    "host_name" : "ecs",
    "host_ip" : "xxx.xxx.xxx.xxx",
    "agent_id" : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "cve_num" : 1,
    "cve_id_list" : [ "CVE-2022-1664" ],
    "status" : "vul_status_ignored",
    "repair_cmd" : "zypper update update-alternatives",
    "app_path" : "/root/apache-tomcat-8.5.15/bin/bootstrap.jar",
    "support_restore" : true
  } ]
}
```

状态码

状态码	描述
200	Vul host info list

错误码

请参见错误码。

3.11.3 修改漏洞的状态

功能介绍

修改漏洞的状态

URI

PUT /v5/{project_id}/vulnerability/status

表 3-326 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID

表 3-327 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-328 请求 Header 参数

参数	是否必选	参数类型	描述
x-auth-token	是	String	iam token

表 3-329 请求 Body 参数

参数	是否必选	参数类型	描述
operate_type	是	String	操作类型 • ignore : 忽略 • not_ignore : 取消忽略 • immediate_repair : 修复 • manual_repair: 人工修复 • verify : 验证 • add_to_whitelist : 加入白名单
remark	否	String	备注
select_type	否	String	选择全部漏洞类型 • all_vul : 选择全部漏洞 • all_host : 选择全部主机漏洞
type	否	String	漏洞类型，默认为linux_vul，包括如下： • linux_vul : 漏洞类型-linux漏洞 • windows_vul : 漏洞类型-windows漏洞 • web_cms : Web-CMS漏洞 • app_vul : 应用漏洞 • urgent_vul : 应急漏洞

参数	是否必选	参数类型	描述
data_list	是	Array of **VulOperateInfo** objects	漏洞列表
host_data_list	否	Array of **HostVulOperateInfo** objects	主机维度漏洞列表
backup_info_id	否	String	本次漏洞处理的备份信息id，若不传该参数，则不进行备份
custom_backup_hosts	否	Array of **custom_backup_hosts** objects	自定义备份主机使用的存储库及备份名称；不在该列表中的主机备份时系统会自动选取剩余空间最大的存储库，并自动生成备份名称

表 3-330 VulOperateInfo

参数	是否必选	参数类型	描述
vul_id	是	String	漏洞ID
host_id_list	是	Array of strings	主机列表

表 3-331 HostVulOperateInfo

参数	是否必选	参数类型	描述
host_id	是	String	主机ID
vul_id_list	是	Array of strings	漏洞列表

表 3-332 custom_backup_hosts

参数	是否必选	参数类型	描述
host_id	否	String	主机id
vault_id	否	String	存储库id
backup_name	否	String	备份名称

响应参数

状态码：200

successful response

无

请求示例

修改ID为71a15ecc-049f-4cca-bd28-5e90aca1817f的服务器的漏洞状态，将EulerOS-SA-2021-1894漏洞状态修改为忽略。

```
{
  "operate_type" : "ignore",
  "data_list" : [ {
    "vul_id" : "EulerOS-SA-2021-1894",
    "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ]
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.11.4 查询单台服务器漏洞信息

功能介绍

查询单台服务器漏洞信息

URI

GET /v5/{project_id}/vulnerability/host/{host_id}

表 3-333 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
host_id	是	String	服务器id

表 3-334 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps
type	否	String	漏洞类型，默认为linux_vul，包括如下： ● linux_vul : 漏洞类型-linux漏洞 ● windows_vul : 漏洞类型-windows漏洞 ● web_cms : Web-CMS漏洞 ● app_vul : 应用漏洞 ● urgent_vul : 应急漏洞
vul_name	否	String	漏洞名称
limit	否	Integer	每页显示个数
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
handle_status	否	String	处置状态，包含如下: ● unhandled ： 未处理 ● handled : 已处理
status	否	String	漏洞状态，包含如下： ● vul_status_unfix : 未处理 ● vul_status_ignored : 已忽略 ● vul_status_verified : 验证中 ● vul_status_fixing : 修复中 ● vul_status_fixed : 修复成功 ● vul_status_reboot : 修复成功待重启 ● vul_status_failed : 修复失败 ● vul_status_fix_after_reboot : 请重启主机再次修复

请求参数

表 3-335 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）

响应参数

状态码：200

表 3-336 响应 Body 参数

参数	参数类型	描述
total_num	Long	总数
data_list	Array of **HostVulInfo** objects	服务器上的漏洞列表

表 3-337 HostVulInfo

参数	参数类型	描述
vul_name	String	漏洞名称
vul_id	String	漏洞ID
label_list	Array of strings	漏洞标签列表
repair_necessity	String	修复紧急度，包括如下： • immediate_repair : 尽快修复 • delay_repair : 延后修复 • not_needed_repair : 暂可不修复
scan_time	Long	最近扫描时间
type	String	漏洞类型，包含如下： -linux_vul : linux漏洞 -windows_vul : windows漏洞 -web_cms : Web-CMS漏洞 -app_vul : 应用漏洞

参数	参数类型	描述
app_list	Array of **app_list** objects	服务器上受该漏洞影响的软件列表
severity_level	String	危险程度 • Critical：漏洞cvss评分大于等于9；对应控制台页面的高危 • High：漏洞cvss评分大于等于7，小于9；对应控制台页面的中危 • Medium：漏洞cvss评分大于等于4，小于7；对应控制台页面的中危 • Low：漏洞cvss评分小于4；对应控制台页面的低危
solution_detail	String	解决方案
url	String	URL链接
description	String	漏洞描述
repair_cmd	String	修复命令行
status	String	漏洞状态 • vul_status_unfix：未处理 • vul_status_ignored：已忽略 • vul_status_verified：验证中 • vul_status_fixing：修复中 • vul_status_fixed：修复成功 • vul_status_reboot：修复成功待重启 • vul_status_failed：修复失败 • vul_status_fix_after_reboot：请重启主机再次修复
repair_success_num	Integer	HSS全网修复该漏洞的次数
cve_list	Array of **cve_list** objects	CVE列表
is_affect_business	Boolean	是否影响业务
first_scan_time	Long	首次扫描时间
app_name	String	软件名称
app_version	String	软件版本
app_path	String	软件路径
version	String	主机配额

