Host Security Service

API Reference（Kuala Lumpur Region）

Date 2025-09-24

Contents

1 Before You Start

Overview

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

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

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

Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. Obtain the regions and endpoints from the enterprise administrator.

Basic Concepts

- Account

  An account has full access permissions for all the resources and cloud services. It can be used to reset user passwords and grant users 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 domain name, username, and password will be required for API authentication.

- Region

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

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

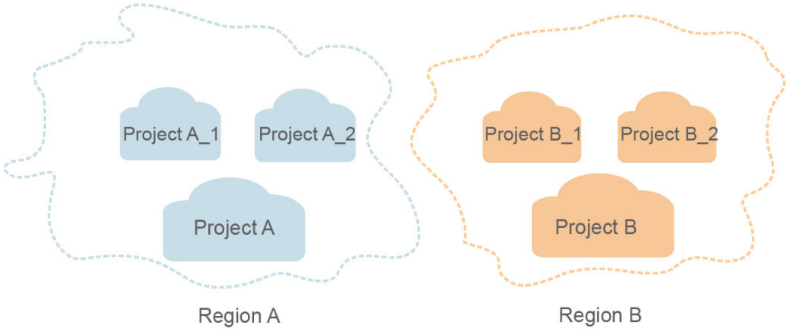
- Availability Zone (AZ)

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

- Project

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

  Figure 1-1 Project isolation model



- Enterprise Project

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

Limitations and Constraints

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

For more constraints, see API description.

2 Calling APIs

2.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

- **URI-scheme**:

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

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

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

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

NOTE

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

Request Methods

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

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

For example, in the case of the API used to , the request method is POST. The request is as follows:

Request Header

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

Common request header fields are as follows:

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

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

NOTE

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

For more information, see .

Request Body

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

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

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

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

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

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

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

2.2 Authentication

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

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

Token-based Authentication

NOTE

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

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

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

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

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

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

AK/SK-based Authentication

NOTE

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

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

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

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

NOTICE

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

2.3 Response

Status Code

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

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

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

Response Header

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

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

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

(Optional) Response Body

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

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

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

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

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

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

3 API Description

3.1 Intrusion Detection

3.1.1 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 3-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-2 Query Parameters

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

Parameter	Mandatory	Type	Description
container_id	No	String	Container ID

Request Parameters

Table 3-3 Request header parameters

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

Table 3-4 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
operate_event_list	Yes	Array of **OperateEventRequestInfo** objects	Operated event list

Parameter	Mandatory	Type	Description
event_white_rule_list	No	Array of **EventWhiteRuleListRequestInfo** objects	User-defined alarm whitelist

Table 3-5 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.

Table 3-6 EventDetailRequestInfo

Parameter	Mandatory	Type	Description
agent_id	No	String	Agent ID
process_pid	No	Integer	Process ID

Parameter	Mandatory	Type	Description
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
container_name	No	String	Container name

Table 3-7 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"
field_value	Yes	String	Whitelist field value
judge_type	Yes	String	Wildcard. The options are as follows: • "equal" • "contain"

Response Parameters

Status code: 200

success

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**.

3.1.2 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 3-8 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-9 Query Parameters

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

Parameter	Mandatory	Type	Description
event_types	No	Array of integers	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
handle_status	No	String	Status. Its value can be: • unhandled • handled
severity	No	String	Threat level. Its value can be: • Security • Low • Medium • High • Critical
category	Yes	String	Event category. Its value can be: • host: host security event • container: container security event
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.

Parameter	Mandatory	Type	Description
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.

Parameter	Mandatory	Type	Description
event_class_ids	No	Array of strings	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

Parameter	Mandatory	Type	Description
severity_list	No	Array of strings	Threat level. The options are as follows: • Security • Low • Medium • High • Critical
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
asset_value	No	String	Asset importance. The options are as follows: • important • common • test
tag_list	No	Array of strings	Event tag list, for example, ["hot event"].

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.
event_name	No	String	Alarm name
auto_block	No	Boolean	Whether to automatically block alarms.

Request Parameters

Table 3-10 Request header parameters

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

Response Parameters

Status code: 200

Table 3-11 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number

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

Table 3-12 EventManagementResponseInfo

Parameter	Type	Description
event_id	String	Event ID

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

Parameter	Type	Description
		• procdet_0001: Abnormal process behavior • procdet_0002: Process privilege escalation • procreport_0001: High-risk command • user_1001: Account change • user_1002: Unsafe account • vmescape_0001: Sensitive command executed on VM • vmescape_0002: Sensitive file accessed by virtualization process • vmescape_0003: Abnormal VM port access • webshell_0001: Web shell • network_1001: Mining • network_1002: DDoS attacks • network_1003: Malicious scanning • network_1004: Attack in sensitive areas • 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

Parameter	Type	Description
		• 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 • 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

Parameter	Type	Description
		• 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 • 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

Parameter	Type	Description
		• 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
agent_status	String	Agent status. Its value can be: • installed • not_installed • online • offline • install_failed • installing
protect_status	String	Protection status. Its value can be: • closed • opened

Parameter	Type	Description
asset_value	String	Asset importance. The options are as follows: ● important ● common ● test
attack_phase	String	Attack phase. Its value can be: ● reconnaissance ● weaponization ● delivery ● exploit ● installation ● command_and_control ● actions
attack_tag	String	Attack tag. Its value can be: ● attack_success ● attack_attempt ● attack_blocked ● abnormal_behavior ● collapsible_host ● system_vulnerability
occur_time	Integer	Occurrence time, accurate to milliseconds.
handle_time	Integer	Handling time, accurate to milliseconds.
handle_status	String	Processing status. Its value can be: ● unhandled ● handled
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

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

Table 3-13 EventDetailResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
process_pid	Integer	Process ID

Parameter	Type	Description
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 3-14 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

Parameter	Type	Description
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 3-15 EventProcessResponseInfo

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

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

Table 3-16 EventUserResponseInfo

Parameter	Type	Description
user_id	Integer	User UID
user_gid	Integer	User GID
user_name	String	User name
user_group_name	String	User group name
user_home_dir	String	User home directory
login_ip	String	User login IP address
service_type	String	Login service type
service_port	Integer	Login service port
login_mode	Integer	Login mode
login_last_time	Long	Last login time
login_fail_count	Integer	Number of failed login attempts
pwd_hash	String	Password hash
pwd_with_fuzzing	String	Masked password
pwd_used_days	Integer	Password age (days)
pwd_min_days	Integer	Minimum password validity period
pwd_max_days	Integer	Maximum password validity period
pwd_warn_left_days	Integer	Advance warning of password expiration (days)

Table 3-17 EventFileResponseInfo

Parameter	Type	Description
file_path	String	File path
file_alias	String	File alias
file_size	Integer	File size
file_mtime	Long	Time when a file was last modified
file_atime	Long	Time when a file was last accessed
file_ctime	Long	Time when the status of a file was last changed
file_hash	String	File hash
file_md5	String	File MD5

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

Example Requests

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

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

Example Responses

Status code: 200

Intrusion list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "attack_phase" : "exploit",
    "attack_tag" : "abnormal_behavior",
    "event_class_id" : "lgin_1002",
    "event_id" : "d8a12cf7-6a43-4cd6-92b4-aabf1e917",
    "event_name" : "different locations",
    "event_type" : 4004,
    "forensic_info" : {
      "country" : "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**.

3.1.3 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 3-18 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-19 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
hash	No	String	SHA256

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
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**.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-20 Request header parameters

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

Response Parameters

Status code: 200

Table 3-21 Response body parameters

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

Table 3-22 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"
field_value	String	Whitelist fields value
judge_type	String	Wildcard. The options are as follows: • "equal" • "contain"
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**.

3.2 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 3-23 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-24 Query Parameters

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

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	No	Integer	Number of records displayed on each page.
host_name	No	String	Server name
os_type	No	String	OS type. Its value can be: • Linux • Windows
host_ip	No	String	Server IP address
host_status	No	String	Server status. Its value can be: • If no parameter is transferred, it indicates all items. – ACTIVE – SHUTOFF
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.

Request Parameters

Table 3-25 Request header parameters

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

Response Parameters

Status code: 200

Table 3-26 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **ProtectionServer-Info** objects	Query the servers protected against ransomware.

Table 3-27 ProtectionServerInfo

Parameter	Type	Description
host_id	String	Server ID
agent_id	String	Agent ID
host_name	String	Server name
host_ip	String	EIP
private_ip	String	Private IP address
os_type	String	OS type. Its value can be: • Linux • Windows
os_name	String	OS name
host_status	String	Server status. The options are as follows: • ACTIVE • SHUTOFF
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.
agent_version	String	Agent version

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: • closed • opened: protection enabled
group_id	String	Server group ID
group_name	String	Server group name
protect_policy_id	String	Policy ID
protect_policy_name	String	Protection policy name
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
count_protect_event	Integer	Number of protection events
count_backuped	Integer	Existing backups
agent_status	String	Agent status
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
host_source	String	Indicates the server type. The options are as follows: • ecs : • outside: on-premises servers • workspace: cloud desktop

Parameter	Type	Description
vault_id	String	Vault ID
vault_name	String	Vault name
vault_size	Integer	Total capacity, in GB.
vault_used	Integer	Used capacity, in MB.
vault_allocated	Integer	Allocated bound server capacity, in GB.
vault_charging_mode	String	Repository mode, the value can be post_paid (pay-per-use).
vault_status	String	Vault status can be: • available • lock • frozen • deleting • error
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.
backup_policy_name	String	Backup policy name
backup_policy_enabled	Boolean	Whether the policy is enabled
resources_num	Integer	Bound servers

Table 3-28 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.

Parameter	Type	Description
error_description	String	Error description

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 3-29 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-30 Query Parameters

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

Request Parameters

Table 3-31 Request header parameters

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

Response Parameters

Status code: 200

Table 3-32 Response body parameters

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

Table 3-33 ProtectionPolicyInfo

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

Parameter	Type	Description
deploy_mode	String	Whether to enable honeypot protection. The options are as follows. By default, dynamic honeypot protection is disabled. • opened • closed
protection_directory	String	Protected directory
protection_type	String	Protected file type
exclude_directory	String	(Optional) excluded directory
runtime_detection_status	String	Whether to perform runtime checks. The options are as follows. Currently, it can only be disabled. This field is reserved. • opened • closed
runtime_detection_directory	String	Directory to be checked during running. To check all directories, set it to a slash (/). This field is reserved.
count_associated_server	Integer	Number of associated servers
operating_system	String	OS type
process_whitelist	Array of **TrustProcessInfo** objects	Process whitelist
default_policy	Integer	Indicates whether the policy is the default policy. The options are as follows: • 0: non-default policy • 1: default policy

Table 3-34 TrustProcessInfo

Parameter	Type	Description
path	String	Indicates the process path.
hash	String	Process hash

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 3-35 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-36 Query Parameters

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

Request Parameters

Table 3-37 Request header parameters

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

Table 3-38 Request body parameters

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

Parameter	Mandatory	Type	Description
protection_directory	Yes	String	Protected directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
protection_type	Yes	String	Protected file type
exclude_directory	No	String	(Optional) Excluded directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
agent_id_list	No	Array of strings	Associated server
operating_system	Yes	String	OS. Its value can be: • Windows • Linux
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
process_whitelist	No	Array of **TrustProcessInfo** objects	Process whitelist

Table 3-39 TrustProcessInfo

Parameter	Mandatory	Type	Description
path	No	String	Indicates the process path.
hash	No	String	Process hash

Response Parameters

Status code: 200

success

None

Example Requests

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

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

{
  "bait_protection_status" : "opened",
  "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 3-40 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-41 Query Parameters

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

Request Parameters

Table 3-42 Request header parameters

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

Table 3-43 Request body parameters

Parameter	Mandatory	Type	Description
operating_system	Yes	String	OS. Its value can be: • Windows • Linux
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.

Parameter	Mandatory	Type	Description
protection_policy_id	No	String	Protection policy ID. If you select an existing policy, this parameter is mandatory.
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.
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.
backup_policy_id	No	String	Backup policy ID
backup_cycle	No	**UpdateBackupPolicyRequestInfo1** object	Backup policy.
agent_id_list	Yes	Array of strings	IDs of agents where protection is enabled
host_id_list	Yes	Array of strings	IDs of servers where protection is enabled

Table 3-44 ProtectionProxyInfoRequestInfo

Parameter	Mandatory	Type	Description
policy_id	No	String	Policy ID. This parameter is optional for a new policy.
policy_name	No	String	Policy name. This parameter is mandatory when you create a protection policy.

