Host Security Service

API Reference

Issue 01

Date 2022-09-16

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Before You Start

1.1 Overview

Host Security Service () 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 prevent threats.

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

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

1.2 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.

See the descriptions of specific APIs.

1.3 Basic Concepts

- Account

  A domain is created after your registration. The domain 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**

  An IAM user is created using an account to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  The account name, username, and password are 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.

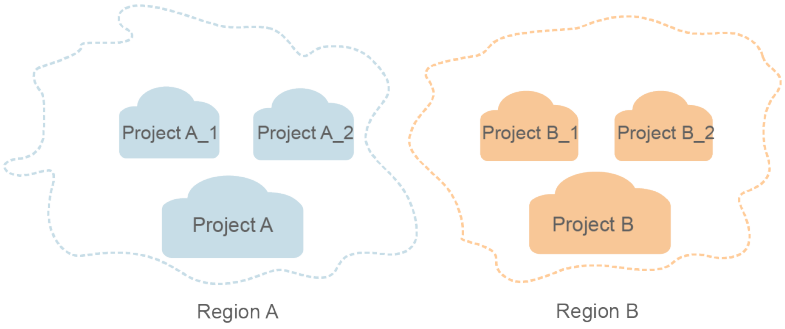
- Availability Zone (AZ)

  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

  Projects group and isolate compute, storage, and network resources across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific 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**.

2 Calling APIs

2.1 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-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. 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.

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.

The token can be obtained by calling the required API. For more information, see Obtaining a User Token. A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. 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 **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

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.

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 in conjunction 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.

NOTICE

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

2.2 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.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/asset/statistics

Table 3-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

Table 3-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **128**
host_id	No	String	host id Minimum: **1** Maximum: **128**
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **1** Maximum: **64**

Request Parameters

Table 3-3 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-4 Response body parameters

Parameter	Type	Description
account_num	Long	Number of accounts Minimum: **0** Maximum: **2147483647**
port_num	Long	Number of open ports Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
process_num	Long	Number of processes Minimum: **0** Maximum: **2147483647**
app_num	Long	Pieces of software Minimum: **0** Maximum: **2147483647**
auto_launch_num	Long	Number of auto-started items Minimum: **0** Maximum: **2147483647**
web_framework_num	Long	Number of web frameworks Minimum: **0** Maximum: **2147483647**
web_site_num	Long	Number of websites Minimum: **0** Maximum: **2147483647**
jar_package_num	Long	Number of JAR packages Minimum: **0** Maximum: **2147483647**
kernel_module_num	Long	Number of kernel modules Minimum: **0** Maximum: **2147483647**
web_service_num	Long	Number of web services Minimum: **0** Maximum: **2147483647**
web_app_num	Long	Number of web applications Minimum: **0** Maximum: **2147483647**
database_num	Long	Number of databases Minimum: **0** Maximum: **2147483647**
core_conf_file_num	Long	Number of key configuration files Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
environment_num	Long	Number of environment variables Minimum: **0** Maximum: **2147483647**

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,
  "core_conf_file_num" : 1,
  "database_num" : 1,
  "environment_num" : 0,
  "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 Querying the Account List

Function

This API is used to query the account list. The number of servers can be queried based on the account name parameter.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-5 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

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: !@.-. Chinese punctuations are not allowed. Minimum: **1** Maximum: **128**
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **128**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **200** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **2000000** Default: **0**

Parameter	Mandatory	Type	Description
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**

Request Parameters

Table 3-7 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-8 Response body parameters

Parameter	Type	Description
total_num	Integer	Container ID Minimum: **0** Maximum: **10000**
data_list	Array of **UserStatisticInfoResponseInfo** objects	Instance name of enterprise edition image Array Length: **0 - 10000**

Table 3-9 UserStatisticInfoResponseInfo

Parameter	Type	Description
user_name	String	Instance URL of enterprise edition image Minimum: **1** Maximum: **128**

Parameter	Type	Description
num	Integer	Asset importance. The options are as follows: • important • common • test Minimum: **0** Maximum: **10000**

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 Querying Open Port Statistics

Function

This API is used to query the list of open ports. The number of servers can be queried by port or protocol type.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-10 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

Table 3-11 Query Parameters

Parameter	Mandatory	Type	Description
port	No	Integer	Port number, which is used for exact match. Minimum: **1** Maximum: **65535**
port_string	No	String	Port string, which is used for fuzzy match. Minimum: **1** Maximum: **256**
type	No	String	Port type Minimum: **1** Maximum: **256**
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **128**
sort_key	No	String	Sort key. Currently, sorting by port number is supported. Minimum: **1** Maximum: **128**
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc Minimum: **1** Maximum: **32**

Parameter	Mandatory	Type	Description
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **200** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **2000000** Default: **0**
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**

Request Parameters

Table 3-12 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-13 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of open ports Minimum: **0** Maximum: **10000**
data_list	Array of **PortStatistic ResponseInfo** objects	Open port statistics list Array Length: **0 - 10000**

Table 3-14 PortStatisticResponseInfo

Parameter	Type	Description
port	Integer	Port number Minimum: **0** Maximum: **65535**
type	String	Type Minimum: **1** Maximum: **256**
num	Integer	Number of ports Minimum: **0** Maximum: **10000**
status	String	Risk type: danger or unknown Minimum: **1** Maximum: **16**

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, quantity, and risk status.

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

Status Codes

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

Error Codes

See **Error Codes**.

3.1.4 Querying the Process List

Function

This API is used to query the process list and query the number of servers based on the process path parameter.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-15 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

Table 3-16 Query Parameters

Parameter	Mandatory	Type	Description
path	No	String	Path Minimum: **1** Maximum: **256**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**

Parameter	Mandatory	Type	Description
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**

Request Parameters

Table 3-17 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-18 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of process statistics Minimum: **0** Maximum: **10000**
data_list	Array of **ProcessStatisticResponseInfo** objects	Process statistics list Array Length: **0 - 10000**

Table 3-19 ProcessStatisticResponseInfo

Parameter	Type	Description
path	String	Process name Minimum: **1** Maximum: **256**

Parameter	Type	Description
num	Integer	Number of processes Minimum: **0** Maximum: **100000**

Example Requests

The first 10 accounts 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**.

3.1.5 Querying the Software List

Function

This API is used to query the software list. The number of servers can be queried by software name.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-20 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-21 Query Parameters

Parameter	Mandatory	Type	Description
app_name	No	String	Software name Minimum: **1** Maximum: **256**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Offset, which is the number of pages multiplied by the number of records displayed on each page. Minimum: **0** Maximum: **10000** Default: **0**
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**

Request Parameters

Table 3-22 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-23 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of process statistics Minimum: **0** Maximum: **10000**
data_list	Array of **AppStatisticResponseInfo** objects	Process statistics list Array Length: **0 - 10000**

Table 3-24 AppStatisticResponseInfo

Parameter	Type	Description
app_name	String	Software name Minimum: **1** Maximum: **128**
num	Integer	Number of processes Minimum: **0** Maximum: **100000**

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**.

3.1.6 Querying Automatic Startup Item Information

Function

This API is used to query the automatic startup information. The startup type and number of servers can be queried based on the automatic startup name.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-26 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Auto-started item name Minimum: **1** Maximum: **256**
type	No	String	Auto-started item type Minimum: **1** Maximum: **256**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**

Request Parameters

Table 3-27 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-28 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of auto-started items Minimum: **0** Maximum: **10000**
data_list	Array of **AutoLaunchStatisticsResponseInfo** objects	List of auto-started item statistics Array Length: **0 - 10000**

Table 3-29 AutoLaunchStatisticsResponseInfo

Parameter	Type	Description
name	String	Auto-started item name Minimum: **1** Maximum: **256**
type	String	Auto-started item type Minimum: **1** Maximum: **11**
num	Integer	Quantity Minimum: **0** Maximum: **10000**

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**.

3.1.7 Querying the Server List of an Account

Function

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

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/asset/users

Table 3-30 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **128**

Table 3-31 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID Minimum: **0** Maximum: **128**
user_name	No	String	Account name Minimum: **0** Maximum: **32**

Parameter	Mandatory	Type	Description
host_name	No	String	Server name Minimum: **0** Maximum: **128**
private_ip	No	String	Server private IP address Minimum: **0** Maximum: **128**
login_permission	No	Boolean	Whether login is allowed.
root_permission	No	Boolean	Whether the user has root permissions
user_group	No	String	User group Minimum: **0** Maximum: **128**
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**. Minimum: **0** Maximum: **128**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **200** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **2000000** Default: **0**
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

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. Minimum: **1** Maximum: **32768**

Response Parameters

Status code: 200

Table 3-33 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **UserResponseInfo** objects	Account information list Array Length: **0 - 10000**

Table 3-34 UserResponseInfo

Parameter	Type	Description
agent_id	String	agent_id Minimum: **1** Maximum: **128**
host_id	String	Server ID Minimum: **1** Maximum: **128**
host_name	String	Server name Minimum: **1** Maximum: **128**

Parameter	Type	Description
host_ip	String	Server IP address Minimum: **1** Maximum: **128**
user_name	String	Username Minimum: **1** Maximum: **128**
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 Minimum: **1** Maximum: **128**
user_home_dir	String	User home directory Minimum: **1** Maximum: **256**
shell	String	User startup shell Minimum: **1** Maximum: **128**
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond. Minimum: **0** Maximum: **4070880000000**
recent_scan_time	Long	Latest scan time Minimum: **0** Maximum: **4070880000000**
container_id	String	Container ID Minimum: **1** Maximum: **128**
container_name	String	Container name Minimum: **1** Maximum: **256**

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,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_home_dir" : "/bin",
    "user_name" : "bin",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6"
  } ]
}
```

Status Codes

Status Code	Description
200	Account information list

Error Codes

See **Error Codes**.

3.1.8 Querying the Open Port List of a Single Server

Function

This API is used to query the open port list of a single server.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/asset/ports

Table 3-35 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-36 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID Minimum: **0** Maximum: **128**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
port	No	Integer	Port number Minimum: **1** Maximum: **65535**
type	No	String	Port type Minimum: **0** Maximum: **128**
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**

Parameter	Mandatory	Type	Description
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**

Request Parameters

Table 3-37 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-38 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **PortResponseInfo** objects	Port information list Array Length: **0 - 10000**

Table 3-39 PortResponseInfo

Parameter	Type	Description
host_id	String	Server ID Minimum: **1** Maximum: **128**

Parameter	Type	Description
laddr	String	Listening IP address Minimum: **1** Maximum: **128**
status	String	Port status. • normal • "danger" • "unknow" Minimum: **1** Maximum: **10**
port	Integer	Port number Minimum: **0** Maximum: **65535**
type	String	Type Minimum: **1** Maximum: **64**
pid	Integer	Process ID Minimum: **1** Maximum: **65535**
path	String	Program file Minimum: **1** Maximum: **256**
agent_id	String	agent id Minimum: **1** Maximum: **64**
container_id	String	Container ID Minimum: **0** Maximum: **128**

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


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


Status Codes

Status Code	Description
200	Port information list

Error Codes

See **Error Codes**.

3.1.9 Querying the Server List of the Software

Function

This API is used to query the server list of the software.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/asset/apps

Table 3-40 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

Table 3-41 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID Minimum: **0** Maximum: **128**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
app_name	No	String	Software name Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
version	No	String	Version number Minimum: **0** Maximum: **128**
install_dir	No	String	Installation directory Minimum: **0** Maximum: **512**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**

Parameter	Mandatory	Type	Description
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**
category	No	String	Type. The default value is host. The options are as follows: • host • container Minimum: **0** Maximum: **64**
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-42 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-43 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **AppResponseInfo** objects	Software list Array Length: **0 - 10000**

Table 3-44 AppResponseInfo

Parameter	Type	Description
agent_id	String	agent_id Minimum: **0** Maximum: **128**
host_id	String	Server ID Minimum: **1** Maximum: **128**
host_name	String	Server name Minimum: **1** Maximum: **256**
host_ip	String	Server IP address Minimum: **1** Maximum: **256**
app_name	String	Software name Minimum: **1** Maximum: **128**
version	String	Version number Minimum: **1** Maximum: **128**
update_time	Long	Update time Minimum: **0** Maximum: **2147483647**
recent_scan_time	Long	Latest scan time Minimum: **0** Maximum: **2147483647**
container_id	String	Container ID Minimum: **1** Maximum: **128**
container_name	String	Container name Minimum: **1** Maximum: **256**

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


Status Codes

Status Code	Description
200	Applications installed on a host

Error Codes

See **Error Codes**.

3.1.10 Querying the Service List of Auto-Started Items

Function

This API is used to query the service list of auto-started items.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-45 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **1** Maximum: **256**

Table 3-46 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID Minimum: **1** Maximum: **128**
host_name	No	String	Server name Minimum: **1** Maximum: **128**
name	No	String	Auto-started item name Minimum: **1** Maximum: **256**
host_ip	No	String	Server IP address Minimum: **1** Maximum: **128**
type	No	String	Auto-started item type Minimum: **1** Maximum: **128**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-47 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-48 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **AutoLauchResponseInfo** objects	Auto-started item list Array Length: **0 - 10000**

Table 3-49 AutoLauchResponseInfo

Parameter	Type	Description
agent_id	String	agent_id Minimum: **0** Maximum: **128**
host_id	String	Server ID Minimum: **1** Maximum: **128**
host_name	String	Server name Minimum: **1** Maximum: **256**
host_ip	String	Server IP address Minimum: **1** Maximum: **256**

Parameter	Type	Description
name	String	Auto-started item name Minimum: **1** Maximum: **256**
type	Integer	Auto-started item type Minimum: **0** Maximum: **11**
path	String	Path Minimum: **1** Maximum: **256**
hash	String	File hash Minimum: **1** Maximum: **128**
run_user	String	User who starts the execution Minimum: **1** Maximum: **128**
recent_scan_time	Long	Latest scan time Minimum: **0** Maximum: **4824430336000**

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**.

3.1.11 Obtaining the Account Change History

Function

This API is used to obtain the account change history.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-50 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-51 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Username Minimum: **1** Maximum: **128**
host_id	No	String	Server ID Minimum: **1** Maximum: **128**
root_permission	No	Boolean	Whether the user has root permissions

Parameter	Mandatory	Type	Description
host_name	No	String	Server name Minimum: **1** Maximum: **128**
private_ip	No	String	Server private IP address Minimum: **1** Maximum: **128**
change_type	No	String	Change type. Its value can be: • ADD • DELETE • MODIFY Minimum: **1** Maximum: **128**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**
enterprise_project_id	No	String	Enterprise project Minimum: **1** Maximum: **256**
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **4070880000000**
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **4070880000000**

Request Parameters

Table 3-52 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-53 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000000**
data_list	Array of **UserChangeHistoryResponseInfo** objects	Account change history Array Length: **0 - 200**

Table 3-54 UserChangeHistoryResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID Minimum: **1** Maximum: **128**
change_type	String	Change type. Its value can be: • ADD • DELETE • MODIFY Minimum: **1** Maximum: **128**
host_id	String	Server ID Minimum: **1** Maximum: **128**

Parameter	Type	Description
host_name	String	Server name Minimum: **1** Maximum: **128**
private_ip	String	Server private IP address Minimum: **1** Maximum: **128**
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 Minimum: **1** Maximum: **128**
user_home_dir	String	User home directory Minimum: **1** Maximum: **128**
shell	String	User startup shell Minimum: **1** Maximum: **128**
user_name	String	Account name Minimum: **1** Maximum: **128**
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond. Minimum: **0** Maximum: **4070880000000**
recent_scan_time	Long	Change time Minimum: **0** Maximum: **4070880000000**

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" : "13xxxxxxxece69",
    "private_ip" : "192.168.0.1",
    "host_name" : "test",
    "user_home_dir" : "/test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_name" : "bin",
    "change_type" : "test"
  } ]
}
```


Status Codes

Status Code	Description
200	account change history

Error Codes

See **Error Codes**.

