

Host Security Service

API Reference

Issue 06
Date 2025-01-17



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Before You Start.....	1
2 Calling APIs.....	3
2.1 Making an API Request.....	3
2.2 Authentication.....	6
2.3 Response.....	7
3 API Description.....	9
3.1 Asset Management.....	9
3.1.1 Collecting Asset Statistics, Including Accounts, Ports, and Processes.....	9
3.1.2 Querying the Account List.....	14
3.1.3 Querying Open Port Statistics.....	19
3.1.4 Querying the Process List.....	24
3.1.5 Querying the Software List.....	29
3.1.6 Querying Automatic Startup Item Information.....	34
3.1.7 Querying the Server List of an Account.....	39
3.1.8 Querying the Open Port List of a Single Server.....	44
3.1.9 Querying the Server List of the Software.....	50
3.1.10 Querying the Service List of Auto-Started Items.....	55
3.1.11 Obtaining the Account Change History.....	61
3.1.12 Obtaining the Historical Change Records of Software Information.....	66
3.1.13 Obtaining the Historical Change Records of Auto-started Items.....	72
3.1.14 Asset Fingerprints - Process - Server List.....	78
3.1.15 Asset Fingerprints - Port - Server List.....	83
3.1.16 Querying the Middleware List.....	89
3.1.17 Querying the Server List of a Specified Middleware.....	93
3.2 Ransomware Prevention.....	99
3.2.1 Querying the Servers Protected Against Ransomware.....	99
3.2.2 Querying the Protection Policy List of Ransomware.....	107
3.2.3 Modifying Ransomware Protection Policies.....	113
3.2.4 Enabling Ransomware Prevention.....	120
3.2.5 Disabling Ransomware Prevention.....	132
3.2.6 Querying the Backup Policy Bound to HSS Protection Vault.....	137
3.2.7 Modifying the Backup Policy Bound to Vault.....	144

3.3 Baseline Management.....	153
3.3.1 Querying the Weak Password Detection Result List.....	153
3.3.2 Querying the Password Complexity Policy Detection Report.....	159
3.3.3 Querying the Result List of Server Security Configuration Check.....	165
3.3.4 Querying the Check Result of a Security Configuration Item.....	171
3.3.5 Querying the Checklist of a Security Configuration Item.....	177
3.3.6 Querying the List of Affected Servers of a Security Configuration Item.....	184
3.3.7 Querying the Report of a Check Item in a Security Configuration Check.....	189
3.3.8 Ignoring, Unignoring, Repairing, or Verifying the Failed Configuration Check Items.....	195
3.4 Quota Management.....	205
3.4.1 Querying Quota Information.....	205
3.4.2 Querying Quota Details.....	211
3.4.3 Creating an Order Quota by HSS.....	219
3.4.4 Querying Product and Offering Information.....	225
3.5 Container Management.....	231
3.5.1 Querying the Container Node List.....	231
3.5.2 Querying Basic Container Information List.....	237
3.6 Event Management.....	242
3.6.1 Querying the List of Blocked IP Addresses.....	242
3.6.2 Unblocking a Blocked IP Address.....	248
3.6.3 Querying the List of Isolated Files.....	253
3.6.4 Restoring Isolated Files.....	269
3.6.5 Querying Export Tasks.....	274
3.6.6 Downloading Export Files.....	279
3.7 Intrusion Detection.....	283
3.7.1 Handling Alarm Events.....	283
3.7.2 Querying the Detected Intrusion List.....	301
3.7.3 Querying the Alarm Whitelist.....	334
3.8 Server Management.....	343
3.8.1 Querying ECSs.....	343
3.8.2 Changing the Protection Status.....	354
3.8.3 Querying Server Groups.....	360
3.8.4 Creating a Server Group.....	365
3.8.5 Editing a Server Group.....	369
3.8.6 Deleting a Server Group.....	375
3.9 Container Image.....	379
3.9.1 Querying the Image List in the SWR Image Repository.....	379
3.9.2 Scanning Images in the Image Repository in Batches.....	388
3.9.3 Querying the Local Image List.....	397
3.9.4 Querying Image Vulnerability Information.....	404
3.9.5 CVE Information Corresponding to the Vulnerability.....	410
3.9.6 Synchronizing the Image List from SWR.....	415

3.9.7 Querying the List of Image Security Configuration Detection Results.....	420
3.9.8 Querying the Check Item List of a Specified Security Configuration Item of an Image.....	426
3.9.9 Querying the Mirror Configuration Check Report.....	432
3.10 Policy Management.....	438
3.10.1 Querying the Policy Group List.....	438
3.10.2 Applying a Policy Group.....	444
3.11 Vulnerability Management.....	449
3.11.1 Querying the Vulnerability List.....	449
3.11.2 Exporting Information About Vulnerabilities and Their Affected Servers.....	458
3.11.3 Querying the Servers Affected by a Vulnerability.....	465
3.11.4 Changing the Status of a Vulnerability.....	474
3.11.5 Querying Vulnerability Information About a Server.....	481
3.11.6 Creating a Vulnerability Scan Task.....	491
3.11.7 Querying a Vulnerability Scan Policy.....	499
3.11.8 Modifying a Vulnerability Scan Policy.....	504
3.11.9 Querying the Vulnerability Scan Tasks.....	509
3.11.10 Querying the List of Servers Corresponding to a Vulnerability Scan Task.....	515
3.11.11 Querying Vulnerability Management Statistics.....	521
3.12 Web Tamper Protection.....	525
3.12.1 Querying the Protection List.....	526
3.12.2 Enabling or Disabling WTP.....	532
3.12.3 Enabling or Disabling Dynamic WTP.....	537
3.12.4 Querying the Status of Static WTP for a Server.....	542
3.12.5 Querying the Status of Dynamic WTP for a Server.....	548
3.13 Tag Management.....	554
3.13.1 Creating Tags in Batches.....	554
3.13.2 Deleting a Resource Tag.....	559
3.14 Cluster Management.....	563
3.14.1 Deleting a Cluster Daemonset.....	563
3.14.2 Updating a Cluster Daemonset.....	567
3.14.3 Creating a CCE Integrated Protection Configuration.....	572
3.14.4 Obtaining Cluster Configurations.....	577
3.15 Installation and Configuration.....	582
3.15.1 Querying the Multi-Account List.....	582
3.15.2 Deleting an Account.....	587
3.15.3 Adding Accounts in Batches.....	592
3.15.4 Querying an Account Organization.....	598
3.15.5 Querying the Agent Installation Script.....	603
A Appendixes.....	608
A.1 Status Code.....	608
A.2 Error Codes.....	609

1 Before You Start

Overview

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

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

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

Endpoints

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

Basic Concepts

- **Account**
An account is created upon successful registration with the cloud platform. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.
- **User**
A user is created using a domain to use cloud services. Each user has its own identity credentials (password and access keys).
The account name, username, and password will be required for API authentication.
- **Region**
Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same

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

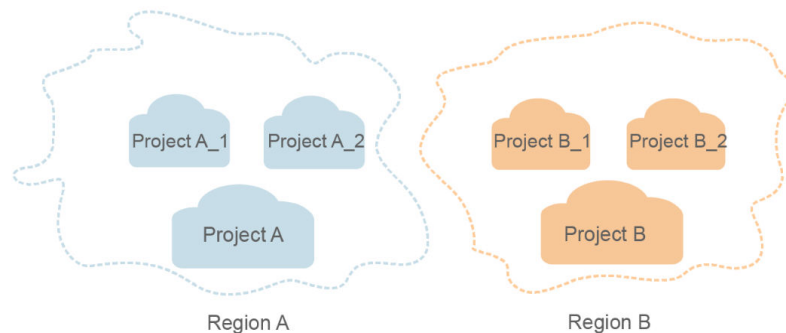
- Availability Zone (AZ)

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

- Project

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

Figure 1-1 Project isolating model



- Enterprise Project

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

For details about how to obtain enterprise project IDs and features, see [Enterprise Management User Guide](#).