Parameter	Mandatory	Type	Description
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.
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
protection_directory	No	String	Protected directory. This parameter is mandatory when you create a protection policy.
protection_type	No	String	Protection type. This parameter is mandatory when you create a protection policy.
exclude_directory	No	String	(Optional) Excluded directory
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
operating_system	No	String	OS. This parameter is mandatory when you create a protection policy. Its value can be: • Windows • Linux
process_whitelist	No	Array of **TrustProcessInfo** objects	Process whitelist

Table 3-45 TrustProcessInfo

Parameter	Mandatory	Type	Description
path	No	String	Indicates the process path.
hash	No	String	Process hash

Table 3-46 BackupResources

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

Table 3-47 ResourceInfo

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
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.

Table 3-48 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.

Parameter	Mandatory	Type	Description
operation_definition	No	**OperationDefinitionRequestInfo** object	Scheduling parameter.
trigger	No	**BackupTriggerRequestInfo1** object	Time scheduling rule for the policy.

Table 3-49 OperationDefinitionRequestInfo

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

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

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

Table 3-50 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 3-51 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'.

Response Parameters

Status code: 200

Ransomware protection enabled.

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 3-52 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-53 Query Parameters

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

Request Parameters

Table 3-54 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.

Table 3-55 Request body parameters

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

Response Parameters

Status code: 200

Ransomware protection disabled.

None

Example Requests

Disable ransomware protection for the server. The target server ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f, and the agent ID of the target server is c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	Ransomware protection disabled.

Error Codes

See **Error Codes**.

3.2.6 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 3-56 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-57 Query Parameters

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

Request Parameters

Table 3-58 Request header parameters

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

Response Parameters

Status code: 200

Table 3-59 Response body parameters

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

Table 3-60 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
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
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
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

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.
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.
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

Table 3-61 BackupTriggerInfo

Parameter	Type	Description
id	String	Scheduler ID
name	String	Scheduler name
type	String	Scheduler type. Currently, only time can be configured.
properties	**BackupTriggerPropertiesInfo** object	Scheduler attribute

Table 3-62 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.
start_time	String	Scheduler start time. Example: 2020-01-08 09:59:49

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 3-63 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-64 Query Parameters

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

Request Parameters

Table 3-65 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.

Table 3-66 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
operation_definition	No	**OperationDefinitionRequestInfo** object	Scheduling parameter.
trigger	No	**BackupTriggerRequestInfo** object	Time scheduling rule for the policy

Table 3-67 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

Parameter	Mandatory	Type	Description
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
month_backups	No	Integer	Maximum number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter is not affected by the maximum number of retained backup. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured. Minimum value: 0. Maximum value: 100
retention_duration_days	No	Integer	Duration of retaining a backup, in days. The maximum value is 99999. If the value is set to -1, backups will not be cleared even though the configured retention duration is exceeded. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum value: 1. Maximum value: 99999. Default value: -1

Parameter	Mandatory	Type	Description
timezone	No	String	Time zone where the user is located, for example, UTC +08:00. Set this parameter only after you have configured any of the parameters day_backups, week_backups, month_backups, and year_backups.
week_backups	No	Integer	Maximum number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured.
year_backups	No	Integer	Maximum number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is specified, timezone must be configured. Minimum value: 0. Maximum value: 100

Table 3-68 BackupTriggerRequestInfo

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

Table 3-69 BackupTriggerPropertiesRequestInfo

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

Response Parameters

Status code: 200

Table 3-70 Response body parameters

Parameter	Type	Description
error_code	Integer	Error code. If the operation is successful, 0 is returned.
error_description	String	Error description. If the operation is successful, success is returned.

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 3-71 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-72 Query Parameters

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

Request Parameters

Table 3-73 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.

Response Parameters

Status code: 200

Table 3-74 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of weak passwords
data_list	Array of **WeakPwdListInfoResponseInfo** objects	Weak password list

Table 3-75 WeakPwdListInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
public_ip	String	Server public IP address
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	List of accounts with weak passwords

Table 3-76 WeakPwdAccountInfoResponseInfo

Parameter	Type	Description
user_name	String	Name of accounts with weak passwords
service_type	String	Account type
duration	Integer	Validity period of a weak password, in days.

Example Requests

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

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

Example Responses

Status code: 200

Weak password check result

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

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 3-77 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-78 Query Parameters

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

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 the user token.

Response Parameters

Status code: 200

Table 3-80 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of password complexity policies
data_list	Array of **PwdPolicyInfoResponseInfo** objects	List of password complexity policy detection

Table 3-81 PwdPolicyInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID (displayed when the cursor is placed on a server name)
host_name	String	Server name
host_ip	String	Server IP address
public_ip	String	Server public IP address
min_length	Boolean	Minimum password length
uppercase_letter	Boolean	Uppercase letter
lowercase_letter	Boolean	Lowercase letter
number	Boolean	Digital
special_character	Boolean	Special characters

Parameter	Type	Description
suggestion	String	Modification suggestion

Example Requests

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

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

Example Responses

Status code: 200

Password complexity policy check report

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

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 3-82 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-83 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
check_name	No	String	Baseline name
group_id	No	String	Indicates the policy group ID.
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High
standard	No	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
host_id	No	String	Server ID
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

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 the user token.

Response Parameters

Status code: 200

Table 3-85 Response body parameters

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

Table 3-86 SecurityCheckInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline type
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
check_rule_num	Integer	Number of check items

Parameter	Type	Description
failed_rule_num	Integer	Number of risk items
host_num	Integer	Number of affected servers
scan_time	Long	Last scan time
check_type_desc	String	Baseline description

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 3-87 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID
check_name	Yes	String	Baseline name

Table 3-88 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried.
limit	No	Integer	Number of records on each page.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

Request Parameters

Table 3-89 Request header parameters

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

Response Parameters

Status code: 200

Table 3-90 Response body parameters

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_type	String	Baseline type
check_type_desc	String	Baseline description
check_rule_num	Integer	Total number of check items
failed_rule_num	Integer	Number of failed check items
passed_rule_num	Integer	Number of passed check items
ignored_rule_num	Integer	Number of ignored check items
host_num	Long	Number of affected servers

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 3-91 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID
check_name	Yes	String	Baseline name

Table 3-92 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
result_type	No	String	Result type. Its value can be: • safe: The item passed the check. • unhandled: The item failed the check and is not ignored. • ignored: The item failed the check but is ignored.
check_rule_name	No	String	Check item name. Fuzzy match is supported.
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High • Critical
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried.
limit	No	Integer	Number of items per page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

Request Parameters

Table 3-93 Request header parameters

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

Response Parameters

Status code: 200

Table 3-94 Response body parameters

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

Table 3-95 CheckRuleRiskInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline name
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
check_rule_name	String	Check item
check_rule_id	String	Check item ID

Parameter	Type	Description
host_num	Integer	Number of affected servers
scan_result	String	Detection result. Its value can be: • pass • failed
status	String	Status. Its value can be: • safe • ignored • unhandled • fixing • fix-failed • verifying
enable_fix	Integer	Indicates whether one-click repair is supported. 1: yes; 0: no.
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

Table 3-96 CheckRuleFixParamInfo

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

Example Requests

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

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

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

Example Responses

Status code: 200

checklist of the specified security configuration item

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_rule_id" : "1.1",
    "check_rule_name" : "Rule:Ensure that permissions on /etc/ssh/sshd_config are configured.",
    "check_type" : "SSH",
    "host_num" : 2,
    "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 3-97 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID
check_name	Yes	String	Baseline name

Table 3-98 Query Parameters

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

Request Parameters

Table 3-99 Request header parameters

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

Response Parameters

Status code: 200

Table 3-100 Response body parameters

Parameter	Type	Description
total_num	Long	Total number of data volume
data_list	Array of **SecurityCheckHostInfoResponseInfo** objects	Data list

Table 3-101 SecurityCheckHostInfoResponseInfo

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

Example Requests

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

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

Example Responses

Status code: 200

servers affected by the security configuration item

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

Status Codes

Status Code	Description
200	servers affected by the security configuration item

Error Codes

See **Error Codes**.

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

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-102 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-103 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
check_name	Yes	String	Baseline name
check_type	Yes	String	Baseline type
check_rule_id	Yes	String	Check item ID
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
host_id	No	String	Host ID

Request Parameters

Table 3-104 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.

Response Parameters

Status code: 200

Table 3-105 Response body parameters

Parameter	Type	Description
description	String	Description
reference	String	Scenario
audit	String	Audit description

Parameter	Type	Description
remediation	String	Modification suggestion
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	Test cases

Table 3-106 CheckRuleCheckCaseResponseInfo

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

Example Requests

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

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

Example Responses

Status code: 200

Configuration item check report

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

Status Codes

Status Code	Description
200	Configuration item check report

Error Codes

See **Error Codes**.

3.3.8 Ignoring, Unignoring, Repairing, or Verifying the Failed Configuration Check Items

Function

Ignore, unignore, repair, or verify the failed configuration check items.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-107 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID

Table 3-108 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**.
host_id	No	String	Server ID. If this parameter is not specified, all the servers of the user are queried.

Parameter	Mandatory	Type	Description
action	Yes	String	Action. • ignore • unignore • fix • verify

Request Parameters

Table 3-109 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token. It can be obtained by calling an IAM API. The value of X-Subject-Token in the response header is the user token.

Table 3-110 Request body parameters

Parameter	Mandatory	Type	Description
check_rules	No	Array of **CheckRuleKeyInfoRequestInfo** objects	Check item ID list

Table 3-111 CheckRuleKeyInfoRequestInfo

Parameter	Mandatory	Type	Description
check_name	No	String	Baseline name
check_rule_id	No	String	Check item ID
standard	No	String	Baseline standards. The options are as follows: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard

Parameter	Mandatory	Type	Description
fix_values	No	Array of CheckRuleFixValuesInfo objects	User-entered repair parameters of check items

Table 3-112 CheckRuleFixValuesInfo

Parameter	Mandatory	Type	Description
rule_param_id	No	Integer	Parameter ID of the check item
fix_value	No	Integer	Parameter value of the check item

Response Parameters

Status code: 200

Execution complete

None

Example Requests

- This API is used to ignore the configuration check items whose baseline name is SSH, check item ID is 1.11, check standard is cloud security practice standard, and enterprise project ID is xxx. This operation applies to all affected servers.

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

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

- This API is used to restore the configuration check items whose baseline name is SSH, check item ID is 1.11, check standard is cloud security practice standard, and enterprise project ID is xxx. This operation applies only to the server whose ID is xxx. The restoration parameters are as follows: Set the value of the repair item whose ID is 1 to 5 and the value of the repair item whose ID is 2 to 20.

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

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

```
    "fix_value" : 5
  }, {
    "rule_param_id" : 2,
    "fix_value" : 20
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Execution complete

Error Codes

See **Error Codes**.

3.4 Vulnerability Management

3.4.1 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 3-113 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-114 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise user ID
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
vul_id	No	String	Vulnerability ID
vul_name	No	String	Vulnerability name
limit	No	Integer	Number of records displayed on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
repair_priority	No	String	Fix Priority Critical High Medium Low
handle_status	No	String	description: |- Handling status. The options are as follows: - unhandled - handled
cve_id	No	String	Vulnerability ID
label_list	No	String	Vulnerability tag
status	No	String	Vulnerability status
asset_value	No	String	Asset importance important common test

Parameter	Mandatory	Type	Description
group_name	No	String	Server group name

Request Parameters

Table 3-115 Request header parameters

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

Response Parameters

Status code: 200

Table 3-116 Response body parameters

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

Table 3-117 VulInfo

Parameter	Type	Description
vul_name	String	Vulnerability name
vul_id	String	Vulnerability ID
label_list	Array of strings	Vulnerability tag
repair_necessity	String	Necessity to repair
severity_level	String	Vulnerability level
host_num	Integer	Number of affected servers
unhandle_host_num	Integer	Number of unhandled servers

Parameter	Type	Description
scan_time	Long	Last scan time
solution_detail	String	Solution
url	String	Vulnerability URL
description	String	Vulnerability description
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
host_id_list	Array of strings	Host list
cve_list	Array of **cve_list** objects	CVE list
patch_url	String	Patch address
repair_priority	String	Fix Priority Critical High Medium Low
hosts_num	**VulnerabilityHostNumberInfo** object	Affected server
repair_success_num	Integer	Number of successful repairs
fixed_num	Long	Number of repairs
ignored_num	Long	Number of ignored items
verify_num	Integer	Number of verifications

Table 3-118 cve_list

Parameter	Type	Description
cve_id	String	CVE ID
cvss	Float	CVSS score

Table 3-119 VulnerabilityHostNumberInfo

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

Example Requests

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

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

Example Responses

Status code: 200

vulnerability list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "description" : "It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, or possibly execute arbitrary code.",
    "host_id_list" : [ "caa958ad-a481-4d46-b51e-6861b8864515" ],
    "host_num" : 1,
    "scan_time" : 1661752185836,
    "severity_level" : "Critical",
    "repair_necessity" : "Critical",
    "solution_detail" : "To upgrade the affected software",
    "type" : "linux_vul",
    "unhandle_host_num" : 0,
    "url" : "https://ubuntu.com/security/CVE-2022-27405",
    "vul_id" : "USN-5528-1",
    "vul_name" : "USN-5528-1: FreeType vulnerabilities"
  } ]
}
```

Status Codes

Status Code	Description
200	vulnerability list

Error Codes

See **Error Codes**.