参数	参数类型	描述
support_restore	Boolean	是否可以回滚到修复漏洞时创建的备份

表 3-338 app_list

参数	参数类型	描述
app_name	String	软件名称
app_version	String	软件版本
upgrade_version	String	修复漏洞软件需要升级到的版本
app_path	String	应用软件的路径（只有应用漏洞有该字段）

表 3-339 cve_list

参数	参数类型	描述
cve_id	String	CVE ID
cvss	Float	CVSS分值

请求示例

查询id为xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx的服务器上的漏洞列表前10条数据

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/host/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx?offset=0&limit=10
```

响应示例

状态码：200

服务器上的漏洞列表

```
{
  "data_list" : [ {
    "app_list" : [ {
      "app_name" : "Apache Log4j API(Apache Log4j API)",
      "app_version" : "2.8.2",
      "upgrade_version" : "2.8.3",
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"
    }, {
      "app_name" : "Apache Log4j Core(Apache Log4j Core)",
      "app_version" : "2.8.2",
      "upgrade_version" : "2.8.3",
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"
    } ],
    "app_name" : "Apache Log4j API(Apache Log4j API)",
    "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar",
    "app_version" : "2.8.2",
    "cve_list" : [ {
```

```
      "cve_id" : "CVE-2021-45046",
      "cvss" : 9
    } ],
    "description" : "发现在某些非默认配置中， Apache Log4j 2.15.0中针对CVE-2021-44228的修复不完整。当日志记录配置使用具有上下文查找（例如$${ctx:loginId}）或线程上下文映射模式（%X, %mdc或%MDC）使用JNDI查找模式构建恶意输入数据，从而在某些环境中导致信息泄漏和远程代码执行。Log4j 2.16.0 (Java 8)和2.12.2 (Java 7)通过删除对消息查找模式的支持并在默认情况下禁用JNDI功能来修复此问题。",
    "first_scan_time" : 1688956612533,
    "is_affect_business" : true,
    "label_list" : [ ],
    "repair_necessity" : "Critical",
    "scan_time" : 1690469489713,
    "severity_level" : "Critical",
    "repair_cmd" : "yum update tcpdump",
    "solution_detail" : "针对该漏洞的官方修复建议已发布，您可点击链接按照建议进行修复：\nhttps://logging.apache.org/log4j/2.x/security.html\n针对该漏洞的补丁可参考：\nhttps://www.oracle.com/security-alerts/cpujan2022.html\n针对该漏洞的非官方修复建议可参考：\nhttp://www.openwall.com/lists/oss-security/2021/12/14/4\nhttps://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html\nhttps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd\nhttp://www.openwall.com/lists/oss-security/2021/12/15/3\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf\nhttps://www.kb.cert.org/vuls/id/930724\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf\nhttps://www.debian.org/security/2021/dsa-5022\nhttps://www.oracle.com/security-alerts/alert-cve-2021-44228.html\nhttps://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032\nhttp://www.openwall.com/lists/oss-security/2021/12/18/1\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EOKPQGV24RRBBI4TBZUDQMM4MEH7MXCY/\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SIG7FZULMNK2XF6FZRU4VWYDQXNMUGAJ/\n针对该漏洞的漏洞利用/POC已曝光，可参考下方链接进行验证：\nhttps://github.com/X1pe0/Log4J-Scan-Win\nhttps://github.com/cckuailong/Log4j_CVE-2021-45046\nhttps://github.com/BobTheShoplifter/CVE-2021-45046-Info\nhttps://github.com/tejas-nagchandi/CVE-2021-45046\nhttps://github.com/pravin-pp/log4j2-CVE-2021-45046\nhttps://github.com/mergebase/log4j-samples\nhttps://github.com/lukepasek/log4jjndilookupremove\nhttps://github.com/ludy-dev/cve-2021-45046\nhttps://github.com/lijiejie/log4j2_vul_local_scanner\nhttps://github.com/CaptanMoss/Log4Shell-Sandbox-Signature\nhttps://github.com/taise-hub/log4j-poc",
    "status" : "vul_status_unfix",
    "type" : "app_vul",
    "url" : "[\"https://www.oracle.com/security-alerts/cpujan2022.html\"]",
    "version" : "hss.version.wtp",
    "vul_id" : "HCVD-APP-CVE-2021-45046",
    "vul_name" : "CVE-2021-45046",
    "repair_success_num" : 3,
    "support_restore" : true
  } ],
  "total_num" : 31
}
```


状态码

状态码	描述
200	服务器上的漏洞列表

错误码

请参见**错误码**。

3.11.5 创建漏洞扫描任务

功能介绍

创建漏洞扫描任务

URI

POST /v5/{project_id}/vulnerability/scan-task

表 3-340 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 3-341 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID

请求参数

表 3-342 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）

表 3-343 请求 Body 参数

参数	是否必选	参数类型	描述
manual_scan_type	否	Array of strings	操作类型,包含如下: -linux_vul : linux漏洞 -windows_vul : windows漏洞 -web_cms : Web-CMS漏洞 -app_vul : 应用漏洞 -urgent_vul : 应急漏洞
batch_flag	否	Boolean	是否是批量操作,为true时扫描所有支持的主机
range_type	否	String	扫描主机的范围，包含如下: -all_host : 扫描全部主机,此类型不需要填写agent_id_list -specific_host : 扫描指定主机

参数	是否必选	参数类型	描述
agent_id_list	否	Array of strings	主机列表

参数	是否必选	参数类型	描述
urgent_vul_id_list	否	Array of strings	扫描的应急漏洞id列表，若为空则扫描所有应急漏洞 包含如下： "URGENT-CVE-2023-46604 Apache ActiveMQ远程代码执行漏洞" "URGENT-HSSVD-2020-1109 Elasticsearch 未授权访问漏洞" "URGENT-CVE-2022-26134 Atlassian Confluence OGNL 远程代码执行漏洞（CVE-2022-26134）" "URGENT-CVE-2023-22515 Atlassian Confluence Data Center and Server 权限提升漏洞(CVE-2023-22515)" "URGENT-CVE-2023-22518 Atlassian Confluence Data Center & Server 授权机制不恰当漏洞(CVE-2023-22518)" "URGENT-CVE-2023-28432 MinIO 信息泄露漏洞（CVE-2023-28432）" "URGENT-CVE-2023-37582 Apache RocketMQ 远程代码执行漏洞(CVE-2023-37582)" "URGENT-CVE-2023-33246 Apache RocketMQ 远程代码执行漏洞(CVE-2023-33246)" "URGENT-CNVD-2023-02709 禅道项目管理系统远程命令执行漏洞(CNVD-2023-02709)" "URGENT-CVE-2022-36804 Atlassian Bitbucket Server 和 Data Center 命令注入漏洞 (CVE-2022-36804)" "URGENT-CVE-2022-22965 Spring Framework JDK >= 9 远程代码执行漏洞" "URGENT-CVE-2022-25845 fastjson <1.2.83 远程代码执行漏洞" "URGENT-CVE-2019-14439 Jackson-databind远程命令执行漏洞（CVE-2019-14439）"

参数	是否必选	参数类型	描述
			"URGENT-CVE-2020-13933 Apache Shiro身份验证绕过漏洞（CVE-2020-13933）" "URGENT-CVE-2020-26217 XStream < 1.4.14 远程代码执行漏洞（CVE-2020-26217）" "URGENT-CVE-2021-4034 Linux Polkit 权限提升漏洞预警（CVE-2021-4034）" "URGENT-CVE-2021-44228 Apache Log4j2 远程代码执行漏洞（CVE-2021-44228、CVE-2021-45046）" "URGENT-CVE-2022-0847 Dirty Pipe - Linux 内核本地提权漏洞（CVE-2022-0847）"

响应参数

状态码：200

表 3-344 响应 Body 参数

参数	参数类型	描述
task_id	String	检测任务id

请求示例

创建agent_id为0253edfd-30e7-439d-8f3f-17c54c997064，检测漏洞Id列表为urgent_vul_id_list的应急漏洞检测任务

