Host Security Service

API Reference

Issue 02

Date 2025-09-22

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Before You Start

Overview

Thank you for choosing Host Security Service (HSS). HSS helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

This document describes how to use application programming interfaces (APIs) to perform operations on HSS.

If you plan to access HSS through an API, ensure that you are familiar with HSS concepts. For details, see **Service Overview**.

Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of services, see **Regions and Endpoints**.

Basic Concepts

- Account

  An account is created upon successful registration with the cloud platform. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.

- User

  A user is created using a domain to use cloud services. Each user has its own identity credentials (password and access keys).

  The account name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same

region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

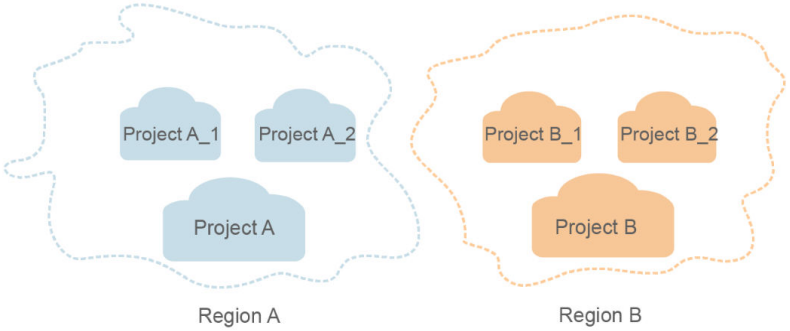
- Availability Zone (AZ)

  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are connected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Projects group and isolate resources (including compute, storage, and network resources) across physical regions. Users can be granted permissions in a default project to access all resources in the region associated with the project. For more refined access control, create subprojects under a project and purchase resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

  Figure 1-1 Project isolation model



- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

  For details about how to obtain enterprise project IDs and features, see **Enterprise Management User Guide**.

Limitations and Constraints

An API can be accessed up to 600 times/minute, in which a single user or IP address can access an API for up to five times/minute.

For more constraints, see API description.

2 Calling APIs

2.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

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

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from .

  For example, the endpoint of IAM in region **EU-Dublin** is **iam.eu-west-101.myhuaweicloud.com**.
- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string**:

  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in region **EU-Dublin**, obtain the endpoint of IAM (**iam.eu-west-101.myhuaweicloud.com**) for this region and the **resource-**

path (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens
```

NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **Authorization**: specifies signature authentication information. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request.
- **X-Sdk-Date**: specifies the time when a request is sent. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.
- **X-Project-ID**: specifies subproject ID. This field is optional and can be used in multi-project scenarios. The **X-Project-ID** field is mandatory in the request header for accessing resources in a subproject through AK/SK-based authentication.

- **X-Domain-ID**: account ID, which is optional. When you call APIs of global services using AK/SK-based authentication, **X-Domain-ID** needs to be configured in the request header.

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

NOTE

In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.

For more information, see **AK/SK-based Authentication**.

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace the italic fields in bold with the actual values.

- **accountid**: ID of the account to which the IAM user belongs.
- **username**: IAM username to be created.
- **email**: email address of the IAM user.
- **************: password of the IAM user.

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens

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"
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding.

2.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

- The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.
- Ensure that the token is valid when you use it. Using a token that will soon expire may cause API calling failures.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

You can **obtain a token** by calling an API. A project-level token is required for calling DEW APIs. When calling an API to obtain a user token, set **project** in **auth.scope** in the request body, as shown in the following example.

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

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFG....**, add **X-Auth-Token: ABCDEFG....** to a request as follows:

```
GET https://iam.eu-west-101.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```


AK/SK-based Authentication

NOTE

- AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.
- You can use the AK/SK in a permanent or temporary access key. The **X-Security-Token** field must be configured if the AK/SK in a temporary access key is used, and the field value is **security_token** of the temporary access key.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Request Signing Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

2.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Code**.

For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

Response Header

A response header corresponds to a request header, for example, **Content-Type**.

Figure 2-1 shows the response header for the API of **obtaining a user token**, in which **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 2-1 Header of the response to the request for obtaining a user token

(Optional) Response Body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

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

If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:

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

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

3 API Description

3.1 Asset Management

3.1.1 Collecting Asset Statistics, Including Accounts, Ports, and Processes

Function

This API is used to collect statistics on assets, such as accounts, ports, and processes.

URI

GET /v5/{project_id}/asset/statistics

Table 3-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 3-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-3 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-4 Response body parameters

Parameter	Type	Description
account_num	Long	Number of server accounts
port_num	Long	Number of open ports
process_num	Long	Number of processes
app_num	Long	Pieces of software
auto_launch_num	Long	Number of auto-startup processes
web_framework_num	Long	Number of web frameworks
web_site_num	Long	Number of websites
jar_package_num	Long	Number of JAR packages
kernel_module_num	Long	Number of kernel modules
web_service_num	Long	Number of web services

Parameter	Type	Description
web_app_num	Long	Number of web applications
database_num	Long	Number of databases

Example Requests

This API is used to query the fingerprint information, accounts, ports, and processes of a server.

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

Example Responses

Status code: 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,
  "database_num" : 1,
  "web_app_num" : 8,
  "web_service_num" : 2
}
```

Status Codes

Status Code	Description
200	Asset statistic info

Error Codes

See **Error Codes**.

3.1.2 Asset Fingerprint - Account Information

Function

This API is used to check account information in asset fingerprints.

URI

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

Table 3-5 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-6 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Account name. It must comply with the Windows file naming rules. The value can contain letters, digits, underscores (_), and the following special characters: !@.-.
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-7 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-8 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of accounts
data_list	Array of **UserStatisticIn-foResponseInfo** objects	Account statistics list

Table 3-9 UserStatisticInfoResponseInfo

Parameter	Type	Description
user_name	String	Account name. It must comply with the Windows file naming rules. The value can contain letters, digits, underscores (_), and the following special characters: !@.-.
num	Integer	Number of servers of the account

Example Requests

The first 10 accounts are queried by default.

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

Example Responses

Status code: 200

Number of servers having the account

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

Status Codes

Status Code	Description
200	Number of servers having the account

Error Codes

See **Error Codes**.

3.1.3 Asset Fingerprint - Process Information

Function

This API is used to check process information in asset fingerprints.

URI

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

Table 3-10 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-11 Query Parameters

Parameter	Mandatory	Type	Description
path	No	String	Executable process path
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-12 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-13 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of process statistics
data_list	Array of **ProcessStatisticResponseInfo** objects	Process statistics list

Table 3-14 ProcessStatisticResponseInfo

Parameter	Type	Description
path	String	Path of the executable files for the process
num	Integer	Number of processes

Example Requests

The first 10 processes whose type is host are queried by default.

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

Example Responses

Status code: 200

Number of servers having the process

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



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

Status Codes

Status Code	Description
200	Number of servers having the process

Error Codes

See **Error Codes**.

3.1.4 Asset Fingerprint - Software Information

Function

This API is used to check software information in asset fingerprints.

URI

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

Table 3-15 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-16 Query Parameters

Parameter	Mandatory	Type	Description
app_name	No	String	Software name
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-17 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-18 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of process statistics
data_list	Array of **AppStatisticResponseInfo** objects	Process statistics list

Table 3-19 AppStatisticResponseInfo

Parameter	Type	Description
app_name	String	Software name
num	Integer	Number of processes

Example Requests

The first 10 software lists whose type is host are queried by default.

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

Example Responses

Status code: 200

Number of servers having the software

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



```
  "num" : 13
 } ]
}
```

Status Codes

Status Code	Description
200	Number of servers having the software

Error Codes

See **Error Codes**.

3.1.5 Asset Fingerprint - Auto-Started Item Information

Function

This API is used to check auto-started items in asset fingerprints.

URI

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

Table 3-20 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-21 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Auto-started item name
type	No	String	Auto-started item type • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-22 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-23 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of auto-started items
data_list	Array of **AutoLaunchStatisticsResponseInfo** objects	List of auto-started item statistics

Table 3-24 AutoLaunchStatisticsResponseInfo

Parameter	Type	Description
name	String	Auto-started item name

Parameter	Type	Description
type	String	Auto-started item type • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
num	Integer	Indicates the number of servers of auto-started items.

Example Requests

The first 10 auto-startup items are queried by default.

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

Example Responses

Status code: 200

Number of servers having the process

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

Status Codes

Status Code	Description
200	Number of servers having the process

Error Codes

See **Error Codes**.

3.1.6 Querying the Server List of an Account

Function

This API is used to query the server list of an account.

URI

GET /v5/{project_id}/asset/users

Table 3-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-26 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID
user_name	No	String	Account name
host_name	No	String	Host name
private_ip	No	String	Server private IP address
login_permission	No	Boolean	Whether login is allowed.
root_permission	No	Boolean	Whether the user has root permissions
user_group	No	String	Server user group
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-27 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-28 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of accounts
data_list	Array of **UserResponseInfo** objects	Account information list

Table 3-29 UserResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
host_id	String	Host ID
host_name	String	Server name
host_ip	String	Server IP address
user_name	String	Username
login_permission	Boolean	Whether the user has the login permission
root_permission	Boolean	Whether the user has root permissions
user_group_name	String	User group name
user_home_dir	String	User home directory
shell	String	User startup shell

Parameter	Type	Description
recent_scan_time	Long	Latest scan time

Example Requests

Query servers list whose account is daemon by default.

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

Example Responses

Status code: 200

account information list

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

Status Codes

Status Code	Description
200	account information list

Error Codes

See **Error Codes**.

3.1.7 Asset Fingerprint of a Server - Open Port Information

Function

This API is used to check open port information in the asset fingerprints of a server.

URI

GET /v5/{project_id}/asset/ports

Table 3-30 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-31 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
host_name	No	String	Server name
host_ip	No	String	Server IP address
port	No	Integer	Port number
type	No	String	Port type: TCP or UDP.
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-32 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-33 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of open ports
data_list	Array of **PortResponseInfo** objects	Port information list

Table 3-34 PortResponseInfo

Parameter	Type	Description
host_id	String	Server ID
laddr	String	Listening IP address
status	String	port status, normal, danger or unknow • normal • danger • unknown
port	Integer	Port number
type	String	Port type: TCP or UDP.
pid	Integer	Process ID
path	String	Path of the process execution file.
agent_id	String	agent id
container_id	String	Container ID

Example Requests

The first 10 open ports whose host_id is dd91cd32-a238-4c0e-bc01-3b11653714ac are queried by default.

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

Example Responses

Status code: 200

Port information list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "3702fbd6-xxxx-xxxx-xxxx-6715770bxxxx",
    "agent_id" : "eb5d03f02fffd85aaf5d0ba5c992d97713244f420e0b076dcf6ae0574c78aa4b",
    "container_id" : "",
```



```
    "laddr" : "0.0.0.0",
    "path" : "/usr/sbin/",
    "pid" : 1554,
    "port" : 22,
    "status" : "unknow",
    "type" : "TCP"
  } ]
}
```

Status Codes

Status Code	Description
200	Port information list

Error Codes

See **Error Codes**.

3.1.8 Asset Fingerprint of a Server - Software

Function

This API is used to check software information in the asset fingerprints of a server.

URI

GET /v5/{project_id}/asset/apps

Table 3-35 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 3-36 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
host_name	No	String	Server name
app_name	No	String	Software name
host_ip	No	String	Server IP address

Parameter	Mandatory	Type	Description
version	No	String	Software version
install_dir	No	String	Installation directory
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-37 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-38 Response body parameters

Parameter	Type	Description
total_num	Integer	Total software
data_list	Array of **AppResponseInfo** objects	Software list

Table 3-39 AppResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID of HSS
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
app_name	String	Software name
version	String	Version number
update_time	Long	Latest update time, in milliseconds.
recent_scan_time	Long	Last scanned, in ms.

Example Requests

The first 10 servers whose software name is ACL are queried by default.

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

Example Responses

Status code: 200

Applications installed on a host

```
{
  "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
  } ]
}
```

Status Codes

Status Code	Description
200	Applications installed on a host

Error Codes

See **Error Codes**.

3.1.9 Asset Fingerprint of a Server - Auto-Started Items

Function

This API is used to check auto-started items in the asset fingerprints of a server.

