企业主机安全

API 参考

文档版本 03

发布日期 2021-12-10

华为技术有限公司

商标声明


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

注意

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

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

目 录

1 使用前必读 1
1.1 概述 1
1.2 调用说明 1
1.3 终端节点 1
1.4 约束与限制 2
1.5 基本概念 2
2 如何调用 API 4
2.1 构造请求 4
2.2 认证鉴权 6
2.3 返回结果 8
3 API 说明 10
3.1 主机管理 10
3.1.1 查询弹性云服务器状态列表 10
3.2 入侵检测 17
3.2.1 查入侵事件列表 17
4 历史 API 24
4.1 主机管理 24
4.1.1 查询弹性云服务器状态列表 24
A 附录 32
A.1 状态码 32
A.2 错误码 32
B 修订记录 33

1 使用前必读

1.1 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服务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**。

1.2 调用说明

企业主机安全提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

同时企业主机安全还提供多种编程语言的SDK供您使用，SDK的使用方法请参见**SDK概述**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同。

企业主机安全服务的终端节点如**表1-1**所示，请您根据业务需要选择对应区域的终端节点。

表 1-1 企业主机安全服务的终端节点

区域名称	区域	终端节点（Endpoint）	协议类型
华北-北京一	cn-north-1	hss.cn-north-1.myhuaweicloud.com	HTTPS

区域名称	区域	终端节点（Endpoint）	协议类型
华北-北京四	cn-north-4	hss.cn-north-4.myhuaweicloud.com	HTTPS
西南-贵阳一	cn-southwest-2	hss.cn-southwest-2.myhuaweicloud.com	HTTPS
华东-上海二	cn-east-2	hss.cn-east-2.myhuaweicloud.com	HTTPS
华东-上海一	cn-east-3	hss.cn-east-3.myhuaweicloud.com	HTTPS
华南-广州	cn-south-1	hss.cn-south-1.myhuaweicloud.com	HTTPS
华南-深圳	cn-south-2	hss.cn-south-2.myhuaweicloud.com	HTTPS
中国-香港	ap-southeast-1	hss.ap-southeast-1.myhuaweicloud.com	HTTPS
亚太-曼谷	ap-southeast-2	hss.ap-southeast-2.myhuaweicloud.com	HTTPS
亚太-新加坡	ap-southeast-3	hss.ap-southeast-3.myhuaweicloud.com	HTTPS

1.4 约束与限制

更详细的限制请参见具体API的说明。

1.5 基本概念

- 帐号

  用户注册时的帐号，帐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。由于帐号是付费主体，为了确保帐号安全，建议您不要直接使用帐号进行日常管理工作，而是创建用户并使用他们进行日常管理工作。
- 帐号

  帐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。由于帐号是付费主体，为了确保帐号安全，建议您不要直接使用帐号进行日常管理工作，而是创建用户并使用他们进行日常管理工作。
- 用户

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

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

- 用户

  由帐号在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，您需要用到帐号、用户和密码等信息。

- 区域（Region）

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

  详情请参见**区域和可用区**。

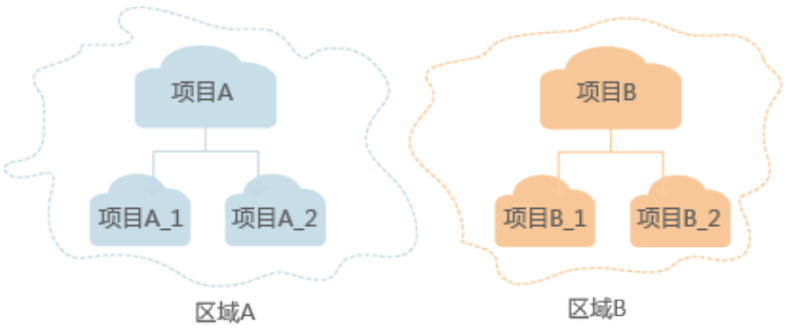
- 可用区（AZ，Availability Zone）

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

- 项目

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

  图 1-1 项目隔离模型

- 企业项目

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

  关于企业项目ID的获取及企业项目特性的详细信息，请参见**企业管理服务用户指南**。

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的**获取用户Token**说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