Limitations and Constraints

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

For more constraints, see API description.

2 Calling APIs

2.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

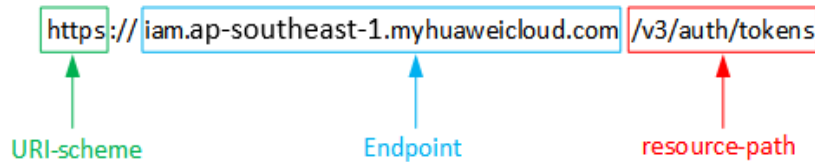
- **URI-scheme:**
Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint:**
Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from [Regions and Endpoints](#).
For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path:**
Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string:**
Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com)) for this region and

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

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 2-1 Example URI



NOTE

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

Request Methods

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

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

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

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Request Header

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

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

 NOTE

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

For more information, see [AK/SK-based Authentication](#).

The API used to [obtain a user token](#) does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

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

Request Body

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

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

In the case of the API used to [obtain a user token](#), the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set **username** to the name of a user, **domainname** to the name of the account that the user belongs to, ********* to the user's login password, and **xxxxxxxxxxxxxxxxxxxx** to the project name. You can learn more information about projects from [Regions and Endpoints](#). Check the value of the **Region** column.

 NOTE

The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see [Obtaining a User Token](#).

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

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

```
}  
}
```

If all data required for the API request is available, you can send the request to call the API through [curl](#), [Postman](#), or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

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-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

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

The token can be obtained by calling the required API. For more information, see [Obtaining a User Token](#). A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. Example:

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

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

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

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

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

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

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see [API Signature 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 [create an IAM user](#), the request is successful.

Response Header

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

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

```

connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTCCEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOansiZXhwaXJlc19hdCI6IiwMTktMDItMTNUMC
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkajACgkIQ01wi4JIGzrpd1.8LGXK5bdfq4lqHCYb8P4NaYONYejeAgzVefYtLWT1GSO0zxKZmlQHq82HBqHdgIZO9fuEebL5dMhdavj+33wEI
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwRtnfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MUbvpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;

```

(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": "xxxxxxx",
            .....

```

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

```

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

```

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

3 API Description

3.1 Asset Management

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

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/asset/statistics

Table 3-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
host_id	No	String	Host ID
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

Request Parameters

Table 3-3 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-4 Response body parameters

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

Request succeeded.

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


SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowAssetStatisticSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowAssetStatisticRequest request = new ShowAssetStatisticRequest();
        try {
            ShowAssetStatisticResponse response = client.showAssetStatistic(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```

```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ShowAssetStatisticRequest()
    response = client.show_asset_statistic(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAssetStatisticRequest{}
    response, err := client.ShowAssetStatistic(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.2 Querying the Account List

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-5 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-6 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Account name. It must comply with the Windows file naming rules. The value can contain letters, digits, underscores (_), and the following special characters: !@.-. Chinese punctuations are not allowed.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

Request Parameters

Table 3-7 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-8 Response body parameters

Parameter	Type	Description
total_num	Integer	Container ID
data_list	Array of UserStatisticInfoResponseInfo objects	Instance name of enterprise edition image

Table 3-9 UserStatisticInfoResponseInfo

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

Example Requests

The first 10 accounts are queried by default.

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListUserStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListUserStatisticsRequest request = new ListUserStatisticsRequest();
        try {
            ListUserStatisticsResponse response = client.listUserStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListUserStatisticsRequest()
    response = client.list_user_statistics(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListUserStatisticsRequest{}
    response, err := client.ListUserStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.3 Querying Open Port Statistics

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-10 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-11 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

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
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	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

Request Parameters

Table 3-12 Request header parameters

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

Response Parameters

Status code: 200

Table 3-13 Response body parameters

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

Table 3-14 PortStatisticResponseInfo

Parameter	Type	Description
port	Integer	Port number
type	String	Port 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListPortStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListPortStatisticsRequest request = new ListPortStatisticsRequest();
        try {
            ListPortStatisticsResponse response = client.listPortStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPortStatisticsRequest()
        response = client.list_port_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
    request := &model.ListPortStatisticsRequest{}
    response, err := client.ListPortStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.4 Querying the Process List

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-15 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-16 Query Parameters

Parameter	Mandatory	Type	Description
path	No	String	Executable process path
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

Request Parameters

Table 3-17 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-18 Response body parameters

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

Table 3-19 ProcessStatisticResponseInfo

Parameter	Type	Description
path	String	Path of the executable files for the process
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListProcessStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListProcessStatisticsRequest request = new ListProcessStatisticsRequest();
        try {
            ListProcessStatisticsResponse response = client.listProcessStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
```



```
.with_credentials(credentials) \  
.with_region(HssRegion.value_of("<YOUR REGION>")) \  
.build()  
  
try:  
    request = ListProcessStatisticsRequest()  
    response = client.list_process_statistics(request)  
    print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.ListProcessStatisticsRequest{}  
    response, err := client.ListProcessStatistics(request)  
    if err == nil {  
        fmt.Printf("%v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.5 Querying the Software List

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-20 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-21 Query Parameters

Parameter	Mandatory	Type	Description
app_name	No	String	Software name

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

Request Parameters

Table 3-22 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-23 Response body parameters

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

Table 3-24 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
```

```
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAppStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAppStatisticsRequest request = new ListAppStatisticsRequest();
        try {
            ListAppStatisticsResponse response = client.listAppStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()
```

```

try:
    request = ListAppStatisticsRequest()
    response = client.list_app_statistics(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)

```

Go

```

package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAppStatisticsRequest{}
    response, err := client.ListAppStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.6 Querying Automatic Startup Item Information

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-26 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Auto-started item name
type	No	String	Auto-started item type <ul style="list-style-type: none">• 0: auto-started service• 1: scheduled task• 2: Preload dynamic library• 3: Run registry key• 4: startup folder

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-27 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-28 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 3-29 AutoLaunchStatisticsResponseInfo

Parameter	Type	Description
name	String	Auto-started item name
type	String	Auto-started item type <ul style="list-style-type: none"> 0: auto-started service 1: scheduled task 2: Preload dynamic library 3: Run registry key 4: startup folder
num	Integer	Number of servers that have the auto-startup items.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAutoLaunchStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAutoLaunchStatisticsRequest request = new ListAutoLaunchStatisticsRequest();
        try {
            ListAutoLaunchStatisticsResponse response = client.listAutoLaunchStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListAutoLaunchStatisticsRequest()
    response = client.list_auto_launch_statistics(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAutoLaunchStatisticsRequest{}
    response, err := client.ListAutoLaunchStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.7 Querying the Server List of an Account

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/asset/users

Table 3-30 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-31 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Host ID
user_name	No	String	Account name
host_name	No	String	Host name
private_ip	No	String	Server private IP address
login_permission	No	Boolean	Whether login is allowed
root_permission	No	Boolean	Whether the user has root permissions
user_group	No	String	Server user group

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-32 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>

Response Parameters

Status code: 200

Table 3-33 Response body parameters

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

Table 3-34 UserResponseInfo

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

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxe69",
    "host_ip" : "192.168.0.1",
    "host_name" : "test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_home_dir" : "/bin",
    "user_name" : "bin",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListUsersSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListUsersRequest request = new ListUsersRequest();
        try {
            ListUsersResponse response = client.listUsers(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        }
    }
}
```