URI

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

Table 3-40 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-41 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_name	No	String	Server name
name	No	String	Auto-started item name
host_ip	No	String	Server IP address
type	No	String	Auto-started item type • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-42 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-43 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of auto-startup items
data_list	Array of **AutoLauchResponseInfo** objects	Auto-started item list

Table 3-44 AutoLauchResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
name	String	Auto-started item name
type	Integer	Auto-started item type • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
path	String	Path of the auto-startup item

Parameter	Type	Description
hash	String	Hash value of the file generated using the SHA256 algorithm
run_user	String	User who starts the execution
recent_scan_time	Long	Latest scan time

Example Requests

The first 10 services whose auto-startup item name is S50multi-queue are queried by default.

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

Example Responses

Status code: 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
  } ]
}
```

Status Codes

Status Code	Description
200	auto launch list

Error Codes

See **Error Codes**.

3.1.10 Obtaining the Account Change History

Function

This API is used to obtain the account change history.

URI

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

Table 3-45 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-46 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Username
host_id	No	String	Server ID
root_permission	No	Boolean	Whether the user has root permissions
host_name	No	String	Server name
private_ip	No	String	Server private IP address
change_type	No	String	Account change type. The options are as follows: • ADD • DELETE • MODIFY
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-47 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-48 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of changed accounts
data_list	Array of **UserChangeHistoryResponseInfo** objects	Account change history

Table 3-49 UserChangeHistoryResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
change_type	String	Change type. Its value can be: • ADD • DELETE • MODIFY
host_id	String	Host ID
host_name	String	Server name
private_ip	String	Server private IP address
login_permission	Boolean	Whether the user has the login permission
root_permission	Boolean	Whether the user has root permissions

Parameter	Type	Description
user_group_name	String	User group name
user_home_dir	String	User home directory
shell	String	User startup shell
user_name	String	Account name
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond.
recent_scan_time	Long	Time when an account is added, modified, or deleted.

Example Requests

The first 10 account change records whose start time is 1700446129130 and end time is 1701050929130 are queried by default.

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

Example Responses

Status code: 200

account change history

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxece69",
    "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" : "ADD"
  } ]
}
```

Status Codes

Status Code	Description
200	account change history

Error Codes

See **Error Codes**.

3.1.11 Asset Fingerprint - Software Information - Change History

Function

This API is used to check the change history of software in the asset fingerprints of a server.

URI

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

Table 3-50 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-51 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_ip	No	String	Server IP address
host_name	No	String	Server name
app_name	No	String	Software name
variation_type	No	String	Change type. Its value can be: • add • delete • modify
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
sort_key	No	String	Sort key. Currently, sorting by recent_scan_time is supported.
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: desc

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-52 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-53 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of software changes
data_list	Array of **AppChangeResponseInfo** objects	Account change history

Table 3-54 AppChangeResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
variation_type	String	Type of change. • add • delete • modify
host_id	String	host_id
app_name	String	Software name
host_name	String	Host name
host_ip	String	Server IP address
version	String	Version number
update_time	Long	Updated
recent_scan_time	Long	Last scanned, in ms.

Example Requests

The first 10 software change records whose start time is 1700446175490 and end time is 1701050975490 are queried by default.

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

Example Responses

Status code: 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
  } ]
}
```


Status Codes

Status Code	Description
200	App change history info list

Error Codes

See **Error Codes**.

3.1.12 Asset Fingerprint - Open Port Information

Function

This API is used to check open port information in asset fingerprints.

URI

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

Table 3-55 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-56 Query Parameters

Parameter	Mandatory	Type	Description
port	No	Integer	Port number
type	No	String	Port type
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Default value: 0
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-57 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-58 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of open ports
data_list	Array of **PortStatisticResponseInfo** objects	Open port statistics list

Table 3-59 PortStatisticResponseInfo

Parameter	Type	Description
port	Integer	Port number
type	String	Port type: TCP or UDP.
num	Integer	Number of ports

Example Requests

The first 10 open ports whose port number is 123 and type is host are queried by default.

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

Example Responses

Status code: 200

Returns the port information, including the port number, type, and quantity.


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

Status Codes

Status Code	Description
200	Returns the port information, including the port number, type, and quantity.

Error Codes

See **Error Codes**.

3.1.13 Asset Fingerprint - Auto-started Item - Change History

Function

This API is used to check the change history of auto-started items in the asset fingerprints of a server.

URI

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

Table 3-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-61 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_ip	No	String	Server IP address
host_name	No	String	Server name
auto_launch_name	No	String	Auto-started item name

Parameter	Mandatory	Type	Description
type	No	Integer	Auto-started item type. • 0: auto-started service • 1: scheduled task • 2: Preload the dynamic library. • 3: Run registry key • 4: startup folder
variation_type	No	String	Change type. Its value can be: • add • delete • modify
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
sort_key	No	String	Sort key. Currently, sorting by recent_scan_time is supported.
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: desc
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-62 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-63 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of changes of auto-started items
data_list	Array of **AutoLaunchChangeResponseInfo** objects	Account change history

Table 3-64 AutoLaunchChangeResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
variation_type	String	Type of change. • add • delete • modify
type	Integer	Auto-started item type • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
host_id	String	host_id

Parameter	Type	Description
host_name	String	ECS name
host_ip	String	Server IP address
path	String	Path of the auto-startup item
hash	String	Hash value of the file generated using the SHA256 algorithm
run_user	String	User who starts the execution
name	String	Auto-started item name
recent_scan_time	Long	Last update time. The value is a 13-bit timestamp.

Example Requests

The first 10 auto-startup item change records whose start time is 1693101881568 and end time is 1701050681569 are queried by default.

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

Example Responses

Status code: 200

App change history info list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxxx",
    "variation_type" : "add",
    "type" : 0,
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "path" : "/path",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxx",
    "run_user" : "SYSTEM",
    "name" : "S12hostguard",
    "recent_scan_time" : 1668246126302
  } ]
}
```

Status Codes

Status Code	Description
200	App change history info list

Error Codes

See **Error Codes**.

3.2 Ransomware Prevention

3.2.1 Querying the Protection Policy List of Ransomware

Function

This API is used to query the the protection policy list of ransomware.

URI

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

Table 3-65 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-66 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	No	Integer	Number of records displayed on each page.
policy_name	No	String	Policy name
operating_system	No	String	OSs supported by the policy. The options are as follows: • Windows • Linux

Request Parameters

Table 3-67 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-68 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of policies
data_list	Array of **ProtectionPolicyInfo** objects	Query the list of policies.

Table 3-69 ProtectionPolicyInfo

Parameter	Type	Description
policy_id	String	Policy ID
policy_name	String	Policy name
protection_mode	String	Action. Its value can be: • alarm_and_isolation: Report an alarm and isolate. • alarm_only: Only report alarms.
bait_protection_status	String	Whether to enable honeypot protection. By default, the protection is enabled. Its value can be: • opened • closed

Parameter	Type	Description
protection_directory	String	Protected directory
protection_type	String	Protected file type, for example, .docx, .txt, and .avi.
exclude_directory	String	(Optional) excluded directory
runtime_detection_status	String	Whether to perform runtime checks. The options are as follows. Currently, it can only be disabled. This field is reserved. • opened • closed
runtime_detection_directory	String	Directory to be checked during running. This field is reserved.
count_associated_server	Integer	Number of associated servers
operating_system	String	OS type. Its value can be: • Linux • Windows

Example Requests

Query the protection policy list of ransomware. If limit is not specified, 10 records are returned by default.

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

Example Responses

Status code: 200

Linux protection policy list

```
{
  "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"
  } ]
}
```


Status Codes

Status Code	Description
200	Linux protection policy list

Error Codes

See **Error Codes**.

3.2.2 Modifying Ransomware Protection Policies

Function

This API is used to modify ransomware protection policies.

URI

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

Table 3-70 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-71 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-72 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Parameter	Mandatory	Type	Description
region	Yes	String	Region ID

Table 3-73 Request body parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID
policy_name	Yes	String	Policy name
protection_mode	Yes	String	Action. Its value can be: • alarm_and_isolation: Report an alarm and isolate. • alarm_only: Only report alarms.
bait_protection_status	Yes	String	Whether to enable honeypot protection. By default, the protection is enabled. Its value can be: • opened • closed
protection_directory	Yes	String	Protected directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
protection_type	Yes	String	Protected file type, for example, .docx, .txt, and .avi.
exclude_directory	No	String	(Optional) Excluded directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
agent_id_list	No	Array of strings	Specifies the IDs of agents for which the ransomware protection policy is enabled.
operating_system	Yes	String	OSs supported by the policy. The options are as follows: • Windows • Linux

Parameter	Mandatory	Type	Description
runtime_detection_status	No	String	Whether to perform runtime checks. The options are as follows. Currently, it can only be disabled. This field is reserved. • opened • closed

Response Parameters

Status code: 200

success

None

Example Requests

Modify the ransomware protection policy. Set the OS type to Linux, protection policy ID to 0253edfd-30e7-439d-8f3f-17c54c997064, and protection action to alert only.

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

{
  "bait_protection_status" : "opened",
  "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" : [ "" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success

Error Codes

See **Error Codes**.

3.2.3 Disabling Ransomware Prevention

Function

This API is used to disable ransomware prevention.

URI

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

Table 3-74 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-75 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-76 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Table 3-77 Request body parameters

Parameter	Mandatory	Type	Description
host_id_list	Yes	Array of strings	IDs of servers where ransomware protection needs to be disabled

Parameter	Mandatory	Type	Description
agent_id_list	Yes	Array of strings	IDs of agents where ransomware prevention needs to be disabled
close_protection_type	Yes	String	Type of disabled protection. The options are as follows: • close_anti: Disable ransomware protection. Currently, backup protection cannot be disabled. Go to the CBR service to unbind a vault.

Response Parameters

Status code: 200

Ransomware protection disabled.

None

Example Requests

Disable ransomware protection for the server. The target server ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f, and the agent ID of the target server is 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" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Ransomware protection disabled.

Error Codes

See **Error Codes**.

3.2.4 Modifying the Backup Policy Bound to HSS Protection Vault

Function

This API is used to modify the backup policy associated with the vault

URI

PUT /v5/{project_id}/backup/policy

Table 3-78 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-79 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-80 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Table 3-81 Request body parameters

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether the policy is enabled. The default value is true.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Backup policy ID
operation_definition	No	**OperationDefinitionRequestInfo** object	Scheduling parameter.
trigger	No	**BackupTriggerRequestInfo** object	Time scheduling rule for the policy

Table 3-82 OperationDefinitionRequestInfo

Parameter	Mandatory	Type	Description
day_backups	No	Integer	Maximum number of retained daily backups. The latest backup of each day is saved in the long term. This parameter is not affected by the maximum number of retained backup. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured. Minimum value: 0. Maximum value: 100
max_backups	No	Integer	Maximum number of automated backups that can be retained for an object. The value can be -1 or ranges from 0 to 99999. If the value is set to -1, the backups will not be cleared even though the configured retained backup quantity limit is exceeded. If this parameter and retention_duration_days are left blank at the same time, the backups will be retained permanently. Minimum value: 1. Maximum value: 99999. Default value: -1

Parameter	Mandatory	Type	Description
month_backups	No	Integer	Maximum number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter is not affected by the maximum number of retained backup. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured. Minimum value: 0. Maximum value: 100
retention_duration_days	No	Integer	Duration of retaining a backup, in days. The maximum value is 99999. If the value is set to -1, backups will not be cleared even though the configured retention duration is exceeded. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum value: 1. Maximum value: 99999. Default value: -1
timezone	No	String	Time zone where the user is located, for example, UTC +08:00. Set this parameter only after you have configured any of the parameters day_backups, week_backups, month_backups, and year_backups.
week_backups	No	Integer	Maximum number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured.

Parameter	Mandatory	Type	Description
year_backups	No	Integer	Maximum number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured. Minimum value: 0. Maximum value: 100

Table 3-83 BackupTriggerRequestInfo

Parameter	Mandatory	Type	Description
properties	Yes	**BackupTriggerPropertiesRequestInfo** object	Time rule for the policy execution.

Table 3-84 BackupTriggerPropertiesRequestInfo

Parameter	Mandatory	Type	Description
pattern	Yes	Array of strings	Scheduling rule A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only parameters FREQ, BYDAY, BYHOUR, BYMINUTE, and INTERVAL. FREQ can be set only to WEEKLY or DAILY. BYDAY can be set to MO, TU, WE, TH, FR, SA, or SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 minutes to 59 minutes. The scheduling interval must not be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00. To start scheduling at 14:00 every day, the rule is as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00'.