3.1.12 Obtaining the Historical Change Records of Software Information

Function

This API is used to obtain the historical change records of software information.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-55 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-56 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
app_name	No	String	Software name Minimum: **0** Maximum: **128**
variation_type	No	String	Change type. Its value can be: • add • delete • modify Minimum: **0** Maximum: **10**
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **256**
sort_key	No	String	Sort key Minimum: **1** Maximum: **128**

Parameter	Mandatory	Type	Description
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc Minimum: **1** Maximum: **32**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **10000** Default: **0**
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **9007199254740992**
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **9007199254740992**

Request Parameters

Table 3-57 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-58 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **AppChangeResponseInfo** objects	Account change history Array Length: **0 - 10000**

Table 3-59 AppChangeResponseInfo

Parameter	Type	Description
agent_id	String	agent_id Minimum: **0** Maximum: **128**
variation_type	String	Type of change. • add • delete • modify Minimum: **0** Maximum: **10**
host_id	String	host_id Minimum: **1** Maximum: **128**
app_name	String	Software name Minimum: **1** Maximum: **128**
host_name	String	ECS name Minimum: **1** Maximum: **128**
host_ip	String	Server IP address Minimum: **1** Maximum: **256**
version	String	Version number Minimum: **1** Maximum: **128**

Parameter	Type	Description
update_time	Long	Update time Minimum: **0** Maximum: **4824430336000**
recent_scan_time	Long	Change time Minimum: **0** Maximum: **4824430336000**

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**.

3.1.13 Obtaining the Historical Change Records of Auto-started Items

Function

This API is used to obtain the historical change records of auto-startup items.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-61 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
auto_launch_name	No	String	Auto-started item name Minimum: **0** Maximum: **128**

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 Minimum: **0** Maximum: **100**
variation_type	No	String	Change type. Its value can be: • add • delete • modify Minimum: **0** Maximum: **10**
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **256**
sort_key	No	String	Sort key Minimum: **0** Maximum: **128**
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc Minimum: **0** Maximum: **32**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **200** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **2000000** Default: **0**

Parameter	Mandatory	Type	Description
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **9007199254740992**
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp. Minimum: **0** Maximum: **9007199254740992**

Request Parameters

Table 3-62 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Response Parameters

Status code: 200

Table 3-63 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **10000**
data_list	Array of **AutoLaunchChangeResponseInfo** objects	Account change history Array Length: **0 - 10000**

Table 3-64 AutoLaunchChangeResponseInfo

Parameter	Type	Description
agent_id	String	agent_id Minimum: **0** Maximum: **128**
variation_type	String	Type of change. • add • delete • modify Minimum: **0** Maximum: **10**
type	Integer	Auto-started item type Minimum: **0** Maximum: **11**
host_id	String	host_id Minimum: **1** Maximum: **128**
host_name	String	ECS name Minimum: **1** Maximum: **256**
host_ip	String	Server IP address Minimum: **1** Maximum: **256**
path	String	Path Minimum: **1** Maximum: **256**
hash	String	File hash Minimum: **1** Maximum: **128**
run_user	String	User who starts the execution Minimum: **1** Maximum: **64**
name	String	Auto-started item name Minimum: **1** Maximum: **256**

Parameter	Type	Description
recent_scan_time	Long	Last update time Minimum: **0** Maximum: **4824430336000**

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" : "abnormal_behavior",
    "type" : 0,
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "path" : "/path",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxx",
    "run_user" : 1668246126302,
    "name" : 1668246126302,
    "recent_scan_time" : 1668246126302
  } ]
}
```

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 Servers Protected Against Ransomware

Function

This API is used to query the list of servers protected against ransomware. This API needs to be used together with Cloud Backup and Recovery (CBR). Ensure the site has CBR before using ransomware-related APIs.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/ransomware/server

Table 3-65 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

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**. Default: **0** Minimum: **1** Maximum: **256**
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**. Minimum: **0** Maximum: **2000000** Default: **0**

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. Minimum: **10** Maximum: **200** Default: **10**
host_name	No	String	Server name
os_type	No	String	OS type. Its value can be: • Linux • Windows Minimum: **0** Maximum: **64**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **256**
host_status	No	String	Server status. Its value can be: • If no parameter is transferred, it indicates all items. – ACTIVE – SHUTOFF Minimum: **1** Maximum: **32**
last_days	No	Integer	Number of days in the query time range. To query records in the last seven days, set last_days=7. If this parameter is not specified, the events and existing backups in the last day are queried by default. Minimum: **1** Maximum: **30**

Request Parameters

Table 3-67 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-68 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **2097152**
data_list	Array of **ProtectionServerInfo** objects	Query the servers protected against ransomware. Array Length: **0 - 10241**

Table 3-69 ProtectionServerInfo

Parameter	Type	Description
host_id	String	Server ID Minimum: **0** Maximum: **128**
agent_id	String	Agent ID Minimum: **0** Maximum: **128**

Parameter	Type	Description
host_name	String	Server name Minimum: **0** Maximum: **128**
host_ip	String	EIP Minimum: **0** Maximum: **128**
private_ip	String	Private IP address Minimum: **0** Maximum: **128**
os_type	String	OS type. Its value can be: ● Linux ● Windows Minimum: **0** Maximum: **128**
os_name	String	OS name Minimum: **0** Maximum: **128**
host_status	String	Server status. The options are as follows: ● ACTIVE ● SHUTOFF Minimum: **1** Maximum: **32**
ransom_protection_status	String	Ransomware protection status. The options are as follows: ● closed ● opened ● opening: The function is being enabled. ● closing: The function is being disabled. Minimum: **0** Maximum: **128**
agent_version	String	Agent version Minimum: **1** Maximum: **128**

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: • closed • opened: protection enabled Minimum: **1** Maximum: **32**
group_id	String	Server group ID Minimum: **1** Maximum: **128**
group_name	String	Server group name Minimum: **1** Maximum: **128**
protect_policy_id	String	Policy ID Minimum: **1** Maximum: **128**
protect_policy_name	String	Protection policy name Minimum: **1** Maximum: **128**
backup_error	**backup_error** object	Backup error message
backup_protection_status	String	Whether to enable backup. The options are as follows: • failed_to_turn_on_backup: Backup cannot be enabled. • closed • opened Minimum: **0** Maximum: **128**
count_protect_event	Integer	Number of protection events Minimum: **0** Maximum: **2097152**
count_backuped	Integer	Existing backups Minimum: **0** Maximum: **2097152**
agent_status	String	Agent status Minimum: **1** Maximum: **128**

Parameter	Type	Description
version	String	HSS edition. Its value can be: • hss.version.null • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **32**
host_source	String	Indicates the server type. The options are as follows: • ecs : • outside: on-premises servers • workspace: cloud desktop Minimum: **1** Maximum: **32**
vault_id	String	Vault ID Minimum: **0** Maximum: **128**
vault_name	String	Vault name Minimum: **0** Maximum: **128**
vault_size	Integer	Total capacity, in GB. Minimum: **0** Maximum: **2097152**
vault_used	Integer	Used capacity, in MB. Minimum: **0** Maximum: **2097152**
vault_allocated	Integer	Allocated bound server capacity, in GB. Minimum: **0** Maximum: **2097152**
vault_charging_mode	String	Repository mode, the value can be post_paid (pay-per-use) or pre_paid. Minimum: **0** Maximum: **128**

Parameter	Type	Description
vault_status	String	Vault status can be: • available • lock • frozen • deleting • error Minimum: **0** Maximum: **128**
backup_policy_id	String	Specifies the backup policy ID. If this parameter is empty, the backup policy is not bound. If this parameter is not empty, check whether the backup policy is enabled based on the backup_policy_enabled field. Minimum: **1** Maximum: **128**
backup_policy_name	String	Backup policy name Minimum: **1** Maximum: **128**
backup_policy_enabled	Boolean	Whether the policy is enabled
resources_num	Integer	Bound servers Minimum: **0** Maximum: **2097152**

Table 3-70 backup_error

Parameter	Type	Description
error_code	Integer	Error code. The options are as follows: • 0: No error information. • 1: Backup cannot be enabled because another vault has been bound. • 2: The number of backup vaults exceeds the upper limit. • 3: An exception occurs when the CBR API is called. Minimum: **0** Maximum: **128**

Parameter	Type	Description
error_description	String	Error description Minimum: **1** Maximum: **128**

Example Requests

Query the list of ransomware protection servers. If the limit parameter is not set, 10 records are returned by default.

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

Example Responses

Status code: 200

List of servers protected against ransomware