```
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListUsersRequest()
        response = client.list_users(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```



```
auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListUsersRequest{}
response, err := client.ListUsers(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.8 Querying the Open Port List of a Single Server

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/asset/ports

Table 3-35 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-36 Query Parameters

Parameter	Mandatory	Type	Description
host_id	Yes	String	Server ID
host_name	No	String	Server name
host_ip	No	String	Server IP address
port	No	Integer	Port number
type	No	String	Port type: TCP or UDP.
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container

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 user token.

Response Parameters

Status code: 200

Table 3-38 Response body parameters

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

Table 3-39 PortResponseInfo

Parameter	Type	Description
host_id	String	Server ID
laddr	String	Listening IP address
status	String	Port status. <ul style="list-style-type: none"> • normal • danger • unknown
port	Integer	Port number
type	String	Port type: TCP or UDP.
pid	Integer	Process ID
path	String	Path of the process execution file.
agent_id	String	Agent ID
container_id	String	Container ID

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListPortsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        environment variables and decrypted during use to ensure security.
    }
}
```

```
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ListPortsRequest request = new ListPortsRequest();
try {
    ListPortsResponse response = client.listPorts(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPortsRequest()
        response = client.list_ports(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPortsRequest{}
    response, err := client.ListPorts(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.9 Querying the Server List of the Software

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/asset/apps

Table 3-40 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-41 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	Software version
install_dir	No	String	Installation directory

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-42 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-43 Response body parameters

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

Table 3-44 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
update_time	Long	Latest update time, in milliseconds.
recent_scan_time	Long	Latest scanning time, in milliseconds.
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAppsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ListAppsRequest request = new ListAppsRequest();
        try {
            ListAppsResponse response = client.listApps(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAppsRequest()
        response = client.list_apps(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
{
    request := &model.ListAppsRequest{}
    response, err := client.ListApps(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.10 Querying the Service List of Auto-Started Items

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-45 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-46 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 <ul style="list-style-type: none"> ● 0: auto-started service ● 1: scheduled task ● 2: Preload dynamic library ● 3: Run registry key ● 4: startup folder
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-47 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	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 user token.

Response Parameters

Status code: 200

Table 3-48 Response body parameters

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

Table 3-49 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 <ul style="list-style-type: none"> 0: auto-started service 1: scheduled task 2: Preload dynamic library 3: Run registry key 4: startup folder
path	String	Path of the auto-startup item

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

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109axxxxxxxxx",
    "run_user" : "user",
    "recent_scan_time" : 1668240858425
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAutoLaunchsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
```

```
environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ListAutoLaunchsRequest request = new ListAutoLaunchsRequest();
try {
    ListAutoLaunchsResponse response = client.listAutoLaunchs(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAutoLaunchsRequest()
        response = client.list_auto_launchs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```



```
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAutoLaunchesRequest{}
    response, err := client.ListAutoLaunches(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.11 Obtaining the Account Change History

Function

This API is used to obtain the account change history.

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-50 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-51 Query Parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Username
host_id	No	String	Server ID
root_permission	No	Boolean	Whether the user has root permissions
host_name	No	String	Server name
private_ip	No	String	Server private IP address
change_type	No	String	Account change type. The options are as follows: <ul style="list-style-type: none">• ADD• DELETE• MODIFY
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-52 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>

Response Parameters

Status code: 200

Table 3-53 Response body parameters

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

Table 3-54 UserChangeHistoryResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
change_type	String	Change type. Its value can be: <ul style="list-style-type: none"> • ADD • DELETE • MODIFY
host_id	String	Host ID
host_name	String	Server name
private_ip	String	Server private IP address
login_permission	Boolean	Whether the user has the login permission
root_permission	Boolean	Whether the user has root permissions
user_group_name	String	User group name
user_home_dir	String	User home directory
shell	String	User startup shell
user_name	String	Account name
expire_time	Long	Expiration time, which is a timestamp. The default unit is millisecond.
recent_scan_time	Long	Time when an account is added, modified, or deleted.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxxxxece69",
    "private_ip" : "192.168.0.1",
    "host_name" : "test",
    "user_home_dir" : "/test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "expire_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_name" : "bin",
    "change_type" : "ADD"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListUserChangeHistoriesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListUserChangeHistoriesRequest request = new ListUserChangeHistoriesRequest();
        try {
            ListUserChangeHistoriesResponse response = client.listUserChangeHistories(request);
        }
    }
}
```

```
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListUserChangeHistoriesRequest()
        response = client.list_user_change_histories(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
```

```

example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListUserChangeHistoriesRequest{}
response, err := client.ListUserChangeHistories(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.12 Obtaining the Historical Change Records of Software Information

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-55 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-56 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_ip	No	String	Server IP address
host_name	No	String	Server name
app_name	No	String	Software name
variation_type	No	String	Change type. Its value can be: <ul style="list-style-type: none"> • add • delete • modify
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
sort_key	No	String	Key value used for sorting. Currently, data can only be sorted by recent_scan_time, and the value of sort_dir determines whether to sort the data in ascending or descending order.

Parameter	Mandatory	Type	Description
sort_dir	No	String	Sorting order. The default order is descending. If sort_key is set to recent_scan_time, this parameter determines the sorting order. If sort_key is set to other values, data is sort in descending order. <ul style="list-style-type: none"> • asc: ascending order • desc: descending order
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
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 3-57 Request header parameters

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

Response Parameters

Status code: 200

Table 3-58 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of software changes

Parameter	Type	Description
data_list	Array of AppChangeResponseInfo objects	Account change history

Table 3-59 AppChangeResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
variation_type	String	Type of change. <ul style="list-style-type: none"> • add • delete • modify
host_id	String	host_id
app_name	String	Software name
host_name	String	Server name
host_ip	String	Server IP address
version	String	Version number
update_time	Long	Updated
recent_scan_time	Long	Last scanned

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

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxx",
    "variation_type" : "add",
    "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  
}]  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListAppChangeHistoriesSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ListAppChangeHistoriesRequest request = new ListAppChangeHistoriesRequest();  
        try {  
            ListAppChangeHistoriesResponse response = client.listAppChangeHistories(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

Python

```
# coding: utf-8  
  
import os
```

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAppChangeHistoriesRequest()
        response = client.list_app_change_histories(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAppChangeHistoriesRequest{}
    response, err := client.ListAppChangeHistories(request)
    if err == nil {
```

```

    fmt.Printf("%+v\n", response)
  } else {
    fmt.Println(err)
  }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.13 Obtaining the Historical Change Records of Auto-started Items

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-61 Query Parameters

Parameter	Mandatory	Type	Description
host_id	No	String	Server ID
host_ip	No	String	Server IP address

Parameter	Mandatory	Type	Description
host_name	No	String	Server name
auto_launch_name	No	String	Auto-started item name
type	No	Integer	Auto-started item type. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • add • delete • modify
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
sort_key	No	String	Key value used for sorting. Currently, data can only be sorted by recent_scan_time, and the value of sort_dir determines whether to sort the data in ascending or descending order.

Parameter	Mandatory	Type	Description
sort_dir	No	String	Sorting order. The default order is descending. If sort_key is set to recent_scan_time, this parameter determines the sorting order. If sort_key is set to other values, data is sort in descending order. <ul style="list-style-type: none"> • asc: ascending order • desc: descending order
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
start_time	No	Long	Start time of a change. Its value is a 13-digit timestamp.
end_time	No	Long	End time of a change. Its value is a 13-digit timestamp.