您还可以通过这个视频教程了解如何构造请求调用API：**https://bbs.huaweicloud.com/videos/102987**。

请求 URI

请求URI由如下部分组成。

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

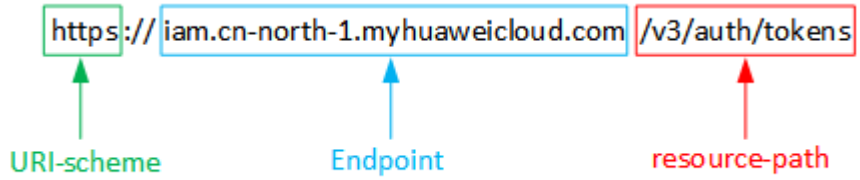
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme**：
  表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：
  指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**获取。
  例如IAM服务在“华北-北京一”区域的Endpoint为“iam.cn-north-1.myhuaweicloud.com”。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **query-string**：
  查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“华北-北京一”区域的Token，则需使用“华北-北京一”区域的Endpoint（iam.cn-north-1.myhuaweicloud.com），并在**获取用户Token**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

图 2-1 URI 示意图



说明

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

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

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

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

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

请求消息头

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

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。

  说明

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

  AK/SK认证的详细说明请参见**AK/SK认证**。

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

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

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

对于**获取用户Token**接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的帐号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxxx***为project的名称，如“cn-north-1”，您可以从**地区和终端节点**获取，对应地区和终端节点页面的“区域”字段的值。

说明

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

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json

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

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

2.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。

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

Token 认证

说明

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

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

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

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

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

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

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

AK/SK 认证

说明

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

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

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。

- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见**API签名指南**。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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

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

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

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

图 2-2 获取用户 Token 响应消息头

```
connection → keep-alive
content-type → application/json
date → Tue, 12 Feb 2019 06:52:13 GMT
server → Web Server
strict-transport-security → max-age=31536000; includeSubdomains;
transfer-encoding → chunked
via → proxy A
x-content-type-options → nosniff
x-download-options → noopen
x-frame-options → SAMEORIGIN
x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5
x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JlGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdglZO9fuEbL5dMhdavj+33wEl
xHRCE9l87o+k9-
j+CMZSEB7bUGd5Uj6eRASXI1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==
x-xss-protection → 1; mode=block;
```

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 主机管理

3.1.1 查询弹性云服务器状态列表

功能介绍

查询弹性云服务器状态列表

调试

您可以在**API Explorer**中调试该接口。

URI

GET /v1/{project_id}/api/host-management/hosts

表 3-1 路径参数

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

表 3-2 Query 参数

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5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。
agent_status	否	String	Agent状态，包含如下3种。 ● not_register： 未注册。 ● online： 在线。 ● offline： 离线。
host_status	否	String	Agent状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。
protect_status	否	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
detect_result	否	String	防护状态，包含如下3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。
host_name	否	String	云主机名称
host_ip	否	String	云主机私有IP
public_ip	否	String	云主机公网IP
os_type	否	String	操作系统类型
charging_mode	否	String	收费模式，包含如下2种。 ● packet_cycle： 包年/包月。 ● on_demand： 按需。
limit	否	Integer	默认10

参数	是否必选	参数类型	描述
offset	否	Integer	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	Integer	总数
data_list	Array of **Host** objects	查询弹性云服务器状态列表

表 3-5 Host

参数	参数类型	描述
agent_id	String	agent id
host_id	String	云主机id
host_name	String	云主机名称
host_ip	String	云主机私有IP
public_ip	String	云主机公网IP
enterprise_project_name	String	所属企业项目名称
group_name	String	服务器组名称
expire_time	Long	服务到期时间

参数	参数类型	描述
policy_group_name	String	策略组名称
host_status	String	Agent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。 ● uninstall： 未注册。 ● online： 在线。 ● offline： 离线。
version	String	主机开通的版本，包含如下5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。
protect_status	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
os_image	String	系统镜像
os_type	String	系统类型
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3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。
risk_port_num	Integer	资产风险个数
risk_vul_num	Integer	漏洞风险个数
risk_intrusion_num	Integer	入侵风险个数
risk_baseline_num	Integer	基线风险个数