3.4.2 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 3-120 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID

Table 3-121 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**.
vul_id	Yes	String	Vulnerability ID
type	Yes	String	Vulnerability type • linux_vul: Linux vulnerability • windows_vul: Windows vulnerability • app_vul: application vulnerability • urgent_vul: emergency vulnerability -web_cms: Web-CMS vulnerability
host_name	No	String	Affected asset name
host_ip	No	String	IP address of the affected asset

Parameter	Mandatory	Type	Description
status	No	String	Vulnerability status. • vul_status_unfix: not fixed • vul_status_ignored: ignored – vul_status_verified: verification in progress – vul_status_fixing: The fix is in progress. – vul_status_fixed: The fix succeeded. – vul_status_reboot: The issue is fixed and waiting for restart. – vul_status_failed: The issue failed to be fixed. – vul_status_fix_after_reboot: Restart the server and try again.
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset
asset_value	No	String	Asset importance important common test
group_name	No	String	Server group name
handle_status	No	String	description: |- Handling status. The options are as follows: - unhandled - handled
severity_level	No	String	Risk level. The value can be Critical, High, Medium, or Low.
is_affect_business	No	Boolean	Indicates whether services are affected. The value can be y or n.

Request Parameters

Table 3-122 Request header parameters

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

Response Parameters

Status code: 200

Table 3-123 Response body parameters

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

Table 3-124 VulHostInfo

Parameter	Type	Description
host_id	String	Server ID

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.
host_name	String	Affected asset name
host_ip	String	IP address of the affected asset
agent_id	String	The corresponding agent ID of the server
cve_num	Integer	Vulnerability CVEs
cve_id_list	Array of strings	CVE list
status	String	Vulnerability status. • vul_status_unfix: not fixed • vul_status_ignored: ignored • vul_status_verified: verification in progress • vul_status_fixing: The fix is in progress. • vul_status_fixed: The fix succeeded. • vul_status_reboot: The issue is fixed and waiting for restart. • vul_status_failed: The issue failed to be fixed. • vul_status_fix_after_reboot: Restart the server and try again.
repair_cmd	String	Repair command

Parameter	Type	Description
app_path	String	Path of the application software (This field is available only for application vulnerabilities.)
region_name	String	Region
public_ip	String	Server public IP address
private_ip	String	Server private IP address
group_id	String	Server group ID
group_name	String	Server group name
os_type	String	Operating system (OS)
asset_value	String	Asset importance. The options are as follows: • important • common • test
is_affect_business	Boolean	Whether services are affected
first_scan_time	Long	First scan time
scan_time	Long	Scan time
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**.

3.4.3 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 3-125 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-126 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**.

Request Parameters

Table 3-127 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Table 3-128 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Operation type. • ignore • not_ignore: unignore • immediate_repair: fix • verify
remark	No	String	Remarks
select_type	No	String	Select vulnerabilities. • all_vul: Select all vulnerabilities. • all_host: Select all server vulnerabilities.
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
data_list	Yes	Array of **VulOperateInfo** objects	Vulnerability list
host_data_list	No	Array of **HostVulOperateInfo** objects	Vulnerability list in the server dimension

Parameter	Mandatory	Type	Description
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.
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.

Table 3-129 VulOperateInfo

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

Table 3-130 HostVulOperateInfo

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
vul_id_list	Yes	Array of strings	Vulnerability list

Table 3-131 custom_backup_hosts

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID
vault_id	No	String	Vault ID
backup_name	No	String	Backup name

Response Parameters

Status code: 200

successful response

None

Example Requests

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.4.4 Querying Vulnerability Information About a Server

Function

This API is used to query the vulnerability information about a server.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-132 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID.
host_id	Yes	String	Server ID.

Table 3-133 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**.
type	No	String	Vulnerability type. The default value is **linux_vul**. The options are as follows: ● linux_vul: Linux vulnerability ● windows_vul: Windows vulnerability ● app_vul: application vulnerability ● urgent_vul: emergency vulnerability -web_cms: Web-CMS vulnerability
vul_name	No	String	Vulnerability name
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
handle_status	No	String	Handling status. The options are as follows: - unhandled - handled

Parameter	Mandatory	Type	Description
status	No	String	Vulnerability status. The options are as follows: • 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.

Request Parameters

Table 3-134 Request header parameters

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

Response Parameters

Status code: 200

Table 3-135 Response body parameters

Parameter	Type	Description
total_num	Long	Total

Parameter	Type	Description
data_list	Array of **HostVulInfo** objects	List of vulnerabilities on a server

Table 3-136 HostVulInfo

Parameter	Type	Description
vul_name	String	Vulnerability name
vul_id	String	Vulnerability ID
label_list	Array of strings	Vulnerability tag list
repair_necessity	String	Repair urgency. The options are as follows: • immediate_repair: The problem must be rectified as soon as possible. • delay_repair: The problem can be fixed later. • not_needed_repair: The problem does not need to be fixed.
scan_time	Long	Latest scan time
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
app_list	Array of **app_list** objects	List of software affected by the vulnerability on the server

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.
solution_detail	String	Solution
url	String	URL
description	String	Vulnerability description
repair_cmd	String	Repair command
status	String	Vulnerability status • vul_status_unfix: not fixed • vul_status_ignored: ignored • vul_status_verified: verification in progress • vul_status_fixing: The fix is in progress. • vul_status_fixed: The fix succeeded. • vul_status_reboot : The issue is fixed and waiting for restart. • vul_status_failed: The issue failed to be fixed. • vul_status_fix_after_reboot: Restart the server and try again.
repair_success_num	Integer	Total times that the vulnerability is fixed by HSS on the entire network
cve_list	Array of **cve_list** objects	CVE list

Parameter	Type	Description
is_affect_business	Boolean	Whether services are affected
first_scan_time	Long	First scan time
app_name	String	Software
app_version	String	Version
app_path	String	Software path
version	String	ECS quota
support_restore	Boolean	Indicates whether data can be rolled back to the backup created when the vulnerability was fixed.

Table 3-137 app_list

Parameter	Type	Description
app_name	String	Software
app_version	String	Software Version
upgrade_version	String	Version that the software with vulnerability needs to be upgraded to
app_path	String	Path of the application software (This field is available only for application vulnerabilities.)

Table 3-138 cve_list

Parameter	Type	Description
cve_id	String	CVE ID
cvss	Float	CVSS score

Example Requests

Query the first 10 vulnerabilities on the server whose ID is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.

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

Example Responses

Status code: 200

List of vulnerabilities on a server


```
{
  "data_list" : [ {
    "app_list" : [ {
      "app_name" : "Apache Log4j API(Apache Log4j API)",
      "app_version" : "2.8.2",
      "upgrade_version" : "2.8.3",
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"
    }, {
      "app_name" : "Apache Log4j Core(Apache Log4j Core)",
      "app_version" : "2.8.2",
      "upgrade_version" : "2.8.3",
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"
    } ],
    "app_name" : "Apache Log4j API(Apache Log4j API)",
    "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar",
    "app_version" : "2.8.2",
    "cve_list" : [ {
      "cve_id" : "CVE-2021-45046",
      "cvss" : 9
    } ],
    "description" : "It was found that the fix for address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in some non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern, leading to information leakage and remote code execution in some environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for the message search mode and disabling the JNDI function by default.",
    "first_scan_time" : 1688956612533,
    "is_affect_business" : true,
    "label_list" : [ ],
    "repair_necessity" : "Critical",
    "scan_time" : 1690469489713,
    "severity_level" : "Critical",
    "repair_cmd" : "yum update tcpdump",
    "solution_detail" : "The official fixing suggestions for this vulnerability have been released. You can visit the following website and fix the vulnerability accordingly:\nhttps://logging.apache.org/log4j/2.x/security.html\nFor details about the patch for this vulnerability, visit the following website:\nhttps://www.oracle.com/security-alerts/cpujan2022.html\nFor details about unofficial fixing suggestions for this vulnerability, visit the following website:\nhttp://www.openwall.com/lists/oss-security/2021/12/14/4\nhttps://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html\nhttps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd\nhttp://www.openwall.com/lists/oss-security/2021/12/15/3\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf\nhttps://www.kb.cert.org/vuls/id/930724\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf\nhttps://www.debian.org/security/2021/dsa-5022\nhttps://www.oracle.com/security-alerts/alert-cve-2021-44228.html\nhttps://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032\nhttp://www.openwall.com/lists/oss-security/2021/12/18/1\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EOKPQGV24RRBBI4TBZUDQMM4MEH7MXCY/\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SIG7FZULMNK2XF6FZRU4VWYDQXNMUGAJ/\nThe vulnerability exploitation/POC of this vulnerability has been exposed. You can verify the vulnerability by referring to the following links:\nhttps://github.com/X1pe0/Log4J-Scan-Win\nhttps://github.com/cckuailong/Log4j_CVE-2021-45046\nhttps://github.com/BobTheShoplifter/CVE-2021-45046-Info\nhttps://github.com/tejas-nagchandi/CVE-2021-45046\nhttps://github.com/pravin-pp/log4j2-CVE-2021-45046\nhttps://github.com/mergebase/log4j-samples\nhttps://github.com/lukepasek/log4jjndilookupremove\nhttps://github.com/ludy-dev/cve-2021-45046\nhttps://github.com/lijiejie/log4j2_vul_local_scanner\nhttps://github.com/CaptanMoss/Log4Shell-Sandbox-Signature\nhttps://github.com/taise-hub/log4j-poc",
    "status" : "vul_status_unfix",
    "type" : "app_vul",
    "url" : "[\"https://www.oracle.com/security-alerts/cpujan2022.html\"]",
    "version" : "hss.version.wtp",
    "vul_id" : "HCVD-APP-CVE-2021-45046",
    "vul_name" : "CVE-2021-45046",
    "repair_success_num" : 3,
    "support_restore" : true
  } ],
  "total_num" : 31
}
```

Status Codes

Status Code	Description
200	List of vulnerabilities on a server

Error Codes

See **Error Codes**.

3.4.5 Creating a Vulnerability Scan Task

Function

This API is used to create a vulnerability scan task.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-139 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-140 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID of the tenant

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 an IAM API. The value of X-Subject-Token in the response header is the user token.

Table 3-142 Request body parameters

Parameter	Mandatory	Type	Description
manual_scan_type	No	Array of strings	Operation type. The options are as follows: -linux_vul: Linux vulnerability -windows_vul: windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability -urgent_vul: emergency vulnerability
batch_flag	No	Boolean	Specifies whether the operation is performed in batches. If the value is true, all supported servers are scanned.
range_type	No	String	Range of servers to be scanned. The options are as follows: -all_host: Scan all servers. You do not need to set agent_id_list for this type. -specific_host:
agent_id_list	No	Array of strings	Server list

Parameter	Mandatory	Type	Description
urgent_vul_id_list	No	Array of strings	Scan all ID list of emergency vulnerabilities. If this parameter is left blank, all emergency vulnerabilities are scanned. Its value can be: URGENT-CVE-2023-46604 Apache ActiveMQ Remote Code Execution Vulnerability URGENT-HSSVD-2020-1109 Elasticsearch Unauthorized Access Vulnerability URGENT-CVE-2022-26134 Atlassian Confluence OGNL Remote Code Execution Vulnerability (Cve-2022-26134) URGENT-CVE-2023-22515 Atlassian Confluence Data Center and Server Privilege Escalation Vulnerability (CVE-2023-22515) URGENT-CVE-2023-22518 Atlassian Confluence Data Center & Server Inappropriate Authorization Mechanism Vulnerability (CVE-2023-22518) URGENT-CVE-2023-28432 MinIO Information Disclosure Vulnerability (CVE-2023-28432) URGENT-CVE-2023-37582 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-37582) URGENT-CVE-2023-33246 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-33246) URGENT-CNVD-2023-02709 ZENTAO Project Management System Remote Command Execution Vulnerability (CNVD-2023-02709) URGENT-CVE-2022-36804 Atlassian Bitbucket Server and

Parameter	Mandatory	Type	Description
			Data Center Command Injection Vulnerability (CVE-2022-36804) URGENT-CVE-2022-22965 Spring Framework JDK >= 9 Remote Code Execution Vulnerability URGENT-CVE-2022-25845 fastjson <1.2.83 Remote Code Execution Vulnerability URGENT-CVE-2019-14439 Jackson-databind Remote Command Execution Vulnerability (CVE-2019-14439) URGENT-CVE-2020-13933 Apache Shiro Authentication Bypass Vulnerability (CVE-2020-13933) URGENT-CVE-2020-26217 XStream < 1.4.14 Remote Code Execution Vulnerability (CVE-2020-26217) URGENT-CVE-2021-4034 Linux Polkit Privilege Escalation Vulnerability (CVE-2021-4034) URGENT-CVE-2021-44228 Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228 and CVE-2021-45046) URGENT-CVE-2022-0847 Dirty Pipe - Linux Kernel Local Privilege Escalation Vulnerability (CVE-2022-0847)

Response Parameters

Status code: 200

Table 3-143 Response body parameters

Parameter	Type	Description
task_id	String	Detection task ID

Example Requests

Create an emergency vulnerability detection task whose agent_id is 0253edfd-30e7-439d-8f3f-17c54c997064 and vulnerability ID list is urgent_vul_id_list.