Request Parameters

Table 3-62 Request header parameters

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

Response Parameters

Status code: 200

Table 3-63 Response body parameters

Parameter	Type	Description
total_num	Integer	Number of changes of auto-started items

Parameter	Type	Description
data_list	Array of AutoLaunchChangeResponseInfo objects	Account change history

Table 3-64 AutoLaunchChangeResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
variation_type	String	Type of change. <ul style="list-style-type: none"> • add • delete • modify
type	Integer	Auto-started item type <ul style="list-style-type: none"> • 0: auto-started service • 1: scheduled task • 2: Preload dynamic library • 3: Run registry key • 4: startup folder
host_id	String	host_id
host_name	String	ECS name
host_ip	String	Server IP address
path	String	Path of the auto-startup item
hash	String	Hash value of the file generated using the SHA256 algorithm
run_user	String	User who starts the execution
name	String	Auto-started item name
recent_scan_time	Long	Last update time. The value is a 13-bit timestamp.

Example Requests

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

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


Example Responses

Status code: 200

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44xxxxxxxx",
    "variation_type" : "add",
    "type" : 0,
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "path" : "/path",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109xxxxxxxx",
    "run_user" : "SYSTEM",
    "name" : "S12hostguard",
    "recent_scan_time" : 1668246126302
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAutoLaunchChangeHistoriesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAutoLaunchChangeHistoriesRequest request = new ListAutoLaunchChangeHistoriesRequest();
        try {
            ListAutoLaunchChangeHistoriesResponse response = client.listAutoLaunchChangeHistories(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
```

```
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAutoLaunchChangeHistoriesRequest()
        response = client.list_auto_launch_change_histories(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
```

```

sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListAutoLaunchChangeHistoriesRequest{}
response, err := client.ListAutoLaunchChangeHistories(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.14 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 3-65 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-66 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
host_name	No	String	Server name
host_ip	No	String	Server IP address
path	No	String	Process executable file path
category	No	String	<p>Type. The default value is host. The options are as follows:</p> <ul style="list-style-type: none"> • host • container
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-67 Request header parameters

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

Response Parameters

Status code: 200

Table 3-68 Response body parameters

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

Table 3-69 ProcessesHostResponseInfo

Parameter	Type	Description
hash	String	The SHA256 value of the path.
host_ip	String	Server IP address
host_name	String	Server name
launch_params	String	Startup parameter
launch_time	Long	Start time
process_path	String	Path of the process execution file.
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListProcessesHostSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
```

```
        .build();
ListProcessesHostRequest request = new ListProcessesHostRequest();
try {
    ListProcessesHostResponse response = client.listProcessesHost(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListProcessesHostRequest()
        response = client.list_processes_host(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListProcessesHostRequest{}
response, err := client.ListProcessesHost(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.15 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 3-70 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-71 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
host_name	No	String	Server name
host_ip	No	String	Server IP address
port	Yes	Integer	Port number
type	No	String	Port type: TCP or UDP.
category	No	String	Type. The default value is host. The options are as follows: <ul style="list-style-type: none"> host container
limit	No	Integer	Number of records on each page

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-72 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 user token.

Response Parameters

Status code: 200

Table 3-73 Response body parameters

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

Table 3-74 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	Path of the process execution file.

Parameter	Type	Description
pid	Integer	pid
port	Integer	Port
status	String	Status
type	String	Port type: TCP or UDP.
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

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "03117200-xxxx-xxxx-xxxx-a89a10e66d6e",
    "host_ip" : "192.168.0.1",
    "host_name" : "ecs-eule",
    "laddr" : "0.0.0.0",
    "path" : "C:\\Windows\\system32\\svchost.exe",
    "port" : 888,
    "status" : "unknow",
    "type" : "UDP",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1WO6",
    "agent_id" : "03jjj-xxxx-xxxx-wwwsedf"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;
```

```
public class ListPortHostSolution {
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListPortHostRequest request = new ListPortHostRequest();
        try {
            ListPortHostResponse response = client.listPortHost(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPortHostRequest()
        response = client.list_port_host(request)
```

```
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPortHostRequest{}
    response, err := client.ListPortHost(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.16 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 3-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-76 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
file_name	No	String	JAR file name

Parameter	Mandatory	Type	Description
category	No	String	Type. Its value can be: <ul style="list-style-type: none"> • host • container
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-77 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 3-78 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of JAR packages
data_list	Array of JarPackageStatisticsResponseInfo objects	JAR package statistics list

Table 3-79 JarPackageStatisticsResponseInfo

Parameter	Type	Description
file_name	String	JAR file name

Parameter	Type	Description
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListJarPackageStatisticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
```



```
        .withRegion(HssRegion.valueOf("<YOUR REGION>"))
        .build();
ListJarPackageStatisticsRequest request = new ListJarPackageStatisticsRequest();
try {
    ListJarPackageStatisticsResponse response = client.listJarPackageStatistics(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListJarPackageStatisticsRequest()
        response = client.list_jar_package_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListJarPackageStatisticsRequest{}
    response, err := client.ListJarPackageStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.1.17 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 3-80 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-81 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
file_name	Yes	String	File name
category	No	String	Type. Its value can be: <ul style="list-style-type: none"> • host • container
host_name	No	String	Server name
host_ip	No	String	Server IP address
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Parameter	Mandatory	Type	Description
part_match	No	Boolean	Whether fuzzy match is used. The default value is false.

Request Parameters

Table 3-82 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 3-83 Response body parameters

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

Table 3-84 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

Parameter	Type	Description
file_type	String	JAR package suffix
version	String	JAR package version
path	String	JAR package path
hash	String	JAR package hash
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

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListJarPackageHostInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListJarPackageHostInfoRequest request = new ListJarPackageHostInfoRequest();
        try {
            ListJarPackageHostInfoResponse response = client.listJarPackageHostInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListJarPackageHostInfoRequest()
        response = client.list_jar_package_host_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
    request := &model.ListJarPackageHostInfoRequest{}
    response, err := client.ListJarPackageHostInfo(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-85 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-86 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records displayed on each page.
host_name	No	String	Server name
os_type	No	String	<p>OS type. Its value can be:</p> <ul style="list-style-type: none"> • Linux • Windows
host_ip	No	String	Server IP address
host_status	No	String	<p>Server status. Its value can be:</p> <ul style="list-style-type: none"> • If no parameter is transferred, it indicates all items. <ul style="list-style-type: none"> - 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 3-87 Request header parameters

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

Response Parameters

Status code: 200

Table 3-88 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of ProtectionServerInfo objects	Query the servers protected against ransomware.