参数	参数类型	描述
charging_mode	String	收费模式，包含如下2种。 ● packet_cycle ： 包年/包月。 ● on_demand ： 按需。
resource_id	String	云服务资源实例ID（UUID）

请求示例

示例：查询已购买企业主机安全版本为旗舰版、服务器系统为Windows的信息。

请求URL：

https://hss-{region_id}.myhuaweicloud.com/v1/{project_id}/api/host-management/hosts?version=hss.version.enterprise

填写请求参数如**图3-1**所示，请求参数详情请参见**表3-6**。

图 3-1 请求参数

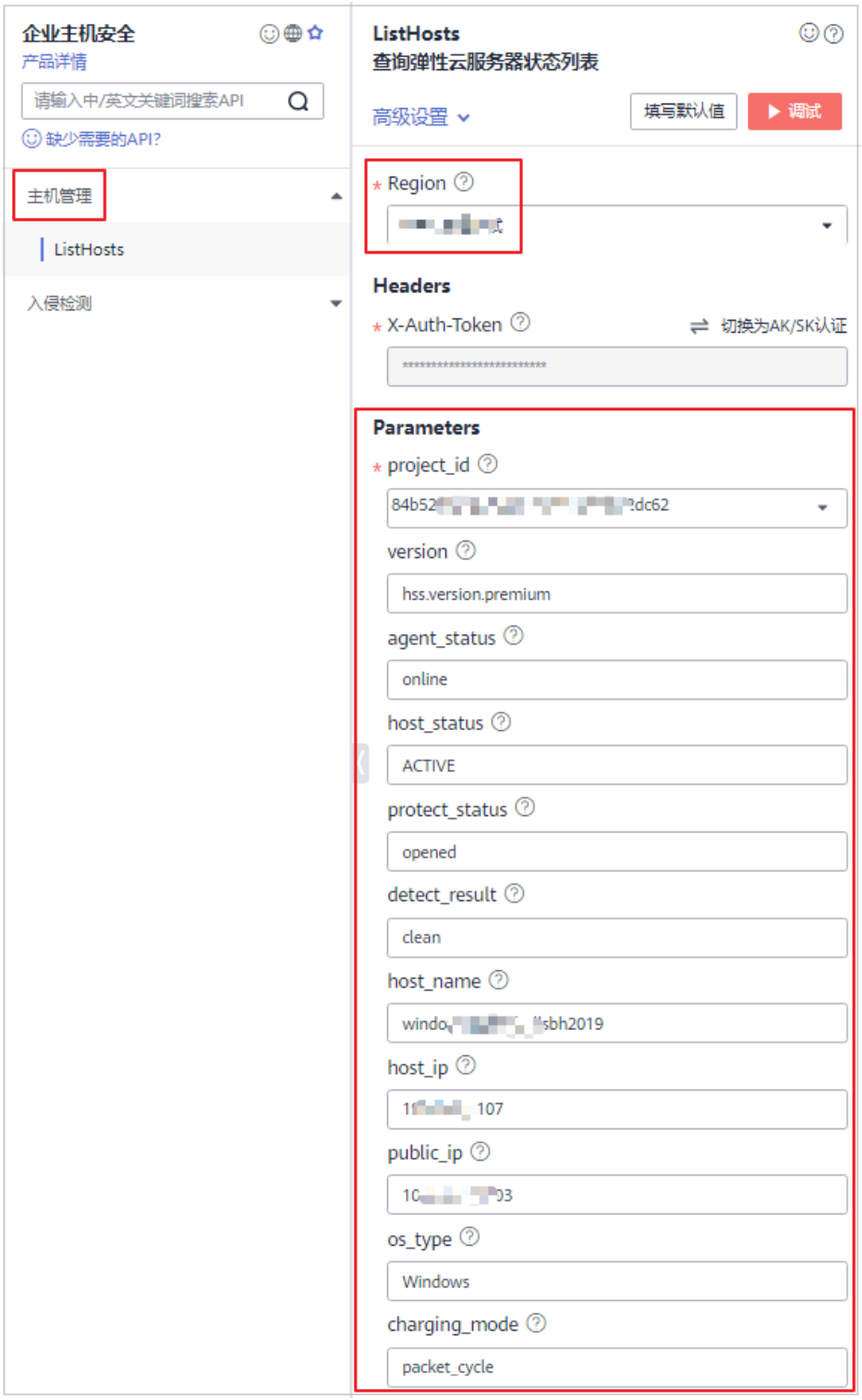


表 3-6 主机管理 Parameters 说明

参数名称	参数类型	参数说明	取值样例
project_id	String	项目ID，登录后自动填充。	-
version	String	主机开通的版本，包含如下5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。	hss.version.premium
agent_status	String	Agent状态，包含如下3种。 ● uninstall： 未注册。 ● online： 在线。 ● offline： 离线。	online
host_status	String	Agent状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。	ACTIVE
protect_status	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。	opened
detect_result	String	云主机安全检测结果，包含如下3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。	clean
host_name	String	云主机名称	-
host_ip	String	云主机私有ip	-
public_ip	String	云主机公网ip	-
os_type	String	操作系统类型	Windows
charging_mode	String	收费模式，包含如下2种。 ● packet_cycle： 包年/包月。 ● on_demand： 按需。	packet_cycle

响应示例

响应结果中一个“data_list”数组为一台服务器的信息详情。


```
{
 "data_list": [
  {
   "agent_id": "480c5                                    7e2efe9e684",
   "agent_status": "online",
   "charging_mode": "packet_cycle",
   "detect_result": "risk",
   "enterprise_project_name": "default",
   "expire_time": 163          9000,
   "group_name": "11",
   "host_id": "419c                                    -ef65dd94d50b",
   "host_ip": "192.1          107",