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

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

Example Responses

Status code: 200

Succeeded in manually detecting vulnerabilities

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

Status Codes

Status Code	Description
200	Succeeded in manually detecting vulnerabilities

Error Codes

See **Error Codes**.

3.4.6 Querying a Vulnerability Scan Policy

Function

This API is used to query a vulnerability scan policy.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-144 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-145 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**.

Request Parameters

Table 3-146 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token. It can be obtained by calling an IAM API. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 3-147 Response body parameters

Parameter	Type	Description
scan_period	String	Scan period • one_day • three_day • one_week
scan_vul_types	Array of strings	List of scanned vulnerability types
scan_range_type	String	Range of hosts to be scanned. The options are as follows: -all_host -specific_host

Parameter	Type	Description
host_ids	Array of strings	Specifies the host ID list. When scan_range_type is set to specific_host, this parameter indicates the list of hosts to be scanned.
total_host_num	Long	Total number of hosts that can be scanned for vulnerabilities
status	String	Scan policy status. The options are as follows: -open: enabled -close: disabled

Example Requests

Query the vulnerability scan policy whose project_id is 2b31ed520xxxxxxebedb6e57xxxxxxxx.

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

Example Responses

Status code: 200

Vulnerability scan policy

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

Status Codes

Status Code	Description
200	Vulnerability scan policy

Error Codes

See **Error Codes**.

3.4.7 Modifying a Vulnerability Scan Policy

Function

This API is used to modify a vulnerability scan policy.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-148 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-149 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise user ID. Note: The vulnerability scan policy affects the scan behavior of all servers under the tenant. Therefore, this parameter must be set to all_granted_eps if the multi-enterprise project is enabled.

Request Parameters

Table 3-150 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token. It can be obtained by calling an IAM API. The value of X-Subject-Token in the response header is the user token.

Table 3-151 Request body parameters

Parameter	Mandatory	Type	Description
scan_period	Yes	String	Scan period • one_day • three_day • one_week
scan_range_type	Yes	String	Range of hosts to be scanned. The options are as follows: -all_host -specific_host
host_ids	No	Array of strings	Specifies the host ID list. This parameter is mandatory when scan_range_type is set to specific_host.
scan_vul_types	No	Array of strings	List of scanned vulnerability types
status	Yes	String	Scan policy status. The options are as follows: -open: enabled -close: disabled

Response Parameters

Status code: 200

successful response

None

Example Requests

Modify a vulnerability scan policy. The scan period is daily, scan scope is specified host, host ID is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, and policy status is enabled.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.4.8 Querying the Vulnerability Scan Tasks

Function

This API is used to query the vulnerability scan tasks.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-152 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID.

Table 3-153 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.
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

Parameter	Mandatory	Type	Description
scan_type	No	String	Type of a scan task. The options are as follows: -manual -schedule
task_id	No	String	Scan task ID.
min_start_time	No	Long	Minimum start time of a scan task.
max_start_time	No	Long	Maximum start time of a scan task.

Request Parameters

Table 3-154 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token. It can be obtained by calling an IAM API. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 3-155 Response body parameters

Parameter	Type	Description
total_num	Long	Total number
data_list	Array of **VulScanTaskInfo** objects	Vulnerability scan tasks

Table 3-156 VulScanTaskInfo

Parameter	Type	Description
id	String	Task ID

Parameter	Type	Description
scan_type	String	Type of a scan task. The options are as follows: -manual -schedule
start_time	Long	Start time of a scan task.
end_time	Long	End time of a scan task.
scan_vul_types	Array of strings	List of vulnerability types scanned by the task
status	String	Execution status of a scan task. The options are as follows: -running -finished
scanning_host_num	Integer	Number of servers are being scanned
success_host_num	Integer	Number of servers have been successfully scanned
failed_host_num	Integer	Number of servers fail to be scanned

Example Requests

Query information about the vulnerability scan task whose type is manual scan and task_id is 195db604-2008-4e8b-a49e-389ab0175beb. By default, 10 records on the first page are queried.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	Vulnerability scan tasks

Error Codes

See **Error Codes**.

3.4.9 Querying the List of Servers Corresponding to a Vulnerability Scan Task

Function

This API is used to query the list of servers corresponding to a vulnerability scan task.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-157 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID
task_id	Yes	String	Task ID

Table 3-158 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**.
limit	No	Integer	Number of records displayed on each page.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
scan_status	No	String	Scan status of the server. The options are as follows: • scanning • success • failed

Request Parameters

Table 3-159 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token. It can be obtained by calling an IAM API. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 3-160 Response body parameters

Parameter	Type	Description
total_num	Long	Total number
data_list	Array of **VulScanTaskHostInfo** objects	Indicates the list of servers corresponding to a vulnerability scan task.

Table 3-161 VulScanTaskHostInfo

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Server name
public_ip	String	EIP
private_ip	String	Private IP address
asset_value	String	Asset importance. The options are as follows: • important • common • test
scan_status	String	Scan status of the server. The options are as follows: -scanning -success -failed:

Parameter	Type	Description
failed_reasons	Array of **failed_reasons** objects	List of scan failure causes

Table 3-162 failed_reasons

Parameter	Type	Description
vul_type	String	Type of the vulnerability that fails to be scanned. The options are as follows: -linux_vul: Linux vulnerability -windows_vul: windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability
failed_reason	String	Cause of the scanning failure.

Example Requests

This API is used to query details of vulnerability scan task whose ID is 2b31ed520xxxxxxebedb6e57xxxxxxxx. The list of failed servers and failure causes are displayed. By default, 10 servers on the first page are queried.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	Indicates the list of servers corresponding to a vulnerability scan task.

Error Codes

See **Error Codes**.

3.4.10 Querying Vulnerability Management Statistics

Function

This API is used to query vulnerability management statistics.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/vulnerability/statistics

Table 3-163 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-164 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**.

Request Parameters

Table 3-165 Request header parameters

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

Response Parameters

Status code: 200

Table 3-166 Response body parameters

Parameter	Type	Description
need_urgent_repair	Integer	Number of vulnerabilities that need to be fixed urgently
unrepair	Integer	Number of vulnerabilities not fixed
existed_vul_hosts	Integer	Number of servers with vulnerabilities
today_handle	Integer	Vulnerabilities handled today
all_handle	Integer	Total handled vulnerabilities
supported	Integer	Supported vulnerabilities
vul_library_update_time	Long	Vulnerability library updated

Example Requests

Query vulnerability statistics whose project_id is 2b31ed520xxxxxxebedb6e57xxxxxxxx.

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

Example Responses

Status code: 200

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

Status Codes

Status Code	Description
200	

Error Codes

See **Error Codes**.

3.5 Tag Management

3.5.1 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 3-167 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID
resource_type	Yes	String	Resource type. The value is hss.
resource_id	Yes	String	Resource ID

Request Parameters

Table 3-168 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.

Table 3-169 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **ResourceTagInfo** objects	Tag List
sys_tags	No	Array of **ResourceTagInfo** objects	Tag List

Table 3-170 ResourceTagInfo

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

Response Parameters

Status code: 200

success

None

Example Requests

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

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.5.2 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 3-171 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID
resource_type	Yes	String	Resource type. The value is hss.
resource_id	Yes	String	Resource ID
key	Yes	String	Key to be deleted

Request Parameters

Table 3-172 Request header parameters

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

Response Parameters

Status code: 200

success

None

Example Requests

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.6 Quota Management

3.6.1 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 3-173 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-174 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**.
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
charging_mode	No	String	Billing mode. Its value can be: • on_demand: pay-per-use

Request Parameters

Table 3-175 Request header parameters

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

Response Parameters

Status code: 200

Table 3-176 Response body parameters

Parameter	Type	Description
data_list	Array of **ResourceQuotasInfo** objects	Quota statistics list

Table 3-177 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
total_num	Integer	Total quotas
used_num	Integer	Used quotas
available_num	Integer	Total quotas
available_resources_list	Array of **AvailableResourceIdsInfo** objects	Available resource list

Table 3-178 AvailableResourceIdsInfo

Parameter	Type	Description
resource_id	String	Resource ID
current_time	String	Current time

Parameter	Type	Description
shared_quota	String	Whether quotas are shared. Its value can be: • shared • unshared

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**.

3.6.2 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 3-179 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

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**.
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
category	No	String	Type. Its value can be: • host_resource • container_resource
quota_status	No	String	Quota status. It can be: • QUOTA_STATUS_NORMAL – QUOTA_STATUS_EXPIRED – QUOTA_STATUS_FREEZE

Parameter	Mandatory	Type	Description
used_status	No	String	Usage status. It can be: • USED_STATUS_IDLE • USED_STATUS_USED
host_name	No	String	Server name
resource_id	No	String	Resource ID
charging_mode	No	String	Billing mode. Its value can be: • on_demand: pay-per-use
limit	No	Integer	Number of items per page
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

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.

Response Parameters

Status code: 200

Table 3-182 Response body parameters

Parameter	Type	Description
packet_cycle_num	Integer	Quota
on_demand_num	Integer	Pay-per-Use quotas
used_num	Integer	Used quotas
idle_num	Integer	Idle quotas

Parameter	Type	Description
normal_num	Integer	Normal quotas
expired_num	Integer	Expired quotas
freeze_num	Integer	Frozen quotas
quota_statistics_list	Array of **QuotaStatistics-ResponseInfo** objects	Quota statistics list
total_num	Integer	Total number
data_list	Array of **QuotaResourcesResponseInfo** objects	Quota list

Table 3-183 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
total_num	Integer	Total number

Table 3-184 QuotaResourcesResponseInfo

Parameter	Type	Description
resource_id	String	Resource ID of an HSS quota

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
quota_status	String	Quota status. It can be: • normal • expired • freeze
used_status	String	Usage status. Its value can be: • idle • used
host_id	String	Server ID
host_name	String	Server name
charging_mode	String	Billing mode. The value can be: • on_demand: pay-per-use
tags	Array of **TagInfo** objects	Tag
expire_time	Long	Expiration time. The value -1 indicates that the resource will not expire.
shared_quota	String	Whether quotas are shared. Its value can be: • shared • unshared
enterprise_project_id	String	Enterprise project ID
enterprise_project_name	String	Enterprise project name

Table 3-185 TagInfo

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

Example Requests

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

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

Example Responses

Status code: 200

Quota details

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

3.7 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 3-186 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-187 Query Parameters

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

Parameter	Mandatory	Type	Description
group_id	No	String	Policy group ID

Request Parameters

Table 3-188 Request header parameters

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

Response Parameters

Status code: 200

Table 3-189 Response body parameters

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

Table 3-190 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

Parameter	Type	Description
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 3-191 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-192 Query Parameters

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

Request Parameters

Table 3-193 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.

Table 3-194 Request body parameters

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

Response Parameters

Status code: 200

success

None

Example Requests

Deploy a server protection policy. The target server ID is 15462c0e-32c6-4217-a869-bbd131a00ecf, and the target policy ID is f671f7-2677-4705-a320-de1a62bff306.