Table 3-89 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: <ul style="list-style-type: none"> Linux Windows
os_name	String	OS name

Parameter	Type	Description
host_status	String	Server status. The options are as follows: <ul style="list-style-type: none"> ACTIVE SHUTOFF
ransom_protection_status	String	Ransomware protection status. The options are as follows: <ul style="list-style-type: none"> closed opened opening: The function is being enabled. closing: The function is being disabled.
agent_version	String	Agent version
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> failed_to_turn_on_backup: Backup cannot be enabled. closed opened
count_protect_event	Integer	Number of protection events
count_backups	Integer	Existing backups
agent_status	String	Agent status

Parameter	Type	Description
version	String	HSS edition. Its value can be: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • ecs : • outside: on-premises servers • workspace: cloud desktop
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) or pre_paid.
vault_status	String	Vault status can be: <ul style="list-style-type: none"> • 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

Parameter	Type	Description
backup_policy_enabled	Boolean	Whether the policy is enabled
resources_num	Integer	Bound servers

Table 3-90 backup_error

Parameter	Type	Description
error_code	Integer	Error code. The options are as follows: <ul style="list-style-type: none"> • 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.
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListProtectionServerSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListProtectionServerRequest request = new ListProtectionServerRequest();
        try {
            ListProtectionServerResponse response = client.listProtectionServer(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListProtectionServerRequest()
        response = client.list_protection_server(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
    request := &model.ListProtectionServerRequest{}
    response, err := client.ListProtectionServer(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.2.2 Querying the Protection Policy List of Ransomware

Function

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

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-91 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-92 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
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	<p>OSs supported by the policy. The options are as follows:</p> <ul style="list-style-type: none"> ● Windows ● Linux

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.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-94 Response body parameters

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

Table 3-95 ProtectionPolicyInfo

Parameter	Type	Description
policy_id	String	Policy ID
policy_name	String	Policy name
protection_mode	String	Action. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> • opened • closed
protection_directory	String	Protected directory
protection_type	String	Protected file type, for example, .docx, .txt, and .avi.
exclude_directory	String	(Optional) excluded directory
runtime_detection_status	String	Whether to perform runtime checks. The options are as follows. Currently, it can only be disabled. This field is reserved. <ul style="list-style-type: none"> • opened • closed
runtime_detection_directory	String	Directory to be checked during running. This field is reserved.
count_associated_server	Integer	Number of associated servers
operating_system	String	OS type. <ul style="list-style-type: none"> • Linux • Windows
process_whitelist	Array of TrustProcessInfo objects	Process whitelist
default_policy	Integer	Indicates whether the policy is the default policy. The options are as follows: <ul style="list-style-type: none"> • 0: non-default policy • 1: default policy

Table 3-96 TrustProcessInfo

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

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListProtectionPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
```

```
        .withRegion(HssRegion.valueOf("<YOUR REGION>"))
        .build();
ListProtectionPolicyRequest request = new ListProtectionPolicyRequest();
try {
    ListProtectionPolicyResponse response = client.listProtectionPolicy(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListProtectionPolicyRequest()
        response = client.list_protection_policy(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListProtectionPolicyRequest{}
    response, err := client.ListProtectionPolicy(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.2.3 Modifying Ransomware Protection Policies

Function

This API is used to modify ransomware protection policies.

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-97 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-98 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-99 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-100 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: <ul style="list-style-type: none"> alarm_and_isolation: Report an alarm and isolate. alarm_only: Only report alarms.
bait_protection_status	No	String	Whether to enable honeypot protection. By default, the protection is enabled. Its value can be: <ul style="list-style-type: none"> opened closed
protection_directory	Yes	String	Protected directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
protection_type	Yes	String	Protected file type, for example, .docx, .txt, and .avi.
exclude_directory	No	String	(Optional) Excluded directory. Separate multiple directories with semicolons (;). You can configure up to 20 directories.
agent_id_list	No	Array of strings	Specifies the IDs of agents for which the ransomware protection policy is enabled.
operating_system	Yes	String	OSs supported by the policy. The options are as follows: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> opened closed
process_whitelist	No	Array of TrustProcessInfo objects	Process whitelist