   "host_name": "windo          lsbh2019",
   "host_status": "ACTIVE",
   "os_bit": "64",
   "os_type": "Windows",
   "policy_group_name": "default_premium_policy_group",
   "protect_status": "opened",
   "public_ip": "10          103",
   "resource_id": "4d4fba                    e60d80fele3",
   "risk_baseline_num": 0,
   "risk_intrusion_num": 0,
   "risk_port_num": 0,
   "risk_vul_num": 0,
   "version": "hss.version.premium"
  }
 ],
 "total_num": 1
}
```


状态码

状态码	描述
200	获取主机列表成功

错误码

请参见错误码。

3.2 入侵检测

3.2.1 查入侵事件列表

功能介绍

查入侵事件列表

调试

您可以在**API Explorer**中调试该接口。

URI

GET /v1/{project_id}/api/event-management/events

表 3-7 路径参数

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

表 3-8 Query 参数

参数	是否必选	参数类型	描述
begin_time	是	String	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
end_time	是	String	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
host_name	否	String	云主机名称

参数	是否必选	参数类型	描述
event_types	是	Array	事件类型，包含如下: ● Abnormal Login : 账户异常登录 ● Invalid System Account : 风险账号 ● Brute Force Cracking : 账号暴力破解 ● System Start Script Change : 自启动检测 ● Process Abnormal Activity : 进程异常行为 ● Process Privilege Escalation : 进程提权操作 ● File Privilege Escalation : 文件提权操作 ● General Malware : 恶意程序（云查杀） ● Abnormal Shell : 异常shell ● Reverse Shell : 反弹Shell ● High-Risk Command Execution : 高危命令执行 ● Key File Change : 关键文件变更 ● Webshell : 网站后门
handle_status	否	String	是否已处理，包含如下类型: ● "unhandled"： 未处理 ● "handled"： 已处理
limit	否	Integer	默认10
offset	否	Integer	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	Integer	总数
data_list	Array of **Event** objects	查询弹性云服务器状态列表