```
POST https://{endpoint}/v5/{project_id}/vulnerability/scan-task?enterprise_project_id=XXX

{
  "manual_scan_type" : "urgent_vul",
  "batch_flag" : false,
  "range_type" : "specific_host",
  "agent_id_list" : [ "0253edfd-30e7-439d-8f3f-17c54c997064" ],
  "urgent_vul_id_list" : [ "URGENT-CVE-2023-46604", "URGENT-HSSVD-2020-1109", "URGENT-CVE-2022-26134", "URGENT-CVE-2023-22515", "URGENT-CVE-2023-22518", "URGENT-CVE-2023-28432", "URGENT-CVE-2023-37582", "URGENT-CVE-2023-33246", "URGENT-CNVD-2023-02709", "URGENT-CVE-2022-36804", "URGENT-CVE-2022-22965", "URGENT-CVE-2022-25845", "URGENT-CVE-2019-14439", "URGENT-CVE-2020-13933", "URGENT-CVE-2020-26217", "URGENT-CVE-2021-4034", "URGENT-CVE-2021-44228", "URGENT-CVE-2022-0847" ]
}
```

响应示例

状态码：200

手动检测漏洞成功

```
{
  "task_id" : "d8a12cf7-6a43-4cd6-92b4-aabf1e917"
}
```

状态码

状态码	描述
200	手动检测漏洞成功

错误码

请参见**错误码**。

3.11.6 查询漏洞扫描策略

功能介绍

查询漏洞扫描策略

URI

GET /v5/{project_id}/vulnerability/scan-policy

表 3-345 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

表 3-346 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-347 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）

响应参数

状态码：200

表 3-348 响应 Body 参数

参数	参数类型	描述
scan_period	String	扫描周期 ● one_day : 每天 ● three_day : 每三天 ● one_week : 每周
scan_vul_types	Array of strings	扫描的漏洞类型列表
scan_range_type	String	扫描主机的范围，包含如下： -all_host : 扫描全部主机 -specific_host : 扫描指定主机
host_ids	Array of strings	主机ID列表；当scan_range_type的值为specific_host时表示扫描的主机列表
total_host_num	Long	可进行漏洞扫描的主机总数
status	String	扫描策略状态，包含如下： -open : 开启 -close : 关闭

请求示例

查询project_id为2b31ed520xxxxxxebedb6e57xxxxxxxx的漏洞扫描策略

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/scan-policy
```

响应示例

状态码：200

漏洞扫描策略

```
{
  "scan_period" : "one_day",
  "scan_vul_types" : [ "linux_vul" ],
  "scan_range_type" : "specific_host",
  "host_ids" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
  "total_host_num" : 5,
  "status" : "open"
}
```