Response Parameters

Status code: 200

Modify a backup policy.

None

Example Requests

Modify the backup policy. The target backup policy ID is 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" ]
    }
  }
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Modify a backup policy.

Error Codes

See **Error Codes**.

3.3 Baseline Management

3.3.1 Querying the Weak Password Detection Result List

Function

This API is used to query the list of weak password detection results.

URI

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

Table 3-85 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-86 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
host_name	No	String	Server name
host_ip	No	String	Server IP address
user_name	No	String	Name of the account using a weak password
host_id	No	String	Host ID. If this parameter is not specified, all hosts of a user are queried.
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-87 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token, which can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is the IAM token.

Response Parameters

Status code: 200

Table 3-88 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of weak passwords

Parameter	Type	Description
data_list	Array of **WeakPwdListInfoResponseInfo** objects	Weak password list

Table 3-89 WeakPwdListInfoResponseInfo

Parameter	Type	Description
host_id	String	Host ID
host_name	String	Server name
host_ip	String	Server IP address (private IP address)
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	List of accounts with weak passwords

Table 3-90 WeakPwdAccountInfoResponseInfo

Parameter	Type	Description
user_name	String	Name of accounts with weak passwords
service_type	String	Account type. The options are as follows: • system • mysql • redis
duration	Integer	Validity period of a weak password, in days.

Example Requests

Query the weak password of servers whose enterprise project ID is xxx. Data on the first page (the first 10 records) is returned by default.

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

Example Responses

Status code: 200

weak password check result


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


Status Codes

Status Code	Description
200	weak password check result

Error Codes

See **Error Codes**.

3.3.2 Querying the Password Complexity Policy Detection Report

Function

This API is used to query the password complexity policy detection report.

URI

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

Table 3-91 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-92 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
host_name	No	String	Server name
host_ip	No	String	Server IP address
host_id	No	String	Host ID. If this parameter is not specified, all hosts of a user are queried.
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-93 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is the IAM token.

Response Parameters

Status code: 200

Table 3-94 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of password complexity policies

Parameter	Type	Description
data_list	Array of **PwdPolicyInfoResponseInfo** objects	List of password complexity policy detection

Table 3-95 PwdPolicyInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID (displayed when the cursor is placed on a server name)
host_name	String	Server name
host_ip	String	Server IP address
min_length	Boolean	Indicates whether the minimum password length meets the requirements. If the value is true, the minimum password length meets the requirements. If the value is false, the minimum password length does not meet the requirements.
uppercase_letter	Boolean	Indicates whether the uppercase letters meet the requirements. If the value is true, the uppercase letters meet the requirements. If the value is false, the uppercase letters do not meet the requirements.
lowercase_letter	Boolean	Indicates whether the lowercase letters meet the requirements. If the value is true, the lowercase letters meet the requirements. If the value is false, the lowercase letters do not meet the requirements.
number	Boolean	Indicates whether the number meets the requirements. If the value is true, the number meets the requirements. If the value is false, the number does not meet the requirements.
special_character	Boolean	Indicates whether the special character meets the requirements. If the value is true, the special character meets the requirements. If the value is false, the special character does not meet the requirements.

Parameter	Type	Description
suggestion	String	Modification suggestion

Example Requests

Query the password complexity of the server whose enterprise project ID is xxx. Data on the first page (the first 10 records) is returned by default.

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

Example Responses

Status code: 200

password complexity policy check report

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "76fa440a-5a08-43fa-ac11-d12183ab3a14",
    "host_ip" : "192.168.0.59",
    "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
  } ]
}
```

Status Codes

Status Code	Description
200	password complexity policy check report

Error Codes

See **Error Codes**.

3.3.3 Querying the Result List of Server Security Configuration Check

Function

This API is used to query the result list of a user's server security configuration check.

URI

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

Table 3-96 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-97 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
check_name	No	String	Baseline name, for example, SSH, CentOS 7, and Windows.
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High
standard	No	String	hw_standard: Cloud security practice standard
host_id	No	String	Host ID
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-98 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is the IAM token.

Response Parameters

Status code: 200

Table 3-99 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of records
data_list	Array of **SecurityCheckInfoResponseInfo** objects	Server configuration check result list

Table 3-100 SecurityCheckInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_name	String	Baseline name, for example, SSH, CentOS 7, and Windows.
check_type	String	Baseline type. The values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2.

Parameter	Type	Description
standard	String	hw_standard: Cloud security practice standard
check_rule_num	Integer	Indicates the total number of check items of the current configuration check (baseline) type. For example, if the standard type of the SSH baseline is hw_standard, server security provides 17 check items, but only five check items of the SSH baseline are detected on all servers. Therefore, the value of check_rule_num is 5. All check items are checked on a server. The value of check_rule_num is 17.
failed_rule_num	Integer	Number of failed check items. If a server fails to pass a check item in check_rule_num, the item is counted in failed_rule_num.
host_num	Integer	The number of servers on which the current baseline detection is performed.
scan_time	Long	Latest detection time (ms)
check_type_desc	String	Description of the baseline type, including the standards for the check items and the issues that can be audited.

Example Requests

This API is used to query the server baseline configuration check list whose enterprise project ID is xxx. Data on the first page (the first 10 records) is returned by default.

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

Example Responses

Status code: 200

server security configuration check result

```
{
  "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"
  } ]
}
```

Status Codes

Status Code	Description
200	server security configuration check result

Error Codes

See **Error Codes**.

3.3.4 Querying the Check Result of a Security Configuration Item

Function

This API is used to query the check result of a specified security configuration item.

URI

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

Table 3-101 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
check_name	Yes	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.

Table 3-102 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
standard	Yes	String	hw_standard: Cloud security practice standard

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried.
limit	No	Integer	Number of records on each page.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-103 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-104 Response body parameters

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_type	String	Configuration check (baseline) type, for example, SSH, CentOS 7, Windows Server 2019 R2, Windows Server 2016 R2 and MySQL5-Windows.
check_type_desc	String	Description of the baseline type, including the standards for the check items and the issues that can be audited.

Parameter	Type	Description
check_rule_num	Integer	Indicates the total number of check items of the current configuration check (baseline) type. For example, if the standard type of the SSH baseline is hw_standard, server security provides 17 check items, but only five check items of the SSH baseline are detected on all servers. Therefore, the value of check_rule_num is 5. All check items are checked on a server. The value of check_rule_num is 17.
failed_rule_num	Integer	Number of failed check items. If a server fails to pass a check item in check_rule_num, the item is counted in failed_rule_num.
passed_rule_num	Integer	Number of passed check items. If a server passes a check item in check_rule_num, the check item is counted in passed_rule_num.
ignored_rule_num	Integer	Number of ignored check items. If a server ignores a check item in check_rule_num, the check item is counted in ignored_rule_num.
host_num	Long	The number of servers on which the current baseline detection is performed.

Example Requests

This API is used to query the configuration check list whose baseline name is SSH, check standard is cloud security practice standard, and enterprise project ID is xxx.

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

Example Responses

Status code: 200

security configuration item check result

```
{
  "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"
}
```


Status Codes

Status Code	Description
200	security configuration item check result

Error Codes

See **Error Codes**.

3.3.5 Querying the Checklist of a Security Configuration Item

Function

This API is used to query the checklist of a specified security configuration item.

URI

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

Table 3-105 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
check_name	Yes	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.

Table 3-106 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
standard	Yes	String	hw_standard: Cloud security practice standard

Parameter	Mandatory	Type	Description
result_type	No	String	Result type. Its value can be: • safe: The item passed the check. • unhandled: The item failed the check and is not ignored. • ignored: The item failed the check but is ignored.
check_rule_name	No	String	Check item name. Fuzzy match is supported.
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High • Critical
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried.
limit	No	Integer	Number of items per page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-107 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-108 Response body parameters

Parameter	Type	Description
total_num	Long	Total risks
data_list	Array of **CheckRuleRiskInfoResponseInfo** objects	Data list

Table 3-109 CheckRuleRiskInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_name	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.
check_type	String	Baseline type. The values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2.
standard	String	hw_standard: Cloud security practice standard
check_rule_name	String	Check item name
check_rule_id	String	Check item ID
host_num	Integer	The number of servers on which the current baseline detection is performed.
scan_result	String	Detection result. Its value can be: • pass • failed

Parameter	Type	Description
status	String	Status. Its value can be: • safe • ignored • unhandled
enable_fix	Integer	Indicates whether one-click repair is supported. 1: yes; 0: no.
rule_params	Array of **CheckRuleFixParamInfo** objects	Range of parameters applicable to the check items that can be fixed by parameter transfer. This API is returned only for check items that support parameter transfer fix.

Table 3-110 CheckRuleFixParamInfo

Parameter	Type	Description
rule_param_id	Integer	Check item parameter ID
rule_desc	String	Check item parameter description
default_value	Integer	Default values of check item parameters
range_min	Integer	Minimum value of check item parameters
range_max	Integer	Minimum value of check item parameters

Example Requests

This API is used to query the check items whose baseline name is SSH, check standard is cloud security practice standard, and enterprise project ID is xxx.

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

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

Example Responses

Status code: 200

checklist of the specified security configuration item

```
{
  "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,
  "scan_result" : "failed",
  "severity" : "High",
  "status" : "unhandled",
  "enable_fix" : 1,
  "enable_click" : true,
  "rule_params" : [ {
    "rule_param_id" : 1,
    "rule_desc" : "Set the timeout duration.",
    "default_value" : 5,
    "range_min" : 1,
    "range_max" : 10
  }, {
    "rule_param_id" : 2,
    "rule_desc" : "Set the number of restarts.",
    "default_value" : 10,
    "range_min" : 1,
    "range_max" : 20
  } ]
 } ]
}
```


Status Codes

Status Code	Description
200	checklist of the specified security configuration item

Error Codes

See **Error Codes**.

3.3.6 Querying the List of Affected Servers of a Security Configuration Item

Function

This API is used to query the list of affected servers of a specified security configuration item.

URI

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

Table 3-111 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
check_name	Yes	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.

Table 3-112 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
standard	Yes	String	hw_standard: Cloud security practice standard
host_name	No	String	Server name
host_ip	No	String	Server IP address
limit	No	Integer	Number of items per page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-113 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-114 Response body parameters

Parameter	Type	Description
total_num	Long	Total amount of data affected by configuration check
data_list	Array of **SecurityCheckHostInfoResponseInfo** objects	Data list

Table 3-115 SecurityCheckHostInfoResponseInfo

Parameter	Type	Description
host_id	String	Host ID
host_name	String	Server name
host_public_ip	String	Server public IP address
host_private_ip	String	Server private IP address
scan_time	Long	Scan time (ms)
failed_num	Integer	Number of risk items
passed_num	Integer	Number of passed items

Example Requests

This API is used to query the list of affected servers whose baseline name is SSH, check standard is cloud security practice standard, and enterprise project ID is xxx.

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

Example Responses

Status code: 200

servers affected by the security configuration item

```
{
  "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
  } ]
}
```


Status Codes

Status Code	Description
200	servers affected by the security configuration item

Error Codes

See **Error Codes**.

3.3.7 Querying the Report of a Check Item in a Security Configuration Check

Function

This API is used to query the report of a check item in a security configuration check.

URI

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

Table 3-116 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-117 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
check_name	Yes	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.

Parameter	Mandatory	Type	Description
check_type	Yes	String	Baseline type. You can obtain the value by calling API /v5/{project_id}/baseline/risk-configs. Note that the values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2, while check_name can be set to Windows.
check_rule_id	Yes	String	Check item ID, which can be obtained from the return data of this API: /v5/{project_id}/baseline/risk-config/{check_name}/check-rules
standard	Yes	String	hw_standard: Cloud security practice standard
host_id	No	String	Host ID

Request Parameters

Table 3-118 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token, which can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is the IAM token.

Response Parameters

Status code: 200

Table 3-119 Response body parameters

Parameter	Type	Description
description	String	Description of the current check item (detection rule).
reference	String	Basis for the check item (rule) setting
audit	String	Audit description of the check item (rule)
remediation	String	Modification suggestions for the check item (rule)
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	Test cases

Table 3-120 CheckRuleCheckCaseResponseInfo

Parameter	Type	Description
check_description	String	Test case description
current_value	String	Current result
suggest_value	String	Expected result

Example Requests

This API is used to query the report of the configuration check items whose baseline name is SSH, check item ID is 1.12, check standard is cloud security practice standard, and enterprise project ID is xxx.