Table 3-101 TrustProcessInfo

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

Response Parameters

None

Example Requests

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

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
```

```
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdateProtectionPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateProtectionPolicyRequest request = new UpdateProtectionPolicyRequest();
        UpdateProtectionPolicyInfoRequestInfo body = new UpdateProtectionPolicyInfoRequestInfo();
        List<String> listbodyAgentIdList = new ArrayList<>();
        listbodyAgentIdList.add("");
        body.withRuntimeDetectionStatus("closed");
        body.withOperatingSystem("Linux");
        body.withAgentIdList(listbodyAgentIdList);
        body.withExcludeDirectory("");
        body.withProtectionType("docx");
        body.withProtectionDirectory("/root");
        body.withBaitProtectionStatus("opened");
        body.withProtectionMode("alarm_only");
        body.withPolicyName("aaa");
        body.withPolicyId("0253edfd-30e7-439d-8f3f-17c54c997064");
        request.withBody(body);
        try {
            UpdateProtectionPolicyResponse response = client.updateProtectionPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

```
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateProtectionPolicyRequest()
        listAgentIdListbody = [
            ""
        ]
        request.body = UpdateProtectionPolicyInfoRequestInfo(
            runtime_detection_status="closed",
            operating_system="Linux",
            agent_id_list=listAgentIdListbody,
            exclude_directory="",
            protection_type="docx",
            protection_directory="/root",
            bait_protection_status="opened",
            protection_mode="alarm_only",
            policy_name="aaa",
            policy_id="0253edfd-30e7-439d-8f3f-17c54c997064"
        )
        response = client.update_protection_policy(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```

ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateProtectionPolicyRequest{}
var listAgentIdListbody = []string{
    "",
}
runtimeDetectionStatusUpdateProtectionPolicyInfoRequestInfo:= "closed"
excludeDirectoryUpdateProtectionPolicyInfoRequestInfo:= ""
baitProtectionStatusUpdateProtectionPolicyInfoRequestInfo:= "opened"
request.Body = &model.UpdateProtectionPolicyInfoRequestInfo{
    RuntimeDetectionStatus: &runtimeDetectionStatusUpdateProtectionPolicyInfoRequestInfo,
    OperatingSystem: "Linux",
    AgentIdList: &listAgentIdListbody,
    ExcludeDirectory: &excludeDirectoryUpdateProtectionPolicyInfoRequestInfo,
    ProtectionType: "docx",
    ProtectionDirectory: "/root",
    BaitProtectionStatus: &baitProtectionStatusUpdateProtectionPolicyInfoRequestInfo,
    ProtectionMode: "alarm_only",
    PolicyName: "aaa",
    PolicyId: "0253edfd-30e7-439d-8f3f-17c54c997064",
}
response, err := client.UpdateProtectionPolicy(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-102 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-103 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-104 Request header parameters

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

Table 3-105 Request body parameters

Parameter	Mandatory	Type	Description
operating_system	Yes	String	OSs of the server to be protected. The options are as follows: <ul style="list-style-type: none"> Windows Linux
ransom_protection_status	Yes	String	Whether ransomware protection is enabled. Its value can be: <ul style="list-style-type: none"> closed opened If this parameter is enabled, either protection_policy_id or create_protection_policy must be specified.
protection_policy_id	No	String	Ransomware 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.

Parameter	Mandatory	Type	Description
backup_protection_status	Yes	String	Whether to back up data on the server. Its value can be: <ul style="list-style-type: none"> 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 3-106 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.
protection_mode	No	String	Protection action. This parameter is mandatory when you create a protection policy. The options are as follows: <ul style="list-style-type: none"> alarm_and_isolation: Report an alarm and isolate. alarm_only: Only report alarms.

Parameter	Mandatory	Type	Description
bait_protection_status	No	String	Whether to enable honeypot protection. This parameter is mandatory when you create a protection policy. The options are as follows. By default, honeypot protection is enabled. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • opened • closed
operating_system	No	String	OS. This parameter is mandatory when you create a protection policy. Its value can be: <ul style="list-style-type: none"> • Windows • Linux
process_whitelist	No	Array of TrustProcessInfo objects	Process whitelist

Table 3-107 TrustProcessInfo

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

Table 3-108 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 3-109 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 3-110 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.
operation_definition	No	OperationDefinitionRequestInfo object	Scheduling parameter.
trigger	No	BackupTriggerRequestInfo1 object	Time scheduling rule for the policy.

Table 3-111 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
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

Parameter	Mandatory	Type	Description
retention_duration_days	No	Integer	Duration of retaining a backup, in days. The maximum value is 99999. If the value is set to -1, backups will not be cleared even though the configured retention duration is exceeded. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum value: 1. Maximum value: 99999. Default value: -1
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 3-112 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 3-113 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 <code>FREQ</code> , <code>BYDAY</code> , <code>BYHOUR</code> , <code>BYMINUTE</code> , and <code>INTERVAL</code> . <code>FREQ</code> can be set only to <code>WEEKLY</code> or <code>DAILY</code> . <code>BYDAY</code> can be set to <code>MO</code> , <code>TU</code> , <code>WE</code> , <code>TH</code> , <code>FR</code> , <code>SA</code> , or <code>SU</code> (seven days of a week). <code>BYHOUR</code> ranges from 0 to 23 hours. <code>BYMINUTE</code> 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: <code>FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00</code> . To start scheduling at 14:00 every day, the rule is as follows: <code>FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00</code> .

Response Parameters

None

Example Requests

Enable ransomware protection for the server. The OS type is Linux, the target server ID is 71a15ecc-049f-4cca-bd28-5e90aca1817f, and the agent ID of the target server is c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8. Server backup is disabled.

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class StartProtectionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
    }
}
```

```
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
StartProtectionRequest request = new StartProtectionRequest();
ProtectionInfoRequestInfo body = new ProtectionInfoRequestInfo();
List<String> listbodyHostIdList = new ArrayList<>();
listbodyHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
List<String> listbodyAgentIdList = new ArrayList<>();
listbodyAgentIdList.add("c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8");
ProtectionProxyInfoRequestInfo createProtectionPolicybody = new ProtectionProxyInfoRequestInfo();
createProtectionPolicybody.withPolicyName("test111")
    .withProtectionMode("alarm_only")
    .withBaitProtectionStatus("opened")
    .withProtectionDirectory("/etc/test")
    .withProtectionType("docx")
    .withExcludeDirectory("");
body.withHostIdList(listbodyHostIdList);
body.withAgentIdList(listbodyAgentIdList);
body.withBackupProtectionStatus("closed");
body.withCreateProtectionPolicy(createProtectionPolicybody);
body.withProtectionPolicyId("");
body.withRansomProtectionStatus("opened");
body.withOperatingSystem("Linux");
request.withBody(body);
try {
    StartProtectionResponse response = client.startProtection(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = StartProtectionRequest()
        listHostIdListbody = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        listAgentIdListbody = [
            "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8"
        ]
        createProtectionPolicybody = ProtectionProxyInfoRequestInfo(
            policy_name="test111",
            protection_mode="alarm_only",
            bait_protection_status="opened",
            protection_directory="/etc/test",
            protection_type="docx",
            exclude_directory=""
        )
        request.body = ProtectionInfoRequestInfo(
            host_id_list=listHostIdListbody,
            agent_id_list=listAgentIdListbody,
            backup_protection_status="closed",
            create_protection_policy=createProtectionPolicybody,
            protection_policy_id="",
            ransom_protection_status="opened",
            operating_system="Linux"
        )
        response = client.start_protection(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.StartProtectionRequest{}
    var listHostIdListbody = []string{
        "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    }
    var listAgentIdListbody = []string{
        "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
    }
    policyNameCreateProtectionPolicy:= "test111"
    protectionModeCreateProtectionPolicy:= "alarm_only"
    baitProtectionStatusCreateProtectionPolicy:= "opened"
    protectionDirectoryCreateProtectionPolicy:= "/etc/test"
    protectionTypeCreateProtectionPolicy:= "docx"
    excludeDirectoryCreateProtectionPolicy:= ""
    createProtectionPolicybody := &model.ProtectionProxyInfoRequestInfo{
        PolicyName: &policyNameCreateProtectionPolicy,
        ProtectionMode: &protectionModeCreateProtectionPolicy,
        BaitProtectionStatus: &baitProtectionStatusCreateProtectionPolicy,
        ProtectionDirectory: &protectionDirectoryCreateProtectionPolicy,
        ProtectionType: &protectionTypeCreateProtectionPolicy,
        ExcludeDirectory: &excludeDirectoryCreateProtectionPolicy,
    }
    protectionPolicyIdProtectionInfoRequestInfo:= ""
    request.Body = &model.ProtectionInfoRequestInfo{
        HostIdList: listHostIdListbody,
        AgentIdList: listAgentIdListbody,
        BackupProtectionStatus: "closed",
        CreateProtectionPolicy: createProtectionPolicybody,
        ProtectionPolicyId: &protectionPolicyIdProtectionInfoRequestInfo,
        RansomProtectionStatus: "opened",
        OperatingSystem: "Linux",
    }
    response, err := client.StartProtection(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-114 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-115 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-116 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-117 Request body parameters

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

Parameter	Mandatory	Type	Description
agent_id_list	Yes	Array of strings	IDs of agents where ransomware prevention needs to be disabled
close_protection_type	Yes	String	Type of disabled protection. The options are as follows: <ul style="list-style-type: none">close_anti: Disable ransomware protection. Currently, backup protection cannot be disabled. Go to the CBR service to unbind a vault.

Response Parameters

None

Example Requests

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

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
```

```
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class StopProtectionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        StopProtectionRequest request = new StopProtectionRequest();
        CloseProtectionInfoRequestInfo body = new CloseProtectionInfoRequestInfo();
        List<String> listbodyAgentIdList = new ArrayList<>();
        listbodyAgentIdList.add("c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8");
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
        body.withCloseProtectionType("close_anti");
        body.withAgentIdList(listbodyAgentIdList);
        body.withHostIdList(listbodyHostIdList);
        request.withBody(body);
        try {
            StopProtectionResponse response = client.stopProtection(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = StopProtectionRequest()
        listAgentIdListbody = [
            "c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8"
        ]
        listHostIdListbody = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        request.body = CloseProtectionInfoRequestInfo(
            close_protection_type="close_anti",
            agent_id_list=listAgentIdListbody,
            host_id_list=listHostIdListbody
        )
        response = client.stop_protection(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
```

```
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.StopProtectionRequest{}
var listAgentIdListbody = []string{
    "c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8",
}
var listHostIdListbody = []string{
    "71a15ecc-049f-4cca-bd28-5e90aca1817f",
}
request.Body = &model.CloseProtectionInfoRequestInfo{
    CloseProtectionType: "close_anti",
    AgentIdList: listAgentIdListbody,
    HostIdList: listHostIdListbody,
}
response, err := client.StopProtection(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-118 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-119 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-120 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-121 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: <ul style="list-style-type: none"> • backup • replication
operation_definition	OperationDefinitionInfo object	Policy attribute. Reserved rule.
trigger	BackupTriggerInfo object	Backup policy scheduling rule

Table 3-122 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

Parameter	Type	Description
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
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 3-123 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 3-124 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowBackupPolicyInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowBackupPolicyInfoRequest request = new ShowBackupPolicyInfoRequest();
        try {
            ShowBackupPolicyInfoResponse response = client.showBackupPolicyInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
        }
    }
}
```

```
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowBackupPolicyInfoRequest()
        response = client.show_backup_policy_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
```

```

Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ShowBackupPolicyInfoRequest{}
response, err := client.ShowBackupPolicyInfo(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-125 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-126 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-127 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-128 Request body parameters

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether the policy is enabled. The default value is true.
policy_id	Yes	String	Backup policy ID

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

Table 3-129 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 3-130 BackupTriggerRequestInfo

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

Table 3-131 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

None

Example Requests

Modify the backup policy. The target backup policy ID is af4d08ad-2b60-4916-a5cf-8d6a23956dda.

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