状态码

状态码	描述
200	漏洞扫描策略

错误码

请参见错误码。

3.11.7 修改漏洞扫描策略

功能介绍

修改漏洞扫描策略

URI

PUT /v5/{project_id}/vulnerability/scan-policy

表 3-349 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

表 3-350 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，注：修改漏洞扫描策略将影响租户账号下所有主机的漏洞扫描行为，因此开通了多企业项目的用户，该参数须填写“all_granted_eps”才能执行漏洞策略修改。

请求参数

表 3-351 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）

表 3-352 请求 Body 参数

参数	是否必选	参数类型	描述
scan_period	是	String	扫描周期 • one_day : 每天 • three_day : 每三天 • one_week : 每周
scan_range_type	是	String	扫描主机的范围，包含如下： -all_host : 扫描全部主机 -specific_host : 扫描指定主机
host_ids	否	Array of strings	主机ID列表；当scan_range_type的值为specific_host时必填
scan_vul_types	否	Array of strings	扫描的漏洞类型列表
status	是	String	扫描策略状态，包含如下： -open : 开启 -close : 关闭

响应参数

状态码：200

successful response

无

请求示例

修改漏洞扫描策略，扫描周期为每天，扫描范围为指定主机，指定的主机id为xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx，策略状态为开启

```
PUT https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/scan-policy?enterprise_project_id=all_granted_eps
```

```
{
  "scan_period" : "one_day",
  "scan_range_type" : "specific_host",
  "host_ids" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
  "status" : "open"
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

3.11.8 查询漏洞扫描任务列表

功能介绍

查询漏洞扫描任务列表

URI

GET /v5/{project_id}/vulnerability/scan-tasks

表 3-353 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

表 3-354 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
limit	否	Integer	每页显示个数
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0

参数	是否必选	参数类型	描述
scan_type	否	String	扫描任务的类型，包含如下： -manual：手动扫描任务 -schedule：定时扫描任务
task_id	否	String	扫描任务ID
min_start_time	否	Long	扫描任务开始时间的最小值
max_start_time	否	Long	扫描任务开始时间的最大值

请求参数

表 3-355 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）

响应参数

状态码：200

表 3-356 响应 Body 参数

参数	参数类型	描述
total_num	Long	总数
data_list	Array of VulScanTaskInfo objects	漏洞扫描任务列表

表 3-357 VulScanTaskInfo

参数	参数类型	描述
id	String	任务ID

参数	参数类型	描述
scan_type	String	扫描任务的类型，包含如下： -manual：手动扫描任务 -schedule：定时扫描任务
start_time	Long	扫描任务开始的时间
end_time	Long	扫描任务结束的时间
scan_vul_types	Array of strings	该任务扫描的漏洞类型列表
status	String	扫描任务的执行状态，包含如下： -running：扫描中 -finished：扫描完成
scanning_host_num	Integer	该任务处于扫描中状态的主机数量
success_host_num	Integer	该任务已扫描成功的主机数量
failed_host_num	Integer	该任务已扫描失败的主机数量

请求示例

查询任务类型为手动扫描，task_id为195db604-2008-4e8b-a49e-389ab0175beb漏洞扫描任务信息，默认查询第一页10条

```
GET https://{endpoint}/v5/{project_id}/vulnerability/scan-tasks?offset=0&limit=10&enterprise_project_id=XXX
```

```
{
  "scan_type" : "manual",
  "task_id" : "195db604-2008-4e8b-a49e-389ab0175beb"
}
```

响应示例

无

状态码

状态码	描述
200	漏洞扫描任务列表

错误码

请参见**错误码**。

3.11.9 查询漏洞扫描任务对应的主机列表

功能介绍

查询漏洞扫描任务对应的主机列表

URI

GET /v5/{project_id}/vulnerability/scan-task/{task_id}/hosts

表 3-358 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
task_id	是	String	任务ID

表 3-359 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，查询所有企业项目时填写：all_granted_eps
limit	否	Integer	每页显示个数
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
scan_status	否	String	主机的扫描状态，包含如下： -scanning : 扫描中 -success : 扫描成功 -failed : 扫描失败

请求参数

表 3-360 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）

响应参数

状态码：200

表 3-361 响应 Body 参数

参数	参数类型	描述
total_num	Long	总数
data_list	Array of **VulScanTaskHostInfo** objects	漏洞扫描任务对应的主机列表

表 3-362 VulScanTaskHostInfo

参数	参数类型	描述
host_id	String	主机ID
host_name	String	主机名称
public_ip	String	弹性公网IP地址
private_ip	String	私有IP地址
asset_value	String	资产重要性，包含如下: ● important： 重要资产 ● common： 一般资产 ● test： 测试资产
scan_status	String	主机的扫描状态，包含如下: -scanning : 扫描中 -success : 扫描成功 -failed : 扫描失败
failed_reasons	Array of **failed_reasons** objects	扫描失败的原因列表

表 3-363 failed_reasons

参数	参数类型	描述
vul_type	String	扫描失败的漏洞类型，包含如下： -linux_vul : linux漏洞 -windows_vul : windows漏洞 -web_cms : Web-CMS漏洞 -app_vul : 应用漏洞 -urgent_vul : 应急漏洞
failed_reason	String	扫描失败的原因

请求示例

查询漏洞扫描任务id为2b31ed520xxxxxxebedb6e57xxxxxxxx详情信息，展示失败的主机列表，包含失败原因，默认查询第一页10条

```
GET https://{endpoint}/v5/{project_id}/vulnerability/scan-task/{task_id}/hosts?
offset=0&limit=10&scan_status=failed&enterprise_project_id=XXX