表 3-11 Event

参数	参数类型	描述
host_id	String	云主机id
host_name	String	云主机名称
event_type	String	事件类型，包含如下: • Abnormal Login : 账户异常登录 • Invalid System Account : 风险账号 • Brute Force Cracking : 账号暴力破解 • System Start Script Change : 自启动检测 • Process Abnormal Activity : 进程异常行为 • Process Privilege Escalation : 进程提权操作 • File Privilege Escalation : 文件提权操作 • General Malware : 恶意程序（云查杀） • Abnormal Shell : 异常shell • Reverse Shell : 反弹Shell • High-Risk Command Execution : 高危命令执行 • Key File Change : 关键文件变更 • Webshell : 网站后门
occur_time	Long	发生时间，毫秒
handle_time	Long	处理时间，毫秒
handle_status	String	处理状态，包含如下类型: • "unhandled"：未处理 • "handled"：已处理

参数	参数类型	描述
handle_method	String	处理方式，包含如下类型： ● "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
append_info	Object	事件详细信息，json格式

请求示例

示例：查询事件类型为风险账号和帐号异常登录的信息。

请求URL：

https://hss-{region_id}.myhuaweicloud.com/v1/{project_id}/api/event-management/events?begin_time=1637828147000&end_time=1637917370561&event_types=General+Malware+&event_types=Invalid+System+Account+&event_types=Abnormal+Shel