```
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
```

Example Responses

Status code: 200

configuration item check report

{"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"}
```

Status Codes

Status Code	Description
200	configuration item check report

Error Codes

See **Error Codes**.

3.4 Quota Management

3.4.1 Querying Quota Details

Function

This API is used to query quota details.

URI

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

Table 3-121 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-122 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Parameter	Mandatory	Type	Description
version	No	String	HSS edition. Its value can be: • hss.version.null • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition
category	No	String	Type. Its value can be: • host_resource • container_resource
quota_status	No	String	Quota status. It can be: • QUOTA_STATUS_NORMAL – QUOTA_STATUS_EXPIRED – QUOTA_STATUS_FREEZE
used_status	No	String	Usage status. It can be: • USED_STATUS_IDLE • USED_STATUS_USED
host_name	No	String	Server name
resource_id	No	String	Specifies the resource ID of the HSS quota.
charging_mode	No	String	on_demand: pay-per-use
limit	No	Integer	Number of items per page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-123 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	No	String	Region ID

Response Parameters

Status code: 200

Table 3-124 Response body parameters

Parameter	Type	Description
on_demand_num	Integer	Pay-per-Use quotas
used_num	Integer	Used quotas
idle_num	Integer	Idle quotas
normal_num	Integer	Normal quotas
expired_num	Integer	Expired quotas
freeze_num	Integer	Frozen quotas
quota_statistics_list	Array of **QuotaStatistics-ResponseInfo** objects	Quota statistics list
total_num	Integer	Total quotas
data_list	Array of **QuotaResourcesResponseInfo** objects	Quota list

Table 3-125 QuotaStatisticsResponseInfo

Parameter	Type	Description
version	String	Resource flavor. Its value can be: • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container: container edition
total_num	Integer	Total quotas

Table 3-126 QuotaResourcesResponseInfo

Parameter	Type	Description
resource_id	String	Resource ID of an HSS quota
version	String	Resource flavor. Its value can be: • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container: container edition
quota_status	String	Quota status. It can be: • normal – expired – freeze
used_status	String	Usage status. Its value can be: • idle • used
host_id	String	Host ID
host_name	String	Server name
charging_mode	String	on_demand: pay-per-use
tags	Array of **TagInfo** objects	Tag
expire_time	Long	Expiration time. The value -1 indicates that the resource will not expire.

Parameter	Type	Description
shared_quota	String	Whether quotas are shared. Its value can be: • shared • unshared
enterprise_project_id	String	Enterprise project ID
enterprise_project_name	String	Enterprise project name

Table 3-127 TagInfo

Parameter	Type	Description
key	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank.
value	String	Value. Each tag value can contain a maximum of 255 Unicode characters.

Example Requests

This API is used to query quotas details in all enterprise projects.

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

Example Responses

Status code: 200

quota details

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


Status Codes

Status Code	Description
200	quota details

Error Codes

See **Error Codes**.

3.5 Intrusion Detection

3.5.1 Querying the Detected Intrusion List

Function

This API is used to query the detected intrusion list.

URI

GET /v5/{project_id}/event/events

Table 3-128 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-129 Query Parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Event category. Its value can be: • host: host security event • container: container security event

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
last_days	No	Integer	Number of days to be queried. This parameter is mutually exclusive with **begin_time** and **end_time**.
host_name	No	String	Server name
host_id	No	String	Host ID
private_ip	No	String	Server IP address
container_name	No	String	Container instance name
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	No	Integer	Number of records displayed on each page

Parameter	Mandatory	Type	Description
event_types	No	Array of integers	Intrusion type. Its value can be: • 1001: Malware • 1010: Rootkit • 1011: Ransomware • 1015: Web shell • 1017: Reverse shell • 2001: Common vulnerability exploit • 3002: File privilege escalation • 3003: Process privilege escalation • 3004: Important file change • 3005: File/Directory change • 3007: Abnormal process behavior • 3015: High-risk command execution • 3018: Abnormal shell • 3027: Suspicious crontab tasks • 4002: Brute-force attack • 4004: Abnormal login • 4006: Invalid system account
handle_status	No	String	Status. Its value can be: • unhandled • handled
severity	No	String	Threat level. Its value can be: • Security • Low • Medium • High • Critical

Parameter	Mandatory	Type	Description
begin_time	No	String	Customized start time of a segment. The timestamp is accurate to seconds. The **begin_time** should be no more than two days earlier than the **end_time**. This parameter is mutually exclusive with the queried duration.
end_time	No	String	Customized end time of a segment. The timestamp is accurate to seconds. The **begin_time** should be no more than two days earlier than the **end_time**. This parameter is mutually exclusive with the queried duration.

Request Parameters

Table 3-130 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-131 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of alarm events

Parameter	Type	Description
data_list	Array of **EventManagementResponseInfo** objects	Event list

Table 3-132 EventManagementResponseInfo

Parameter	Type	Description
event_id	String	Event ID

Parameter	Type	Description
event_class_id	String	Event category. Its value can be: • container_1001: Container namespace • container_1002: Container open port • container_1003: Container security option • container_1004: Container mount directory • containerescape_0001: High-risk system call • containerescape_0002: Shocker attack • containerescape_0003: Dirty Cow attack • containerescape_0004: Container file escape • dockerfile_001: Modification of user-defined protected container file • dockerfile_002: Modification of executable files in the container file system • dockerproc_001: Abnormal container process • fileprotect_0001: File privilege escalation • fileprotect_0002: Key file change • fileprotect_0003: AuthorizedKeysFile path change • fileprotect_0004: File directory change • login_0001: Brute-force attack attempt • login_0002: Brute-force attack succeeded • login_1001: Succeeded login • login_1002: Remote login • login_1003: Weak password • malware_0001: Shell change • malware_0002: Reverse shell • malware_1001: Malicious program

Parameter	Type	Description
		• procdet_0001: Abnormal process behavior • procdet_0002: Process privilege escalation • procreport_0001: High-risk command • user_1001: Account change • user_1002: Unsafe account • vmescape_0001: Sensitive command executed on VM • vmescape_0002: Sensitive file accessed by virtualization process • vmescape_0003: Abnormal VM port access • webshell_0001: Web shell • network_1001: Mining • network_1002: DDoS attacks • network_1003: Malicious scanning • network_1004: Attack in sensitive areas • crontab_1001: Suspicious crontab task
event_type	Integer	Intrusion type. Its value can be: • 1001: Malware • 1010: Rootkit • 1011: Ransomware • 1015: Web shell • 1017: Reverse shell • 2001: Common vulnerability exploit • 3002: File privilege escalation • 3003: Process privilege escalation • 3004: Important file change • 3005: File/Directory change • 3007: Abnormal process behavior • 3015: High-risk command execution • 3018: Abnormal shell • 3027: Suspicious crontab tasks • 4002: Brute-force attack • 4004: Abnormal login • 4006: Invalid system account

Parameter	Type	Description
event_name	String	Event name
severity	String	Threat level. Its value can be: • Security • Low • Medium • High • Critical
container_name	String	Container instance name. This API is available only for container alarms.
image_name	String	Image name. This API is available only for container alarms.
host_name	String	Server name
host_id	String	Host ID
private_ip	String	Server private IP address
public_ip	String	Elastic IP address
os_type	String	OS type. Its value can be: • Linux • Windows
host_status	String	Server status. The options are as follows: • ACTIVE • SHUTOFF • BUILDING • ERROR
agent_status	String	Agent status. Its value can be: • installed • not_installed • online • offline • install_failed • installing
protect_status	String	Protection status. Its value can be: • closed • opened

Parameter	Type	Description
asset_value	String	Asset importance. The options are as follows: • important • common • test
attack_phase	String	Attack phase. Its value can be: • reconnaissance • weaponization • delivery • exploit • installation • command_and_control • actions
attack_tag	String	Attack tag. Its value can be: • attack_success • attack_attempt • attack_blocked • abnormal_behavior • collapsible_host • system_vulnerability
occur_time	Integer	Occurrence time, accurate to milliseconds.
handle_time	Integer	Handling time, in milliseconds. This API is available only for handled alarms.
handle_status	String	Processing status. Its value can be: • unhandled • handled
handle_method	String	Handling method. This API is available only for handled alarms. The options are as follows: • mark_as_handled • ignore • add_to_alarm_whitelist • add_to_login_whitelist • isolate_and_kill
handler	String	Remarks. This API is available only for handled alarms.

Parameter	Type	Description
operate_accept_list	Array of strings	Supported processing operation
operate_detail_list	Array of **EventDetailResponseInfo** objects	Operation details list (not displayed on the page)
forensic_info	Object	Attack information, in JSON format.
resource_info	**EventResourceResponseInfo** object	Resource information
geo_info	Object	Geographical location, in JSON format.
malware_info	Object	Malware information, in JSON format.
network_info	Object	Network information, in JSON format.
app_info	Object	Application information, in JSON format.
system_info	Object	System information, in JSON format.
extend_info	Object	Extended event information, in JSON format
recommendation	String	Handling suggestions
process_info_list	Array of **EventProcessResponseInfo** objects	Process information list
user_info_list	Array of **EventUserResponseInfo** objects	User information list
file_info_list	Array of **EventFileResponseInfo** objects	File information list
event_details	String	Brief description of the event.

Table 3-133 EventDetailResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
process_pid	Integer	Process ID
is_parent	Boolean	Whether a process is a parent process
file_hash	String	File hash

Parameter	Type	Description
file_path	String	File path
file_attr	String	File attribute
private_ip	String	Server private IP address
login_ip	String	Login source IP address
login_user_name	String	Login username
keyword	String	Alarm event keyword, which is used only for the alarm whitelist.
hash	String	Alarm event hash, which is used only for the alarm whitelist.

Table 3-134 EventResourceResponseInfo

Parameter	Type	Description
domain_id	String	User account ID
project_id	String	Project ID
enterprise_project_id	String	Enterprise project ID
region_name	String	Region name
vpc_id	String	VPC ID
cloud_id	String	ECS ID
vm_name	String	VM name
vm_uuid	String	Specifies the VM UUID, that is, the server ID.
container_id	String	Container ID
image_id	String	Image ID
image_name	String	Image name
host_attr	String	Host attribute
service	String	Service
micro_service	String	Microservice
sys_arch	String	System CPU architecture
os_bit	String	OS bit version
os_type	String	OS type

Parameter	Type	Description
os_name	String	OS name
os_version	String	OS version

Table 3-135 EventProcessResponseInfo

Parameter	Type	Description
process_name	String	Process name
process_path	String	Process file path
process_pid	Integer	Process ID
process_uid	Integer	Process user ID
process_username	String	Process username
process_cmdline	String	Process file command line
process_filename	String	Process file name
process_start_time	Long	Process start time
process_gid	Integer	Process group ID
process_egid	Integer	Valid process group ID
process_euid	Integer	Valid process user ID
parent_process_name	String	Parent process name
parent_process_path	String	Parent process file path
parent_process_pid	Integer	Parent process ID
parent_process_uid	Integer	Parent process user ID
parent_process_cmdline	String	Parent process file command line
parent_process_filename	String	Parent process file name
parent_process_start_time	Long	Parent process start time
parent_process_gid	Integer	Parent process group ID

Parameter	Type	Description
parent_process_egid	Integer	Valid parent process group ID
parent_process_euid	Integer	Valid parent process user ID
child_process_name	String	Subprocess name
child_process_path	String	Subprocess file path
child_process_pid	Integer	Subprocess ID
child_process_uid	Integer	Subprocess user ID
child_process_cmdline	String	Subprocess file command line
child_process_filename	String	Subprocess file name
child_process_start_time	Long	Subprocess start time
child_process_gid	Integer	Subprocess group ID
child_process_egid	Integer	Valid subprocess group ID
child_process_euid	Integer	Valid subprocess user ID
virt_cmd	String	Virtualization command
virt_process_name	String	Virtualization process name
escape_mode	String	Escape mode
escape_cmd	String	Commands executed after escape
process_hash	String	Process startup file hash

Table 3-136 EventUserResponseInfo

Parameter	Type	Description
user_id	Integer	User UID
user_gid	Integer	User GID
user_name	String	User name
user_group_name	String	User group name
user_home_dir	String	User home directory

Parameter	Type	Description
login_ip	String	User login IP address
service_type	String	Service type. The options are as follows: • system • mysql • redis
service_port	Integer	Login service port
login_mode	Integer	Login mode
login_last_time	Long	Last login time
login_fail_count	Integer	Number of failed login attempts
pwd_hash	String	Password hash
pwd_with_fuzzing	String	Masked password
pwd_used_days	Integer	Password age (days)
pwd_min_days	Integer	Minimum password validity period
pwd_max_days	Integer	Maximum password validity period
pwd_warn_left_days	Integer	Advance warning of password expiration (days)

Table 3-137 EventFileResponseInfo

Parameter	Type	Description
file_path	String	File path
file_alias	String	File alias
file_size	Integer	File size
file_mtime	Long	Time when a file was last modified
file_atime	Long	Time when a file was last accessed
file_ctime	Long	Time when the status of a file was last changed
file_hash	String	The hash value calculated using the SHA256 algorithm.
file_md5	String	File MD5
file_sha256	String	File SHA256
file_type	String	File type

Parameter	Type	Description
file_content	String	File content
file_attr	String	File attribute
file_operation	Integer	File operation type
file_action	String	File action
file_change_attr	String	Old/New attribute
file_new_path	String	New file path
file_desc	String	File description
file_key_word	String	File keyword
is_dir	Boolean	Whether it is a directory
fd_info	String	File handle information
fd_count	Integer	Number of file handles

Example Requests

Query the first 50 unprocessed server events whose enterprise project is xxx.