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.8 Event Management

3.8.1 Querying the List of Blocked IP Addresses

Function

This API is used to query the list of blocked IP addresses.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-195 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-196 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.
last_days	No	Integer	Number of days to be queried. This parameter is manually exclusive with **begin_time** and **end_time**.
host_name	No	String	Server name
src_ip	No	String	Attack source IP address
intercept_status	No	String	Interception status. The options are as follows: • intercepted • canceled (unblocked) • cancelling
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**.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-197 Request header parameters

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

Response Parameters

Status code: 200

Table 3-198 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **BlockedIpResponseInfo** objects	Blocked IP address details

Table 3-199 BlockedIpResponseInfo

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Server name
src_ip	String	Attack source IP address
login_type	String	Login type. The options are as follows: • "mysql" # MySQL service • "rdp" # RDP service • "ssh" # SSH service • "vsftp" # vsftp service
intercept_num	Integer	Blocks

Parameter	Type	Description
intercept_status	String	Interception status. The options are as follows: • intercepted • canceled (unblocked) • cancelling
block_time	Long	Interception start time, in milliseconds.
latest_time	Long	Latest interception time, in milliseconds.

Example Requests

Query the first 10 blocked IP addresses.

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

Example Responses

Status code: 200

Blocked IP address list

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

Status Codes

Status Code	Description
200	Blocked IP address list

Error Codes

See **Error Codes**.

3.8.2 Unblocking a Blocked IP Address

Function

This API is used to unblock a blocked IP address.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-201 Query Parameters

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

Request Parameters

Table 3-202 Request header parameters

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

Table 3-203 Request body parameters

Parameter	Mandatory	Type	Description
data_list	No	Array of **BlockedIpRequestInfo** objects	List of IP addresses to be unblocked

Table 3-204 BlockedIpRequestInfo

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
src_ip	Yes	String	Attack source IP address
login_type	Yes	String	Login type. The options are as follows: • "mysql" # MySQL service • "rdp" # RDP service • "ssh" # SSH service • "vsftp" # vsftp service

Response Parameters

Status code: 200

successful response

None

Example Requests

Remove the blocked IP address 192.168.1.6 of the host af423efds-214432fgsdaf-gfdsaggbvf in SSH mode.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.8.3 Querying the List of Isolated Files

Function

This API is used to query the list of isolated files.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-205 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-206 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.
last_days	No	Integer	Number of days to be queried. This parameter is manually exclusive with **begin_time** and **end_time**.
host_name	No	String	Server name

Parameter	Mandatory	Type	Description
isolation_status	No	String	Isolation status. The options are as follows: • isolated • restored • isolating • restoring
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**.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-207 Request header parameters

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

Response Parameters

Status code: 200

Table 3-208 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **IsolatedFileResponseInfo** objects	Isolated file details

Table 3-209 IsolatedFileResponseInfo

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Server name
file_hash	String	File hash
file_path	String	File path
isolation_status	String	Isolation status. The options are as follows: • isolated • restored • isolating • restoring
file_attr	String	File attribute
update_time	Integer	Update time, in milliseconds

Example Requests

Query the first 10 isolated files.

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

Example Responses

Status code: 200

Isolated files list

```
{
  "data_list" : [ {
    "file_attr" : "0",
    "file_hash" : "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path" : "C:\\Users\\Public\\Public Docker\\system32.exe",
    "host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
    "host_name" : "ecs-wi-800211",
    "isolation_status" : "isolated",
    "update_time" : 1698304933717
  } ],
  "total_num" : 1
}
```

Status Codes

Status Code	Description
200	Isolated files list

Error Codes

See **Error Codes**.

3.8.4 Restoring Isolated Files

Function

This API is used to restore isolated files.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-210 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

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.

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.

Table 3-213 Request body parameters

Parameter	Mandatory	Type	Description
data_list	No	Array of **IsolatedFileRequestInfo** objects	List of files to be restored

Table 3-214 IsolatedFileRequestInfo

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
file_hash	No	String	File hash
file_path	No	String	File path
file_attr	No	String	File attribute

Response Parameters

Status code: 200

successful response

None

Example Requests

Cancel the isolation of the file C:\Users\Public\test.exe on host 5a41ca47-8ea7-4a65-a8fb-950d03d8638e.

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

{
  "data_list" : [ {
    "file_attr" : "0",
    "file_hash" : "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path" : "C:\\Users\\Public\\test.exe",
    "host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.9 Asset Management

3.9.1 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 3-215 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-216 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project
host_id	No	String	host id

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

Request Parameters

Table 3-217 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-218 Response body parameters

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

Example Requests

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

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

Example Responses

Status code: 200

Asset statistic info

```
{
  "account_num" : 5,
  "port_num" : 5,
  "process_num" : 5,
  "app_num" : 5,
  "auto_launch_num" : 5,
  "web_framework_num" : 5,
  "web_site_num" : 5,
  "jar_package_num" : 5,
  "kernel_module_num" : 5,
  "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**.

3.9.2 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 3-219 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-220 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.
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-221 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-222 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of accounts

Parameter	Type	Description
data_list	Array of **UserStatisticIn-foResponseInfo** objects	Account statistics list

Table 3-223 UserStatisticInfoResponseInfo

Parameter	Type	Description
user_name	String	Account name
num	Integer	Number of accounts

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**.

3.9.3 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 3-224 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-225 Query Parameters

Parameter	Mandatory	Type	Description
port	No	Integer	Port number, which is used for exact match.
port_string	No	String	Port string, which is used for fuzzy match.
type	No	String	Port type
enterprise_project_id	No	String	Enterprise project
sort_key	No	String	Sort key. Currently, sorting by port number is supported.
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-226 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-227 Response body parameters

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

Table 3-228 PortStatisticResponseInfo

Parameter	Type	Description
port	Integer	Port number
type	String	Type
num	Integer	Number of ports
status	String	Risk type: danger or unknown

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**.

3.9.4 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 3-229 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-230 Query Parameters

Parameter	Mandatory	Type	Description
path	No	String	Path
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10

Parameter	Mandatory	Type	Description
offset	No	Integer	Default value: 0
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-231 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-232 Response body parameters

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

Table 3-233 ProcessStatisticResponseInfo

Parameter	Type	Description
path	String	Process name
num	Integer	Number of processes

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**.

3.9.5 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 3-234 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-235 Query Parameters

Parameter	Mandatory	Type	Description
app_name	No	String	Software name

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10
offset	No	Integer	Offset, which is the number of pages multiplied by the number of records displayed on each page.
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-236 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-237 Response body parameters

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

Table 3-238 AppStatisticResponseInfo

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

Example Requests

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

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

Example Responses

Status code: 200

Number of servers having the software

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

Status Codes

Status Code	Description
200	Number of servers having the software

Error Codes

See **Error Codes**.

3.9.6 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 3-239 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-240 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Auto-started item name
type	No	String	Auto-started item type
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0

Request Parameters

Table 3-241 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-242 Response body parameters

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

Table 3-243 AutoLaunchStatisticsResponseInfo

Parameter	Type	Description
name	String	Auto-started item name
type	String	Auto-started item type
num	Integer	Quantity

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**.

3.9.7 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 3-244 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-245 Query Parameters

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

Request Parameters

Table 3-246 Request header parameters

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

Response Parameters

Status code: 200

Table 3-247 Response body parameters

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

Table 3-248 UserResponseInfo

Parameter	Type	Description
agent_id	String	agent_id
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
user_name	String	Username
login_permission	Boolean	Whether the user has the login permission
root_permission	Boolean	Whether the user has root permissions
user_group_name	String	User group name
user_home_dir	String	User home directory
shell	String	User startup shell
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond.
recent_scan_time	Long	Latest scan time
container_id	String	Container ID
container_name	String	Container name

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**.

3.9.8 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 3-249 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-250 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
host_name	No	String	Server name
host_ip	No	String	Server IP address
port	No	Integer	Port number
type	No	String	Port type
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
category	No	String	Type. The default value is host. The options are as follows: • host • container

Request Parameters

Table 3-251 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-252 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **PortResponseInfo** objects	Port information list

Table 3-253 PortResponseInfo

Parameter	Type	Description
host_id	String	Server ID
laddr	String	Listening IP address
status	String	Port status. • normal • "danger" • "unknow"
port	Integer	Port number
type	String	Type
pid	Integer	Process ID
path	String	Program file

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**.

3.9.9 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 3-254 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-255 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_name	No	String	Server name
app_name	No	String	Software name
host_ip	No	String	Server IP address
version	No	String	Version number
install_dir	No	String	Installation directory
enterprise_project_id	No	String	Enterprise project
limit	No	Integer	Default value: 10

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

Request Parameters

Table 3-256 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-257 Response body parameters

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

Table 3-258 AppResponseInfo

Parameter	Type	Description
agent_id	String	agent_id
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
app_name	String	Software name
version	String	Version number

Parameter	Type	Description
update_time	Long	Update time
recent_scan_time	Long	Latest scan time
container_id	String	Container ID
container_name	String	Container name

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**.

3.9.10 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 3-259 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-260 Query Parameters

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

Request Parameters

Table 3-261 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-262 Response body parameters

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

Table 3-263 AutoLauchResponseInfo

Parameter	Type	Description
agent_id	String	agent_id
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
name	String	Auto-started item name
type	Integer	Auto-started item type
path	String	Path
hash	String	File hash
run_user	String	User who starts the execution
recent_scan_time	Long	Latest scan time

Example Requests

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

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

Example Responses

Status code: 200

auto launch list

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "9e742932bff2894e3d0869d03989b05cefb27a6cbc201d98c4465296xxxxxxxx",
    "host_id" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "host_name" : "name",
    "host_ip" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "name" : "S12hostguard",
    "type" : 0,
    "path" : "/etc/hostguard",
```

```
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxx",
    "run_user" : "user",
    "recent_scan_time" : 1668240858425
  } ]
}
```

Status Codes

Status Code	Description
200	auto launch list

Error Codes

See **Error Codes**.

3.9.11 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 3-264 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-265 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Username
host_id	No	String	Server ID
root_permission	No	Boolean	Whether the user has root permissions
host_name	No	String	Server name
private_ip	No	String	Server private IP address

Parameter	Mandatory	Type	Description
change_type	No	String	Change type. Its value can be: • ADD • DELETE • MODIFY
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
enterprise_project_id	No	String	Enterprise project
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-266 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-267 Response body parameters

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

Table 3-268 UserChangeHistoryResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID

Parameter	Type	Description
change_type	String	Change type. Its value can be: • ADD • DELETE • MODIFY
host_id	String	Server ID
host_name	String	Server name
private_ip	String	Server private IP address
login_permission	Boolean	Whether the user has the login permission
root_permission	Boolean	Whether the user has root permissions
user_group_name	String	User group name
user_home_dir	String	User home directory
shell	String	User startup shell
user_name	String	Account name
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond.
recent_scan_time	Long	Change time

Example Requests

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

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

Example Responses

Status code: 200

account change history

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxece69",
    "private_ip" : "192.168.0.1",
    "host_name" : "test",
    "user_home_dir" : "/test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
```