填写请求参数如**查入侵事件列表**所示，请求参数详情请参见**表3-12**。

图 3-2 入侵事件参数填写

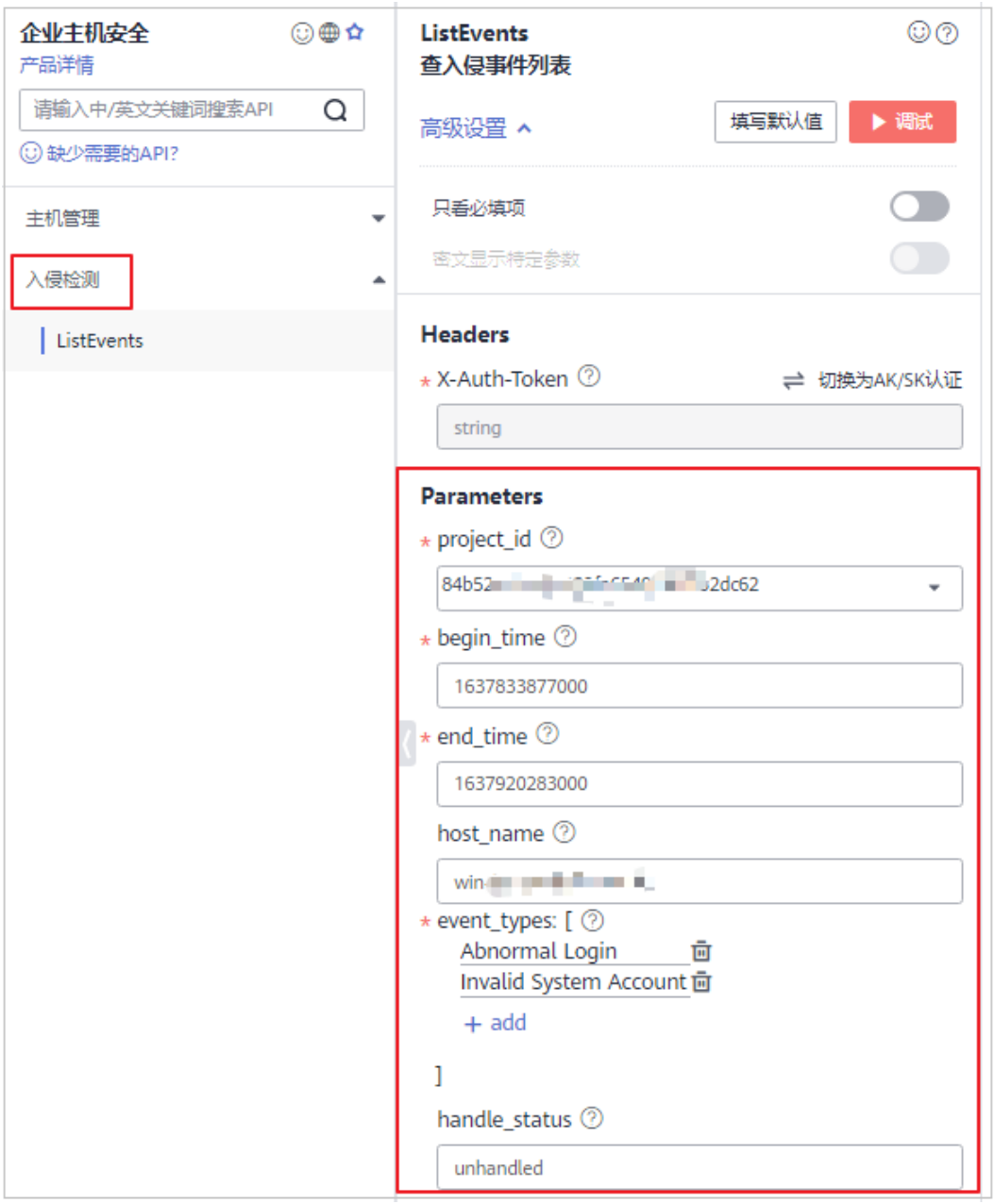


表 3-12 入侵检测 Parameters 说明

参数名称	参数类型	参数说明	取值样例
project_id	String	项目ID，登录后会自动填充。	-
begin_time	String	查询时间段的开始时间，毫秒级时间戳。	1637833877000
end_time	String	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。	1637920283000

参数名称	参数类型	参数说明	取值样例
host_name	String	云主机名称	-
event_types	String	事件类型 当选择多个事件类型进行查询时，响应结果只显示有值的事件类型。	["Invalid System Account","Abnormal Login"]
handle_status	String	是否已处理，包含如下类型: • "unhandled" : 未处理 • "handled" : 已处理	unhandled

响应示例

响应结果中一个“data_list”数组为一台服务器的信息详情。

```
{
 "data_list": [
  {
   "append_info": {
    "dir": "",
    "exception": "该账号的SID与其它账号相同，可能是影子账号。",
    "gid": 545,
    "group_name_list": "Us  s",
    "shell": "",
    "uid": "0C  D",
    "user_name": "chao",
    "user_root_dir": ""
   },
   "event_type": "Invalid System Account",
   "handle_status": "unhandled",
   "host_id": "57fe4e  2-96e2e7f2ad96",
   "host_name": "win-fo  ",
   "occur_time": 1637859536223
  }
 ],
 "total_num": 1
}
```

状态码

状态码	描述
200	获取入侵事件列表成功

错误码

请参见**错误码**。

4 历史 API

4.1 主机管理

4.1.1 查询弹性云服务器状态列表

功能介绍

查询弹性云服务器状态列表

URI

GET /hss/v1/{project_id}/api/host-management/hosts

表 4-1 路径参数

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

表 4-2 Query 参数

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5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。
agent_status	否	String	Agent状态，包含如下3种。 ● not_register： 未注册。 ● online： 在线。 ● offline： 离线。
host_status	否	String	Agent状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。
protect_status	否	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
detect_result	否	String	防护状态，包含如下3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。
host_name	否	String	云主机名称
host_ip	否	String	云主机私有IP
public_ip	否	String	云主机公网IP
os_type	否	String	操作系统类型
charging_mode	否	String	收费模式，包含如下2种。 ● packet_cycle： 包年/包月。 ● on_demand： 按需。
limit	否	Integer	默认10

参数	是否必选	参数类型	描述
offset	否	Integer	默认0

请求参数

表 4-3 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 4-4 响应 Body 参数

参数	参数类型	描述
total_num	Integer	总数
data_list	Array of 表1-5 objects	查询弹性云服务器状态列表

表 4-5 Host

参数	参数类型	描述
agent_id	String	agent id
host_id	String	云主机id
host_name	String	云主机名称
host_ip	String	云主机私有IP
public_ip	String	云主机公网IP
enterprise_project_name	String	所属企业项目名称
group_name	String	服务器组名称