```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "agent_status" : "online",
    "backup_error" : {
      "error_code" : 1,
      "error_description" : "Backup cannot be enabled because another vault has been bound."
    },
    "ransom_protection_status" : "opened",
    "backup_protection_status" : "failed_to_turn_on_backup",
    "count_backuped" : 0,
    "count_protect_event" : 0,
    "group_id" : "7c659ea3-006f-4687-9f1c-6d975d955f37",
    "group_name" : "333",
    "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
    "host_ip" : "100.85.119.68",
    "host_name" : "Euler",
    "host_status" : "ACTIVE",
    "os_name" : "EulerOS",
    "os_type" : "Linux",
    "private_ip" : "100.85.123.9",
    "protect_policy_id" : "0253edfd-30e7-439d-8f3f-17c54c99706",
    "protect_policy_name" : "tst",
    "protect_status" : "opened"
  } ]
}
```


Status Codes

Status Code	Description
200	List of servers protected against ransomware

Error Codes

See **Error Codes**.

3.2.2 Querying a Protection Policy List

Function

This API is used to query the list of protection policies.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-71 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-72 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**. Default: **0** Minimum: **1** Maximum: **256**
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**. Minimum: **0** Maximum: **2000000** Default: **0**
limit	No	Integer	Number of records displayed on each page. Minimum: **10** Maximum: **200** Default: **10**

Parameter	Mandatory	Type	Description
policy_name	No	String	Policy name Minimum: **0** Maximum: **128**
protect_policy_id	No	String	Policy ID Minimum: **0** Maximum: **128**
operating_system	No	String	OS supported by the policy Minimum: **0** Maximum: **128**

Request Parameters

Table 3-73 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-74 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number Minimum: **0** Maximum: **2097152**

Parameter	Type	Description
data_list	Array of **ProtectionPolicyInfo** objects	Query the list of policies. Array Length: **0 - 10241**

Table 3-75 ProtectionPolicyInfo

Parameter	Type	Description
policy_id	String	Policy ID Minimum: **0** Maximum: **128**
policy_name	String	Policy name Minimum: **0** Maximum: **128**
protection_mode	String	Action. Its value can be: • alarm_and_isolation: Report an alarm and isolate. • alarm_only: Only report alarms. Minimum: **0** Maximum: **128**
bait_protection_status	String	Whether to enable honeypot protection. By default, the protection is enabled. Its value can be: • opened • closed Minimum: **0** Maximum: **128**
deploy_mode	String	Whether to enable honeypot protection. The options are as follows. By default, dynamic honeypot protection is disabled. • opened • closed Minimum: **0** Maximum: **128**
protection_directory	String	Protected directory Minimum: **1** Maximum: **128**

Parameter	Type	Description
protection_type	String	Protected file type Minimum: **0** Maximum: **128**
exclude_directory	String	(Optional) excluded directory Minimum: **1** Maximum: **128**
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 Minimum: **0** Maximum: **128**
runtime_detection_directory	String	Directory to be checked during running. To check all directories, set it to a slash (/). This field is reserved. Minimum: **1** Maximum: **128**
count_associated_server	Integer	Number of associated servers Minimum: **0** Maximum: **2097152**
operating_system	String	OS type Minimum: **0** Maximum: **128**
process_whitelist	Array of **TrustProcessInfo** objects	Process whitelist Array Length: **0 - 20**
default_policy	Integer	Indicates whether the policy is the default policy. The options are as follows: • 0: non-default policy • 1: default policy Minimum: **0** Maximum: **10**

Table 3-76 TrustProcessInfo

Parameter	Type	Description
path	String	Indicates the process path. Minimum: **0** Maximum: **128**
hash	String	Process hash Minimum: **0** Maximum: **128**

Example Requests

Query protection policies. 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

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	Protection policy list

Error Codes

See **Error Codes**.

3.2.3 Modifying a Protection Policy

Function

This API is used to modify a protection policy.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-77 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-78 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-79 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. Minimum: **1** Maximum: **32768**

Parameter	Mandatory	Type	Description
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-80 Request body parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID Minimum: **0** Maximum: **128**
policy_name	Yes	String	Policy name Minimum: **0** Maximum: **128**
protection_mode	Yes	String	Action. Its value can be: • alarm_and_isolation: Report an alarm and isolate. • alarm_only: Only report alarms. Minimum: **0** Maximum: **128**
bait_protection_status	Yes	String	Whether to enable honeypot protection. By default, the protection is enabled. Its value can be: • opened • closed Minimum: **0** Maximum: **128**
protection_directory	Yes	String	Protected directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories. Minimum: **1** Maximum: **128**
protection_type	Yes	String	Protected file type Minimum: **1** Maximum: **128**

Parameter	Mandatory	Type	Description
exclude_directory	No	String	(Optional) Excluded directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories. Minimum: **1** Maximum: **128**
agent_id_list	No	Array of strings	Associated server Minimum: **1** Maximum: **128** Array Length: **0 - 10000**
operating_system	Yes	String	OS. Its value can be: • Windows • Linux Minimum: **0** Maximum: **64**
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 Minimum: **0** Maximum: **128**
process_whitelist	No	Array of **TrustProcessInfo** objects	Process whitelist Array Length: **0 - 20**

Table 3-81 TrustProcessInfo

Parameter	Mandatory	Type	Description
path	No	String	Indicates the process path. Minimum: **0** Maximum: **128**
hash	No	String	Process hash Minimum: **0** Maximum: **128**

Response Parameters

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

Example Responses

None

Status Codes

Status Code	Description
200	success

Error Codes

See **Error Codes**.

3.2.4 Enabling Ransomware Prevention

Function

To enable ransomware protection, ensure CBR is available in the region. Ransomware prevention works with CBR.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-82 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-83 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-84 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-85 Request body parameters

Parameter	Mandatory	Type	Description
operating_system	Yes	String	OS. Its value can be: • Windows • Linux Minimum: **0** Maximum: **64**
ransom_protection_status	Yes	String	Whether ransomware protection is enabled. Its value can be: • closed • opened If this parameter is enabled, either protection_policy_id or create_protection_policy must be specified. Minimum: **0** Maximum: **64**
protection_policy_id	No	String	Protection policy ID. If you select an existing policy, this parameter is mandatory. Minimum: **0** Maximum: **64**
create_protection_policy	No	**ProtectionProxyInfoRequestInfo** object	Create a protection policy. For a new protection policy, leave protection_policy_id blank and specify create_protection_policy.
backup_protection_status	Yes	String	Whether to back up data on the server. Its value can be: • closed • opened If server backup is enabled, backup_cycle is mandatory. Minimum: **0** Maximum: **64**
backup_resources	No	**BackupResources** object	This parameter is mandatory when the backup function is enabled. If this parameter is empty, the vault bound to HSS_projectid is compatible.

Parameter	Mandatory	Type	Description
backup_policy_id	No	String	Backup policy ID Minimum: **0** Maximum: **64**
backup_cycle	No	**UpdateBackupPolicyRequestInfo1** object	Backup policy.
agent_id_list	Yes	Array of strings	IDs of agents where protection is enabled Minimum: **0** Maximum: **64** Array Length: **0 - 24**
host_id_list	Yes	Array of strings	IDs of servers where protection is enabled Minimum: **0** Maximum: **64** Array Length: **0 - 24**

Table 3-86 ProtectionProxyInfoRequestInfo

Parameter	Mandatory	Type	Description
policy_id	No	String	Policy ID. This parameter is optional for a new policy. Minimum: **0** Maximum: **64**
policy_name	No	String	Policy name. This parameter is mandatory when you create a protection policy. Minimum: **0** Maximum: **64**
protection_mode	No	String	Protection action. This parameter is mandatory when you create a protection policy. The options are as follows: • alarm_and_isolation: Report an alarm and isolate. • alarm_only: Only report alarms. Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
bait_protection_status	No	String	Whether to enable honeypot protection. This parameter is mandatory when you create a protection policy. The options are as follows. By default, honeypot protection is enabled. • opened • closed Minimum: **0** Maximum: **64**
protection_directory	No	String	Protected directory. This parameter is mandatory when you create a protection policy. Minimum: **0** Maximum: **64**
protection_type	No	String	Protection type. This parameter is mandatory when you create a protection policy. Minimum: **0** Maximum: **64**
exclude_directory	No	String	(Optional) Excluded directory Minimum: **0** Maximum: **64**
runtime_detection_status	No	String	(Optional) Whether to perform runtime checks. The options are as follows. Currently, it can only be disabled. This field is reserved. • opened • closed Minimum: **0** Maximum: **64**
operating_system	No	String	OS. This parameter is mandatory when you create a protection policy. Its value can be: • Windows • Linux Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
process_whitelist	No	Array of **TrustProcessInfo** objects	Process whitelist Array Length: **0 - 20**

Table 3-87 TrustProcessInfo

Parameter	Mandatory	Type	Description
path	No	String	Indicates the process path. Minimum: **0** Maximum: **128**
hash	No	String	Process hash Minimum: **0** Maximum: **128**

Table 3-88 BackupResources

Parameter	Mandatory	Type	Description
vault_id	No	String	Select the ID of the vault to be bound. The value cannot be empty. Minimum: **0** Maximum: **64**
resource_list	No	Array of **ResourceInfo** objects	List of servers for which the backup function needs to be enabled Array Length: **0 - 20**

Table 3-89 ResourceInfo

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
history_backup_status	No	String	Whether to enable backup status depends on error_message or status of available servers. If error_message is empty, backup is not enabled and the value of this field is closed. If error_message is not empty, the value of this field is opened. Minimum: **0** Maximum: **128**

Table 3-90 UpdateBackupPolicyRequestInfo1

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether the policy is enabled. The default value is true.
policy_id	No	String	Policy ID. This parameter is mandatory if backup protection is enabled. Minimum: **1** Maximum: **256**
operation_definition	No	**OperationDefinitionRequestInfo** object	Scheduling parameter.
trigger	No	**BackupTriggerRequestInfo1** object	Time scheduling rule for the policy.

Table 3-91 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 Minimum: **0** Maximum: **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 Minimum: **-1** Maximum: **99999**
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 Minimum: **0** Maximum: **100**

Parameter	Mandatory	Type	Description
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 Minimum: **-1** Maximum: **99999**
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. Minimum: **0** Maximum: **256**
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. Minimum: **0** Maximum: **100**

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 Minimum: **0** Maximum: **100**

Table 3-92 BackupTriggerRequestInfo1

Parameter	Mandatory	Type	Description
properties	No	**BackupTriggerPropertiesRequestInfo1** object	Time rule for policy execution. This parameter is mandatory if the backup function is enabled with ransomware protection.

Table 3-93 BackupTriggerPropertiesRequestInfo1

Parameter	Mandatory	Type	Description
pattern	No	Array of strings	Scheduling rule. This parameter is mandatory if the backup function is enabled with ransomware protection. 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'. Minimum: **1** Maximum: **256** Array Length: **0 - 24**

Response Parameters

None

Example Requests

Enable ransomware protection for the server. The OS type is Linux, the target server ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f, and the agent ID of the target server is

c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8. Server backup is disabled.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	Ransomware protection enabled.

Error Codes

See **Error Codes**.

3.2.5 Disabling Ransomware Prevention

Function

This API is used to disable ransomware prevention.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-94 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-95 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-96 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-97 Request body parameters

Parameter	Mandatory	Type	Description
host_id_list	Yes	Array of strings	IDs of servers where ransomware protection needs to be disabled Minimum: **0** Maximum: **64** Array Length: **0 - 20**
agent_id_list	Yes	Array of strings	IDs of agents where ransomware prevention needs to be disabled Minimum: **0** Maximum: **64** Array Length: **0 - 20**
close_protection_type	Yes	String	Type of disabled protection. The options are as follows: • close_all: Disable all protection. • close_anti: Ransomware prevention is disabled. • close_backup: Disable the backup function. Minimum: **0** Maximum: **64**

Response Parameters

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**.

3.2.6 Querying the Backup Policy Bound to HSS Protection Vault

Function

This API is used to query the backup policy bound to the HSS protection vault. Ensure that a ransomware protection vault has been purchased in CBR. Such a vault is named in the HSS_projectid format.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/backup/policy

Table 3-98 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-99 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-100 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-101 Response body parameters

Parameter	Type	Description
enabled	Boolean	Whether the policy is enabled
id	String	Policy ID Minimum: **1** Maximum: **128**
name	String	Policy name Minimum: **1** Maximum: **128**
operation_type	String	Backup type. Its value can be: • backup • replication Minimum: **1** Maximum: **128**
operation_definition	**OperationDefinitionInfo** object	Policy attribute. Reserved rule.
trigger	**BackupTriggerInfo** object	Backup policy scheduling rule

Table 3-102 OperationDefinitionInfo

Parameter	Type	Description
day_backups	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 Minimum: **0** Maximum: **100**
max_backups	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 Minimum: **-1** Maximum: **99999**
month_backups	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 Minimum: **0** Maximum: **100**
retention_duration_days	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 Minimum: **-1** Maximum: **99999**

Parameter	Type	Description
timezone	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. Minimum: **0** Maximum: **256**
week_backups	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. Minimum: **0** Maximum: **100**
year_backups	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 Minimum: **0** Maximum: **100**

Table 3-103 BackupTriggerInfo

Parameter	Type	Description
id	String	Scheduler ID Minimum: **0** Maximum: **256**
name	String	Scheduler name Minimum: **0** Maximum: **256**

Parameter	Type	Description
type	String	Scheduler type. Currently, only time can be configured. Minimum: **0** Maximum: **256**
properties	**BackupTriggerPropertiesInfo** object	Scheduler attribute

Table 3-104 BackupTriggerPropertiesInfo

Parameter	Type	Description
pattern	Array of strings	Scheduling policy. The value contains a maximum of 10,240 characters and complies with iCalendar RFC 2445. However, only FREQ, BYDAY, BYHOUR, and BYMINUTE are supported. FREQ can be set to only WEEKLY or DAILY. BYDAY can be set to the seven days in a week (MO, TU, WE, TH, FR, SA and SU). BYHOUR can be set to 0 to 23 hours. BYMINUTE can be set to 0 to 59 minutes. The interval between time points cannot be less than one hour. Multiple backup time points can be set in a backup policy, and up to 24 time points can be set for a day. Minimum: **0** Maximum: **256** Array Length: **0 - 24**
start_time	String	Scheduler start time. Example: 2020-01-08 09:59:49 Minimum: **0** Maximum: **256**

Example Requests

This API is used to query the backup policy associated with the vault.

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

Example Responses

Status code: 200

Backup policy information