```
  "user_group_name" : "bin",
  "user_name" : "bin",
  "change_type" : "test"
 } ]
}
```

Status Codes

Status Code	Description
200	account change history

Error Codes

See **Error Codes**.

3.9.12 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 3-269 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-270 Query Parameters

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

Parameter	Mandatory	Type	Description
variation_type	No	String	Change type. Its value can be: • add • delete • modify
enterprise_project_id	No	String	Enterprise project
sort_key	No	String	Sort key
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-271 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-272 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **AppChangeResponseInfo** objects	Account change history

Table 3-273 AppChangeResponseInfo

Parameter	Type	Description
agent_id	String	agent_id
variation_type	String	Type of change. • add • delete • modify
host_id	String	host_id
app_name	String	Software name
host_name	String	ECS name
host_ip	String	Server IP address
version	String	Version number
update_time	Long	Update time
recent_scan_time	Long	Change time

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**.

3.9.13 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 3-274 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-275 Query Parameters

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

Parameter	Mandatory	Type	Description
type	No	Integer	Auto-started item type. • 0: auto-started service • 1: scheduled task • 2: Preload the dynamic library. • 3: Run registry key • 4: startup folder
variation_type	No	String	Change type. Its value can be: • add • delete • modify
enterprise_project_id	No	String	Enterprise project
sort_key	No	String	Sort key
sort_dir	No	String	Whether to sort data in ascending or descending order. Default value: asc
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-276 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-277 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **AutoLaunchChangeResponseInfo** objects	Account change history

Table 3-278 AutoLaunchChangeResponseInfo

Parameter	Type	Description
agent_id	String	agent_id
variation_type	String	Type of change. • add • delete • modify
type	Integer	Auto-started item type
host_id	String	host_id
host_name	String	ECS name
host_ip	String	Server IP address
path	String	Path
hash	String	File hash
run_user	String	User who starts the execution
name	String	Auto-started item name
recent_scan_time	Long	Last update time

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**.

3.9.14 Asset Fingerprints - Process - Server List

Function

Servers or containers having the process

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-279 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-280 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project

Parameter	Mandatory	Type	Description
host_name	No	String	Server name
host_ip	No	String	Server IP address
path	No	String	Process path
category	No	String	Type. The default value is host. The options are as follows: • host • container
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0

Request Parameters

Table 3-281 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-282 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of server statistics
data_list	Array of **ProcessesHostResponseInfo** objects	Server statistics list

Table 3-283 ProcessesHostResponseInfo

Parameter	Type	Description
hash	String	File hash
host_ip	String	Server IP address
host_name	String	Server name

Parameter	Type	Description
launch_params	String	Startup parameter
launch_time	Long	Start time
process_path	String	Process path
process_pid	Integer	PID of the process
run_permission	String	File permission
container_id	String	Container ID
container_name	String	Container name

Example Requests

The first 10 servers whose process path is /usr/bin/bash are queried by default.

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

Example Responses

Status code: 200

Servers having the process


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


Status Codes

Status Code	Description
200	Servers having the process

Error Codes

See **Error Codes**.

3.9.15 Asset Fingerprints - Port - Server List

Function

Servers or containers having the port

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-284 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-285 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project
host_name	No	String	Server name
host_ip	No	String	Server IP address
port	Yes	Integer	Port number
type	No	String	Port type
category	No	String	Type. The default value is host. The options are as follows: • host • container
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0

Request Parameters

Table 3-286 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	iam token

Response Parameters

Status code: 200

Table 3-287 Response body parameters

Parameter	Type	Description
total_num	Integer	Total servers
data_list	Array of **PortHostResponseInfo** objects	Server information list

Table 3-288 PortHostResponseInfo

Parameter	Type	Description
container_id	String	Image ID
host_id	String	Server ID
host_ip	String	Server IP address
host_name	String	Server name
laddr	String	Listening IP address
path	String	Program file path
pid	Integer	pid
port	Integer	Port
status	String	Status
type	String	Type
container_name	String	Container name
agent_id	String	agent id

Example Requests

The first 10 servers whose port number is 22 are queried by default.

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

Example Responses

Status code: 200

Servers having the port

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

Status Codes

Status Code	Description
200	Servers having the port

Error Codes

See **Error Codes**.

3.9.16 Querying the Middleware List

Function

This API is used to query the middleware list. The server list can be queried by middleware name.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/asset/midwares

Table 3-289 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-290 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID of the tenant
file_name	No	String	JAR file name
category	No	String	Type. Its value can be: • host • container
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0

Request Parameters

Table 3-291 Request header parameters

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

Response Parameters

Status code: 200

Table 3-292 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of JAR packages

Parameter	Type	Description
data_list	Array of **JarPackageStatisticsResponseInfo** objects	JAR package statistics list

Table 3-293 JarPackageStatisticsResponseInfo

Parameter	Type	Description
file_name	String	JAR file name
num	Integer	Total number of JAR packages

Example Requests

The first 10 middleware records whose name is rt.jar and type is host are queried by default.

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

Example Responses

Status code: 200

JarPackage statistics

```
{
  "data_list" : [ {
    "file_name" : "rt.jar",
    "num" : 18
  } ],
  "total_num" : 1
}
```

Status Codes

Status Code	Description
200	JarPackage statistics

Error Codes

See **Error Codes**.

3.9.17 Querying the Server List of a Specified Middleware

Function

This API is used to query the server list of a specified middleware. You can query the middleware server list by its middleware name.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-294 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-295 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID of the tenant
file_name	Yes	String	File name
category	No	String	Type. Its value can be: • host • container
host_name	No	String	Server name
host_ip	No	String	Server IP address
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-296 Request header parameters

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

Response Parameters

Status code: 200

Table 3-297 Response body parameters

Parameter	Type	Description
total_num	Integer	Total
data_list	Array of **JarPackageHostInfo** objects	Server list

Table 3-298 JarPackageHostInfo

Parameter	Type	Description
agent_id	String	agent_id
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address
file_name	String	JAR package name
name	String	JAR package name (without suffix)
catalogue	String	JAR package type
file_type	String	JAR package suffix
version	String	JAR package version
path	String	JAR package path
hash	String	JAR package hash

Parameter	Type	Description
size	Integer	JAR package size
uid	Integer	uid
gid	Integer	gid
mode	String	File permissions
pid	Integer	Process ID
proc_path	String	Process executable file path
container_id	String	Container instance ID
container_name	String	Container name
package_path	String	Package path
is_embedded	Integer	Whether to display a nested package
record_time	Long	Scan time

Example Requests

The first 10 servers whose middleware name is log4j-core-2.8.2.jar and type is host are queried by default.

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

Example Responses

Status code: 200

ListJarPackageHostInfo


```
{
  "data_list" : [ {
    "agent_id" : "2d0fe7824005bf001220ad9d892e86f8af44a7d3608dab11165008ce439d3583",
    "catalogue" : "util",
    "container_id" : "",
    "file_name" : "rt.jar",
    "file_type" : "jar",
    "gid" : 0,
    "hash" : "04bf14e3b1da55d95561ca78cb29caa909410051dbe047e91ad6f5c1dedb8d6d",
    "host_id" : "103ed820-62e5-4754-b0f8-3e47b6dd49d2",
    "host_ip" : "192.168.1.76",
    "host_name" : "Do not delete the test.",
    "mode" : "-rw-------",
    "name" : "Java Runtime Environment",
    "path" : "/CloudResetPwdUpdateAgent/depend/jre/lib/rt.jar",
    "pid" : 1614,
    "proc_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
    "record_time" : 1690513169986,
    "uid" : 0,
    "version" : "1.8.0_252",
    "size" : 128,
    "container_name" : "aaaa",
    "package_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
    "is_embedded" : 0
```

```
 } ],
 "total_num" : 1
}
```

Status Codes

Status Code	Description
200	ListJarPackageHostInfo

Error Codes

See **Error Codes**.

3.10 Web Tamper Protection

3.10.1 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 3-299 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-300 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project
host_name	No	String	Server name
host_id	No	String	Cloud server ID
public_ip	No	String	EIP

Parameter	Mandatory	Type	Description
private_ip	No	String	Private IP address
group_name	No	String	Server group name
os_type	No	String	OS type. Its value can be: • linux • windows
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled
agent_status	No	String	Agent status. Its value can be: • not_installed: The agent is not installed. • online: The agent is online. • offline: The agent is offline.
limit	No	Integer	Default value: 10
offset	No	Integer	Default value: 0

Request Parameters

Table 3-301 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token

Response Parameters

Status code: 200

Table 3-302 Response body parameters

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

Table 3-303 WtpProtectHostResponseInfo

Parameter	Type	Description
host_name	String	Server name
host_id	String	Cloud server ID
public_ip	String	EIP
private_ip	String	Private IP address
group_name	String	Server group name
os_bit	String	OS bit version
os_type	String	OS (linux or windows)
protect_status	String	Protection status. Its value can be: ● closed ● opened
rasp_protect_status	String	Dynamic WTP status. ● closed ● opened
anti_tampering_times	Long	Number of blocked tampering attacks
detect_tampering_times	Long	Number of detected tampering attacks
last_detect_time	Long	Last scan time
scheduled_shutdown_status	String	Status of scheduled protection. ● opened ● closed
agent_status	String	Agent status. ● not_installed: The agent is not installed. ● online: The agent is online. ● offline: The agent is offline.

Example Requests

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**.

3.10.2 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 3-304 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID

Table 3-305 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project

Request Parameters

Table 3-306 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token

Table 3-307 Request body parameters

Parameter	Mandatory	Type	Description
status	No	Boolean	Status (enabled or disabled)
host_id_list	No	Array of strings	HostId list
resource_id	No	String	Resource ID
charging_mode	No	String	Billing mode. The value can be: • on_demand: pay-per-use

Response Parameters

Status code: 200

successful response

None

Example Requests

Enable WTP, set the target server IDs to a and b, and set the billing mode to pay-per-use.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.10.3 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 3-308 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID

Table 3-309 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project

Request Parameters

Table 3-310 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token

Table 3-311 Request body parameters

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

Response Parameters

Status code: 200

successful response

None

Example Requests

Enable dynamic WTP for servers a and b.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.10.4 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 3-312 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Table 3-313 Query Parameters

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

Request Parameters

Table 3-314 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token

Response Parameters

Status code: 200

Table 3-315 Response body parameters

Parameter	Type	Description
host_name	String	Server name
protect_status	String	Protection status. Its value can be: • close • opened
total_num	Long	total number
data_list	Array of **HostProtectHistoryResponseInfo** objects	data list

Table 3-316 HostProtectHistoryResponseInfo

Parameter	Type	Description
occr_time	Long	Detection time
file_path	String	Tampered file path
file_operation	String	Types of file operations • add • delete • modify • attribute • unknown
host_name	String	Server name
host_ip	String	Server IP address
process_id	String	Process ID

Parameter	Type	Description
process_name	String	Process name
process_cmd	String	Process command line

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**.

3.10.5 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 3-317 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID

Table 3-318 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project
host_id	Yes	String	Host Id
start_time	Yes	Long	Start time
end_time	Yes	Long	End time
limit	Yes	Integer	limit
offset	Yes	Integer	offset
alarm_level	No	Integer	Alarm severity
severity	No	String	Threat level. Its value can be: • Security • Low: low risk • Medium: medium risk • High: high risk • Critical
protect_status	No	String	Protection status. • closed: disabled • opened: protection enabled

Request Parameters

Table 3-319 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM token

Response Parameters

Status code: 200

Table 3-320 Response body parameters

Parameter	Type	Description
total_num	Long	total number
data_list	Array of **HostRaspProtectHistoryResponseInfo** objects	data list

Table 3-321 HostRaspProtectHistoryResponseInfo

Parameter	Type	Description
host_ip	String	Server IP address
host_name	String	Server name
alarm_time	Long	Alarm time
threat_type	String	Threat type
alarm_level	Integer	Alarm severity
source_ip	String	Source IP address
attacked_url	String	Attack URL

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**.

3.11 Server Management

3.11.1 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 3-322 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-323 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID
version	No	String	HSS edition. Its value can be: • hss.version.null • 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
agent_status	No	String	Agent status. Its value can be: • not_ installed • online • offline • install_failed • installing • not_online: All status except **online**, which is used only as a query condition.
detect_result	No	String	Detection result. Its value can be: • undetected • clean • risk • scanning
host_name	No	String	Server name

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_status	No	String	Host status. Its value can be: • ACTIVE • SHUTOFF • BUILDING • ERROR
os_type	No	String	OS type. Its value can be: • Linux • Windows
private_ip	No	String	Server private IP address
public_ip	No	String	Server public IP address
ip_addr	No	String	Public or private IP address
protect_status	No	String	Protection status. Its value can be: • closed • opened
group_id	No	String	Server group ID
group_name	No	String	Server group name
has_intrusion	No	Boolean	Alarms exist.
policy_group_id	No	String	Policy group ID
policy_group_name	No	String	Policy group name
charging_mode	No	String	Billing mode. Its value can be: • on_demand: pay-per-use
refresh	No	Boolean	Whether to forcibly synchronize servers from ECSs
above_version	No	Boolean	Whether to return all the versions later than the current version
outside_host	No	Boolean	Whether a server is a Cloud server

Parameter	Mandatory	Type	Description
asset_value	No	String	Asset importance. Its value can be: • important • common • test
label	No	String	Asset tag
server_group	No	String	Asset server group
agent_upgradable	No	Boolean	Whether the agent can be upgraded
protect_interrupt	No	Boolean	Whether the protection is interrupted
protect_degradation	No	Boolean	Whether the protection is degraded
limit	No	Integer	Number of records displayed on each page. The default value is **10**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.

Request Parameters

Table 3-324 Request header parameters

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

Response Parameters

Status code: 200

Table 3-325 Response body parameters

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

Table 3-326 Host

Parameter	Type	Description
host_name	String	Server name
host_id	String	Server ID
agent_id	String	Agent ID
private_ip	String	Private IP address
public_ip	String	Elastic IP address
enterprise_project_id	String	Enterprise project ID
enterprise_project_name	String	Enterprise project name
host_status	String	Server status. Its value can be: • ACTIVE • SHUTOFF • BUILDING • ERROR
agent_status	String	Agent status. Its value can be: • not_ installed • online • offline • install_failed • installing

Parameter	Type	Description
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
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
protect_status	String	Protection status. Its value can be: • closed • opened
os_image	String	System disk image
os_type	String	OS type. Its value can be: • Linux • Windows
os_bit	String	OS bit version

Parameter	Type	Description
detect_result	String	Server scan result. Its value can be: ● undetected ● clean ● risk ● scanning
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.)
charging_mode	String	Billing mode. Its value can be: ● on_demand: pay-per-use
resource_id	String	Cloud service resource instance ID (UUID)
outside_host	Boolean	Whether a server is on-premises
group_id	String	Server group ID
group_name	String	Server group name
policy_group_id	String	Policy group ID
policy_group_name	String	Policy group name
asset	Integer	Asset risk
vulnerability	Integer	Vulnerability
baseline	Integer	Baseline risks
intrusion	Integer	Intrusion risk
asset_value	String	Asset importance. Its value can be: ● important ● common ● test
labels	Array of strings	Tag list
agent_create_time	Long	Agent installation time, which is a timestamp. The default unit is milliseconds.
agent_update_time	Long	Time when the agent status is changed. This is a timestamp. The default unit is milliseconds.
agent_version	String	Agent version

Parameter	Type	Description
upgrade_status	String	Upgrade status. Its value can be: • not_upgrade: Not upgraded. This is the default status. The customer has not delivered any upgrade command to the server. • upgrading: The upgrade is in progress. • upgrade_failed: The upgrade failed. • upgrade_succeed
upgrade_result_code	String	Upgrade failure cause. This parameter is displayed only if upgrade_status is upgrade_failed. Its value can be: • package_unavailable: The upgrade package fails to be parsed because the upgrade file is incorrect. • network_access_timeout: Failed to download the upgrade package because the network is abnormal. • agent_offline: The agent is offline. • hostguard_abnormal: The agent process is abnormal. • insufficient_disk_space: The disk space is insufficient. • failed_to_replace_file: Failed to replace the file.
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.
protect_interrupt	Boolean	Whether protection is interrupted
protect_degradation	Boolean	Whether the protection is degraded
degradation_reason	String	Protection degradation causes

Example Requests

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

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

Example Responses

Status code: 200

Cloud server list