参数	参数类型	描述
expire_time	Long	服务到期时间
policy_group_name	String	策略组名称
host_status	String	Agent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。 ● uninstall： 未注册。 ● online： 在线。 ● offline： 离线。
version	String	主机开通的版本，包含如下5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。
protect_status	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。
os_image	String	系统镜像
os_type	String	系统类型
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3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。
risk_port_num	Integer	资产风险个数
risk_vul_num	Integer	漏洞风险个数
risk_intrusion_num	Integer	入侵风险个数
risk_baseline_num	Integer	基线风险个数

参数	参数类型	描述
charging_mode	String	收费模式，包含如下2种。 ● packet_cycle： 包年/包月。 ● on_demand： 按需。
resource_id	String	云服务资源实例ID（UUID）

请求示例

示例：查询已购买企业主机安全版本为旗舰版、服务器系统为Windows的信息。

请求URL：

https://hss-{region_id}.myhuaweicloud.com/v1/{project_id}/api/host-management/hosts?version=hss.version.enterprise

填写请求参数如**图4-1**所示，请求参数详情请参见**表4-6**。

图 4-1 请求参数

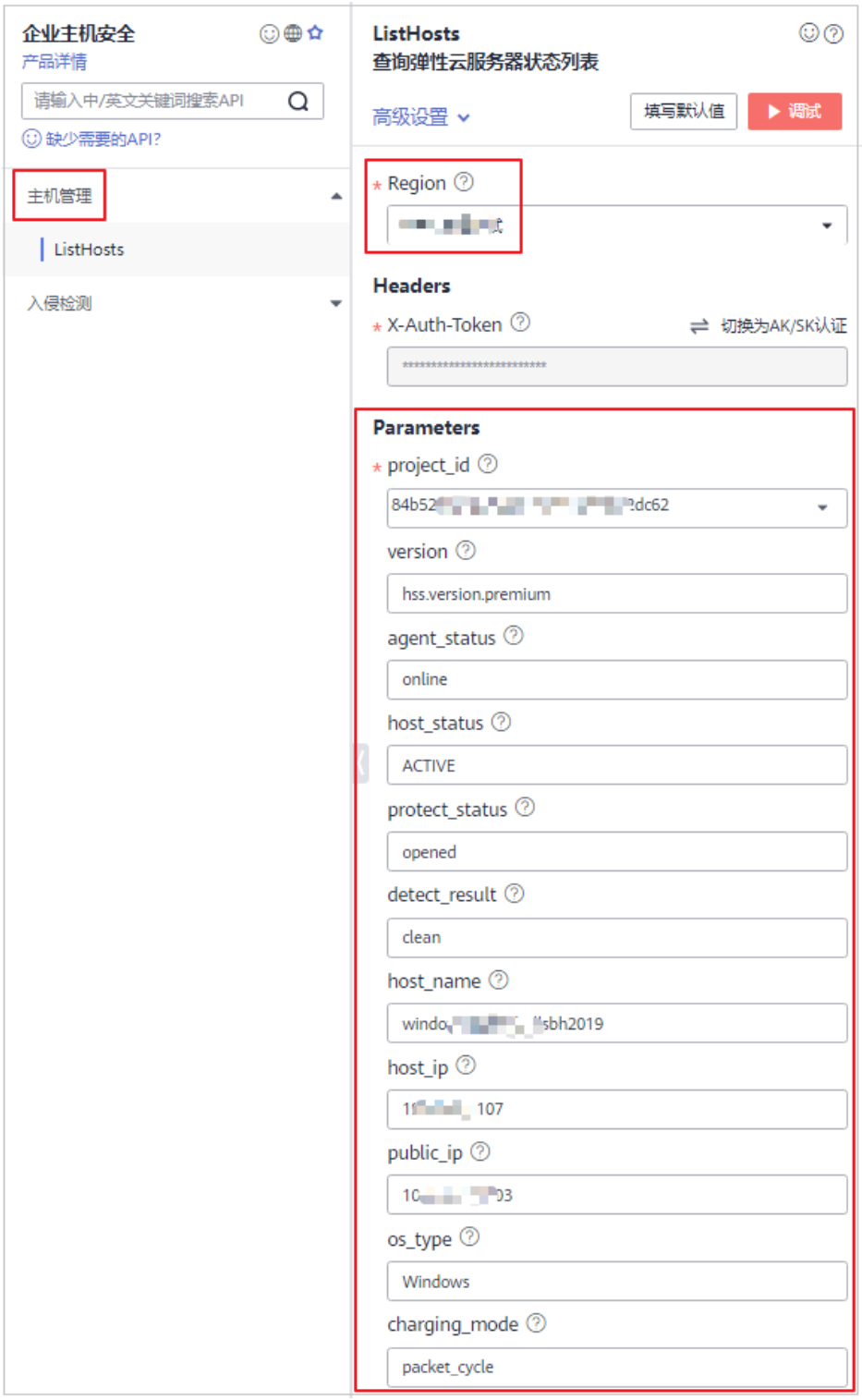


表 4-6 主机管理 Parameters 说明

参数名称	参数类型	参数说明	取值样例
project_id	String	项目ID，登录后自动填充。	-
version	String	主机开通的版本，包含如下5种输入。 ● hss.version.null： 无。 ● hss.version.basic： 基础版。 ● hss.version.enterprise： 企业版。 ● hss.version.premium： 旗舰版。 ● hss.version.wtp： 网页防篡改版。	hss.version.premium
agent_status	String	Agent状态，包含如下3种。 ● uninstall： 未注册。 ● online： 在线。 ● offline： 离线。	online
host_status	String	Agent状态，包含如下4种。 ● ACTIVE： 正在运行。 ● SHUTOFF： 关机。 ● BUILDING： 创建中。 ● ERROR： 故障。	ACTIVE
protect_status	String	防护状态，包含如下2种。 ● closed： 关闭。 ● opened： 开启。	opened
detect_result	String	云主机安全检测结果，包含如下3种。 ● undetect： 未检测。 ● clean： 无风险。 ● risk： 有风险。	clean