```
{
  "enabled" : true,
```

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

Status Codes

Status Code	Description
200	Backup policy information

Error Codes

See **Error Codes**.

3.2.7 Modifying the Backup Policy Bound to Vault

Function

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

Calling Method

For details, see **Calling APIs**.

URI

PUT /v5/{project_id}/backup/policy

Table 3-105 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-107 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-108 Request body parameters

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether the policy is enabled. The default value is true.
policy_id	Yes	String	Policy ID Minimum: **1** Maximum: **256**
operation_definition	No	**OperationDefinitionRequestInfo** object	Scheduling parameter.
trigger	No	**BackupTriggerRequestInfo** object	Time scheduling rule for the policy

Table 3-109 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 Minimum: **0** Maximum: **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 Minimum: **-1** Maximum: **99999**
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 Minimum: **0** Maximum: **100**

Parameter	Mandatory	Type	Description
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 Minimum: **-1** Maximum: **99999**
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. Minimum: **0** Maximum: **256**
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. Minimum: **0** Maximum: **100**

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 Minimum: **0** Maximum: **100**

Table 3-110 BackupTriggerRequestInfo

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

Table 3-111 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'. Minimum: **1** Maximum: **256** Array Length: **0 - 24**

Response Parameters

Status code: 200

Table 3-112 Response body parameters

Parameter	Type	Description
error_code	Integer	Error code. If the operation is successful, 0 is returned. Minimum: **0** Maximum: **100**

Parameter	Type	Description
error_description	String	Error description. If the operation is successful, success is returned. Minimum: **1** Maximum: **256**

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

Status code: 200

Modify a backup policy.

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

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-113 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**

Table 3-114 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID Minimum: **0** Maximum: **64**
host_name	No	String	Server name Minimum: **0** Maximum: **256**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **256**
user_name	No	String	Name of the account using a weak password Minimum: **0** Maximum: **32**

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID. If this parameter is not specified, all hosts of a user are queried. Minimum: **0** Maximum: **64**
limit	No	Integer	Number of records on each page Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-115 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token, which 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 the user token. Minimum: **32** Maximum: **2097152**

Response Parameters

Status code: 200

Table 3-116 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of weak passwords Minimum: **0** Maximum: **2147483647**
data_list	Array of **WeakPwdListInfoResponseInfo** objects	Weak password list Array Length: **0 - 2147483647**

Table 3-117 WeakPwdListInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID Minimum: **0** Maximum: **64**
host_name	String	Server name Minimum: **0** Maximum: **256**
host_ip	String	Server IP address Minimum: **0** Maximum: **256**
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	List of accounts with weak passwords Array Length: **0 - 2147483647**

Table 3-118 WeakPwdAccountInfoResponseInfo

Parameter	Type	Description
user_name	String	Name of accounts with weak passwords Minimum: **0** Maximum: **32**

Parameter	Type	Description
service_type	String	Account type. Its value can be: • system • mysql • redis Minimum: **0** Maximum: **32**
duration	Integer	Validity period of a weak password, in days. Minimum: **0** Maximum: **2147483647**

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-119 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-120 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID Minimum: **0** Maximum: **256**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
host_id	No	String	Server ID. If this parameter is not specified, all hosts of a user are queried. Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The default value is **10**. Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-121 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 the user token. Minimum: **1** Maximum: **32768**

Response Parameters

Status code: 200

Table 3-122 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of password complexity policies Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
data_list	Array of **PwdPolicyInfoResponseInfo** objects	List of password complexity policy detection Array Length: **0 - 2147483647**

Table 3-123 PwdPolicyInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID (displayed when the cursor is placed on a server name) Minimum: **0** Maximum: **64**
host_name	String	Server name Minimum: **0** Maximum: **256**
host_ip	String	Server IP address Minimum: **0** Maximum: **256**
min_length	Boolean	Minimum password length
uppercase_letter	Boolean	Uppercase letter
lowercase_letter	Boolean	Lowercase letter
number	Boolean	Digital
special_character	Boolean	Special characters
suggestion	String	Modification suggestion Minimum: **0** Maximum: **65534**

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-124 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-125 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID Minimum: **0** Maximum: **256**
check_name	No	String	Baseline name Minimum: **0** Maximum: **256**
group_id	No	String	Indicates the policy group ID. Minimum: **0** Maximum: **128**
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High Minimum: **1** Maximum: **32**
standard	No	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **1** Maximum: **32**
host_id	No	String	Server ID Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The default value is **10**. Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-126 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 the user token. Minimum: **1** Maximum: **32768**

Response Parameters

Status code: 200

Table 3-127 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of records Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
data_list	Array of **SecurityCheckInfoResponseInfo** objects	Server configuration check result list Array Length: **0 - 2147483647**

Table 3-128 SecurityCheckInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High Minimum: **1** Maximum: **32**
check_name	String	Baseline name Minimum: **0** Maximum: **256**
check_type	String	Baseline type Minimum: **0** Maximum: **256**
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **1** Maximum: **16**
check_rule_num	Integer	Number of check items Minimum: **0** Maximum: **2097152**
failed_rule_num	Integer	Number of risk items Minimum: **0** Maximum: **2097152**
host_num	Integer	Number of affected servers Minimum: **0** Maximum: **2097152**

Parameter	Type	Description
scan_time	Long	Last scan time Minimum: **0** Maximum: **2097152**
check_type_desc	String	Baseline description Minimum: **0** Maximum: **65534**

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-129 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**
check_name	Yes	String	Baseline name Minimum: **0** Maximum: **256**

Table 3-130 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**. Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **0** Maximum: **32**
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried. Minimum: **0** Maximum: **64**
limit	No	Integer	Number of records on each page. Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-131 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. Minimum: **32** Maximum: **2097152**

Response Parameters

Status code: 200

Table 3-132 Response body parameters

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High Minimum: **0** Maximum: **65534**
check_type	String	Baseline type Minimum: **0** Maximum: **256**
check_type_desc	String	Baseline description Minimum: **0** Maximum: **65534**
check_rule_num	Integer	Total number of check items Minimum: **0** Maximum: **2147483647**
failed_rule_num	Integer	Number of failed check items Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
passed_rule_num	Integer	Number of passed check items Minimum: **0** Maximum: **2147483647**
ignored_rule_num	Integer	Number of ignored check items Minimum: **0** Maximum: **2147483647**
host_num	Long	Number of affected servers Minimum: **0** Maximum: **2147483647**

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-133 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**
check_name	Yes	String	Baseline name Minimum: **0** Maximum: **256**

Table 3-134 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**. Minimum: **0** Maximum: **64**
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **0** Maximum: **32**

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. Default: **unhandled** Minimum: **0** Maximum: **64**
check_rule_name	No	String	Check item name. Fuzzy match is supported. Minimum: **0** Maximum: **2048**
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High • Critical Minimum: **0** Maximum: **255**
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried. Minimum: **0** Maximum: **64**
limit	No	Integer	Number of items per page Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-135 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. Minimum: **32** Maximum: **2097152**

Response Parameters

Status code: 200

Table 3-136 Response body parameters

Parameter	Type	Description
total_num	Long	Total risks Minimum: **0** Maximum: **9223372036854775807**
data_list	Array of **CheckRuleRiskInfoResponseInfo** objects	Data list Array Length: **0 - 2147483647**

Table 3-137 CheckRuleRiskInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High Minimum: **0** Maximum: **255**

Parameter	Type	Description
check_name	String	Baseline name Minimum: **0** Maximum: **256**
check_type	String	Baseline name Minimum: **0** Maximum: **256**
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **0** Maximum: **16**
check_rule_name	String	Check item Minimum: **0** Maximum: **2048**
check_rule_id	String	Check item ID Minimum: **0** Maximum: **64**
host_num	Integer	Number of affected servers Minimum: **0** Maximum: **2147483647**
scan_result	String	Detection result. Its value can be: • pass • failed Minimum: **0** Maximum: **64**
status	String	Status. Its value can be: • safe • ignored • unhandled • fixing • fix-failed • verifying Minimum: **0** Maximum: **64**

Parameter	Type	Description
enable_fix	Integer	Indicates whether one-click repair is supported. 1: yes; 0: no. Minimum: **0** Maximum: **2147483647**
enable_click	Boolean	Indicates whether the repair, ignore, and verify buttons of the check item can be clicked. true: The button can be clicked. false: The button cannot be clicked.
rule_params	Array of **CheckRuleFixParamInfo** objects	Range of parameters applicable to the check items that can be fixed by parameter transfer Array Length: **0 - 2147483647**

Table 3-138 CheckRuleFixParamInfo

Parameter	Type	Description
rule_param_id	Integer	Check item parameter ID Minimum: **0** Maximum: **10**
rule_desc	String	Check item parameter description Minimum: **0** Maximum: **256**
default_value	Integer	Default values of check item parameters Minimum: **0** Maximum: **2147483647**
range_min	Integer	Minimum value of check item parameters Minimum: **0** Maximum: **2147483647**
range_max	Integer	Minimum value of check item parameters Minimum: **0** Maximum: **2147483647**

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,
    "standard" : "hw_standard",
    "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-139 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**
check_name	Yes	String	Baseline name Minimum: **0** Maximum: **256**

Table 3-140 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**. Minimum: **0** Maximum: **64**
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **0** Maximum: **32**
host_name	No	String	Server name Minimum: **0** Maximum: **256**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **256**

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items per page Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-141 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. Minimum: **32** Maximum: **2097152**

Response Parameters

Status code: 200

Table 3-142 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of data volume Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
data_list	Array of **SecurityCheckHostInfoResponseInfo** objects	Data list Array Length: **0 - 2147483647**

Table 3-143 SecurityCheckHostInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID Minimum: **0** Maximum: **64**
host_name	String	Server name Minimum: **0** Maximum: **256**
host_public_ip	String	Server public IP address Minimum: **0** Maximum: **128**
host_private_ip	String	Server private IP address Minimum: **0** Maximum: **256**
scan_time	Long	Scan time Minimum: **0** Maximum: **9223372036854775807**
failed_num	Integer	Number of risk items Minimum: **0** Maximum: **2147483647**
passed_num	Integer	Number of passed items Minimum: **0** Maximum: **2147483647**

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-144 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**

Table 3-145 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID Minimum: **0** Maximum: **64**
check_name	Yes	String	Baseline name Minimum: **0** Maximum: **255**
check_type	Yes	String	Baseline type Minimum: **0** Maximum: **255**
check_rule_id	Yes	String	Check item ID Minimum: **0** Maximum: **255**
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Huawei standard • qt_standard: Qingteng standard Minimum: **0** Maximum: **32**
host_id	No	String	Host ID Minimum: **0** Maximum: **64**

Request Parameters

Table 3-146 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token, which 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 the user token. Minimum: **32** Maximum: **2097152**

Response Parameters

Status code: 200

Table 3-147 Response body parameters

Parameter	Type	Description
description	String	Description Minimum: **0** Maximum: **2048**
reference	String	Scenario Minimum: **0** Maximum: **255**
audit	String	Audit description Minimum: **0** Maximum: **65534**
remediation	String	Modification suggestion Minimum: **0** Maximum: **65534**
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	Test cases Array Length: **0 - 2147483647**

Table 3-148 CheckRuleCheckCaseResponseInfo

Parameter	Type	Description
check_description	String	Test case description Minimum: **0** Maximum: **65534**
current_value	String	Current result Minimum: **0** Maximum: **65534**
suggest_value	String	Expected result Minimum: **0** Maximum: **65534**

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: \n#grep '^ClientAliveInterval' /etc/ssh/sshd_config\nClientAliveInterval 300(default is 0) \n#grep '^ClientAliveCountMax' /etc/ssh/sshd_config\nClientAliveCountMax 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: \nClientAliveInterval 300 \nClientAliveCountMax 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 Information

Function

This API is used to query quota information.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/billing/quotas

Table 3-149 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **128**

Table 3-150 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**. Default: **0** Minimum: **1** Maximum: **256**

Parameter	Mandatory	Type	Description
version	No	String	HSS edition. Its value can be: • hss.version.null • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **64**
charging_mode	No	String	Billing mode. Its value can be: • packet_cycle: yearly/monthly • on_demand: pay-per-use Minimum: **1** Maximum: **32**

Request Parameters

Table 3-151 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. Minimum: **32** Maximum: **4096**
region	No	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-152 Response body parameters

Parameter	Type	Description
data_list	Array of **ResourceQuotasInfo** objects	Quota statistics list Array Length: **0 - 200**

Table 3-153 ResourceQuotasInfo

Parameter	Type	Description
version	String	HSS edition. Its value can be: • hss.version.null • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **64**
total_num	Integer	Total quotas Minimum: **0** Maximum: **2000000**
used_num	Integer	Used quotas Minimum: **0** Maximum: **2000000**
available_num	Integer	Total quotas Minimum: **0** Maximum: **2000000**
available_resources_list	Array of **AvailableResourceIdsInfo** objects	Available resource list Array Length: **0 - 200**

Table 3-154 AvailableResourceIdsInfo

Parameter	Type	Description
resource_id	String	Resource ID Minimum: **1** Maximum: **256**
current_time	String	Current time Minimum: **1** Maximum: **64**
shared_quota	String	Whether quotas are shared. Its value can be: • shared • unshared Minimum: **1** Maximum: **64**

Example Requests

This API is used to query quotas of the basic edition in all enterprise projects.

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

Example Responses

Status code: 200

Quota statistics list

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

Status Codes

Status Code	Description
200	Quota statistics list

Error Codes

See **Error Codes**.

3.4.2 Querying Quota Details

Function

This API is used to query quota details.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-155 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-156 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**. Default: **0** Minimum: **1** Maximum: **256**

Parameter	Mandatory	Type	Description
version	No	String	HSS edition. Its value can be: • hss.version.null • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **64**
category	No	String	Type. Its value can be: • host_resource • container_resource Minimum: **1** Maximum: **64**
quota_status	No	String	Quota status. It can be: • QUOTA_STATUS_NORMAL – QUOTA_STATUS_EXPIRED – QUOTA_STATUS_FREEZE Minimum: **1** Maximum: **64**
used_status	No	String	Usage status. It can be: • USED_STATUS_IDLE • USED_STATUS_USED Minimum: **1** Maximum: **64**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
resource_id	No	String	Resource ID Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
charging_mode	No	String	Billing mode. Its value can be: • packet_cycle: yearly/monthly • on_demand: pay-per-use Minimum: **1** Maximum: **32**
limit	No	Integer	Number of items per page Minimum: **10** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-157 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. Minimum: **32** Maximum: **4096**
region	No	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-158 Response body parameters

Parameter	Type	Description
packet_cycle_num	Integer	Yearly/Monthly quotas Minimum: **0** Maximum: **10000000**
on_demand_num	Integer	Pay-per-Use quotas Minimum: **0** Maximum: **10000000**
used_num	Integer	Used quotas Minimum: **0** Maximum: **10000000**
idle_num	Integer	Idle quotas Minimum: **0** Maximum: **10000000**
normal_num	Integer	Normal quotas Minimum: **0** Maximum: **10000000**
expired_num	Integer	Expired quotas Minimum: **0** Maximum: **10000000**
freeze_num	Integer	Frozen quotas Minimum: **0** Maximum: **10000000**
quota_statistics_list	Array of **QuotaStatisticsResponseInfo** objects	Quota statistics list Array Length: **0 - 200**
total_num	Integer	Total number Minimum: **0** Maximum: **10000000**
data_list	Array of **QuotaResourcesResponseInfo** objects	Quota list Array Length: **0 - 200**

Table 3-159 QuotaStatisticsResponseInfo

Parameter	Type	Description
version	String	Resource flavor. Its value can be: • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container: container edition Minimum: **1** Maximum: **64**
total_num	Integer	Total number Minimum: **0** Maximum: **10000000**

Table 3-160 QuotaResourcesResponseInfo

Parameter	Type	Description
resource_id	String	Resource ID of an HSS quota Minimum: **0** Maximum: **256**
version	String	Resource flavor. Its value can be: • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container: container edition Minimum: **1** Maximum: **64**
quota_status	String	Quota status. It can be: • normal • expired • freeze Minimum: **1** Maximum: **64**

Parameter	Type	Description
used_status	String	Usage status. Its value can be: • idle • used Minimum: **1** Maximum: **64**
host_id	String	Server ID Minimum: **1** Maximum: **64**
host_name	String	Server name Minimum: **1** Maximum: **128**
charging_mode	String	Billing mode. Its value can be: • packet_cycle: yearly/monthly • on_demand: pay-per-use Minimum: **1** Maximum: **64**
tags	Array of **TagInfo** objects	Tag Array Length: **0 - 2097152**
expire_time	Long	Expiration time. The value -1 indicates that the resource will not expire. Minimum: **0** Maximum: **2147483647**
shared_quota	String	Whether quotas are shared. Its value can be: • shared • unshared Minimum: **1** Maximum: **64**
enterprise_project_id	String	Enterprise project ID Minimum: **0** Maximum: **256**
enterprise_project_name	String	Enterprise project name Minimum: **0** Maximum: **256**

Table 3-161 TagInfo

Parameter	Type	Description
key	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank. Minimum: **1** Maximum: **128**
value	String	Value. Each tag value can contain a maximum of 255 Unicode characters. Minimum: **1** Maximum: **255**

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.basic&enterprise_project_id=all_granted_eps
```