{
  "scan_status" : "failed",
  "task_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx"
}
```

响应示例

无

状态码

状态码	描述
200	漏洞扫描任务对应的主机列表

错误码

请参见**错误码**。

3.11.10 查询漏洞管理统计数据

功能介绍

查询漏洞管理统计数据

URI

GET /v5/{project_id}/vulnerability/statistics

表 3-364 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

表 3-365 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业租户ID，“0”表示默认企业项目，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-366 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）

响应参数

状态码：200

表 3-367 响应 Body 参数

参数	参数类型	描述
need_urgent_repair	Integer	需紧急修复的漏洞数
unrepair	Integer	未完成修复的漏洞数
existed_vul_hosts	Integer	存在漏洞的服务器数
today_handle	Integer	今日处理漏洞数
all_handle	Integer	累计处理漏洞数
supported	Integer	已支持漏洞数
vul_library_update_time	Long	漏洞库更新时间

请求示例

查询project_id为2b31ed520xxxxxxebedb6e57xxxxxxxx的漏洞统计数据

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxxx/vulnerability/statistics
```

响应示例

状态码：200

```
{
  "need_urgent_repair" : 22,
  "unrepair" : 23,
  "existed_vul_hosts" : 33,
  "today_handle" : 77,
  "all_handle" : 44,
  "supported" : 78,
  "vul_library_update_time" : 1692170925188
}
```

状态码

状态码	描述
200	

错误码

请参见**错误码**。

3.12 标签管理

3.12.1 批量创建标签

功能介绍

批量创建标签

URI

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

表 3-368 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID
resource_type	是	String	资源类别，hss
resource_id	是	String	资源ID

请求参数

表 3-369 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）

表 3-370 请求 Body 参数

参数	是否必选	参数类型	描述
tags	否	Array of **ResourceTagInfo** objects	标签对象列表
sys_tags	否	Array of **ResourceTagInfo** objects	标签对象列表

表 3-371 ResourceTagInfo

参数	是否必选	参数类型	描述
key	否	String	键。最大长度128个unicode字符。 key不能为空
value	否	String	值

响应参数

状态码：200

success

无

请求示例

创建标签键TESTKEY20220831190155（标签值为2）和标签键test（标签值为hss）。

```
POST https://{endpoint}/v5/05e1e8b7ba8010dd2f80c01070a8d4cd/hss/fbaa9aca-2b5f-11ee-8c64-fa163e139e02/tags/create

{
  "tags" : [ {
    "key" : "TESTKEY20220831190155",
    "value" : "2"
```

```
 }, {
   "key" : "test",
   "value" : "hss"
 } ]
}
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.12.2 删除资源标签

功能介绍

删除单个资源下的标签

URI

DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/{key}

表 3-372 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户ID
resource_type	是	String	资源类别，hss
resource_id	是	String	资源ID
key	是	String	待删除的key

请求参数

表 3-373 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）

响应参数

状态码：200

success

无

请求示例

删除project_id为94b5266c14ce489fa6549817f032dc61、resource_type为hss、resource_id为2acc46ee-34c2-40c2-8060-dc652e6c672a的key为abc的标签

```
DELETE https://{endpoint}/v5/94b5266c14ce489fa6549817f032dc61/hss/2acc46ee-34c2-40c2-8060-dc652e6c672a/tags/abc
```

响应示例

无

状态码

状态码	描述
200	success
400	参数非法
401	鉴权失败
403	权限不足
404	资源未找到
500	系统异常

错误码

请参见**错误码**。

3.13 事件管理

3.13.1 查询已拦截 IP 列表

功能介绍

查询已拦截IP列表

URI

GET /v5/{project_id}/event/blocked-ip

表 3-374 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

表 3-375 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
last_days	否	Integer	查询时间范围天数，与自定义查询时间begin_time，end_time互斥
host_name	否	String	服务器名称
src_ip	否	String	攻击源IP
intercept_status	否	String	拦截状态，包含如下: • intercepted : 已拦截 • canceled : 已解除拦截 • cancelling : 待解除拦截
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

请求参数

表 3-376 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）

响应参数

状态码：200

表 3-377 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of **BlockedIpResponseInfo** objects	已拦截IP详情

表 3-378 BlockedIpResponseInfo

参数	参数类型	描述
host_id	String	服务器ID
host_name	String	服务器名称
src_ip	String	攻击源IP
login_type	String	登录类型，包含如下: • "mysql" # mysql服务 • "rdp" # rdp服务服务 • "ssh" # ssh服务 • "vsftp" # vsftp服务
intercept_num	Integer	拦截次数
intercept_status	String	拦截状态，包含如下: • "intercepted" # 已拦截 • "canceled" # 已解除拦截 • "cancelling" # 待解除拦截

参数	参数类型	描述
block_time	Long	开始拦截时间，毫秒
latest_time	Long	最近拦截时间，毫秒

请求示例

查询前10条已拦截的IP列表

```
GET https://{endpoint}/v5/{project_id}/event/blocked-ip?limit=10&offset=0&enterprise_project_id=xxx
```

响应示例

状态码：200

已拦截IP列表

```
{
  "data_list" : [ {
    "block_time" : 1698715135407,
    "host_id" : "1c62fe52-0c84-4ee4-8dba-d892c5ad0ab0",
    "host_name" : "dfx-a00607964-0011",
    "intercept_num" : 230,
    "intercept_status" : "canceled",
    "latest_time" : 1698715296786,
    "login_type" : "ssh",
    "src_ip" : "100.85.239.180"
  } ],
  "total_num" : 1
}
```

状态码

状态码	描述
200	已拦截IP列表

错误码

请参见**错误码**。

3.13.2 解除已拦截 IP

功能介绍

解除已拦截IP

URI

PUT /v5/{project_id}/event/blocked-ip

表 3-379 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

表 3-380 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-381 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）

表 3-382 请求 Body 参数

参数	是否必选	参数类型	描述
data_list	否	Array of **BlockedIpRequestInfo** objects	需要解除拦截的IP列表

表 3-383 BlockedIpRequestInfo

参数	是否必选	参数类型	描述
host_id	是	String	服务器ID
src_ip	是	String	攻击源IP

参数	是否必选	参数类型	描述
login_type	是	String	登录类型，包含如下: • "mysql" # mysql服务 • "rdp" # rdp服务服务 • "ssh" # ssh服务 • "vsftp" # vsftp服务

响应参数

状态码：200

successful response

无

请求示例

将以SSH方式登录主机af423efds-214432fgsdaf-gfdsaggbvf的被拦截ip192.168.1.6从已拦截IP列表中解除