host_name	String	云主机名称	-
host_ip	String	云主机私有ip	-
public_ip	String	云主机公网ip	-
os_type	String	操作系统类型	Windows
charging_mode	String	收费模式，包含如下2种。 ● packet_cycle： 包年/包月。 ● on_demand： 按需。	packet_cycle

响应示例

响应结果中一个“data_list”数组为一台服务器的信息详情。


```
{
 "data_list": [
  {
   "agent_id": "480c5                                    7e2efe9e684",
   "agent_status": "online",
   "charging_mode": "packet_cycle",
   "detect_result": "risk",
   "enterprise_project_name": "default",
   "expire_time": 163          9000,
   "group_name": "11",
   "host_id": "419c                                    -ef65dd94d50b",
   "host_ip": "192.1          107",
   "host_name": "windo          lsbh2019",
   "host_status": "ACTIVE",
   "os_bit": "64",
   "os_type": "Windows",
   "policy_group_name": "default_premium_policy_group",
   "protect_status": "opened",
   "public_ip": "10          103",
   "resource_id": "4d4fba                    e60d80fele3",
   "risk_baseline_num": 0,
   "risk_intrusion_num": 0,
   "risk_port_num": 0,
   "risk_vul_num": 0,
   "version": "hss.version.premium"
  }
 ],
 "total_num": 1
}
```


状态码

状态码	描述
200	获取主机列表成功

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。
500	Internal Server Error	服务内部错误。

A.2 错误码

当您调用API时，如果遇到“APIGW”开头的错误码，请参见**API网关错误码**进行处理。

更多服务错误码请参见**API错误中心**。

状态码	错误码	错误信息	描述	处理措施
400	HSS.0001	invalid param error	参数不合法	请检查参数是否合法
500	HSS.0041	Query host extend info error	查询信息出错	请检查参数是否合法

B 修订记录

发布日期	修改说明
2021-12-10	第三次正式发布。 终端节点新增中国-香港、亚太-曼谷、亚太-新加坡。
2021-08-17	第二次正式发布。 • 新增**查入侵事件列表**接口。 • 新增**历史API**。
2021-05-19	第一次正式发布。