```
{
  "enabled" : true,
  "policy_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
  "operation_definition" : {
    "day_backups" : 0,
    "max_backups" : -1,
    "month_backups" : 0,
    "retention_duration_days" : 5,
    "timezone" : "UTC+08:00",
    "week_backups" : 0,
  }
}
```

```
"year_backups" : 0
},
"trigger" : {
  "properties" : {
    "pattern" : [ "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00" ]
  }
}
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Modify the backup policy. The target backup policy ID is af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdateBackupPolicyInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateBackupPolicyInfoRequest request = new UpdateBackupPolicyInfoRequest();
        UpdateBackupPolicyRequestInfo body = new UpdateBackupPolicyRequestInfo();
        List<String> listPropertiesPattern = new ArrayList<>();
        listPropertiesPattern.add("FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00");
        BackupTriggerPropertiesRequestInfo propertiesTrigger = new BackupTriggerPropertiesRequestInfo();
        propertiesTrigger.withPattern(listPropertiesPattern);
        BackupTriggerRequestInfo triggerbody = new BackupTriggerRequestInfo();
        triggerbody.withProperties(propertiesTrigger);
        OperationDefinitionRequestInfo operationDefinitionbody = new OperationDefinitionRequestInfo();
```

```
operationDefinitionbody.withDayBackups(0)
    .withMaxBackups(-1)
    .withMonthBackups(0)
    .withRetentionDurationDays(5)
    .withTimezone("UTC+08:00")
    .withWeekBackups(0)
    .withYearBackups(0);
body.withTrigger(triggerbody);
body.withOperationDefinition(operationDefinitionbody);
body.withPolicyId("af4d08ad-2b60-4916-a5cf-8d6a23956dda");
body.withEnabled(true);
request.withBody(body);
try {
    UpdateBackupPolicyInfoResponse response = client.updateBackupPolicyInfo(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Modify the backup policy. The target backup policy ID is af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateBackupPolicyInfoRequest()
        listPatternProperties = [
            "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00"
        ]
        propertiesTrigger = BackupTriggerPropertiesRequestInfo(
            pattern=listPatternProperties
        )
        triggerbody = BackupTriggerRequestInfo(
            properties=propertiesTrigger
        )
```

```
)
operationDefinitionbody = OperationDefinitionRequestInfo(
    day_backups=0,
    max_backups=-1,
    month_backups=0,
    retention_duration_days=5,
    timezone="UTC+08:00",
    week_backups=0,
    year_backups=0
)
request.body = UpdateBackupPolicyRequestInfo(
    trigger=triggerbody,
    operation_definition=operationDefinitionbody,
    policy_id="af4d08ad-2b60-4916-a5cf-8d6a23956dda",
    enabled=True
)
response = client.update_backup_policy_info(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Modify the backup policy. The target backup policy ID is af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateBackupPolicyInfoRequest{}
    var listPatternProperties = []string{
        "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00",
    }
    propertiesTrigger := &model.BackupTriggerPropertiesRequestInfo{
        Pattern: listPatternProperties,
    }
    triggerbody := &model.BackupTriggerRequestInfo{
```

```

    Properties: propertiesTrigger,
  }
  dayBackupsOperationDefinition:= int32(0)
  maxBackupsOperationDefinition:= int32(-1)
  monthBackupsOperationDefinition:= int32(0)
  retentionDurationDaysOperationDefinition:= int32(5)
  timezoneOperationDefinition:= "UTC+08:00"
  weekBackupsOperationDefinition:= int32(0)
  yearBackupsOperationDefinition:= int32(0)
  operationDefinitionbody := &model.OperationDefinitionRequestInfo{
    DayBackups: &dayBackupsOperationDefinition,
    MaxBackups: &maxBackupsOperationDefinition,
    MonthBackups: &monthBackupsOperationDefinition,
    RetentionDurationDays: &retentionDurationDaysOperationDefinition,
    Timezone: &timezoneOperationDefinition,
    WeekBackups: &weekBackupsOperationDefinition,
    YearBackups: &yearBackupsOperationDefinition,
  }
  enabledUpdateBackupPolicyRequestInfo:= true
  request.Body = &model.UpdateBackupPolicyRequestInfo{
    Trigger: triggerbody,
    OperationDefinition: operationDefinitionbody,
    PolicyId: "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
    Enabled: &enabledUpdateBackupPolicyRequestInfo,
  }
  response, err := client.UpdateBackupPolicyInfo(request)
  if err == nil {
    fmt.Printf("%v\n", response)
  } else {
    fmt.Println(err)
  }
}

```

More

For SDK sample code of more programming languages, see the [Sample Code](#) tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-132 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-133 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
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

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-134 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 3-135 Response body parameters

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

Table 3-136 WeakPwdListInfoResponseInfo

Parameter	Type	Description
host_id	String	Host ID
host_name	String	Server name
host_ip	String	Server IP address (private IP address). This field is not deleted for compatibility with users.
private_ip	String	Server private IP address

Parameter	Type	Description
public_ip	String	Server public IP address
weak_pwd_accounts	Array of WeakPwdAccountInfoResponseInfo objects	List of accounts with weak passwords

Table 3-137 WeakPwdAccountInfoResponseInfo

Parameter	Type	Description
user_name	String	Name of accounts with weak passwords
service_type	String	Account type. The options are as follows: <ul style="list-style-type: none"> • system • mysql • redis
duration	Integer	Validity period of a weak password, in days.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_num" : 2,
  "data_list" : [ {
    "host_id" : "caa958adxxxxxa481",
    "host_name" : "ubuntu1",
    "host_ip" : "192.168.0.8",
    "private_ip" : "192.168.0.8",
    "public_ip" : "100.85.85.85",
    "weak_pwd_accounts" : [ {
      "user_name" : "localhost1",
      "service_type" : "system",
      "duration" : 2147483647
    } ]
  }, {
    "host_id" : "caa958adxxxxxa482",
    "host_name" : "ubuntu2",
    "host_ip" : "192.168.0.9",
```

```
"private_ip" : "192.168.0.8",
"public_ip" : "",
"weak_pwd_accounts" : [ {
  "user_name" : "localhost2",
  "service_type" : "system",
  "duration" : 2147483647
} ]
} ]
} }
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListWeakPasswordUsersSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListWeakPasswordUsersRequest request = new ListWeakPasswordUsersRequest();
        try {
            ListWeakPasswordUsersResponse response = client.listWeakPasswordUsers(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListWeakPasswordUsersRequest()
        response = client.list_weak_password_users(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
    request := &model.ListWeakPasswordUsersRequest{}
    response, err := client.ListWeakPasswordUsers(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-138 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-139 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
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 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.

Request Parameters

Table 3-140 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>

Response Parameters

Status code: 200

Table 3-141 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 3-142 PwdPolicyInfoResponseInfo

Parameter	Type	Description
host_id	String	Server ID
host_name	String	Server name
host_ip	String	Server IP address (private IP address). This field is not deleted for compatibility with users.
private_ip	String	Server private IP address
public_ip	String	Server public IP address
min_length	Boolean	Indicates whether the minimum password length meets the requirements. If the value is true, the minimum password length meets the requirements. If the value is false, the minimum password length does not meet the requirements.
uppercase_letter	Boolean	Indicates whether the uppercase letters meet the requirements. If the value is true, the uppercase letters meet the requirements. If the value is false, the uppercase letters do not meet the requirements.
lowercase_letter	Boolean	Indicates whether the lowercase letters meet the requirements. If the value is true, the lowercase letters meet the requirements. If the value is false, the lowercase letters do not meet the requirements.

Parameter	Type	Description
number	Boolean	Indicates whether the number meets the requirements. If the value is true, the number meets the requirements. If the value is false, the number does not meet the requirements.
special_character	Boolean	Indicates whether the special character meets the requirements. If the value is true, the special character meets the requirements. If the value is false, the special character does not meet the requirements.
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

Request succeeded.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "76fa440a-5a08-43fa-ac11-d12183ab3a14",
    "host_ip" : "192.168.0.59",
    "private_ip" : "192.168.0.8",
    "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
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```