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

Example Responses

Status code: 200

intrusion list

```
{
  "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" : "Country/Region",
      "city" : "State/Province",
      "ip" : "127.0.0.1",
      "user" : "zhangsan",
      "sub_division" : "City",
      "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" : ""
   },
   "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
   } ]
  } ]
}
```


Status Codes

Status Code	Description
200	intrusion list

Error Codes

See **Error Codes**.

3.5.2 Querying the Alarm Whitelist

Function

This API is used to query the alarm whitelist.

URI

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

Table 3-138 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-139 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
hash	No	String	Hash value of the event whitelist description (SHA256 algorithm)

Parameter	Mandatory	Type	Description
event_type	No	Integer	Event type. Its value can be: • 1001: malware • 1010 : Rootkit • 1011: ransomware – 1015 : Web shell – 1017: reverse shell – 2001: Common vulnerability exploit – 2047: redis vulnerability exploit – 2048: Hadoop vulnerability exploit – 2049: MySQL vulnerability exploit – 3002: file privilege escalation – 3003: process privilege escalation – 3004: critical file change – 3005: file/directory change – 3007: abnormal process behavior – 3015: high-risk command execution – 3018: abnormal shell – 3027: suspicious crontab task – 4002: brute-force attack – 4004: abnormal login – 4006: Invalid system account
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-140 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-141 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
event_type_list	Array of integers	Types of events that can be filtered
data_list	Array of **AlarmWhiteListResponseInfo** objects	Alarm whitelist details

Table 3-142 AlarmWhiteListResponseInfo

Parameter	Type	Description
enterprise_project_name	String	Enterprise project name
hash	String	Hash value of the event whitelist description (SHA256 algorithm)
description	String	Description

Parameter	Type	Description
event_type	Integer	Intrusion type. Its value can be: • 1001: Malware • 1010: Rootkit • 1011: Ransomware • 1015: Web shell • 1017: Reverse shell • 2001: Common vulnerability exploit • 3002: File privilege escalation • 3003: Process privilege escalation • 3004: Important file change • 3005: File/Directory change • 3007: Abnormal process behavior • 3015: High-risk command execution • 3018: Abnormal shell • 3027: Suspicious crontab tasks • 4002: Brute-force attack • 4004: Abnormal login • 4006: Invalid system account
update_time	Long	Time when the event whitelist is updated, in milliseconds.

Example Requests

Query the first 10 alarm whitelists whose enterprise project is xxx.

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

Example Responses

Status code: 200

Alarm whitelist

```
{
  "data_list" : [ {
    "enterprise_project_name" : "All projects",
    "event_type" : 1001,
    "hash" : "9ab079e5398cba3a368ccffbd478f54c5ec3edadf6284ec049a73c36419f1178",
    "description" : "/opt/cloud/3rdComponent/install/jre-8u201/bin/java",
    "update_time" : 1665715677307
  } ],
  "event_type_list" : [ 1001 ],
  "total_num" : 1
}
```


Status Codes

Status Code	Description
200	Alarm whitelist

Error Codes

See **Error Codes**.

3.5.3 Handling Alarm Events

Function

This API is used to handle alarm events.

URI

POST /v5/{project_id}/event/operate

Table 3-143 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-144 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-145 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Parameter	Mandatory	Type	Description
region	Yes	String	Region ID

Table 3-146 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Handling method. Its value can be: • mark_as_handled • ignore • add_to_alarm_whitelist • add_to_login_whitelist • isolate_and_kill • unhandle • do_not_ignore • remove_from_alarm_whitelist • remove_from_login_whitelist • do_not_isolate_or_kill
handler	No	String	Remarks. This API is available only for handled alarms.
operate_event_list	Yes	Array of **OperateEventRequestInfo** objects	Operated event list

Table 3-147 OperateEventRequestInfo

Parameter	Mandatory	Type	Description
event_class_id	Yes	String	Event category. Its value can be: • container_1001: Container namespace • container_1002: Container open port • container_1003: Container security option • container_1004: Container mount directory • containerescape_0001: High-risk system call • containerescape_0002: Shocker attack • containerescape_0003: Dirty Cow attack • containerescape_0004: Container file escape • dockerfile_001: Modification of user-defined protected container file • dockerfile_002: Modification of executable files in the container file system • dockerproc_001: Abnormal container process • fileprotect_0001: File privilege escalation • fileprotect_0002: Key file change • fileprotect_0003: AuthorizedKeysFile path change • fileprotect_0004: File directory change • login_0001: Brute-force attack attempt • login_0002: Brute-force attack succeeded • login_1001: Succeeded login

Parameter	Mandatory	Type	Description
			• login_1002: Remote login • login_1003: Weak password • malware_0001: Shell change • malware_0002: Reverse shell • malware_1001: Malicious program • procdet_0001: Abnormal process behavior • procdet_0002: Process privilege escalation • procreport_0001: High-risk command • user_1001: Account change • user_1002: Unsafe account • vmescape_0001: Sensitive command executed on VM • vmescape_0002: Sensitive file accessed by virtualization process • vmescape_0003: Abnormal VM port access • webshell_0001: Web shell • network_1001: Mining • network_1002: DDoS attacks • network_1003: Malicious scanning • network_1004: Attack in sensitive areas • crontab_1001: Suspicious crontab task
event_id	Yes	String	Event ID

Parameter	Mandatory	Type	Description
event_type	Yes	Integer	Intrusion type. Its value can be: • 1001: Malware • 1010: Rootkit • 1011: Ransomware • 1015: Web shell • 1017: Reverse shell • 2001: Common vulnerability exploit • 3002: File privilege escalation • 3003: Process privilege escalation • 3004: Important file change • 3005: File/Directory change • 3007: Abnormal process behavior • 3015: High-risk command execution • 3018: Abnormal shell • 3027: Suspicious crontab tasks • 4002: Brute-force attack • 4004: Abnormal login • 4006: Invalid system account
occur_time	Yes	Integer	Occurrence time, accurate to milliseconds.

Parameter	Mandatory	Type	Description
operate_detail_list	Yes	Array of EventDetailRequestInfo objects	Operation details list. If operate_type is set to add_to_alarm_whitelist or remove_from_alarm_whitelist, keyword and hash are mandatory. If operate_type is set to add_to_login_whitelist or remove_from_login_whitelist, the login_ip, private_ip, and login_user_name parameters are mandatory. If operate_type is set to isolate_and_kill or do_not_isolate_or_kill, the agent_id, file_hash, file_path, and process_pid parameters are mandatory. In other cases, the parameters are optional.

Table 3-148 EventDetailRequestInfo

Parameter	Mandatory	Type	Description
agent_id	No	String	Agent ID
process_pid	No	Integer	Process ID
file_hash	No	String	File hash
file_path	No	String	File path
file_attr	No	String	File attribute
keyword	No	String	Alarm event keyword, which is used only for the alarm whitelist.
hash	No	String	Alarm event hash, which is used only for the alarm whitelist.
private_ip	No	String	Server private IP address
login_ip	No	String	Login source IP address
login_user_name	No	String	Login username

Response Parameters

Status code: 200

success

None

Example Requests

```
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"
    } ]
  } ],
  "x-request-examples-description-1" : "Manually handle the intrusion alarms whose alarm event type is Rootkit and alarm event ID is 2a71e1e2-60f4-4d56-b314-2038fdc39de6."
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resource not found.
500	System error.

Error Codes

See **Error Codes**.

3.6 Server Management

3.6.1 Querying ECSs

Function

This API is used to query ECSs.

URI

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

Table 3-149 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-150 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
version	No	String	HSS edition. Its value can be: • hss.version.null: none • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition

Parameter	Mandatory	Type	Description
agent_status	No	String	Agent status. Its value can be: • not_ installed • online • offline • install_failed • installing • not_online: All status except **online**, which is used only as a query condition.
detect_result	No	String	Detection result. Its value can be: • undetected • clean • risk • scanning
host_name	No	String	Server name
host_id	No	String	Server ID
host_status	No	String	Host status. Its value can be: • ACTIVE • SHUTOFF • BUILDING • ERROR
os_type	No	String	OS type. Its value can be: • Linux • Windows
private_ip	No	String	Server private IP address
public_ip	No	String	Server public IP address
ip_addr	No	String	Public or private IP address
protect_status	No	String	Protection status. Its value can be: • closed • opened
group_id	No	String	Server group ID
group_name	No	String	Server group name

Parameter	Mandatory	Type	Description
policy_group_id	No	String	Policy group ID
policy_group_name	No	String	Policy group name
charging_mode	No	String	on_demand: pay-per-use
refresh	No	Boolean	Whether to forcibly synchronize servers from ECSs
above_version	No	Boolean	Whether to return all the versions later than the current version
outside_host	No	Boolean	Whether a server is a Cloud server
asset_value	No	String	Asset importance. Its value can be: • important • common • test
label	No	String	Asset tag
server_group	No	String	Asset server group
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

Request Parameters

Table 3-151 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is a token.
region	No	String	Region ID

Response Parameters

Status code: 200

Table 3-152 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of records
data_list	Array of **Host** objects	Query on the cloud server status and list

Table 3-153 Host

Parameter	Type	Description
host_name	String	Server name
host_id	String	Server ID
agent_id	String	Agent ID
private_ip	String	Private IP address
public_ip	String	Elastic IP address
enterprise_project_id	String	Enterprise project ID
enterprise_project_name	String	Enterprise project name

Parameter	Type	Description
host_status	String	Server status. Its value can be: • ACTIVE • SHUTOFF • BUILDING • ERROR
agent_status	String	Agent status. Its value can be: • not_ installed • online • offline • install_failed • installing
install_result_code	String	Installation result. This API is available only for agents that are installed in batches. The options are as follows: • install_succeed • network_access_timeout: Connection timed out. Network error. • invalid_port • auth_failed: The authentication failed due to incorrect password. • permission_denied: Insufficient permissions. • no_available_vpc: There is no server with an online agent in the current VPC. • install_exception • invalid_param: Incorrect parameter. • install_failed • package_unavailable • os_type_not_support: Incorrect OS type • os_arch_not_support: Incorrect OS architecture

Parameter	Type	Description
version	String	HSS edition. Its value can be: • hss.version.null: none • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition
protect_status	String	Protection status. Its value can be: • closed • opened
os_image	String	System disk image
os_type	String	OS type. Its value can be: • Linux • Windows
os_bit	String	OS bit version
detect_result	String	Server scan result. Its value can be: • undetected • clean • risk • scanning
charging_mode	String	on_demand: pay-per-use
resource_id	String	Cloud service resource instance ID (UUID)
outside_host	Boolean	Whether a server is a Other server
group_id	String	Server group ID
group_name	String	Server group name
policy_group_id	String	Policy group ID
policy_group_name	String	Policy group name
asset	Integer	Asset risk
vulnerability	Integer	Total number of vulnerabilities, including Linux, Windows, Web-CMS, and application vulnerabilities.

Parameter	Type	Description
baseline	Integer	Total number of baseline risks, including configuration risks and weak passwords.
intrusion	Integer	Total intrusion risks
asset_value	String	Asset importance. Its value can be: • important • common • test
labels	Array of strings	Tag list
agent_create_time	Long	Agent installation time, which is a timestamp. The default unit is milliseconds.
agent_update_time	Long	Time when the agent status is changed. This is a timestamp. The default unit is milliseconds.
agent_version	String	Agent version
upgrade_status	String	Upgrade status. Its value can be: • not_upgrade: Not upgraded. This is the default status. The customer has not delivered any upgrade command to the server. • upgrading: The upgrade is in progress. • upgrade_failed: The upgrade failed. • upgrade_succeed
upgrade_result_code	String	Upgrade failure cause. This parameter is displayed only if upgrade_status is upgrade_failed. Its value can be: • package_unavailable: The upgrade package fails to be parsed because the upgrade file is incorrect. • network_access_timeout: Failed to download the upgrade package because the network is abnormal. • agent_offline: The agent is offline. • hostguard_abnormal: The agent process is abnormal. • insufficient_disk_space • failed_to_replace_file: Failed to replace the file.

Parameter	Type	Description
upgradable	Boolean	Whether the agent of the server can be upgraded

Example Requests

Query the 10 Linux servers in all enterprise projects whose agent status is online.