```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "agent_status" : "online",
    "asset" : 0,
    "asset_value" : "common",
    "baseline" : 0,
    "charging_mode" : "on_demand",
    "detect_result" : "risk",
    "enterprise_project_id" : "all_granted_eps",
    "enterprise_project_name" : "default",
    "group_id" : "7c659ea3-006f-4687-9f1c-6d975d955f37",
    "group_name" : "default",
    "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
    "host_name" : "ecs-r00431580-ubuntu",
    "host_status" : "ACTIVE",
    "intrusion" : 0,
    "expire_time" : -1,
    "os_bit" : "64",
    "os_type" : "Linux",
    "outside_host" : false,
    "policy_group_id" : "2758d2a61598fd9144cfa6b201049e7c0af8c3f1280cd24e3ec95a2f0811a2a2",
    "policy_group_name" : "wtp_ecs-r00431580-ubuntu(default)",
    "private_ip" : "192.168.0.182",
    "protect_status" : "opened",
    "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**.

3.11.2 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 3-327 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-328 Query Parameters

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

Request Parameters

Table 3-329 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.

Table 3-330 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
charging_mode	No	String	Billing mode. This parameter is mandatory when **version** is not set to **hss.version.null**. • on_demand: pay-per-use
resource_id	No	String	HSS quota ID. If this parameter is not specified, the quota of the corresponding version is randomly selected.
host_id_list	Yes	Array of strings	Server list
tags	No	Array of **TagInfo** objects	Resource tag list

Table 3-331 TagInfo

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

Response Parameters

Status code: 200

successful response

None

Example Requests

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.11.3 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 3-332 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-333 Query Parameters

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

Request Parameters

Table 3-334 Request header parameters

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

Response Parameters

Status code: 200

Table 3-335 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number

Parameter	Type	Description
data_list	Array of HostGroupItem objects	Server group list

Table 3-336 HostGroupItem

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

3.11.4 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 3-337 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-338 Query Parameters

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

Request Parameters

Table 3-339 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.

Table 3-340 Request body parameters

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

Response Parameters

Status code: 200

success

None

Example Requests

Create a server group named test. The ID of the server in the server group is 15dac7fe-d81b-43bc-a4a7-4710fe673972.

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.11.5 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 3-341 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-342 Query Parameters

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

Request Parameters

Table 3-343 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.

Table 3-344 Request body parameters

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

Response Parameters

Status code: 200

success

None

Example Requests

Edit the server group named test. The server group ID is eca40dbe-27f7-4229-8f9d-a58213129fdc. The IDs of the servers in the server group are 15dac7fe-d81b-43bc-a4a7-4710fe673972 and 21303c5b-36ad-4510-a1b0-cb4ac4c2875c.

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.11.6 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 3-345 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-346 Query Parameters

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

Request Parameters

Table 3-347 Request header parameters

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

Response Parameters

Status code: 200

success

None

Example Requests

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

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

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

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

3.12 Container Management

3.12.1 Querying the Container Node List

Function

This API is used to query the container node list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v5/{project_id}/container/nodes

Table 3-348 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-349 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. To query all enterprise projects, set this parameter to **all_granted_eps**.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	No	Integer	Number of records displayed on each page.
host_name	No	String	Node name.
agent_status	No	String	Agent status. It can be: • not_installed: • online • offline

Parameter	Mandatory	Type	Description
protect_status	No	String	Protection status. Its value can be: • closed • opened
container_tags	No	String	Label, which is used to identify CCE container and self-built nodes. • cce: CCE nodes • self: self-built nodes • other: other nodes

Request Parameters

Table 3-350 Request header parameters

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

Response Parameters

Status code: 200

Table 3-351 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of container nodes
data_list	Array of **ContainerNodeInfo** objects	Container node list

Table 3-352 ContainerNodeInfo

Parameter	Type	Description
agent_id	String	Agent ID

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Node name
host_status	String	Server status. The options are as follows: ● ACTIVE ● SHUTOFF ● BUILDING ● ERROR
agent_status	String	Agent status. It can be: ● not_installed ● online ● offline
protect_status	String	Protection status. Its value can be: ● closed ● opened
protect_interrupt	Boolean	Whether protection is interrupted
protect_degradation	Boolean	Whether the protection is degraded
degradation_reason	String	Protection degradation causes
container_tags	String	Label, which is used to identify CCE container and self-built nodes. ● cce: CCE nodes ● self: self-built nodes ● other: other nodes
private_ip	String	Private IP address
public_ip	String	Elastic IP Address (EIP)
resource_id	String	HSS quota ID (UUID)
group_name	String	Server group ID
enterprise_project_name	String	Enterprise project name

Parameter	Type	Description
detect_result	String	Server scan result. The options are as follows: • undetected • clean: No risk is detected. • risk: Risks are detected. • scanning
asset	Integer	Asset risks
vulnerability	Integer	Vulnerabilities
intrusion	Integer	Intrusion risks
policy_group_id	String	Policy group ID
policy_group_name	String	Policy group name

Example Requests

This API is used to query the container node list. If the limit parameter is not set, 10 records are returned by default.

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

Example Responses

Status code: 200

success response

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

Status Codes

Status Code	Description
200	success response

Error Codes

See **Error Codes**.

3.13 Container Image

3.13.1 Querying the Image List in the SWR Image Repository

Function

This API is used to query the image list in the SWR image repository. To synchronize the latest images from SWR, call the API for synchronizing images from SWR first.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-353 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-354 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.
namespace	No	String	Organization name
image_name	No	String	Image name ID
image_version	No	String	Image tag

Parameter	Mandatory	Type	Description
latest_version	No	Boolean	Display latest image versions only
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**.
limit	No	Integer	Number of records displayed on each page.
image_type	Yes	String	Image type. The options are as follows: ● private_image: private image repository ● shared_image: shared image repository ● local_image ● instance_image: enterprise image
scan_status	No	String	Scanning status. The options are as follows: ● unscan ● success ● scanning ● failed ● download_failed ● image_oversized
instance_name	No	String	Enterprise image instance name
image_size	No	Long	Image size
start_latest_update_time	No	Long	Creation start time.
end_latest_update_time	No	Long	Creation end time.
start_latest_scan_time	No	Long	Specify the start time based on the query condition of latest scan completion.
end_latest_scan_time	No	Long	Specify the end time based on the query condition of latest scan completion.

Parameter	Mandatory	Type	Description
has_malicious_file	No	Boolean	Whether there are malicious files
has_unsafe_setting	No	Boolean	Whether baseline check exists
has_vul	No	Boolean	Whether there are software vulnerabilities
instance_id	No	String	Enterprise repository instance ID. This API is not required for SWR shared edition.

Request Parameters

Table 3-355 Request header parameters

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

Response Parameters

Status code: 200

Table 3-356 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **PrivateImageRepositoryInfo** objects	Querying the image list in the SWR image repository

Table 3-357 PrivateImageRepositoryInfo

Parameter	Type	Description
id	Long	id

Parameter	Type	Description
namespace	String	Namespace
image_name	String	Image name
image_id	String	Image ID
image_digest	String	Image digest
image_version	String	Image tag
image_type	String	Image type. The options are as follows: ● private_image ● shared_image
latest_version	Boolean	Check whether the version is the latest.
scan_status	String	Scan status. The options are as follows: ● unscan ● success ● scanning ● failed ● download_failed ● image_oversized ● waiting_for_scan

Parameter	Type	Description
scan_failed_desc	String	Cause of the scanning failure. The options are as follows: ● "unknown_error" ● "authentication_failed" ● "download_failed": Failed to download the image. ● "image_over_sized": The size of the image exceeds the maximum. ● "image_oversized" ● "failed_to_scan_vulnerability" ● "failed_to_scan_file" ● "failed_to_scan_software" ● "failed_to_check_sensitive_information" ● "failed_to_check_baseline" ● "failed_to_check_software_compliance" ● "failed_to_query_basic_image_information" ● "response_timed_out" ● "database_error" ● "failed_to_send_the_scan_request"
image_size	Long	Image size
latest_update_time	Long	Specifies the last update time of the image version.
latest_scan_time	Long	Last scanned
vul_num	Integer	Vulnerabilities
unsafe_setting_num	Integer	Number of failed baseline scans
malicious_file_num	Integer	Number of malicious files
domain_name	String	Owner (shared image parameter)
shared_status	String	The status of a shared image. The value can be: ● expired ● effective
scannable	Boolean	Scannable or not

Parameter	Type	Description
association_images	Array of AssociateImages objects	Multi-architecture associated image information

Table 3-358 AssociateImages

Parameter	Type	Description
image_name	String	Image name
image_version	String	Image tag
image_type	String	Image type
namespace	String	Namespace
image_digest	String	Image digest
scan_status	String	Scan status. The options are as follows: • unscan • success • scanning • failed • download_failed • image_oversized • waiting_for_scan

Example Requests

Query the image list in the SWR image repository whose image type is private image.

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

Example Responses

Status code: 200

This API is used to query the image list in the SWR image repository, including the private image list and shared image list (controlled by the input parameter image_type).

```
{
  "total_num" : 3,
  "data_list" : [ {
    "id" : "111 (example for private images)",
    "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_name" : "centos7",
```

```
  "image_size" : "1000 (Bytes)",
  "image_type" : "private_image",
  "image_version" : "common",
  "latest_scan_time" : 1691748641788,
  "latest_update_time" : 1687664346000,
  "latest_version" : false,
  "malicious_file_num" : 0,
  "namespace" : "aaa",
  "scan_status" : "success",
  "scannable" : true,
  "unsafe_setting_num" : 1,
  "vul_num" : 111,
  "instance_name" : "",
  "instance_id" : "",
  "instance_url" : ""
 }, {
  "id" : "222 (example for shared image)",
  "domain_name" : "scc_cgs_XXX",
  "shared_status" : "effective",
  "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
  "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
  "image_name" : "mysql",
  "image_size" : "1000 (Bytes)",
  "image_type" : "shared_image",
  "image_version" : "5.5",
  "latest_scan_time" : 1691748641788,
  "latest_update_time" : 1687664346000,
  "latest_version" : false,
  "malicious_file_num" : 0,
  "namespace" : "aaa",
  "scan_status" : "success",
  "scannable" : true,
  "unsafe_setting_num" : 1,
  "vul_num" : 111,
  "instance_name" : "",
  "instance_id" : "",
  "instance_url" : ""
 }, {
  "id" : "333 (example of an enterprise image)",
  "domain_name" : "scc_cgs_XXX",
  "shared_status" : "effective",
  "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
  "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
  "image_name" : "mysql",
  "image_size" : "1000 (Bytes)",
  "image_type" : "shared_image",
  "image_version" : "5.5",
  "latest_scan_time" : 1691748641788,
  "latest_update_time" : 1687664346000,
  "latest_version" : false,
  "malicious_file_num" : 0,
  "namespace" : "aaa",
  "scan_status" : "success",
  "scannable" : true,
  "unsafe_setting_num" : 1,
  "vul_num" : 111,
  "instance_name" : "Enterprise instance name",
  "instance_id" : "",
  "instance_url" : ""
 } ]
}
```

Status Codes

Status Code	Description
200	This API is used to query the image list in the SWR image repository, including the private image list and shared image list (controlled by the input parameter image_type).