Example Responses

Status code: 200

Quota details

```
{
  "data_list" : [ {
    "charging_mode" : "packet_cycle",
    "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,
  "packet_cycle_num" : 60,
  "quota_statistics_list" : [ {
    "total_num" : 8,
    "version" : "hss.version.basic"
  } ],
  "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 Handling Alarm Events

Function

This API is used to handle alarm events.

Calling Method

For details, see **Calling APIs**.

URI

POST /v5/{project_id}/event/operate

Table 3-162 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**

Table 3-163 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**. Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
container_name	No	String	Container instance name
container_id	No	String	Container ID

Request Parameters

Table 3-164 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-165 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

Parameter	Mandatory	Type	Description
operate_event_list	Yes	Array of **OperateEventRequestInfo** objects	Operated event list Array Length: **0 - 100**
event_white_rule_list	No	Array of **EventWhiteRuleListRequestInfo** objects	User-defined alarm whitelist Array Length: **0 - 100**

Table 3-166 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 • ransomware_0001: ransomware attack • ransomware_0002: ransomware attack • ransomware_0003: ransomware attack • fileless_0001: process injection • fileless_0002: dynamic library injection • fileless_0003: key configuration change

Parameter	Mandatory	Type	Description
			• fileless_0004: environment variable change • fileless_0005: memory file process • fileless_0006: VDSO hijacking • crontab_1001: suspicious crontab task • vul_exploit_0001: Redis vulnerability exploit • vul_exploit_0002: Hadoop vulnerability exploit • vul_exploit_0003: MySQL vulnerability exploit • rootkit_0001: suspicious rootkit file • rootkit_0002: suspicious kernel module • RASP_0004: web shell upload • RASP_0018: fileless web shell • blockexec_001: known ransomware attack • hips_0001: Windows Defender disabled • hips_0002: suspicious hacker tool • hips_0003: suspicious ransomware encryption behavior • hips_0004: hidden account creation • hips_0005: user password and credential reading • hips_0006: suspicious SAM file export • hips_0007: suspicious shadow copy deletion • hips_0008: backup file deletion • hips_0009: registry of suspicious ransomware

Parameter	Mandatory	Type	Description
			• hips_0010: suspicious abnormal process • hips_0011: suspicious scan • hips_0012: suspicious ransomware script running • hips_0013: suspicious mining command execution • hips_0014: suspicious windows security center disabling • hips_0015: suspicious behavior of disabling the firewall service • hips_0016: suspicious system automatic recovery disabling • hips_0017: executable file execution in Office • hips_0018: abnormal file creation with macros in Office • hips_0019: suspicious registry operation • hips_0020: Confluence remote code execution • hips_0021: MSDT remote code execution • portscan_0001: common port scan • portscan_0002: secret port scan • k8s_1001: Kubernetes event deletion • k8s_1002: privileged pod creations • k8s_1003: interactive shell used in pod • k8s_1004: pod created with sensitive directory • k8s_1005: pod created with server network • k8s_1006: pod created with host PID space

Parameter	Mandatory	Type	Description
			• k8s_1007: authentication failure when common pods access API server • k8s_1008: API server access from common pod using cURL • k8s_1009: exec in system management space • k8s_1010: pod created in management space • k8s_1011: static pod creation • k8s_1012: DaemonSet creation • k8s_1013: scheduled cluster task creation • k8s_1014: operation on secrets • k8s_1015: allowed operation enumeration • k8s_1016: high privilege RoleBinding or ClusterRoleBinding • k8s_1017: ServiceAccount creation • k8s_1018: Cronjob creation • k8s_1019: interactive shell used for exec in pods • k8s_1020: unauthorized access to API server • k8s_1021: access to API server with curl • k8s_1022: Ingress vulnerability • k8s_1023: man-in-the-middle (MITM) attack • k8s_1024: worm, mining, or Trojan • k8s_1025: K8s event deletion • k8s_1026: SelfSubjectRules-Review • imgblock_0001: image blocking based on whitelist

Parameter	Mandatory	Type	Description
			• imgblock_0002: image blocking based on blacklist • imgblock_0003: image tag blocking based on whitelist • imgblock_0004: image tag blocking based on blacklist • imgblock_0005: container creation blocked based on whitelist • imgblock_0006: container creation blocked based on blacklist • imgblock_0007: container mount proc blocking • imgblock_0008: container seccomp unconfined blocking • imgblock_0009: container privilege blocking • imgblock_0010: container capabilities blocking
event_id	Yes	String	Event ID

Parameter	Mandatory	Type	Description
event_type	Yes	Integer	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 : Rootkit • 1011: ransomware • 1012: hacker tool • 1015 : web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3029: system protection disabled • 3030: backup deletion • 3031: suspicious registry operations

Parameter	Mandatory	Type	Description
			• 3036: container image blocking • 4002: brute-force attack • 4004: abnormal login • 4006: invalid accounts • 4014: account added • 4020: password theft • 6002: port scan • 6003: server scan • 13001: Kubernetes event deletion • 13002: abnormal pod behavior • 13003: enumerating user information • 13004: cluster role binding
occur_time	Yes	Integer	Occurrence time, accurate to milliseconds.
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. Array Length: **0 - 100**

Table 3-167 EventDetailRequestInfo

Parameter	Mandatory	Type	Description
agent_id	No	String	Agent ID

Parameter	Mandatory	Type	Description
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
container_id	No	String	Container ID Minimum: **64** Maximum: **64**
container_name	No	String	Container name Minimum: **1** Maximum: **128**

Table 3-168 EventWhiteRuleListRequestInfo

Parameter	Mandatory	Type	Description
event_type	Yes	Integer	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 : Rootkit • 1011: ransomware • 1012: hacker tool • 1015 : web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3029: system protection disabled • 3030: backup deletion • 3031: suspicious registry operations

Parameter	Mandatory	Type	Description
			• 3036: container image blocking • 4002: brute-force attack • 4004: abnormal login • 4006: invalid accounts • 4014: account added • 4020: password theft • 6002: port scan • 6003: server scan • 13001: Kubernetes event deletion • 13002: abnormal pod behavior • 13003: enumerating user information • 13004: cluster role binding
field_key	Yes	String	Whitelist fields. The options are as follows: • "file/process hash" # process/file hash • "file_path" • "process_path" • "login_ip": login IP address • "reg_key": registry key • "process_cmdline": process command line • "username" Minimum: **1** Maximum: **20**
field_value	Yes	String	Whitelist field value Minimum: **1** Maximum: **128**
judge_type	Yes	String	Wildcard. The options are as follows: • "equal" • "contain" Minimum: **1** Maximum: **10**

Response Parameters

None

Example Requests

Manually handle the intrusion alarms whose alarm event type is Rootkit and alarm event ID is 2a71e1e2-60f4-4d56-b314-2038fdc39de6.

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

{
  "operate_type" : "mark_as_handled",
  "handler" : "test",
  "operate_event_list" : [ {
    "event_class_id" : "rootkit_0001",
    "event_id" : "2a71e1e2-60f4-4d56-b314-2038fdc39de6",
    "occur_time" : 1672046760353,
    "event_type" : 1010,
    "operate_detail_list" : [ {
      "agent_id" : "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
      "file_hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "file_path" : "/usr/test",
      "process_pid" : 3123,
      "file_attr" : 33261,
      "keyword" : "file_path=/usr/test",
      "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "login_ip" : "127.0.0.1",
      "private_ip" : "127.0.0.2",
      "login_user_name" : "root",
      "container_id" : "containerid",
      "container_name" : "/test"
    } ]
  } ]
}
```

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**.

3.5.2 Querying the Detected Intrusion List

Function

This API is used to query the detected intrusion list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/event/events

Table 3-169 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**

Table 3-170 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID of a user Minimum: **0** Maximum: **64**
last_days	No	Integer	Number of days to be queried. This parameter is mutually exclusive with **begin_time** and **end_time**. Minimum: **1** Maximum: **30**
host_name	No	String	Server name Minimum: **1** Maximum: **64**
host_id	No	String	Server ID Minimum: **0** Maximum: **64**
private_ip	No	String	Server IP address Minimum: **1** Maximum: **256**

Parameter	Mandatory	Type	Description
public_ip	No	String	Server public IP address Minimum: **1** Maximum: **256**
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. The default value is **0**. Minimum: **0** Maximum: **2000000** Default: **0**
limit	No	Integer	Number of records displayed on each page Minimum: **10** Maximum: **1000** Default: **10**

Parameter	Mandatory	Type	Description
event_types	No	Array	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 :Rootkit • 1011: ransomware • 1012: hacker tool • 1015 : web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3026: crontab privilege escalation • 3027: suspicious crontab task • 3029: system protection disabled • 3030: backup deletion

Parameter	Mandatory	Type	Description
			• 3031: suspicious registry operations • 3036: container image blocking • 4002: brute-force attack • 4004: abnormal login • 4006: invalid accounts • 4014: account added • 4020: password theft • 6002: port scan • 6003: server scan • 13001: Kubernetes event deletion • 13002: abnormal pod behavior • 13003: enumerating user information • 13004: cluster role binding Minimum: **1000** Maximum: **30000** Array Length: **1 - 500**
handle_status	No	String	Status. Its value can be: • unhandled • handled Minimum: **1** Maximum: **32**
severity	No	String	Threat level. Its value can be: • Security • Low • Medium • High • Critical Minimum: **1** Maximum: **32**

Parameter	Mandatory	Type	Description
category	Yes	String	Event category. Its value can be: • host: host security event • container: container security event Minimum: **0** Maximum: **32**
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. Minimum: **13** Maximum: **13**
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. Minimum: **13** Maximum: **13**

Parameter	Mandatory	Type	Description
event_class_ids	No	Array	Event ID. Its value can be: • container_1001: container namespace • container_1002: container port enabled • container_1003: container security options • 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: key file path change • fileprotect_0004: file/directory change • av_1002: virus • av_1003: worm • av_1004: Trojan • av_1005: botnet • av_1006: backdoor • av_1007: spyware • av_1008: malicious adware • av_1009: phishing

Parameter	Mandatory	Type	Description
			• av_1010 : Rootkit • av_1011: ransomware • av_1012: hacker tool • av_1013: grayware • av_1015 : web shell • av_1016: mining software • login_0001: brute-force cracking • login_0002: successful cracking • login_1001: successful login • login_1002: remote login • login_1003: weak password • malware_0001: shell change report • malware_0002: reverse shell report • malware_1001: malicious program • procdet_0001: abnormal process behavior detection • procdet_0002: process privilege escalation • crontab_0001: crontab script privilege escalation • crontab_0002: malicious path privilege escalation • procreport_0001: risky commands • user_1001: account change • user_1002: risky account • vmescape_0001: VM sensitive command execution • vmescape_0002: access from virtualization process to sensitive file • vmescape_0003: abnormal VM port access • webshell_0001: web shell • network_1001: malicious mining

Parameter	Mandatory	Type	Description
			• network_1002: DDoS attacks • network_1003: malicious scan • network_1004: attack in sensitive areas • ransomware_0001: ransomware attack • ransomware_0002: ransomware attack • ransomware_0003: ransomware attack • fileless_0001: process injection • fileless_0002: dynamic library injection • fileless_0003: key configuration change • fileless_0004: environment variable change • fileless_0005: memory file process • fileless_0006: VDSO hijacking • crontab_1001: suspicious crontab task • vul_exploit_0001: Redis vulnerability exploit • vul_exploit_0002: Hadoop vulnerability exploit • vul_exploit_0003: MySQL vulnerability exploit • rootkit_0001: suspicious rootkit file • rootkit_0002: suspicious kernel module • RASP_0004: web shell upload • RASP_0018: fileless web shell • blockexec_001: known ransomware attack • hips_0001: Windows Defender disabled

Parameter	Mandatory	Type	Description
			• hips_0002: suspicious hacker tool • hips_0003: suspicious ransomware encryption behavior • hips_0004: hidden account creation • hips_0005: user password and credential reading • hips_0006: suspicious SAM file export • hips_0007: suspicious shadow copy deletion • hips_0008: backup file deletion • hips_0009: registry of suspicious ransomware • hips_0010: suspicious abnormal process • hips_0011: suspicious scan • hips_0012: suspicious ransomware script running • hips_0013: suspicious mining command execution • hips_0014: suspicious windows security center disabling • hips_0015: suspicious behavior of disabling the firewall service • hips_0016: suspicious system automatic recovery disabling • hips_0017: executable file execution in Office • hips_0018: abnormal file creation with macros in Office • hips_0019: suspicious registry operation • hips_0020: Confluence remote code execution • hips_0021: MSDT remote code execution

Parameter	Mandatory	Type	Description
			• portscan_0001: common port scan • portscan_0002: secret port scan • k8s_1001: Kubernetes event deletion • k8s_1002: privileged pod creations • k8s_1003: interactive shell used in pod • k8s_1004: pod created with sensitive directory • k8s_1005: pod created with server network • k8s_1006: pod created with host PID space • k8s_1007: authentication failure when common pods access API server • k8s_1008: API server access from common pod using cURL • k8s_1009: exec in system management space • k8s_1010: pod created in management space • k8s_1011: static pod creation • k8s_1012: DaemonSet creation • k8s_1013: scheduled cluster task creation • k8s_1014: operation on secrets • k8s_1015: allowed operation enumeration • k8s_1016: high privilege RoleBinding or ClusterRoleBinding • k8s_1017: ServiceAccount creation • k8s_1018: Cronjob creation • k8s_1019: interactive shell used for exec in pods

Parameter	Mandatory	Type	Description
			• k8s_1020: unauthorized access to API server • k8s_1021: access to API server with curl • k8s_1022: Ingress vulnerability • k8s_1023: man-in-the-middle (MITM) attack • k8s_1024: worm, mining, or Trojan • k8s_1025: K8s event deletion • k8s_1026: SelfSubjectRules-Review • imgblock_0001: image blocking based on whitelist • imgblock_0002: image blocking based on blacklist • imgblock_0003: image tag blocking based on whitelist • imgblock_0004: image tag blocking based on blacklist • imgblock_0005: container creation blocked based on whitelist • imgblock_0006: container creation blocked based on blacklist • imgblock_0007: container mount proc blocking • imgblock_0008: container seccomp unconfined blocking • imgblock_0009: container privilege blocking • imgblock_0010: container capabilities blocking Array Length: **1 - 200**

Parameter	Mandatory	Type	Description
severity_list	No	Array	Threat level. The options are as follows: • Security • Low • Medium • High • Critical Minimum: **0** Maximum: **32** Array Length: **0 - 5**
attack_tag	No	String	Indicates the attack flag. The options are as follows: • attack_success: attack success • attack_attempt: attack attempt • attack_blocked: blocked attack • abnormal_behavior: abnormal behavior • collapsible_host: compromised host • system_vulnerability: system vulnerability Minimum: **0** Maximum: **32**
asset_value	No	String	Asset importance. The options are as follows: • important • common • test Minimum: **0** Maximum: **128**
tag_list	No	Array	Event tag list, for example, ["hot event"]. Minimum: **0** Maximum: **10** Array Length: **0 - 20**

Parameter	Mandatory	Type	Description
att_ck	No	String	ATT&CK attack stage, including: • Reconnaissance: • Initial Access: • Execution: • Persistence: • Privilege Escalation: • Defense Evasion: defense bypass • Credential Access: • Command and Control: • Impact: Damage is affected. Minimum: **0** Maximum: **32**
event_name	No	String	Alarm name Minimum: **1** Maximum: **128**

Request Parameters

Table 3-171 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-172 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **EventManagementResponseInfo** objects	Event list Array Length: **0 - 1000**

Table 3-173 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 • 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

Parameter	Type	Description
		• network_1002: DDoS attacks • network_1003: Malicious scanning • network_1004: Attack in sensitive areas • ransomware_0001: ransomware attack • ransomware_0002: ransomware attack • ransomware_0003: ransomware attack • fileless_0001: process injection • fileless_0002: dynamic library injection • fileless_0003: key configuration change • fileless_0004: environment variable change • fileless_0005: memory file process • fileless_0006: VDSO hijacking • crontab_1001: suspicious crontab task • vul_exploit_0001: Redis vulnerability exploit • vul_exploit_0002: Hadoop vulnerability exploit • vul_exploit_0003: MySQL vulnerability exploit • rootkit_0001: suspicious rootkit file • rootkit_0002: suspicious kernel module • RASP_0004: web shell upload • RASP_0018: fileless web shell • blockexec_001: known ransomware attack • hips_0001: Windows Defender disabled • hips_0002: suspicious hacker tool • hips_0003: suspicious ransomware encryption behavior • hips_0004: hidden account creation • hips_0005: user password and credential reading • hips_0006: suspicious SAM file export • hips_0007: suspicious shadow copy deletion • hips_0008: backup file deletion • hips_0009: registry of suspicious ransomware • hips_0010: suspicious abnormal process • hips_0011: suspicious scan • hips_0012: suspicious ransomware script running