```
PUT https://{endpoint}/v5/{project_id}/event/blocked-ip

{
  "data_list" : [ {
    "host_id" : "af423efds-214432fgsdaf-gfdsaggbvf",
    "src_ip" : "192.168.1.6",
    "login_type" : "ssh"
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见错误码。

3.13.3 查询已隔离文件列表

功能介绍

查询已隔离文件列表

URI

GET /v5/{project_id}/event/isolated-file

表 3-384 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

表 3-385 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps
last_days	否	Integer	查询时间范围天数，与自定义查询时间begin_time，end_time互斥
host_name	否	String	服务器名称
isolation_status	否	String	隔离状态，包含如下: ● isolated : 已隔离 ● restored : 已恢复 ● isolating : 已下发隔离任务 ● restoring : 已下发恢复任务
offset	否	Integer	偏移量：指定返回记录的开始位置，必须为数字，取值范围为大于或等于0，默认0
limit	否	Integer	每页显示个数

请求参数

表 3-386 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）

响应参数

状态码：200

表 3-387 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of IsolatedFileResponseInfo objects	已隔离文件详情

表 3-388 IsolatedFileResponseInfo

参数	参数类型	描述
host_id	String	服务器ID
host_name	String	服务器名称
file_hash	String	文件哈希
file_path	String	文件路径
isolation_status	String	隔离状态，包含如下: • isolated : 已隔离 • restored : 已恢复 • isolating : 已下发隔离任务 • restoring : 已下发恢复任务
file_attr	String	文件属性
update_time	Integer	更新时间，毫秒

请求示例

查询前10条已隔离的文件列表

```
GET https://{endpoint}/v5/{project_id}/event/isolated-file?limit=10&offset=0&enterprise_project_id=xxx
```

响应示例

状态码：200

已隔离文件列表

```
{
  "data_list" : [ {
    "file_attr" : "0",
    "file_hash" : "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path" : "C:\\Users\\Public\\Public Docker\\system32.exe",
```

```
    "host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
    "host_name" : "ecs-wi-800211",
    "isolation_status" : "isolated",
    "update_time" : 1698304933717
  } ],
  "total_num" : 1
}
```

状态码

状态码	描述
200	已隔离文件列表

错误码

请参见**错误码**。

3.13.4 恢复已隔离文件

功能介绍

恢复已隔离文件

URI

PUT /v5/{project_id}/event/isolated-file

表 3-389 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

表 3-390 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	租户企业项目ID，查询所有企业项目时填写：all_granted_eps

请求参数

表 3-391 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）

表 3-392 请求 Body 参数

参数	是否必选	参数类型	描述
data_list	否	Array of **IsolatedFileRequestInfo** objects	需要恢复的文件列表

表 3-393 IsolatedFileRequestInfo

参数	是否必选	参数类型	描述
host_id	否	String	服务器ID
file_hash	否	String	文件哈希
file_path	否	String	文件路径
file_attr	否	String	文件属性

响应参数

状态码：200

successful response

无

请求示例

将主机5a41ca47-8ea7-4a65-a8fb-950d03d8638e已被隔离的文件C:\Users\Public\test.exe从隔离文件中恢复

```
PUT https://{endpoint}/v5/{project_id}/event/isolated-file

{
  "data_list" : [ {
    "file_attr" : "0",
    "file_hash" : "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path" : "C:\\Users
```

```
ublic\\test.exe",
    "host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
  } ]
}
```

响应示例

无

状态码

状态码	描述
200	successful response

错误码

请参见**错误码**。

A 附录

A.1 状态码

状态码	编码	状态说明
200	OK	请求已成功
400	Bad Request	请求参数有误
401	Unauthorized	当前请求需要用户验证
403	Forbidden	禁止访问
404	Not Found	网页未找到
405	Method Not Allowed	请求中指定的方法不被允许
406	Not Acceptable	服务器生成的响应无法被客户端所接受
429	Too Many Requests	请求太频繁
500	Internal Server Error	服务器内部错误
501	Not Implemented	请求未完成，服务器不支持所请求的功能
502	Bad Gateway	请求未完成，服务器从上游服务器收到一个无效的响应
504	Gateway Timeout	网关超时