Error Codes

See **Error Codes**.

3.13.2 Scanning Images in the Image Repository in Batches

Function

This API is used to scan images in the image repository in batches.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-359 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-360 Query Parameters

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

Request Parameters

Table 3-361 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.

Table 3-362 Request body parameters

Parameter	Mandatory	Type	Description
repo_type	No	String	Repository type. Currently, SWR image repositories are connected. The options are as follows: • SWR: SWR image repository
image_info_list	No	Array of **BatchScanSwrImageInfo** objects	Specifies the list of images to be scanned. This parameter is mandatory when operate_all is false.
operate_all	No	Boolean	If this parameter is set to true, all filter criteria can be used for full query. If image_info_list is empty, this parameter is mandatory.
namespace	No	String	Organization name
image_name	No	String	Image name
image_version	No	String	Image tag
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository

Parameter	Mandatory	Type	Description
scan_status	No	String	Scan status. The options are as follows: • unscan • success • scanning • failed • download_failed • image_oversized
latest_version	No	Boolean	Display latest image versions only
image_size	No	Long	Image size
start_latest_update_time	No	Long	Creation start time.
end_latest_update_time	No	Long	Creation end time.
start_latest_scan_time	No	Long	Specify the start time based on the query condition of latest scan completion.
end_latest_scan_time	No	Long	Specify the end time based on the query condition of latest scan completion.

Table 3-363 BatchScanSwrImageInfo

Parameter	Mandatory	Type	Description
namespace	No	String	Namespace
image_name	No	String	Image name
image_version	No	String	Image tag
instance_id	No	String	Enterprise instance ID
instance_url	No	String	Downloading the enterprise image URL

Response Parameters

Status code: 200

successful response

None

Example Requests

- Scan private images in batches. The request body transfers the image list and operate_all does not contain any parameter, indicating that the image list needs to be scanned in batches.

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

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

- Perform a full scan for private images. The request body does not transfer the image list and operate_all is set to true, indicating that the image list needs to be fully scanned.

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

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

Example Responses

None

Status Codes

Status Code	Description
200	successful response

Error Codes

See **Error Codes**.

3.13.3 Querying Image Vulnerability Information

Function

This API is used to query image vulnerability information.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-364 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID
image_id	Yes	String	Image ID

Table 3-365 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.
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository
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**.
limit	No	Integer	Number of records displayed on each page.
instance_id	No	String	Enterprise repository instance ID. This API is not required for SWR shared edition.
namespace	Yes	String	Organization name
image_name	Yes	String	Image name
tag_name	Yes	String	Image tag
repair_necessity	No	String	Risk level. The options are as follows: • immediate_repair: high risk • delay_repair: medium risk • not_needed_repair: low risk

Parameter	Mandatory	Type	Description
vul_id	No	String	Vulnerability ID (fuzzy search supported)
app_name	No	String	Software
type	No	String	Vulnerability type. The options are as follows: -linux_vul: Linux vulnerability -app_vul: application vulnerability

Request Parameters

Table 3-366 Request header parameters

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

Response Parameters

Status code: 200

Table 3-367 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of image vulnerabilities
data_list	Array of **ImageVulInfo** objects	Image vulnerability list

Table 3-368 ImageVulInfo

Parameter	Type	Description
vul_id	String	Vulnerability ID

Parameter	Type	Description
repair_necessity	String	Emergency level. Its values and their meanings are as follows: ● immediate_repair: high risk ● delay_repair: medium risk ● not_needed_repair: low risk
description	String	Vulnerability description
position	String	Image where a vulnerability exists
app_name	String	Vulnerability software name
app_path	String	Path of the application software (This field is available only for application vulnerabilities.)
version	String	Software version
solution	String	Solution
url	String	Patch address

Example Requests

Query the vulnerability information of the private image whose namespace is scc_hss_container, image name is apptest, and image version is V1.

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

Example Responses

Status code: 200

Image vulnerability list

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

Status Codes

Status Code	Description
200	Image vulnerability list

Error Codes

See **Error Codes**.

3.13.4 CVE Information Corresponding to the Vulnerability

Function

This API is used to query the CVE information corresponding to the vulnerability.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-369 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID
vul_id	Yes	String	Vulnerability ID

Table 3-370 Query Parameters

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

Request Parameters

Table 3-371 Request header parameters

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

Response Parameters

Status code: 200

Table 3-372 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **ImageVulCveInfo** objects	List

Table 3-373 ImageVulCveInfo

Parameter	Type	Description
cve_id	String	cve id
cvss_score	Float	CVSS score
publish_time	Long	Release date
description	String	CVE description

Example Requests

Query the CVE information of the vulnerability whose ID is vul_id.

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

Example Responses

Status code: 200

Succeeded in requesting the CVE information list corresponding to the vulnerability.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "cve_id" : "CVE-2021-45960",
    "cvss_score" : 8.8,
    "description" : "In Expat (aka libexpat) XXXX",
    "publish_time" : 1641035700000
  } ]
}
```

Status Codes

Status Code	Description
200	Succeeded in requesting the CVE information list corresponding to the vulnerability.

Error Codes

See **Error Codes**.

3.13.5 Synchronizing the Image List from SWR

Function

This API is used to synchronize the image list from SWR.

Calling Method

For details, see **Calling APIs**.

URI

POST /v5/{project_id}/image/synchronize

Table 3-374 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID

Table 3-375 Query Parameters

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

Request Parameters

Table 3-376 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.

Table 3-377 Request body parameters

Parameter	Mandatory	Type	Description
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository

Response Parameters

Status code: 200

Table 3-378 Response body parameters

Parameter	Type	Description
error_code	Integer	Error code
error_description	String	Error description

Example Requests

Synchronize private or shared images from SWR.

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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See **Error Codes**.

3.13.6 Querying the List of Image Security Configuration Detection Results

Function

This API is used to query the list of image security configuration detection results.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-379 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-380 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.
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository • local_image: local image • instance_image: enterprise image
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**.
limit	No	Integer	Number of records displayed on each page.
namespace	No	String	Organization name
image_name	No	String	Image name
image_version	No	String	Image tag name
check_name	No	String	Baseline name
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High
standard	No	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
instance_id	No	String	Enterprise repository instance ID. This API is not required for SWR shared edition.

Request Parameters

Table 3-381 Request header parameters

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

Response Parameters

Status code: 200

Table 3-382 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of **ImageRiskConfigsInfoResponseInfo** objects	Configuring the detection list

Table 3-383 ImageRiskConfigsInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Security • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline type
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
check_rule_num	Integer	Number of check items

Parameter	Type	Description
failed_rule_num	Integer	Number of risk items
check_type_desc	String	Baseline description

Example Requests

Query the security configuration result list of the private image whose namespace is scc_hss_container, image name is euleros, and image version is 2.2.

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

Example Responses

Status code: 200

This API is used to query the list of image configuration results.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_name" : "CentOS 7",
    "check_rule_num" : 3,
    "check_type" : 3,
    "check_type_desc" : "This document focuses on XXX.",
    "failed_rule_num" : 0,
    "severity" : "Low",
    "standard" : "cn_standard"
  } ]
}
```

Status Codes

Status Code	Description
200	This API is used to query the list of image configuration results.

Error Codes

See **Error Codes**.

3.13.7 Querying the Check Item List of a Specified Security Configuration Item of an Image

Function

This API is used to query the check item list of a specified security configuration item of an image.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-384 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	User project ID
check_name	Yes	String	Baseline name

Table 3-385 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**.
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository • local_image: local image • instance_image: enterprise image
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**.
limit	No	Integer	Number of records displayed on each page.
namespace	No	String	Specifies the organization name. If no image information is available, all images are queried.
image_name	No	String	Image name
image_version	No	String	Image tag name

Parameter	Mandatory	Type	Description
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
result_type	No	String	Result type. Its value can be: • pass: The item passed the check. • failed: The item failed the check.
check_rule_name	No	String	Check item name. Fuzzy match is supported.
severity	No	String	Risk level. Its value can be: • Security • Low • Medium • High • Critical
instance_id	No	String	Enterprise repository instance ID. This API is not required for SWR shared edition.

Request Parameters

Table 3-386 Request header parameters

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

Response Parameters

Status code: 200

Table 3-387 Response body parameters

Parameter	Type	Description
total_num	Integer	Total risks
data_list	Array of **ImageRiskConfigsCheckRulesResponseInfo** objects	Data list

Table 3-388 ImageRiskConfigsCheckRulesResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: • Security • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline type
standard	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
check_rule_name	String	Check items
check_rule_id	String	Check item ID
scan_result	String	Detection result. The options are as follows: • pass • failed

Example Requests

Query the check items of a specified security configuration item whose organization is aaa, image name is centos7, image version is common, and standard type is cloud standard.

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

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: Password locking policy.",
    "check_name" : "CentOS 7",
    "check_type" : "CentOS 7",
    "standard" : "hw_standard",
    "scan_result" : "failed",
    "severity" : "High"
  } ]
}
```


Status Codes

Status Code	Description
200	Checklist of the specified security configuration item

Error Codes

See **Error Codes**.

3.13.8 Querying the Mirror Configuration Check Report

Function

This API is used to query the mirror configuration check report.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 3-389 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant project ID

Table 3-390 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.
image_type	Yes	String	Image type. The options are as follows: • private_image: private image repository • shared_image: shared image repository • local_image: local image • instance_image: enterprise image
namespace	No	String	Specifies the organization name. If no image information is available, all images are queried.
image_name	No	String	Image name
image_version	No	String	Image tag name
check_name	Yes	String	Baseline name
check_type	Yes	String	Baseline Type
check_rule_id	Yes	String	Check item ID
standard	Yes	String	Standard type. Its value can be: • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
instance_id	No	String	Enterprise repository instance ID. This API is not required for SWR shared edition.

Request Parameters

Table 3-391 Request header parameters

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

Response Parameters

Status code: 200

Table 3-392 Response body parameters

Parameter	Type	Description
description	String	Check item description
reference	String	Reference
audit	String	Audit description
remediation	String	Suggestion
check_info_list	Array of **ImageCheckRuleCheckCaseResponseInfo** objects	Test case

Table 3-393 ImageCheckRuleCheckCaseResponseInfo

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

Example Requests

Query the check report of the configuration item whose organization is aaa, image name is centos7, image version is common, baseline name is SSH, check item ID is 1.12, and standard type is cloud standard.

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

Example Responses

Status code: 200

The check report of configuration check items is returned.

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

Status Codes

Status Code	Description
200	The check report of configuration check items is returned.

Error Codes

See **Error Codes**.

A Appendixes

A.1 Status Code

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

A.2 Error Codes

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

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

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

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

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

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

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

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

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

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

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

A.3 Obtaining a Project ID

Scenario

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

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

Obtaining a Project ID by Calling an API

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

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

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
```

```
  }
}
```

Obtaining a Project ID from the Console

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

1. Log in to the management console.
2. Click the username and choose **My Credential** from the drop-down list.

   On the **My Credential** page, view project IDs in the project list.

A.4 Obtaining an Enterprise Project ID

Scenario

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

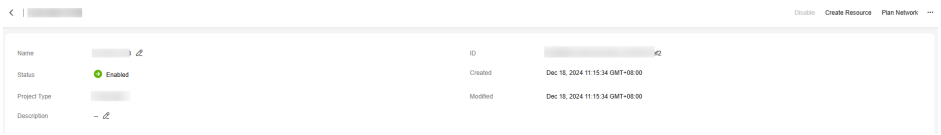
Obtaining an Enterprise Project ID on the Console

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

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

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

   Figure A-1 Viewing the enterprise project ID



A.5 Obtaining Region ID

Scenario

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

Obtaining a Region ID from the Console

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

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

----End

B Change History

Date	Change Description
2025-09-30	This issue is the first official release.