```
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
```

Example Responses

Status code: 200

cloud server list


```
{
  "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",
    "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
  } ]
}
```


Status Codes

Status Code	Description
200	cloud server list

Error Codes

See **Error Codes**.

3.6.2 Changing the Protection Status

Function

This API is used to change the protection status.

URI

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

Table 3-154 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-155 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-156 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Table 3-157 Request body parameters

Parameter	Mandatory	Type	Description
version	No	String	Edition to be enabled. Its value can be: • hss.version.null : VERSION_NULL • hss.version.enterprise : VERSION_ENTERPRISE • hss.version.premium : VERSION_PREMIUM • hss.version.wtp : VERSION_WTP
charging_mode	No	String	on_demand: pay-per-use
resource_id	No	String	Instance ID
host_id_list	No	Array of strings	Server list
tags	No	Array of **TagInfo** objects	Resource tag

Table 3-158 TagInfo

Parameter	Mandatory	Type	Description
key	No	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank.
value	No	String	Value. Each tag value can contain a maximum of 255 Unicode characters.

Response Parameters

Status code: 200

successful response

None

Example Requests

Switch the protection edition of the server whose ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f to the enterprise edition.


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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.6.3 Querying Server Groups

Function

This API is used to query server groups.

URI

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

Table 3-159 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-160 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	No	Integer	Number of records displayed on each page.
group_name	No	String	Server group name

Request Parameters

Table 3-161 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-162 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **HostGroupItem** objects	Server group list

Table 3-163 HostGroupItem

Parameter	Type	Description
group_id	String	Server group ID
group_name	String	Server group name

Parameter	Type	Description
host_num	Integer	Number of associated servers
risk_host_num	Integer	Number of unsafe servers
unprotect_host_num	Integer	Number of unprotected servers
host_id_list	Array of strings	Server ID list

Example Requests

Query the server group whose name is test.

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

Example Responses

Status code: 200

Server group list

```
{
  "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
}
```

Status Codes

Status Code	Description
200	Server group list

Error Codes

See **Error Codes**.

3.6.4 Creating a Server Group

Function

This API is used to create a server group.

URI

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

Table 3-164 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-165 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-166 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region ID

Table 3-167 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Server group name
host_id_list	Yes	Array of strings	Server ID list

Response Parameters

Status code: 200

success

None

Example Requests

Create a server group named test. The ID of the server in the server group is 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" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resource not found.
500	System error.

Error Codes

See **Error Codes**.

3.6.5 Editing a Server Group

Function

This API is used to edit a server group.

URI

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

Table 3-168 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-169 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-170 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region ID

Table 3-171 Request body parameters

Parameter	Mandatory	Type	Description
group_name	No	String	Server group name
group_id	Yes	String	Server group ID
host_id_list	No	Array of strings	Server ID list

Response Parameters

Status code: 200

success

None

Example Requests

Edit the server group named test. The server group ID is eca40dbe-27f7-4229-8f9d-a58213129fdc. The IDs of the servers in the server group are 15dac7fe-d81b-43bc-a4a7-4710fe673972 and 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" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resource not found.
500	System error.

Error Codes

See **Error Codes**.

3.6.6 Deleting a Server Group

Function

This API is used to delete a server group.

URI

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

Table 3-172 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-173 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
group_id	Yes	String	Server group ID

Request Parameters

Table 3-174 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

success

None

Example Requests

Delete the server group whose ID is 34fcf861-402b-45c6-9b6a-13087791aae3.

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

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


Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resource not found.
500	System error.

Error Codes

See **Error Codes**.

3.7 Policy Management

3.7.1 Querying the Policy Group List

Function

This API is used to query the policy group list.

URI

GET /v5/{project_id}/policy/groups

Table 3-175 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-176 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
group_name	No	String	Policy group name
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-177 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-178 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **PolicyGroupResponseInfo** objects	Policy group list

Table 3-179 PolicyGroupResponseInfo

Parameter	Type	Description
group_name	String	Policy group name
group_id	String	Policy group ID
description	String	Description of the policy group
deletable	Boolean	Whether a policy group can be deleted
host_num	Integer	Number of associated servers
default_group	Boolean	Whether a policy group is the default policy group
support_os	String	Supported OS. The options are as follows: • Linux • Windows
support_version	String	Supported versions. The options are as follows: • hss.version.enterprise: policy group of the enterprise edition • hss.version.premium: policy group of the premium edition • hss.version.wtp: policy group of the WTP edition • hss.version.container.enterprise: policy group of the container edition

Example Requests

Query the policy group list of all enterprise projects.

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

Example Responses

Status code: 200

Policy group list

```
{
  "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
}
```


Status Codes

Status Code	Description
200	Policy group list

Error Codes

See **Error Codes**.

3.7.2 Applying a Policy Group

Function

Applying a policy group

URI

POST /v5/{project_id}/policy/deploy

Table 3-180 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-181 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-182 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region ID

Table 3-183 Request body parameters

Parameter	Mandatory	Type	Description
target_policy_group_id	Yes	String	ID of the policy group to be deployed
operate_all	No	Boolean	Whether to deploy the policy on all hosts. If the value is true, you do not need to configure host_id_list. If the value is false, configure host_id_list.
host_id_list	No	Array of strings	IDs of servers where the policy group needs to be deployed

Response Parameters

Status code: 200

success

None

Example Requests

Deploy a server protection policy. The target server ID is 15462c0e-32c6-4217-a869-bbd131a00ecf, and the target policy ID is 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
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resource not found.
500	System error.

Error Codes

See **Error Codes**.

3.8 Vulnerability Management

3.8.1 Querying the Vulnerability List

Function

This API is used to query the list of detected vulnerabilities.

URI

GET /v5/{project_id}/vulnerability/vulnerabilities

Table 3-184 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-185 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. The value **0** indicates the default enterprise project. To query all enterprise projects, set this parameter to **all_granted_eps**.
type	No	String	Vulnerability type. Its value can be: -linux_vul -windows_vul -web_cms
vul_id	No	String	Vulnerability ID
vul_name	No	String	Vulnerability name
limit	No	Integer	Number of records displayed on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of **X-Subject-Token** in the response header is a token.

Response Parameters

Status code: 200

Table 3-187 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of vulnerabilities
data_list	Array of **VulInfo** objects	Software vulnerability list

Table 3-188 VulInfo

Parameter	Type	Description
vul_name	String	Vulnerability name
vul_id	String	Vulnerability ID
label_list	Array of strings	Vulnerability tag

Parameter	Type	Description
repair_necessity	String	Repair necessity • Critical: The CVSS score of the vulnerability is greater than or equal to 9, corresponding to the high risk level on the console. • High: The CVSS score of the vulnerability is greater than or equal to 7 and less than 9, corresponding to the medium risk level on the console. • Medium: The CVSS score of the vulnerability is greater than or equal to 4 and less than 7, corresponding to the medium risk level on the console. • Low: The CVSS score of the vulnerability is less than 4, corresponding to the low risk level on the console.
severity_level	String	Severity • Critical: The CVSS score of the vulnerability is greater than or equal to 9, corresponding to the high risk level on the console. • High: The CVSS score of the vulnerability is greater than or equal to 7 and less than 9, corresponding to the medium risk level on the console. • Medium: The CVSS score of the vulnerability is greater than or equal to 4 and less than 7, corresponding to the medium risk level on the console. • Low: The CVSS score of the vulnerability is less than 4, corresponding to the low risk level on the console.
host_num	Integer	Number of affected servers
unhandle_host_num	Integer	Number of unprocessed servers, excluding ignored and fixed servers.
scan_time	Long	Last scanned, in ms.
solution_detail	String	Vulnerability fixing guide
url	String	Vulnerability URL

Parameter	Type	Description
description	String	Vulnerability description
type	String	Vulnerability type. Its value can be: -linux_vul -windows_vul -web_cms
host_id_list	Array of strings	List of servers that can handle the vulnerability
hosts_num	**VulnerabilityHostNumberInfo** object	Affected server

Table 3-189 VulnerabilityHostNumberInfo

Parameter	Type	Description
important	Integer	Number of important servers
common	Integer	Number of common servers
test	Integer	Number of test servers

Example Requests

Query the first 10 records in the vulnerability list whose project_id is 2b31ed520xxxxxxebedb6e57xxxxxxxx.

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

Example Responses

Status code: 200

vulnerability list


```
{
  "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"
  } ]
}
```

Status Codes

Status Code	Description
200	vulnerability list

Error Codes

See **Error Codes**.

3.8.2 Querying the Servers Affected by a Vulnerability

Function

This API is used to query the servers affected by a vulnerability.

URI

GET /v5/{project_id}/vulnerability/hosts

Table 3-190 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-191 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. The value **0** indicates the default enterprise project. To query all enterprise projects, set this parameter to **all_granted_eps**.
vul_id	Yes	String	Vulnerability ID
type	Yes	String	Vulnerability type. Its value can be: • linux_vul: Linux vulnerability • windows_vul: Windows vulnerability

Parameter	Mandatory	Type	Description
host_name	No	String	Affected server name
host_ip	No	String	IP address of the affected server
status	No	String	Vulnerability status. • vul_status_unfix: not fixed • vul_status_ignored: ignored – vul_status_verified: verification in progress – vul_status_fixing: The fix is in progress. – vul_status_fixed: The fix succeeded. – vul_status_reboot: The issue is fixed and waiting for restart. – vul_status_failed: The issue failed to be fixed. – vul_status_fix_after_reboot: Restart the server and try again.
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-192 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 3-193 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of affected servers
data_list	Array of **VulHostInfo** objects	List of affected ECSs

Table 3-194 VulHostInfo

Parameter	Type	Description
host_id	String	ID of the server affected by the vulnerability
severity_level	String	Risk level. • Critical: The CVSS score of the vulnerability is greater than or equal to 9, corresponding to the high risk level on the console. • High: The CVSS score of the vulnerability is greater than or equal to 7 and less than 9, corresponding to the medium risk level on the console. • Medium: The CVSS score of the vulnerability is greater than or equal to 4 and less than 7, corresponding to the medium risk level on the console. • Low: The CVSS score of the vulnerability is less than 4, corresponding to the low risk level on the console.
host_name	String	Affected server name
host_ip	String	IP address of the affected server
cve_num	Integer	Vulnerability CVEs
cve_id_list	Array of strings	The CVE ID list corresponding to the vulnerability

Parameter	Type	Description
status	String	Vulnerability status. • vul_status_unfix: not fixed • vul_status_ignored: ignored • vul_status_verified: verification in progress • vul_status_fixing: The fix is in progress. • vul_status_fixed: The fix succeeded. • vul_status_reboot : The issue is fixed and waiting for restart. • vul_status_failed: The issue failed to be fixed. • vul_status_fix_after_reboot: Restart the server and try again.
repair_cmd	String	Command line to be executed to fix the vulnerability (This field is available only for Linux vulnerabilities.)

Example Requests

Query the first 10 records in the list of servers with EulerOS-SA-2021-1894 vulnerability.

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

Example Responses

Status code: 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",
    "cve_num" : 1,
    "cve_id_list" : [ "CVE-2022-1664" ],
    "status" : "vul_status_ignored",
    "repair_cmd" : "zypper update update-alternatives"
  } ]
}
```


Status Codes

Status Code	Description
200	Vul host info list

Error Codes

See **Error Codes**.