A.2 错误码

状态码	错误码	错误信息	描述	处理措施
400	HSS.0001	参数不合法	参数不合法	请检查参数是否合法

状态码	错误码	错误信息	描述	处理措施
400	HSS.0002	解析请求失败	解析请求失败	请联系技术支持
400	HSS.0010	拒绝访问	拒绝访问	请检查参数是否合法
400	HSS.0011	请求资源不存在	请求资源不存在	请检查参数是否合法
400	HSS.0013	权限不足	权限不足	请检查用户权限
400	HSS.0014	不允许创建配额	不允许创建配额	请联系技术支持
400	HSS.1001	选中的主机没有关联的agent	选中的主机没有关联的agent	请检查所选主机是否已安装agent
400	HSS.1002	可用配额不足	可用配额不足	无
400	HSS.1003	防护中的主机不可忽略	防护中的主机不可忽略	请关闭防护后再尝试忽略主机
400	HSS.1004	查询策略信息失败	查询策略信息失败	请检查参数是否正确
400	HSS.1005	无效的策略信息	无效的策略信息	请检查参数是否正确
400	HSS.1006	发送Agent指令信息失败	发送Agent指令信息失败	请联系技术支持
400	HSS.1007	Agent离线	Agent离线	请启动agent
400	HSS.1008	查询主机信息失败	查询主机信息失败	请检查参数是否正确
400	HSS.1009	保存网页防篡改信息失败	保存网页防篡改信息失败	请联系技术支持
400	HSS.1010	更新网页防篡改防护目录信息失败	更新网页防篡改防护目录信息失败	请联系技术支持
400	HSS.1011	转换时间格式失败	转换时间格式失败	请检查参数是否正确
400	HSS.1012	所添时间段冲突	所添时间段冲突	请检查参数是否正确
400	HSS.1013	添加停止防护时间段失败	添加停止防护时间段失败	请检查参数是否正确
400	HSS.1014	添加停止防护时间段描述失败	添加停止防护时间段描述失败	请检查参数是否正确

状态码	错误码	错误信息	描述	处理措施
400	HSS.1015	添加特权进程失败	添加特权进程失败	请联系技术支持
400	HSS.1016	设置停止防护周期失败	设置停止防护周期失败	请联系技术支持
400	HSS.1017	查询租户安全报告信息失败	查询租户安全报告信息失败	请检查参数是否正确
400	HSS.1018	无效的文件信息	无效的文件信息	请检查参数是否正确
400	HSS.1019	查询服务器组信息失败	查询服务器组信息失败	请检查参数是否正确
400	HSS.1020	策略组名称已存在	策略组名称已存在	请修改名称
400	HSS.1021	查询策略组信息失败	查询策略组信息失败	请检查参数是否正确
400	HSS.1022	无效的策略组信息	无效的策略组信息	请检查参数是否正确
400	HSS.1023	策略组名称不合法	策略组名称不合法	请修改名称
400	HSS.1024	查询应用进程白名单策略信息失败	查询应用进程白名单策略信息失败	请检查参数是否正确
400	HSS.1025	服务器组名称已存在	服务器组名称已存在	请修改名称
400	HSS.1026	扫描容器私有镜像漏洞失败	扫描容器私有镜像漏洞失败	请联系技术支持
400	HSS.1027	调用CBR云备份服务失败,http连接超时	调用CBR云备份服务失败,http连接超时	请联系技术支持
400	HSS.1028	调用CBR云备份服务失败,Token认证失败	调用CBR云备份服务失败,Token认证失败	请联系技术支持
400	HSS.1029	查询默认备份策略失败	查询默认备份策略失败	请检查参数是否正确
400	HSS.1030	查询安全体检结果信息失败	查询安全体检结果信息失败	请检查参数是否正确
400	HSS.1031	安全报告名称重复	安全报告名称重复	请修改名称

状态码	错误码	错误信息	描述	处理措施
400	HSS.1032	已使用的防护策略不能删除	已使用的防护策略不能删除	请关闭防护后再尝试删除策略
400	HSS.1033	防护策略名称已存在	防护策略名称已存在	请修改名称
400	HSS.1034	添加防护策略失败，策略个数最多不超过20个	添加防护策略失败，策略个数最多不超过20个	无
400	HSS.1035	只能由中文字符、英文字母、数字、逗号、句号、空格及"_"、"-"组成	只能由中文字符、英文字母、数字、逗号、句号、空格及"_"、"-"组成	请参照错误提示修改输入信息
400	HSS.1036	不支持该处理方式	不支持该处理方式	无
400	HSS.1037	不支持的版本类型	不支持的版本类型	请切换其他版本的防护配额
400	HSS.1040	查询容器信息失败	查询容器信息失败	请检查参数是否正确
400	HSS.1041	查询集群资产信息失败	查询集群资产信息失败	请检查参数是否正确
400	HSS.1042	下发容器防火墙策略失败	下发容器防火墙策略失败	请联系技术支持
400	HSS.1043	同步任务已经存在，请耐心等待	同步任务已经存在，请耐心等待	无
400	HSS.1044	导出任务已经存在，请耐心等待	导出任务已经存在，请耐心等待	无
400	HSS.1045	导出任务不存在	导出任务不存在	请检查参数是否正确
400	HSS.1046	导出文件不存在	导出文件不存在	请检查参数是否正确
400	HSS.1047	白名单策略进程未全部确认	白名单策略进程未全部确认	请在应用进程控制页面选择需要开启防护的白名单策略，手动标记进程的信任状态

状态码	错误码	错误信息	描述	处理措施
400	HSS.1048	加入白名单的漏洞总数量超出上限500条	加入白名单的漏洞总数量超出上限500条	无
400	HSS.1049	当前漏洞加入白名单的主机数量已达到上限2000台	当前漏洞加入白名单的主机数量已达到上限2000台	无
400	HSS.1050	agent版本未更新	agent版本未更新	请升级agent版本
400	HSS.1053	登录白名单数量已达到上限50条，请检测当前主机部署的策略并清理不需要的白名单ip	登录白名单数量已达到上限50条，请检测当前主机部署的策略并清理不需要的白名单ip	请参照错误提示处理
400	HSS.1054	您的账号可能存在风险,已根据《用户协议》限制您购买部分按需计费的云服务资源。如有疑问，请联系客服咨询处理。	您的账号可能存在风险,已根据《用户协议》限制您购买部分按需计费的云服务资源。如有疑问，请联系客服咨询处理。	请参照错误提示处理
400	HSS.1055	您的账户余额不足，无法开通资源，请立即充值。	您的账户余额不足，无法开通资源，请立即充值。	请充值
400	HSS.1056	漏洞处置超出最大规格，请分批处置	漏洞处置超出最大规格，请分批处置	请参照错误提示处理
400	HSS.1057	请勿选择不可扫描的服务器（agent状态异常或防护版本低于专业版）	请勿选择不可扫描的服务器（agent状态异常或防护版本低于专业版）	请参照错误提示处理
400	HSS.1058	端口蜜罐防护策略不存在	端口蜜罐防护策略不存在	请检查参数是否正确