Parameter	Type	Description
		• hips_0013: suspicious mining command execution • hips_0014: suspicious windows security center disabling • hips_0015: suspicious behavior of disabling the firewall service • hips_0016: suspicious system automatic recovery disabling • hips_0017: executable file execution in Office • hips_0018: abnormal file creation with macros in Office • hips_0019: suspicious registry operation • hips_0020: Confluence remote code execution • hips_0021: MSDT remote code execution • portscan_0001: common port scan • portscan_0002: secret port scan • k8s_1001: Kubernetes event deletion • k8s_1002: privileged pod creations • k8s_1003: interactive shell used in pod • k8s_1004: pod created with sensitive directory • k8s_1005: pod created with server network • k8s_1006: pod created with host PID space • k8s_1007: authentication failure when common pods access API server • k8s_1008: API server access from common pod using cURL • k8s_1009: exec in system management space • k8s_1010: pod created in management space • k8s_1011: static pod creation • k8s_1012: DaemonSet creation • k8s_1013: scheduled cluster task creation • k8s_1014: operation on secrets • k8s_1015: allowed operation enumeration • k8s_1016: high privilege RoleBinding or ClusterRoleBinding • k8s_1017: ServiceAccount creation • k8s_1018: Cronjob creation

Parameter	Type	Description
		• k8s_1019: interactive shell used for exec in pods • k8s_1020: unauthorized access to API server • k8s_1021: access to API server with curl • k8s_1022: Ingress vulnerability • k8s_1023: man-in-the-middle (MITM) attack • k8s_1024: worm, mining, or Trojan • k8s_1025: K8s event deletion • k8s_1026: SelfSubjectRulesReview • imgblock_0001: image blocking based on whitelist • imgblock_0002: image blocking based on blacklist • imgblock_0003: image tag blocking based on whitelist • imgblock_0004: image tag blocking based on blacklist • imgblock_0005: container creation blocked based on whitelist • imgblock_0006: container creation blocked based on blacklist • imgblock_0007: container mount proc blocking • imgblock_0008: container seccomp unconfined blocking • imgblock_0009: container privilege blocking • imgblock_0010: container capabilities blocking

Parameter	Type	Description
event_type	Integer	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 : Rootkit • 1011: ransomware • 1012: hacker tool • 1015 : web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3029: system protection disabled • 3030: backup deletion • 3031: suspicious registry operations • 3036: container image blocking • 4002: brute-force attack • 4004: abnormal login • 4006: invalid accounts • 4014: account added • 4020: password theft • 6002: port scan • 6003: server scan • 13001: Kubernetes event deletion • 13002: abnormal pod behavior

Parameter	Type	Description
		• 13003: enumerating user information • 13004: cluster role binding
event_name	String	Event name
severity	String	Threat level. Its value can be: • Security • Low • Medium • High • Critical
container_name	String	Container instance name
image_name	String	Image name
host_name	String	Server name
host_id	String	Server 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 Minimum: **1** Maximum: **32**
agent_status	String	Agent status. Its value can be: • installed • not_installed • online • offline • install_failed • installing Minimum: **1** Maximum: **32**

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: • closed • opened Minimum: **1** Maximum: **32**
asset_value	String	Asset importance. The options are as follows: • important • common • test Minimum: **0** Maximum: **128**
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, accurate to milliseconds.
handle_status	String	Processing status. Its value can be: • unhandled • handled

Parameter	Type	Description
handle_method	String	Handling method. Its value can be: • mark_as_handled • ignore • add_to_alarm_whitelist • add_to_login_whitelist • isolate_and_kill
handler	String	Remarks
operate_accept_list	Array of strings	Supported processing operation
operate_detail_list	Array of **EventDetailResponseInfo** objects	Operation details list (not displayed on the page) Array Length: **0 - 100**
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
description	String	Alarm description Minimum: **0** Maximum: **1024**
event_abstract	String	Event abstract Minimum: **0** Maximum: **512**
process_info_list	Array of **EventProcessResponseInfo** objects	Process information list Array Length: **0 - 100**

Parameter	Type	Description
user_info_list	Array of **EventUserResponseInfo** objects	User information list Array Length: **0 - 100**
file_info_list	Array of **EventFileResponseInfo** objects	File information list Array Length: **0 - 100**
event_details	String	Brief description of the event. Minimum: **0** Maximum: **204800**
tag_list	Array of strings	Tags Minimum: **0** Maximum: **10** Array Length: **0 - 20**
event_count	Integer	Event occurrences Minimum: **0** Maximum: **2147483647**

Table 3-174 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
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 3-175 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	VM UUID
container_id	String	Container ID
container_status	String	Container status
pod_uid	String	pod uid
pod_name	String	pod name
namespace	String	namespace
cluster_id	String	Cluster ID
cluster_name	String	Cluster name
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
os_name	String	OS name
os_version	String	OS version

Table 3-176 EventProcessResponseInfo

Parameter	Type	Description
process_name	String	Process name
process_path	String	Process file path
process_pid	Integer	Process ID Minimum: **0** Maximum: **2147483647**
process_uid	Integer	Process user ID Minimum: **0** Maximum: **2147483647**
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 Minimum: **0** Maximum: **9223372036854775807**
process_gid	Integer	Process group ID Minimum: **0** Maximum: **2147483647**
process_egid	Integer	Valid process group ID Minimum: **0** Maximum: **2147483647**
process_euid	Integer	Valid process user ID Minimum: **0** Maximum: **2147483647**
parent_process_name	String	Parent process name
parent_process_path	String	Parent process file path
parent_process_pid	Integer	Parent process ID Minimum: **0** Maximum: **2147483647**

Parameter	Type	Description
parent_process_uid	Integer	Parent process user ID Minimum: **0** Maximum: **2147483647**
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 Minimum: **0** Maximum: **9223372036854775807**
parent_process_gid	Integer	Parent process group ID Minimum: **0** Maximum: **2147483647**
parent_process_egid	Integer	Valid parent process group ID Minimum: **0** Maximum: **2147483647**
parent_process_euid	Integer	Valid parent process user ID Minimum: **0** Maximum: **2147483647**
child_process_name	String	Subprocess name
child_process_path	String	Subprocess file path
child_process_pid	Integer	Subprocess ID Minimum: **0** Maximum: **2147483647**
child_process_uid	Integer	Subprocess user ID Minimum: **0** Maximum: **2147483647**
child_process_cmdline	String	Subprocess file command line
child_process_filename	String	Subprocess file name
child_process_start_time	Long	Subprocess start time Minimum: **0** Maximum: **9223372036854775807**

Parameter	Type	Description
child_process_gid	Integer	Subprocess group ID Minimum: **0** Maximum: **2147483647**
child_process_egid	Integer	Valid subprocess group ID Minimum: **0** Maximum: **2147483647**
child_process_euid	Integer	Valid subprocess user ID Minimum: **0** Maximum: **2147483647**
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 3-177 EventUserResponseInfo

Parameter	Type	Description
user_id	Integer	User UID Minimum: **0** Maximum: **2147483647**
user_gid	Integer	User GID Minimum: **0** Maximum: **2147483647**
user_name	String	User name
user_group_name	String	User group name
user_home_dir	String	User home directory
login_ip	String	User login IP address
service_type	String	Login service type

Parameter	Type	Description
service_port	Integer	Login service port Minimum: **0** Maximum: **2147483647**
login_mode	Integer	Login mode Minimum: **0** Maximum: **2147483647**
login_last_time	Long	Last login time Minimum: **0** Maximum: **9223372036854775807**
login_fail_count	Integer	Number of failed login attempts Minimum: **0** Maximum: **2147483647**
pwd_hash	String	Password hash
pwd_with_fuzzing	String	Masked password
pwd_used_days	Integer	Password age (days) Minimum: **0** Maximum: **2147483647**
pwd_min_days	Integer	Minimum password validity period Minimum: **0** Maximum: **2147483647**
pwd_max_days	Integer	Maximum password validity period Minimum: **0** Maximum: **2147483647**
pwd_warn_left_days	Integer	Advance warning of password expiration (days) Minimum: **0** Maximum: **2147483647**

Table 3-178 EventFileResponseInfo

Parameter	Type	Description
file_path	String	File path
file_alias	String	File alias

Parameter	Type	Description
file_size	Integer	File size Minimum: **0** Maximum: **2147483647**
file_mtime	Long	Time when a file was last modified Minimum: **0** Maximum: **9223372036854775807**
file_atime	Long	Time when a file was last accessed Minimum: **0** Maximum: **9223372036854775807**
file_ctime	Long	Time when the status of a file was last changed Minimum: **0** Maximum: **9223372036854775807**
file_hash	String	File hash
file_md5	String	File MD5
file_sha256	String	File SHA256
file_type	String	File type
file_content	String	File content
file_attr	String	File attribute
file_operation	Integer	File operation type Minimum: **0** Maximum: **2147483647**
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 Minimum: **0** Maximum: **2147483647**

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" : "China",
      "city" : "Lanzhou",
      "ip" : "127.0.0.1",
      "user" : "zhangsan",
      "sub_division" : "Gansu",
      "city_id" : 3110
    },
    "handle_status" : "unhandled",
    "host_name" : "xxx",
    "occur_time" : 1661593036627,
    "operate_accept_list" : [ "ignore" ],
    "operate_detail_list" : [ {
      "agent_id" : "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
      "file_hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "file_path" : "/usr/test",
      "process_pid" : 3123,
      "file_attr" : 33261,
      "keyword" : "file_path=/usr/test",
      "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "login_ip" : "127.0.0.1",
      "private_ip" : "127.0.0.2",
      "login_user_name" : "root",
      "is_parent" : false
    } ],
    "private_ip" : "127.0.0.1",
    "resource_info" : {
      "region_name" : "",
      "project_id" : "",
      "enterprise_project_id" : "0",
      "os_type" : "Linux",
      "os_version" : "2.5",
      "vm_name" : "",
      "vm_uuid" : "71a15ecc",
      "cloud_id" : "",
      "container_id" : "",
      "container_status" : "running / terminated",
      "image_id" : "",
      "pod_uid" : "",
      "pod_name" : "",
      "namespace" : "",
      "cluster_id" : "",
      "cluster_name" : ""
    },
    "severity" : "Medium",
    "extend_info" : "",
```



```
  "os_type" : "Linux",
  "agent_status" : "online",
  "asset_value" : "common",
  "protect_status" : "opened",
  "host_status" : "ACTIVE",
  "event_details" : "file_path:/root/test",
  "user_info_list" : [ {
    "login_ip" : "",
    "service_port" : 22,
    "service_type" : "ssh",
    "user_name" : "zhangsan",
    "login_mode" : 0,
    "login_last_time" : 1661593024,
    "login_fail_count" : 0
  } ],
  "description" : "",
  "event_abstract" : "",
  "tag_list" : [ "Hot Event" ]
 } ]
}
```


Status Codes

Status Code	Description
200	Intrusion list

Error Codes

See **Error Codes**.

3.5.3 Querying the Alarm Whitelist

Function

This API is used to query the alarm whitelist.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-179 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **20** Maximum: **64**

Table 3-180 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**. Minimum: **0** Maximum: **64**
hash	No	String	SHA256 Minimum: **64** Maximum: **64**

Parameter	Mandatory	Type	Description
event_type	No	Integer	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 : Rootkit • 1011: ransomware • 1012: hacker tool • 1015: Web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3029: system protection disabled • 3030: backup deletion • 3031: suspicious registry operations • 4002: brute-force attack

Parameter	Mandatory	Type	Description
			• 4004: abnormal login • 4006: invalid system account • 4014: account added • 4020: password theft • 6003: server scan Minimum: **1000** Maximum: **30000**
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**. Minimum: **0** Maximum: **2000000** Default: **0**
limit	No	Integer	Number of records displayed on each page. Minimum: **10** Maximum: **1000** Default: **10**

Request Parameters

Table 3-181 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-182 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
event_type_list	Array of integers	Types of events that can be filtered Minimum: **0** Maximum: **2147483647** Array Length: **0 - 30000**
data_list	Array of **AlarmWhiteListResponseInfo** objects	Alarm whitelist details Array Length: **0 - 100**

Table 3-183 AlarmWhiteListResponseInfo

Parameter	Type	Description
enterprise_project_name	String	Enterprise project name
hash	String	SHA256
description	String	Description

Parameter	Type	Description
event_type	Integer	Event type. Its value can be: • 1001: common malware • 1002: virus • 1003: worm • 1004: Trojan • 1005: botnet • 1006: backdoor • 1010 : Rootkit • 1011: ransomware • 1012: hacker tool • 1015 : web shell • 1016: mining • 1017: reverse shell • 2001: common vulnerability exploit • 2012: remote code execution • 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 • 3029: system protection disabled • 3030: backup deletion • 3031: suspicious registry operations • 3036: container image blocking • 4002: brute-force attack • 4004: abnormal login • 4006: invalid accounts • 4014: account added • 4020: password theft • 6002: port scan • 6003: server scan • 13001: Kubernetes event deletion • 13002: abnormal pod behavior

Parameter	Type	Description
		• 13003: enumerating user information • 13004: cluster role binding
white_field	String	Whitelist fields. The options are as follows: • "file/process hash" # process/file hash • "file_path" • "process_path" • "login_ip" # login IP address • "reg_key" # registry key • "process_cmdline" # process command line • "username" Minimum: **1** Maximum: **20**
field_value	String	Whitelist fields value Minimum: **1** Maximum: **128**
judge_type	String	Wildcard. The options are as follows: • "equal" • "contain" Minimum: **1** Maximum: **10**
update_time	Integer	Update time, 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,
    "white_field" : "process/file hash",
    "judge_type" : "contain",
    "field_value" : "abcd12345612311112212323"
  } ],
```



```
  "event_type_list" : [ 1001 ],
  "total_num" : 1
}
```

Status Codes

Status Code	Description
200	Alarm whitelist

Error Codes

See **Error Codes**.

3.6 Server Management

3.6.1 Querying ECSs

Function

This API is used to query ECSs.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-184 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-185 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID Default: **0** Minimum: **1** Maximum: **256**
version	No	String	HSS edition. Its value can be: • hss.version.null • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **64**
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. Minimum: **1** Maximum: **20**

Parameter	Mandatory	Type	Description
detect_result	No	String	Detection result. Its value can be: • undetected • clean • risk • scanning Minimum: **1** Maximum: **32**
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 Minimum: **1** Maximum: **32**
os_type	No	String	OS type. Its value can be: • Linux • Windows Minimum: **0** Maximum: **64**
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 Minimum: **1** Maximum: **32**
group_id	No	String	Server group ID
group_name	No	String	Server group name Minimum: **1** Maximum: **64**
has_intrusion	No	Boolean	Alarms exist.