3.8.3 Changing the Status of a Vulnerability

Function

This API is used to change the status of a vulnerability.

URI

PUT /v5/{project_id}/vulnerability/status

Table 3-195 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-196 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. The value **0** indicates the default enterprise project. To query all enterprise projects, set this parameter to **all_granted_eps**.

Request Parameters

Table 3-197 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8

Table 3-198 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Operation type. • ignore • not_ignore: unignore • immediate_repair: fix • verify
data_list	Yes	Array of **VulOperateInfo** objects	Vulnerability list

Table 3-199 VulOperateInfo

Parameter	Mandatory	Type	Description
vul_id	Yes	String	Vulnerability ID
host_id_list	Yes	Array of strings	Server list

Response Parameters

Status code: 200

successful response

None

Example Requests

Change the vulnerability status of the server whose ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f. Change the status of EulerOS-SA-2021-1894 to ignored.

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.9 Web Tamper Protection

3.9.1 Querying the Protection List

Function

This API is used to query the protection list.

URI

GET /v5/{project_id}/webtamper/hosts

Table 3-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-201 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
host_name	No	String	Server name
host_id	No	String	Host ID
public_ip	No	String	EIP
private_ip	No	String	Private IP address
group_name	No	String	Server group name
os_type	No	String	OS type. Its value can be: • linux • windows
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled
agent_status	No	String	Agent status. Its value can be: • not_installed: The agent is not installed. • online: The agent is online. • offline: The agent is offline.
limit	No	Integer	Default value: 10
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0.

Request Parameters

Table 3-202 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-203 Response body parameters

Parameter	Type	Description
data_list	Array of **WtpProtectHostResponseInfo** objects	data list
total_num	Integer	total number of WTP protected servers

Table 3-204 WtpProtectHostResponseInfo

Parameter	Type	Description
host_name	String	Server name
host_id	String	Host ID
public_ip	String	EIP
private_ip	String	Private IP address
group_name	String	Server group name
os_bit	String	OS bit version
os_type	String	OS (linux or windows)
protect_status	String	Protection status. Its value can be: • closed • opened
rasp_protect_status	String	Dynamic WTP status. • closed • opened
anti_tampering_times	Long	Number of blocked tampering attacks
detect_tampering_times	Long	Number of detected tampering attacks
last_detect_time	Long	Latest detection time (ms)

Parameter	Type	Description
scheduled_shutdown_status	String	Status of scheduled protection. • opened • closed
agent_status	String	Agent status. • not_installed: The agent is not installed. • online: The agent is online. • offline: The agent is offline.

Example Requests

None

Example Responses

Status code: 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" : "testGroup",
    "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" : "online"
  } ]
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

3.9.2 Enabling or Disabling WTP

Function

This API is used to enable or disable WTP.

URI

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

Table 3-205 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-206 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID

Request Parameters

Table 3-207 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region Id

Table 3-208 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	Boolean	Status (enabled or disabled)

Parameter	Mandatory	Type	Description
host_id_list	Yes	Array of strings	The value in the array is server ID and the server ID cannot be empty.
resource_id	No	String	Resource ID

Response Parameters

Status code: 200

successful response

None

Example Requests

Enable WTP, set the target server IDs to a and b, and pay for the yearly/monthly billing mode.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.9.3 Enabling or Disabling Dynamic WTP

Function

This API is used to enable or disable dynamic WTP.

URI

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

Table 3-209 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-210 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID

Request Parameters

Table 3-211 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region Id

Table 3-212 Request body parameters

Parameter	Mandatory	Type	Description
host_id_list	No	Array of strings	HostId list
status	No	Boolean	Dynamic WTP status

Response Parameters

Status code: 200

successful response

None

Example Requests

Enable dynamic WTP for servers a and b.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.9.4 Querying the Status of Static WTP for a Server

Function

This API is used to query the status of static WTP for a server.

URI

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

Table 3-213 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-214 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
host_id	No	String	Host ID. If this parameter is left empty, all the servers are queried.
start_time	Yes	Long	Start time (ms)
end_time	Yes	Long	End time (ms)
limit	Yes	Integer	limit
offset	Yes	Integer	offset

Request Parameters

Table 3-215 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-216 Response body parameters

Parameter	Type	Description
host_name	String	Server name
protect_status	String	Protection status. Its value can be: • close • opened
total_num	Long	total number of static WTPs

Parameter	Type	Description
data_list	Array of **HostProtectHistoryResponseInfo** objects	data list

Table 3-217 HostProtectHistoryResponseInfo

Parameter	Type	Description
occr_time	Long	Static WTP detection time (ms)
file_path	String	Tampered file path
process_id	String	Process ID. This parameter is returned if the OS is Windows.
process_name	String	Process name. This parameter is returned if the OS is Windows.
process_cmd	String	Process command line. This parameter is returned if the OS is Windows.

Example Requests

Query the static WTP status of a server where target ID is caa958ad-a481-4d46-b51e-6861b8864515, start time is 1668563099000, and end time is 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
}
```

Example Responses

Status code: 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",
    "process_id" : "18672",
    "process_name" : "program1",
    "process_cmd" : "del test.xml"
```



```
 }]
}
```

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.9.5 Querying the Status of Dynamic WTP for a Server

Function

This API is used to query the status of dynamic WTP for a server.

URI

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

Table 3-218 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-219 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
host_id	No	String	Host ID. If this parameter is left empty, all the servers are queried.
start_time	Yes	Long	Start time (ms)
end_time	Yes	Long	End time (ms)
limit	Yes	Integer	limit
offset	Yes	Integer	offset

Parameter	Mandatory	Type	Description
alarm_level	No	Integer	Alarm severity. The options are as follows: • 1: low-risk • 2: medium risk • 3: high risk • 4: major
severity	No	String	Threat level. Its value can be: • Security • Low: low risk • Medium: medium risk • High: high risk • Critical
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled

Request Parameters

Table 3-220 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-221 Response body parameters

Parameter	Type	Description
total_num	Long	total number of dynamic WTPs

Parameter	Type	Description
data_list	Array of **HostRaspProtectHistoryResponseInfo** objects	data list

Table 3-222 HostRaspProtectHistoryResponseInfo

Parameter	Type	Description
alarm_time	Long	Alarm time of dynamic WTP (ms)
threat_type	String	Threat type
alarm_level	Integer	Alarm severity
source_ip	String	Source IP address of the attacking server
attacked_url	String	URL of the attack request

Example Requests

Query the dynamic WTP status of a server where target ID is caa958ad-a481-4d46-b51e-6861b8864515, start time is 1668563099000, and end time is 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
}
```

Example Responses

Status code: 200

successful response

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


Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.10 Tag Management

3.10.1 Creating Tags in Batches

Function

This API is used to create tags in batches.

URI

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

Table 3-223 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
resource_type	Yes	String	Resource type defined by TMS. When HSS calls the API, the resource type is HSS.
resource_id	Yes	String	Resource ID defined by TMS. When HSS calls the API, the resource ID is the quota ID.

Request Parameters

Table 3-224 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.
Content-Type	No	String	Default value: application/json; charset=utf-8

Table 3-225 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of **ResourceTagInfo** objects	Tag List

Table 3-226 ResourceTagInfo

Parameter	Mandatory	Type	Description
key	Yes	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank.
value	Yes	String	Value.

Response Parameters

Status code: 200

success

None

Example Requests

Create a tag key TESTKEY20220831190155 (the tag value is 2) and a tag key test (the tag value is hss).

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



```
{
  "tags" : [ {
    "key" : "TESTKEY20220831190155",
    "value" : "2"
  }, {
    "key" : "test",
    "value" : "hss"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.
401	Authentication failed.
403	Insufficient permission.
404	Resources not found.
500	System error.

Error Codes

See **Error Codes**.

3.10.2 Deleting a Resource Tag

Function

This API is used to delete a tag from a resource.

URI

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

Table 3-227 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
resource_type	Yes	String	Resource type defined by TMS. When HSS calls the API, the resource type is HSS.

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID defined by TMS. When HSS calls the API, the resource ID is the quota ID.
key	Yes	String	Key to be deleted

Request Parameters

Table 3-228 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token. It can be obtained by calling the IAM API used to obtain an IAM token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

success

None

Example Requests

Delete the tag whose key is abc, project_id is 94b5266c14ce489fa6549817f032dc61, resource_type is hss, and resource_id is 2acc46ee-34c2-40c2-8060-dc652e6c672a.

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

Example Responses

None

Status Codes

Status Code	Description
200	success
400	Invalid parameter.

Status Code	Description
401	Authentication failed.
403	Insufficient permission.
404	Resources not found.
500	System error.

Error Codes

See **Error Codes**.

A Appendixes

A.1 Status Code

Status Code	Status	Description
200	OK	Request succeeded.
400	Bad Request	Invalid request parameters.
401	Unauthorized	The request requires user authentication.
403	Forbidden	Access denied.
404	Not Found	The page is not found.
405	Method Not Allowed	Method specified in the request not allowed.
406	Not Acceptable	Responses from the server failed to be received by the client.
429	Too Many Requests	Too frequent requests.
500	Internal Server Error	Internal Server Error
501	Not Implemented	Failed to complete the request because the server does not support the requested function.
502	Bad Gateway	Failed to complete the request because the server has received an invalid response.
504	Gateway Timeout	Gateway timed out.