状态码	错误码	错误信息	描述	处理措施
400	HSS.1059	没有可处置的漏洞，请检查Agent状态、防护版本、系统版本是否支持漏洞处置	没有可处置的漏洞，请检查Agent状态、防护版本、系统版本是否支持漏洞处置	请参照错误提示处理
400	HSS.1060	没有可进行漏洞扫描的主机，请检查Agent状态、防护版本、漏洞类型是否支持手动扫描	没有可进行漏洞扫描的主机，请检查Agent状态、防护版本、漏洞类型是否支持手动扫描	请参照错误提示处理
400	HSS.1061	一个负载最多能创建50条策略	一个负载最多能创建50条策略	无
400	HSS.1062	一个负载最多关联5条安全组	一个负载最多关联5条安全组	无
400	HSS.1063	上传LOGO超过大小限制	上传LOGO超过大小限制	无
400	HSS.1064	上传LOGO类型错误	上传LOGO类型错误	无
400	HSS.1065	敏感文件过滤路径不合规	敏感文件过滤路径不合规	请检查参数是否正确
400	HSS.1066	获取多云集群deployment模板失败	获取多云集群deployment模板失败	请联系技术支持
400	HSS.1067	集群日志未接入	集群日志未接入	请检查参数是否正确
400	HSS.1068	操作频繁，请等待2分钟后再次同步	操作频繁，请等待2分钟后再次同步	请稍后重试
400	HSS.1069	白名单可信进程数为0，请重新学习后再开启防护	白名单可信进程数为0，请重新学习后再开启防护	请参照错误提示处理
400	HSS.1070	病毒查杀按次计费开关未开启	病毒查杀按次计费开关未开启	请开启病毒查杀按次计费开关
400	HSS.1071	接入集群数已达到上限	接入集群数已达到上限	无

状态码	错误码	错误信息	描述	处理措施
400	HSS.1072	上传文件类型错误	上传文件类型错误	无
400	HSS.1073	查询事件信息失败	查询事件信息失败	请检查参数是否正确
400	HSS.1079	保存cce集成防护配置失败	保存cce集成防护配置失败	请检查参数是否正确
400	HSS.1080	接入镜像仓数已达到上限	接入镜像仓数已达到上限	无
401	HSS.0012	无效的用户TOKEN	无效的用户TOKEN	请检查用户的token是否正确
401	HSS.1039	没有修改漏洞扫描策略的权限	没有修改漏洞扫描策略的权限	请检查用户权限
401	HSS.1051	已选主机中存在正在扫描中的任务	已选主机中存在正在扫描中的任务	无
401	HSS.1052	已选主机已关联其他自定义查杀策略	已选主机已关联其他自定义查杀策略	无
401	HSS.2001	集群证书过期	集群证书过期	请参照错误提示处理
403	HSS.1038	防护版本不支持该操作	防护版本不支持该操作	请切换其他版本的防护配额
429	HSS.0003	服务器忙	服务器忙	请稍后重试
500	HSS.0004	数据库操作失败	数据库操作失败	请联系技术支持
500	HSS.0005	缓存操作失败	缓存操作失败	请联系技术支持
500	HSS.0006	文件操作错误	文件操作错误	请联系技术支持
500	HSS.0007	任务失败	任务失败	请联系技术支持
500	HSS.0008	系统内部错误	系统内部错误	请联系技术支持
500	HSS.0009	访问第三方接口失败	访问第三方接口失败	请联系技术支持
500	HSS.0015	访问ECS接口失败	访问ECS接口失败	请联系技术支持
500	HSS.0016	访问CCE接口失败	访问CCE接口失败	请联系技术支持

状态码	错误码	错误信息	描述	处理措施
500	HSS.0017	访问CBC接口失败	访问CBC接口失败	请联系技术支持
500	HSS.0018	访问IAM接口失败	访问IAM接口失败	请联系技术支持
500	HSS.0019	访问SWR接口失败	访问SWR接口失败	请联系技术支持
500	HSS.0020	访问CBR接口失败	访问CBR接口失败	请联系技术支持
500	HSS.0021	访问VPC接口失败	访问VPC接口失败	请联系技术支持
500	HSS.0041	查询信息出错	查询信息出错	请联系技术支持

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IAM服务的“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ID，所以需要获取到项目ID。项目ID获取步骤如下：

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

A.4 获取企业项目 ID

操作场景

在调用接口时，部分URL中需要填入企业项目ID，所以需要获取到企业项目ID。本章节介绍如何通过控制台获取企业项目ID。

从控制台获取企业项目 ID

1. 登录管理控制台。
2. 单击页面右上方的“企业 > 项目管理”。
   分辨率低的情况下单击页面右上方的“更多 > 企业 > 项目管理”。
3. 单击企业项目名称。
   在企业项目详情中查看“ID”即为企业项目ID。

   图 A-1 查看企业项目 ID

A.5 获取区域 ID

操作场景

在调用接口时，部分请求参数中需要填入Region ID。本章节介绍如何通过控制台获取Region ID。

从控制台获取 Region ID

步骤1 登录云服务平台，进入IAM控制台，选择“项目”页签。

步骤2 “项目”列的内容即为所属区域对应的ID。

----结束

B 修订记录

发布日期	修改说明
2025-09-30	第一次正式发布。