Parameter	Mandatory	Type	Description
policy_group_id	No	String	Policy group ID Minimum: **0** Maximum: **128**
policy_group_name	No	String	Policy group name Minimum: **0** Maximum: **256**
charging_mode	No	String	Billing mode. Its value can be: • packet_cycle: yearly/monthly • on_demand: pay-per-use Minimum: **1** Maximum: **32**
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 Huawei Cloud server
asset_value	No	String	Asset importance. Its value can be: • important • common • test Minimum: **0** Maximum: **128**
label	No	String	Asset tag Minimum: **1** Maximum: **64**
server_group	No	String	Asset server group Minimum: **1** Maximum: **64**
agent_upgradable	No	Boolean	Whether the agent can be upgraded

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The default value is **10**. Minimum: **0** Maximum: **200** Default: **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**. Minimum: **0** Maximum: **2000000** Default: **0**

Request Parameters

Table 3-186 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. Minimum: **1** Maximum: **32768**
region	No	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-187 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of records Minimum: **0** Maximum: **2097152**
data_list	Array of **Host** objects	Query on the cloud server status and list Array Length: **0 - 10241**

Table 3-188 Host

Parameter	Type	Description
host_name	String	Server name Minimum: **0** Maximum: **128**
host_id	String	Server ID Minimum: **0** Maximum: **128**
agent_id	String	Agent ID Minimum: **0** Maximum: **128**
private_ip	String	Private IP address Minimum: **0** Maximum: **128**
public_ip	String	Elastic IP address Minimum: **0** Maximum: **128**
enterprise_project_id	String	Enterprise project ID Minimum: **0** Maximum: **256**
enterprise_project_name	String	Enterprise project name Minimum: **0** Maximum: **256**

Parameter	Type	Description
host_status	String	Server status. Its value can be: • ACTIVE • SHUTOFF • BUILDING • ERROR Minimum: **1** Maximum: **32**
agent_status	String	Agent status. Its value can be: • not_ installed • online • offline • install_failed • installing Minimum: **1** Maximum: **32**
install_result_code	String	Installation result. Its value can be: • 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 are no servers with an online agent in the current VPC. • install_exception • invalid_param • install_failed • package_unavailable • os_type_not_support: Incorrect OS type • os_arch_not_support: Incorrect OS architecture Minimum: **1** Maximum: **32**

Parameter	Type	Description
version	String	HSS edition. Its value can be: • hss.version.null: none • hss.version.basic: basic edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition • hss.version.container.enterprise: container edition Minimum: **1** Maximum: **32**
protect_status	String	Protection status. Its value can be: • closed • opened Minimum: **1** Maximum: **32**
os_image	String	System disk image Minimum: **0** Maximum: **128**
os_type	String	OS type. Its value can be: • Linux • Windows Minimum: **0** Maximum: **128**
os_bit	String	OS bit version Minimum: **0** Maximum: **128**
detect_result	String	Server scan result. Its value can be: • undetected • clean • risk • scanning Minimum: **1** Maximum: **32**

Parameter	Type	Description
expire_time	Long	Expiration time of the trial version. (The value **-1** indicates that the quota is non-trial version. If the value is not **-1**, the value indicates the expiration time of the trial version.) Minimum: **0** Maximum: **4824695185000**
charging_mode	String	Billing mode. Its value can be: • packet_cycle: yearly/monthly • on_demand: pay-per-use Minimum: **1** Maximum: **32**
resource_id	String	Cloud service resource instance ID (UUID) Minimum: **0** Maximum: **128**
outside_host	Boolean	Whether a server is a non-Huawei Cloud server
group_id	String	Server group ID Minimum: **1** Maximum: **128**
group_name	String	Server group name Minimum: **1** Maximum: **128**
policy_group_id	String	Policy group ID Minimum: **1** Maximum: **128**
policy_group_name	String	Policy group name Minimum: **1** Maximum: **128**
asset	Integer	Asset risk Minimum: **0** Maximum: **2097152**
vulnerability	Integer	Vulnerability Minimum: **0** Maximum: **2097152**
baseline	Integer	Baseline risks Minimum: **0** Maximum: **2097152**

Parameter	Type	Description
intrusion	Integer	Intrusion risk Minimum: **0** Maximum: **2097152**
asset_value	String	Asset importance. Its value can be: • important • common • test Minimum: **0** Maximum: **128**
labels	Array of strings	Tag list Minimum: **0** Maximum: **64** Array Length: **0 - 100**
agent_create_time	Long	Agent installation time, which is a timestamp. The default unit is milliseconds. Minimum: **0** Maximum: **4824695185000**
agent_update_time	Long	Time when the agent status is changed. This is a timestamp. The default unit is milliseconds. Minimum: **0** Maximum: **4824695185000**
agent_version	String	Agent version Minimum: **1** Maximum: **32**
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 Minimum: **1** Maximum: **32**

Parameter	Type	Description
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: The disk space is insufficient. • failed_to_replace_file: Failed to replace the file. Minimum: **1** Maximum: **32**
upgradable	Boolean	Whether the agent of the server can be upgraded
open_time	Long	Time when the protection is enabled. This is a timestamp. The default unit is milliseconds. Minimum: **0** Maximum: **4824695185000**
protect_interrupt	Boolean	Whether protection is interrupted

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


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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-189 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-190 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-191 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-192 Request body parameters

Parameter	Mandatory	Type	Description
version	Yes	String	HSS edition. Its value can be: • hss.version.null: protection disabled • hss.version.basic: basic edition • hss.version.advanced: professional edition • hss.version.enterprise: enterprise edition • hss.version.premium: premium edition • hss.version.wtp: WTP edition Minimum: **1** Maximum: **128**
charging_mode	No	String	Payment mode. This parameter is mandatory when version is not set to hss.version.null. • packet_cycle: yearly/monthly • on_demand: on-demand Minimum: **1** Maximum: **64**
resource_id	No	String	HSS quota ID. If this parameter is not specified, the quota of the corresponding version is randomly selected. Minimum: **1** Maximum: **128**
host_id_list	Yes	Array of strings	Server list Minimum: **1** Maximum: **128** Array Length: **0 - 2097152**
tags	No	Array of **TagInfo** objects	Resource tag list Array Length: **0 - 2097152**

Table 3-193 TagInfo

Parameter	Mandatory	Type	Description
key	No	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank. Minimum: **1** Maximum: **128**
value	No	String	Value. Each tag value can contain a maximum of 255 Unicode characters. Minimum: **1** Maximum: **255**

Response Parameters

None

Example Requests

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

```
{
  "version" : "hss.version.basic",
  "charging_mode" : "packet_cycle",
  "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-194 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-195 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**. Default: **0** Minimum: **1** Maximum: **256**
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**. Minimum: **0** Maximum: **2000000** Default: **0**
limit	No	Integer	Number of records displayed on each page. Minimum: **10** Maximum: **200** Default: **10**

Parameter	Mandatory	Type	Description
group_name	No	String	Server group name Minimum: **1** Maximum: **64**

Request Parameters

Table 3-196 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-197 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **HostGroupItem** objects	Server group list Array Length: **0 - 100**

Table 3-198 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
is_outside	Boolean	Indicates whether the server group is an on-premises data center server group.

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-199 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-200 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-201 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. Minimum: **1** Maximum: **32768**

Parameter	Mandatory	Type	Description
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-202 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Server group name Minimum: **1** Maximum: **128**
host_id_list	Yes	Array of strings	Server ID list Minimum: **1** Maximum: **128** Array Length: **1 - 10000**

Response Parameters

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.

Status Code	Description
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-204 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-205 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-206 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

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-207 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-208 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**. Default: **0** Minimum: **1** Maximum: **256**
group_id	Yes	String	Server group ID

Request Parameters

Table 3-209 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

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.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/policy/groups

Table 3-210 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-211 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**. Default: **0** Minimum: **1** Maximum: **256**
group_name	No	String	Policy group name Minimum: **1** Maximum: **256**
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**. Minimum: **0** Maximum: **100000** Default: **0**
limit	No	Integer	Number of records displayed on each page. Minimum: **10** Maximum: **200** Default: **10**

Request Parameters

Table 3-212 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 3-213 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **PolicyGroupResponseInfo** objects	Policy group list Array Length: **0 - 100**

Table 3-214 PolicyGroupResponseInfo

Parameter	Type	Description
group_name	String	Policy group name
group_id	String	Policy group ID
description	String	Description
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: Windows OS is supported.
support_version	String	Supported versions. The options are as follows: • hss.version.basic: policy group of the basic edition • hss.version.advanced: policy group of the professional edition • 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

Function

This API is used to apply a policy.

Calling Method

For details, see **Calling APIs**.

URI

POST /v5/{project_id}/policy/deploy

Table 3-215 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-216 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**. Default: **0** Minimum: **1** Maximum: **256**

Request Parameters

Table 3-217 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. Minimum: **1** Maximum: **32768**
region	Yes	String	region id Minimum: **0** Maximum: **128**

Table 3-218 Request body parameters

Parameter	Mandatory	Type	Description
target_policy_group_id	Yes	String	ID of the policy group to be deployed Minimum: **36** Maximum: **64**
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	Server ID list

Response Parameters

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.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/vulnerability/vulnerabilities

Table 3-219 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID Minimum: **1** Maximum: **256**

Table 3-220 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise user ID Default: **0** Minimum: **0** Maximum: **256**
type	No	String	Vulnerability type. The options are as follows: -linux_vul: Linux vulnerability -windows_vul: windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability Minimum: **0** Maximum: **32**
vul_id	No	String	Vulnerability ID Minimum: **0** Maximum: **256**
vul_name	No	String	Vulnerability name Minimum: **0** Maximum: **256**
limit	No	Integer	Number of records displayed on each page Minimum: **0** Maximum: **200** Default: **10**

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. The default value is **0**. Minimum: **0** Maximum: **2000000** Default: **0**
repair_priority	No	String	Fix Priority Critical High Medium Low Minimum: **1** Maximum: **10**
handle_status	No	String	description: |- Handling status. The options are as follows: - unhandled - handled Default: **unhandled** Minimum: **1** Maximum: **32**
cve_id	No	String	Vulnerability ID Minimum: **0** Maximum: **32**
label_list	No	String	Vulnerability tag Minimum: **0** Maximum: **128**
status	No	String	Vulnerability status Minimum: **0** Maximum: **32**
asset_value	No	String	Asset importance important common test Minimum: **0** Maximum: **32**
group_name	No	String	Server group name Minimum: **0** Maximum: **256**

Request Parameters

Table 3-221 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. Minimum: **1** Maximum: **32768**

Response Parameters

Status code: 200

Table 3-222 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of software vulnerabilities Minimum: **0** Maximum: **2147483647**
data_list	Array of **VulInfo** objects	Software vulnerability list Array Length: **0 - 2147483647**

Table 3-223 VulInfo

Parameter	Type	Description
vul_name	String	Vulnerability name Minimum: **0** Maximum: **256**
vul_id	String	Vulnerability ID Minimum: **0** Maximum: **64**
label_list	Array of strings	Vulnerability tag Minimum: **0** Maximum: **65534** Array Length: **0 - 2147483647**

Parameter	Type	Description
repair_necessity	String	Necessity to repair Minimum: **0** Maximum: **64**
severity_level	String	Vulnerability level Minimum: **0** Maximum: **64**
host_num	Integer	Number of affected servers Minimum: **0** Maximum: **2147483647**
unhandle_host_num	Integer	Number of unhandled servers Minimum: **0** Maximum: **2147483647**
scan_time	Long	Last scan time Minimum: **0** Maximum: **9223372036854775807**
solution_detail	String	Solution Minimum: **0** Maximum: **65534**
url	String	Vulnerability URL Minimum: **0** Maximum: **2083**
description	String	Vulnerability description Minimum: **0** Maximum: **65534**
type	String	Vulnerability type. The options are as follows: -linux_vul: Linux vulnerability -windows_vul: windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability Minimum: **0** Maximum: **128**
host_id_list	Array of strings	Host list Minimum: **0** Maximum: **128** Array Length: **0 - 2147483647**
cve_list	Array of **cve_list** objects	CVE list Array Length: **1 - 10000**

Parameter	Type	Description
patch_url	String	Patch address Minimum: **0** Maximum: **512**
repair_priority	String	Fix Priority Critical High Medium Low Minimum: **1** Maximum: **32**
hosts_num	**VulnerabilityHostNumberInfo** object	Affected server
repair_success_num	Integer	Number of successful repairs Minimum: **0** Maximum: **1000000**
fixed_num	Long	Number of repairs Minimum: **0** Maximum: **1000000**
ignored_num	Long	Number of ignored items Minimum: **0** Maximum: **1000000**
verify_num	Integer	Number of verifications Minimum: **0** Maximum: **1000000**

Table 3-224 cve_list

Parameter	Type	Description
cve_id	String	CVE ID Minimum: **1** Maximum: **32**
cvss	Float	CVSS score Minimum: **0** Maximum: **10**

Table 3-225 VulnerabilityHostNumberInfo

Parameter	Type	Description
important	Integer	Number of important servers Minimum: **0** Maximum: **10000**
common	Integer	Number of common servers Minimum: **0** Maximum: **10000**
test	Integer	Number of test servers Minimum: **0** Maximum: **10000**

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.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/vulnerability/hosts

Table 3-226 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID Minimum: **1** Maximum: **256**

Table 3-227 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise user ID. To query all enterprise projects, set this parameter to **all_granted_eps**. Minimum: **0** Maximum: **128**
vul_id	Yes	String	Vulnerability ID Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
type	Yes	String	Vulnerability type • linux_vul: Linux vulnerability • windows_vul: Windows vulnerability -web_cms: Web-CMS vulnerability • app_vul: application vulnerability • urgent_vul: emergency vulnerability Minimum: **0** Maximum: **64**
host_name	No	String	Affected asset name Minimum: **0** Maximum: **256**
host_ip	No	String	IP address of the affected asset Minimum: **0** Maximum: **128**
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. Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records on each page Minimum: **10** Maximum: **200** Default: **10**
offset	No	Integer	Offset Minimum: **0** Maximum: **2000000** Default: **0**
asset_value	No	String	Asset importance important common test Minimum: **0** Maximum: **32**
group_name	No	String	Server group name Minimum: **0** Maximum: **256**
handle_status	No	String	description: |- Handling status. The options are as follows: - unhandled - handled Minimum: **1** Maximum: **32**
severity_level	No	String	Risk level. The value can be Critical, High, Medium, or Low. Minimum: **0** Maximum: **32**
is_affect_business	No	Boolean	Indicates whether services are affected. The value can be y or n.

Request Parameters

Table 3-228 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. Minimum: **1** Maximum: **32768**

Response Parameters

Status code: 200

Table 3-229 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of affected servers Minimum: **0** Maximum: **10000**
data_list	Array of **VulHostInfo** objects	Number of affected servers Array Length: **1 - 10000**

Table 3-230 VulHostInfo

Parameter	Type	Description
host_id	String	Server ID Minimum: **1** Maximum: **128**

Parameter	Type	Description
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. Minimum: **1** Maximum: **128**
host_name	String	Affected asset name Minimum: **1** Maximum: **256**
host_ip	String	IP address of the affected asset Minimum: **1** Maximum: **256**
agent_id	String	The corresponding agent ID of the server Minimum: **1** Maximum: **128**
cve_num	Integer	Vulnerability CVEs Minimum: **0** Maximum: **10000**
cve_id_list	Array of strings	CVE list Minimum: **1** Maximum: **64** Array Length: **1 - 10000**

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. Minimum: **1** Maximum: **128**
repair_cmd	String	Repair command Minimum: **1** Maximum: **256**
app_path	String	Path of the application software (This field is available only for application vulnerabilities.) Minimum: **1** Maximum: **512**
region_name	String	Region Minimum: **0** Maximum: **128**
public_ip	String	Server public IP address Minimum: **0** Maximum: **128**
private_ip	String	Server private IP address Minimum: **0** Maximum: **128**
group_id	String	Server group ID Minimum: **0** Maximum: **128**
group_name	String	Server group name Minimum: **0** Maximum: **256**

Parameter	Type	Description
os_type	String	Operating system (OS) Minimum: **0** Maximum: **32**
asset_value	String	Asset importance. The options are as follows: • important • common • test Minimum: **0** Maximum: **32**
is_affect_business	Boolean	Whether services are affected
first_scan_time	Long	First scan time Minimum: **0** Maximum: **9223372036854775807**
scan_time	Long	Scan time Minimum: **0** Maximum: **9223372036854775807**
support_restore	Boolean	Indicates whether data can be rolled back to the backup created when the vulnerability was fixed.

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",
    "agent_id" : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "cve_num" : 1,
    "cve_id_list" : [ "CVE-2022-1664" ],
    "status" : "vul_status_ignored",
    "repair_cmd" : "zypper update update-alternatives",
```



```
    "app_path" : "/root/apache-tomcat-8.5.15/bin/bootstrap.jar",
    "support_restore" : true
  } ]
}
```