A.2 Error Codes

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.0001	Invalid parameter.	Invalid parameter.	Check whether the parameters are valid.
400	HSS.0002	Failed to parse the request.	Failed to parse the request.	Contact technical support.
400	HSS.0010	Access denied.	Access denied.	Check whether the parameters are valid.
400	HSS.0011	Requested resource not found.	Requested resource not found.	Check whether the parameters are valid.
400	HSS.0013	Insufficient permissions.	Insufficient permissions.	Check user permissions.
400	HSS.0014	Quota creation not allowed.	Quota creation not allowed.	Contact technical support.
400	HSS.1001	The selected server is not associated with any agent.	The selected server is not associated with any agent.	Check whether the agent has been installed on the selected server.
400	HSS.1002	Available quotas are insufficient.	Available quotas are insufficient.	None
400	HSS.1003	Protected servers cannot be ignored.	Protected servers cannot be ignored.	Disable protection and try again.
400	HSS.1004	Failed to query the policy.	Failed to query the policy.	Check whether the parameter is correct.
400	HSS.1005	Invalid policy.	Invalid policy.	Check whether the parameter is correct.
400	HSS.1006	Failed to send requests to the agent.	Failed to send requests to the agent.	Contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1007	The agent is offline.	The agent is offline.	Start the agent.
400	HSS.1008	Failed to query server information.	Failed to query server information.	Check whether the parameter is correct.
400	HSS.1009	Failed to save WTP information.	Failed to save WTP information.	Contact technical support.
400	HSS.1010	Failed to update protected directory information.	Failed to update protected directory information.	Contact technical support.
400	HSS.1011	Failed to convert the time format.	Failed to convert the time format.	Check whether the parameter is correct.
400	HSS.1012	The added period overlaps with an existing one.	The added period overlaps with an existing one.	Check whether the parameter is correct.
400	HSS.1013	Failed to add an unprotected time period.	Failed to add an unprotected time period.	Check whether the parameter is correct.
400	HSS.1014	Failed to add the description of the unprotected time period.	Failed to add the description of the unprotected time period.	Check whether the parameter is correct.
400	HSS.1015	Failed to add the privileged process.	Failed to add the privileged process.	Contact technical support.
400	HSS.1016	Failed to set the unprotected period.	Failed to set the unprotected period.	Contact technical support.
400	HSS.1017	Failed to load security reports.	Failed to load security reports.	Check whether the parameter is correct.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1018	Invalid file information.	Invalid file information.	Check whether the parameter is correct.
400	HSS.1019	Failed to load server groups.	Failed to load server groups.	Check whether the parameter is correct.
400	HSS.1020	The policy group name already exists.	The policy group name already exists.	Change the name.
400	HSS.1021	Failed to load policy groups.	Failed to load policy groups.	Check whether the parameter is correct.
400	HSS.1022	Invalid policy group settings.	Invalid policy group settings.	Check whether the parameter is correct.
400	HSS.1023	Invalid policy group name.	Invalid policy group name.	Change the name.
400	HSS.1024	Failed to query the application process whitelist.	Failed to query the application process whitelist.	Check whether the parameter is correct.
400	HSS.1025	The server group name already exists.	The server group name already exists.	Change the name.
400	HSS.1026	Failed to scan container private image vulnerabilities.	Failed to scan container private image vulnerabilities.	Contact technical support.
400	HSS.1027	Failed to call CBR. HTTP connection timed out.	Failed to call CBR. HTTP connection timed out.	Contact technical support.
400	HSS.1028	Failed to call CBR. Token authenticatio n failed.	Failed to call CBR. Token authenticatio n failed.	Contact technical support.
400	HSS.1029	Failed to query the default backup policy.	Failed to query the default backup policy.	Check whether the parameter is correct.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1030	Failed to query the security check result.	Failed to query the security check result.	Check whether the parameter is correct.
400	HSS.1031	Duplicate security report name.	Duplicate security report name.	Change the name.
400	HSS.1032	A policy in use cannot be deleted.	A policy in use cannot be deleted.	Disable protection and try again.
400	HSS.1033	The protection policy name already exists.	The protection policy name already exists.	Change the name.
400	HSS.1034	Failed to add the protection policy. Up to 20 policies allowed.	Failed to add the protection policy. Up to 20 policies allowed.	None
400	HSS.1035	Only letters, numbers, commas (,), periods, spaces, hyphens(-) and underscores(_) are allowed.	Only letters, numbers, commas (,), periods, spaces, hyphens(-) and underscores(_) are allowed.	Modify the input according to the error message.
400	HSS.1036	Unsupported operation.	Unsupported operation.	None
400	HSS.1037	Unsupported edition.	Unsupported edition.	Change to another edition.
400	HSS.1040	Failed to query container information.	Failed to query container information.	Check whether the parameter is correct.
400	HSS.1041	Failed to query cluster asset information.	Failed to query cluster asset information.	Check whether the parameter is correct.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1042	Failed to deliver the container firewall policy.	Failed to deliver the container firewall policy.	Contact technical support.
400	HSS.1043	The synchronization task already exists. Please wait.	The synchronization task already exists. Please wait.	None
400	HSS.1044	The export task already exists. Please wait.	The export task already exists. Please wait.	None
400	HSS.1045	The export task does not exist.	The export task does not exist.	Check whether the parameter is correct.
400	HSS.1046	The exported file does not exist.	The exported file does not exist.	Check whether the parameter is correct.
400	HSS.1047	Not all whitelist policy processes are confirmed.	Not all whitelist policy processes are confirmed.	On the Application Process Control page, select a whitelist policy and manually mark the trust status of processes.
400	HSS.1048	The vulnerabilities added to the whitelist exceed 500.	The vulnerabilities added to the whitelist exceed 500.	None
400	HSS.1049	The servers added to the whitelist exceed 2,000.	The servers added to the whitelist exceed 2,000.	None
400	HSS.1050	The agent is not updated.	The agent is not updated.	Upgrade the agent.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1053	The number of login blacklist items has reached 50. Delete unnecessary whitelist IP addresses.	The number of login blacklist items has reached 50. Delete unnecessary whitelist IP addresses.	Rectify the fault according to the error message.
400	HSS.1054	Due to security reasons, your account has been restricted from purchasing certain pay-per-use cloud service resources according to the User Agreement. If you have any questions, contact customer service.	Due to security reasons, your account has been restricted from purchasing certain pay-per-use cloud service resources according to the User Agreement. If you have any questions, contact customer service.	Rectify the fault according to the error message.
400	HSS.1055	Insufficient account balance. Top up your account.	Insufficient account balance. Top up your account.	Top up your account.
400	HSS.1056	The number of vulnerabilities to be handled exceeds the upper limit. Please handle them in multiple batches.	The number of vulnerabilities to be handled exceeds the upper limit. Please handle them in multiple batches.	Rectify the fault according to the error message.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1057	Do not select servers that cannot be scanned (servers with abnormal agents or editions lower than professional).	Do not select servers that cannot be scanned (servers with abnormal agents or editions lower than professional).	Rectify the fault according to the error message.
400	HSS.1058	The honeypot port policy does not exist.	The honeypot port policy does not exist.	Check whether the parameter is correct.
400	HSS.1059	No vulnerabilities can be handled. Check whether the agent status, protection edition, and system version support vulnerability handling.	No vulnerabilities can be handled. Check whether the agent status, protection edition, and system version support vulnerability handling.	Rectify the fault according to the error message.
400	HSS.1060	No servers available for vulnerability scan. Check whether the agent status, protection edition, and vulnerability type support manual scan.	No servers available for vulnerability scan. Check whether the agent status, protection edition, and vulnerability type support manual scan.	Rectify the fault according to the error message.
400	HSS.1061	Up to 50 policies can be created for a workload.	Up to 50 policies can be created for a workload.	None

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1062	A workload can be associated with up to five security groups.	A workload can be associated with up to five security groups.	None
400	HSS.1063	The logo size exceeds the upper limit.	The logo size exceeds the upper limit.	None
400	HSS.1064	Incorrect logo type.	Incorrect logo type.	None
400	HSS.1065	Invalid sensitive file filtering path.	Invalid sensitive file filtering path.	Check whether the parameter is correct.
400	HSS.1066	Failed to obtain the multi-cloud cluster deployment template.	Failed to obtain the multi-cloud cluster deployment template.	Contact technical support.
400	HSS.1067	Cluster logs not collected.	Cluster logs not collected.	Check whether the parameter is correct.
400	HSS.1068	Operation too frequent. Wait for 2 minutes and synchronize again.	Operation too frequent. Wait for 2 minutes and synchronize again.	Try again later.
400	HSS.1069	The number of whitelisted trustworthy processes is 0. Start learning again and then enable protection.	The number of whitelisted trustworthy processes is 0. Start learning again and then enable protection.	Rectify the fault according to the error message.
400	HSS.1070	Pay-per-use antivirus scan is not enabled.	Pay-per-use antivirus scan is not enabled.	Enable pay-per-use virus scan.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1071	The number of clusters has reached the upper limit.	The number of clusters has reached the upper limit.	None
400	HSS.1072	Incorrect file type.	Incorrect file type.	None
400	HSS.1073	Failed to query event information.	Failed to query event information.	Check whether the parameter is correct.
400	HSS.1079	Failed to save the CCE integrated protection configuration.	Failed to save the CCE integrated protection configuration.	Check whether the parameter is correct.
400	HSS.1080	The number of connected image repositories exceeds the upper limit.	The number of connected image repositories exceeds the upper limit.	None
401	HSS.0012	Invalid user token.	Invalid user token.	Check whether the user token is correct.
401	HSS.1039	Insufficient permission for modifying vulnerability scan policies.	Insufficient permission for modifying vulnerability scan policies.	Check user permissions.
401	HSS.1051	A scan task is being performed on the selected server.	A scan task is being performed on the selected server.	None
401	HSS.1052	The selected server has been associated with another custom antivirus policy.	The selected server has been associated with another custom antivirus policy.	None

Status Code	Error Codes	Error Message	Description	Solution
401	HSS.2001	Cluster certificate expired.	Cluster certificate expired.	Rectify the fault according to the error message.
403	HSS.1038	The edition does not support this operation.	The edition does not support this operation.	Change to another edition.
429	HSS.0003	The server is busy.	The server is busy.	Try again later.
500	HSS.0004	Database operation failed.	Database operation failed.	Contact technical support.
500	HSS.0005	Cache operation failed.	Cache operation failed.	Contact technical support.
500	HSS.0006	File operation error.	File operation error.	Contact technical support.
500	HSS.0007	Task failed.	Task failed.	Contact technical support.
500	HSS.0008	Internal system error.	Internal system error.	Contact technical support.
500	HSS.0009	Failed to call the third-party API.	Failed to call the third-party API.	Contact technical support.
500	HSS.0015	Failed to access the ECS API.	Failed to access the ECS API.	Contact technical support.
500	HSS.0016	Failed to access the CCE API.	Failed to access the CCE API.	Contact technical support.
500	HSS.0017	Failed to access the CBC API.	Failed to access the CBC API.	Contact technical support.
500	HSS.0018	Failed to access the IAM API.	Failed to access the IAM API.	Contact technical support.
500	HSS.0019	Failed to access the SWR API.	Failed to access the SWR API.	Contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
500	HSS.0020	Failed to access the CBR API.	Failed to access the CBR API.	Contact technical support.
500	HSS.0021	Failed to access the VPC API.	Failed to access the VPC API.	Contact technical support.
500	HSS.0041	An error occurred during query.	An error occurred during query.	Contact technical support.

A.3 Obtaining a Project ID

Scenario

A project ID is required for some URLs when an API is called. Obtain the required project ID using either of the following methods:

- **Obtaining a Project ID by Calling an API**
- **Obtaining a Project ID from the Console**

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the IAM API used to query project information based on the specified criteria.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from the administrator. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project 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"
```



```
    }
}
```

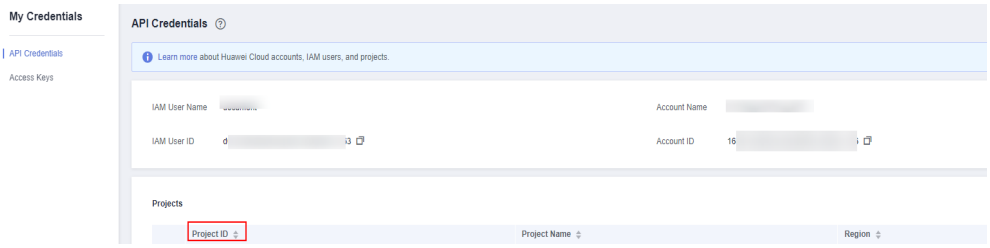
Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following steps:

1. Log in to the management console.
2. Hover the cursor over the username in the upper right corner and select **My Credentials** from the drop-down list.

   On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing project IDs



A.4 Obtaining an Enterprise Project ID

Scenario

Some URLs need to be filled with the enterprise project IDs when APIs are called, so the enterprise project IDs need to be obtained. This section describes how to obtain an enterprise project ID on the management console.

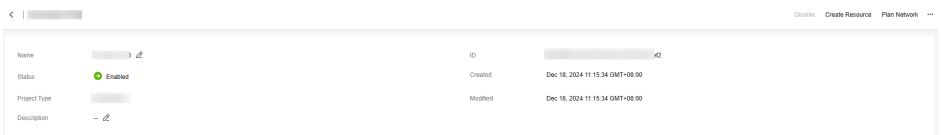
Obtaining an Enterprise Project ID on the Console

1. Log in to the management console.
2. Choose **Enterprise** > **Project Management** in the upper right corner of the page.

   If the screen resolution is low, choose **More** > **Enterprise** > **Project Management**.
3. Locate the target the enterprise project and click its name.

   In the enterprise project details, **ID** is the enterprise project ID.

Figure A-2 Viewing the enterprise project ID



A.5 Obtaining Region ID

Scenario

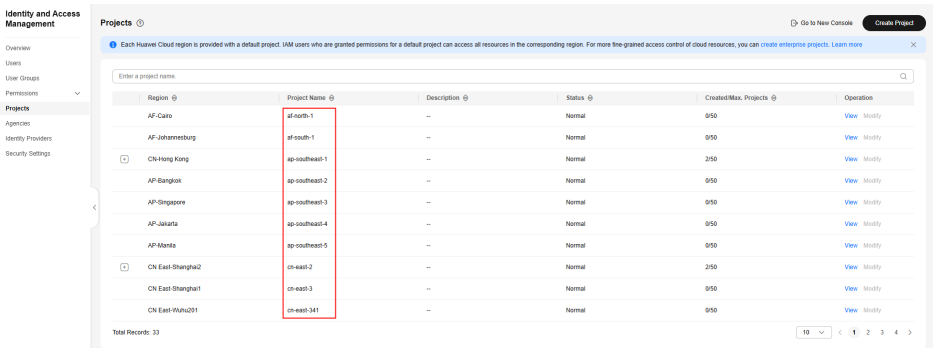
When you call an API, a region ID is required in some request parameters. This section describes how to obtain the region ID on the console.

Obtaining a Region ID from the Console

Step 1 Log in to Huawei Cloudthe cloud platform, go to the IAM console, and choose **Projects**.

Step 2 The value in the **Project Name** column is the ID of the region that the project belongs to.

Figure A-3 Viewing the region ID



----End