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.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v5/{project_id}/vulnerability/status

Table 3-231 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**

Table 3-232 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise user ID. To query all enterprise projects, set this parameter to **all_granted_eps**. Minimum: **0** Maximum: **128**

Request Parameters

Table 3-233 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token Minimum: **32** Maximum: **4096**

Table 3-234 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Operation type. • ignore • not_ignore: unignore • immediate_repair: fix • verify Minimum: **1** Maximum: **64**
remark	No	String	Remarks Minimum: **0** Maximum: **512**
select_type	No	String	Select vulnerabilities. • all_vul: Select all vulnerabilities. • all_host: Select all server vulnerabilities. Minimum: **1** Maximum: **64**

Parameter	Mandatory	Type	Description
type	No	String	Vulnerability type. The default value is **linux_vul**. The options are as follows: • linux_vul: Linux vulnerability • windows_vul: Windows vulnerability • web_cms: Web-CMS vulnerability • app_vul: application vulnerability Minimum: **0** Maximum: **64**
data_list	Yes	Array of **VulOperateInfo** objects	Vulnerability list Array Length: **1 - 500**
host_data_list	No	Array of **HostVulOperateInfo** objects	Vulnerability list in the server dimension Array Length: **1 - 500**
backup_info_id	No	String	Specifies the ID of the backup information processed by the vulnerability. If this parameter is not specified, the backup is not performed. Minimum: **1** Maximum: **128**
custom_backup_hosts	No	Array of **custom_backup_hosts** objects	Customize the vault and backup name used by the backup host. For hosts that are not in the list, the system automatically selects the vault with the largest remaining space and generates a backup name. Array Length: **1 - 50**

Table 3-235 VulOperateInfo

Parameter	Mandatory	Type	Description
vul_id	Yes	String	Vulnerability ID Minimum: **1** Maximum: **64**
host_id_list	Yes	Array of strings	Server list Minimum: **1** Maximum: **64** Array Length: **1 - 500**

Table 3-236 HostVulOperateInfo

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID Minimum: **1** Maximum: **64**
vul_id_list	Yes	Array of strings	Vulnerability list Minimum: **1** Maximum: **64** Array Length: **1 - 500**

Table 3-237 custom_backup_hosts

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID Minimum: **1** Maximum: **128**
vault_id	No	String	Vault ID Minimum: **1** Maximum: **128**
backup_name	No	String	Backup name Minimum: **1** Maximum: **64**

Response Parameters

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.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/webtamper/hosts

Table 3-238 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **0** Maximum: **64**

Table 3-239 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **64**
host_name	No	String	Server name Minimum: **0** Maximum: **256**
host_id	No	String	Cloud server ID Minimum: **0** Maximum: **128**
public_ip	No	String	EIP Minimum: **0** Maximum: **128**
private_ip	No	String	Private IP address Minimum: **0** Maximum: **128**
group_name	No	String	Server group name Minimum: **0** Maximum: **256**
os_type	No	String	OS type. Its value can be: • linux • windows Minimum: **0** Maximum: **32**
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled Minimum: **0** Maximum: **32**

Parameter	Mandatory	Type	Description
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. Minimum: **0** Maximum: **32**
limit	No	Integer	Default value: 10 Minimum: **10** Maximum: **100** Default: **10**
offset	No	Integer	Default value: 0 Minimum: **0** Maximum: **100** Default: **0**

Request Parameters

Table 3-240 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token Minimum: **1** Maximum: **32768**
region	Yes	String	Region Id Minimum: **0** Maximum: **32**

Response Parameters

Status code: 200

Table 3-241 Response body parameters

Parameter	Type	Description
data_list	Array of **WtpProtectHostResponseInfo** objects	data list Array Length: **0 - 200000**
total_num	Integer	total number Minimum: **0** Maximum: **65535**

Table 3-242 WtpProtectHostResponseInfo

Parameter	Type	Description
host_name	String	Server name Minimum: **0** Maximum: **256**
host_id	String	Cloud server ID Minimum: **0** Maximum: **128**
public_ip	String	EIP Minimum: **0** Maximum: **128**
private_ip	String	Private IP address Minimum: **0** Maximum: **128**
group_name	String	Server group name Minimum: **0** Maximum: **256**
os_bit	String	OS bit version Minimum: **0** Maximum: **8**
os_type	String	OS (linux or windows) Minimum: **0** Maximum: **32**

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: • closed • opened Minimum: **0** Maximum: **32**
rasp_protect_status	String	Dynamic WTP status. • closed • opened Minimum: **0** Maximum: **32**
anti_tampering_times	Long	Number of blocked tampering attacks Minimum: **0** Maximum: **2000000000**
detect_tampering_times	Long	Number of detected tampering attacks Minimum: **0** Maximum: **2000000000**
last_detect_time	Long	Last scan time Minimum: **0** Maximum: **4070880000000**
scheduled_shutdown_status	String	Status of scheduled protection. • opened • closed Minimum: **0** Maximum: **32**
agent_status	String	Agent status. • not_installed: The agent is not installed. • online: The agent is online. • offline: The agent is offline. Minimum: **0** Maximum: **32**

Example Requests

This API is used to query the 10 records on the first page of WTP status list of servers whose status is enabled and enterprise project is XX by default.

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



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

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

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-243 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID Minimum: **0** Maximum: **64**

Table 3-244 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **64**

Request Parameters

Table 3-245 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token Minimum: **1** Maximum: **32768**
region	Yes	String	Region Id Minimum: **0** Maximum: **32**

Table 3-246 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	Boolean	Status (enabled or disabled)
host_id_list	Yes	Array of strings	HostId list Minimum: **0** Maximum: **128** Array Length: **0 - 20000**
resource_id	No	String	Resource ID Minimum: **0** Maximum: **64**

Parameter	Mandatory	Type	Description
charging_mode	No	String	Billing mode. • packet_cycle: yearly/monthly Minimum: **0** Maximum: **32**

Response Parameters

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" : "packet_cycle"
}
```

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-247 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID Minimum: **0** Maximum: **64**

Table 3-248 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **64**

Request Parameters

Table 3-249 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token Minimum: **1** Maximum: **32768**
region	Yes	String	Region Id Minimum: **0** Maximum: **32**

Table 3-250 Request body parameters

Parameter	Mandatory	Type	Description
host_id_list	No	Array of strings	HostId list Minimum: **0** Maximum: **128** Array Length: **0 - 20000**
status	No	Boolean	Dynamic WTP status

Response Parameters

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-251 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **0** Maximum: **64**

Table 3-252 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **64**
host_id	Yes	String	Host Id Minimum: **0** Maximum: **128**
start_time	Yes	Long	Start time Minimum: **0** Maximum: **4070880000000**
end_time	Yes	Long	End time Minimum: **0** Maximum: **4070880000000**
limit	Yes	Integer	limit Minimum: **0** Maximum: **100**
offset	Yes	Integer	offset Minimum: **0** Maximum: **100**
host_name	No	String	Server name Minimum: **0** Maximum: **128**
host_ip	No	String	Server IP address Minimum: **0** Maximum: **128**
file_path	No	String	Protected file Minimum: **0** Maximum: **128**
file_operation	No	String	Types of file operations, including: • add • delete • modify • attribute Minimum: **0** Maximum: **128**

Request Parameters

Table 3-253 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token Minimum: **1** Maximum: **32768**
region	Yes	String	Region Id Minimum: **0** Maximum: **32**

Response Parameters

Status code: 200

Table 3-254 Response body parameters

Parameter	Type	Description
host_name	String	Server name Minimum: **0** Maximum: **256**
protect_status	String	Protection status. Its value can be: • close • opened Minimum: **0** Maximum: **32**
total_num	Long	total number Minimum: **0** Maximum: **20000000**
data_list	Array of **HostProtectHistoryResponseInfo** objects	data list Array Length: **0 - 20000**

Table 3-255 HostProtectHistoryResponseInfo

Parameter	Type	Description
occr_time	Long	Detection time Minimum: **0** Maximum: **4070880000000**
file_path	String	Tampered file path Minimum: **0** Maximum: **2000**
file_operation	String	Types of file operations • add • delete • modify • attribute • unknown Minimum: **0** Maximum: **32**
host_name	String	Server name Minimum: **0** Maximum: **64**
host_ip	String	Server IP address Minimum: **0** Maximum: **64**
process_id	String	Process ID Minimum: **0** Maximum: **8**
process_name	String	Process name Minimum: **0** Maximum: **200**
process_cmd	String	Process command line Minimum: **0** Maximum: **8191**

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",
    "host_name" : "hss-test",
    "host_ip" : "192.168.5.98",
    "file_operation" : "add",
    "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-256 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID Minimum: **0** Maximum: **64**

Table 3-257 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project Minimum: **0** Maximum: **64**
host_id	Yes	String	Host Id Minimum: **0** Maximum: **128**
start_time	Yes	Long	Start time Minimum: **0** Maximum: **4070880000000**
end_time	Yes	Long	End time Minimum: **0** Maximum: **4070880000000**
limit	Yes	Integer	limit Minimum: **0** Maximum: **100**
offset	Yes	Integer	offset Minimum: **0** Maximum: **100**
alarm_level	No	Integer	Alarm severity Minimum: **0** Maximum: **100**

Parameter	Mandatory	Type	Description
severity	No	String	Threat level. Its value can be: • Security • Low: low risk • Medium: medium risk • High: high risk • Critical Minimum: **0** Maximum: **32**
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled Minimum: **0** Maximum: **32**

Request Parameters

Table 3-258 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token Minimum: **1** Maximum: **32768**
region	Yes	String	Region Id Minimum: **0** Maximum: **32**

Response Parameters

Status code: 200

Table 3-259 Response body parameters

Parameter	Type	Description
total_num	Long	total number Minimum: **0** Maximum: **200000**

Parameter	Type	Description
data_list	Array of **HostRaspProtectHistoryResponseInfo** objects	data list Array Length: **0 - 200000**

Table 3-260 HostRaspProtectHistoryResponseInfo

Parameter	Type	Description
host_ip	String	Server IP address Minimum: **0** Maximum: **64**
host_name	String	Server name Minimum: **0** Maximum: **64**
alarm_time	Long	Alarm time Minimum: **0** Maximum: **4070880000000**
threat_type	String	Threat type Minimum: **0** Maximum: **64**
alarm_level	Integer	Alarm severity Minimum: **0** Maximum: **100**
source_ip	String	Source IP address Minimum: **0** Maximum: **128**
attacked_url	String	Attack URL Minimum: **0** Maximum: **2000**

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

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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-261 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID Minimum: **1** Maximum: **256**
resource_type	Yes	String	Resource type. The value is hss. Minimum: **1** Maximum: **64**
resource_id	Yes	String	Resource ID Minimum: **0** Maximum: **128**

Request Parameters

Table 3-262 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. Minimum: **32** Maximum: **512**

Table 3-263 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **ResourceTagInfo** objects	Tag List Array Length: **0 - 1024**
sys_tags	No	Array of **ResourceTagInfo** objects	Tag List Array Length: **0 - 1024**

Table 3-264 ResourceTagInfo

Parameter	Mandatory	Type	Description
key	No	String	Key. It can contain up to 128 Unicode characters. The key cannot be left blank. Minimum: **1** Maximum: **128**
value	No	String	Value Minimum: **1** Maximum: **128**

Response Parameters

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.

Status Code	Description
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-265 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID Minimum: **1** Maximum: **256**
resource_type	Yes	String	Resource type. The value is hss. Minimum: **1** Maximum: **64**
resource_id	Yes	String	Resource ID Minimum: **0** Maximum: **128**
key	Yes	String	Key to be deleted Minimum: **1** Maximum: **256**

Request Parameters

Table 3-266 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. Minimum: **32** Maximum: **512**

Response Parameters

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.
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 processing succeeded.
400	Bad Request	Invalid request parameters.
500	Internal Server Error	Internal service error.

A.2 Error Codes

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.0001	invalid param error	invalid param error	Please check the input parameter
500	HSS.0041	Query host extend info error	Query host info error	Please check the input parameter

B Change History

Date	Change Description
2022-09-15	This issue is the first official release.