```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListPasswordComplexitySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListPasswordComplexityRequest request = new ListPasswordComplexityRequest();
        try {
            ListPasswordComplexityResponse response = client.listPasswordComplexity(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```



```
client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListPasswordComplexityRequest()
    response = client.list_password_complexity(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPasswordComplexityRequest{}
    response, err := client.ListPasswordComplexity(request)
    if err == nil {
        fmt.Printf("%v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-143 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-144 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
check_name	No	String	Baseline name, for example, SSH, CentOS 7, and Windows.
group_id	No	String	Indicates the policy group ID.
severity	No	String	<p>Risk level. Its value can be:</p> <ul style="list-style-type: none"> • Security • Low • Medium • High
standard	No	String	<p>Standard type. Its value can be:</p> <ul style="list-style-type: none"> • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
host_id	No	String	Host ID
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-145 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 3-146 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 3-147 SecurityCheckInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: <ul style="list-style-type: none"> Low Medium High
check_name	String	Baseline name, for example, SSH, CentOS 7, and Windows.
check_type	String	Baseline type. The values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2.

Parameter	Type	Description
standard	String	Standard type. Its value can be: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
check_rule_num	Integer	Indicates the total number of check items of the current configuration check (baseline) type. For example, if the standard type of the SSH baseline is hw_standard, server security provides 17 check items, but only five check items of the SSH baseline are detected on all servers. Therefore, the value of check_rule_num is 5. All check items are checked on a server. The value of check_rule_num is 17.
failed_rule_num	Integer	Number of failed check items. If a server fails to pass a check item in check_rule_num, the item is counted in failed_rule_num.
host_num	Integer	The number of servers on which the current baseline detection is performed.
scan_time	Long	Latest detection time (ms)
check_type_desc	String	Description of the baseline type, including the standards for the check items and the issues that can be audited.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListRiskConfigsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListRiskConfigsRequest request = new ListRiskConfigsRequest();
        try {
            ListRiskConfigsResponse response = client.listRiskConfigs(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListRiskConfigsRequest()
        response = client.list_risk_configs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```

Build()
    request := &model.ListRiskConfigsRequest{}
    response, err := client.ListRiskConfigs(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-148 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
check_name	Yes	String	Baseline name, for example, SSH, CentOS 7, and Windows.

Table 3-149 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
standard	Yes	String	<p>Standard type. Its value can be:</p> <ul style="list-style-type: none"> • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
host_id	No	String	<p>Server ID. If this parameter is not specified, all the servers of the user are queried.</p>
limit	No	Integer	<p>Number of records on each page.</p>
offset	No	Integer	<p>Offset, which specifies the start position of the record to be returned.</p>

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 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 3-151 Response body parameters

Parameter	Type	Description
severity	String	Risk level. Its value can be: <ul style="list-style-type: none"> Low Medium High
check_type	String	Configuration check (baseline) type, for example, SSH, CentOS 7, Windows Server 2019 R2, Windows Server 2016 R2 and MySQL5-Windows.
check_type_desc	String	Description of the baseline type, including the standards for the check items and the issues that can be audited.
check_rule_num	Integer	Indicates the total number of check items of the current configuration check (baseline) type. For example, if the standard type of the SSH baseline is hw_standard, server security provides 17 check items, but only five check items of the SSH baseline are detected on all servers. Therefore, the value of check_rule_num is 5. All check items are checked on a server. The value of check_rule_num is 17.
failed_rule_num	Integer	Number of failed check items. If a server fails to pass a check item in check_rule_num, the item is counted in failed_rule_num.

Parameter	Type	Description
passed_rule_num	Integer	Number of passed check items. If a server passes a check item in check_rule_num, the check item is counted in passed_rule_num.
ignored_rule_num	Integer	Number of ignored check items. If a server ignores a check item in check_rule_num, the check item is counted in ignored_rule_num.
host_num	Long	The number of servers on which the current baseline detection is performed.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;
```

```
public class ShowRiskConfigDetailSolution {
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowRiskConfigDetailRequest request = new ShowRiskConfigDetailRequest();
        request.withCheckName("{check_name}");
        try {
            ShowRiskConfigDetailResponse response = client.showRiskConfigDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowRiskConfigDetailRequest()
```

```

request.check_name = "{check_name}"
response = client.show_risk_config_detail(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)

```

Go

```

package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowRiskConfigDetailRequest{}
    request.CheckName = "{check_name}"
    response, err := client.ShowRiskConfigDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-152 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
check_name	Yes	String	Baseline name, for example, SSH, CentOS 7, and Windows.

Table 3-153 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Parameter	Mandatory	Type	Description
standard	Yes	String	Standard type. Its value can be: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
result_type	No	String	Result type. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

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 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 3-155 Response body parameters

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

Table 3-156 CheckRuleRiskInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: <ul style="list-style-type: none"> Low Medium High
check_name	String	Baseline name, for example, SSH, CentOS 7, and Windows.
check_type	String	Baseline type. The values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2.
standard	String	Standard type. Its value can be: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
check_rule_name	String	Check item name
check_rule_id	String	Check item ID
host_num	Integer	The number of servers on which the current baseline detection is performed.

Parameter	Type	Description
scan_result	String	Detection result. Its value can be: <ul style="list-style-type: none"> • pass • failed
status	String	Status. Its value can be: <ul style="list-style-type: none"> • safe • ignored • unhandled • fixing • fix-failed • verifying
enable_fix	Integer	Indicates whether one-click repair is supported. 1: yes; 0: no.
enable_click	Boolean	Whether the Fix, Ignore, and Verify buttons of a check item can be clicked. true: They can be clicked. false: They are grayed out.
rule_params	Array of CheckRuleFixParamInfo objects	Range of parameters applicable to the check items that can be fixed by parameter transfer. This parameter is returned only for check items that support parameter transfer fix.

Table 3-157 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListRiskConfigCheckRulesSolution {

    public static void main(String[] args) {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ListRiskConfigCheckRulesRequest request = new ListRiskConfigCheckRulesRequest();
request.withCheckName("{check_name}");
try {
    ListRiskConfigCheckRulesResponse response = client.listRiskConfigCheckRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListRiskConfigCheckRulesRequest()
```

```
request.check_name = "{check_name}"
response = client.list_risk_config_check_rules(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListRiskConfigCheckRulesRequest{}
    request.CheckName = "{check_name}"
    response, err := client.ListRiskConfigCheckRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-158 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
check_name	Yes	String	Baseline name, for example, SSH, CentOS 7, and Windows.

Table 3-159 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
standard	Yes	String	<p>Standard type. Its value can be:</p> <ul style="list-style-type: none"> 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.

Request Parameters

Table 3-160 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 3-161 Response body parameters

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

Table 3-162 SecurityCheckHostInfoResponseInfo

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

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListRiskConfigHostsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListRiskConfigHostsRequest request = new ListRiskConfigHostsRequest();
        request.withCheckName("{check_name}");
        try {
            ListRiskConfigHostsResponse response = client.listRiskConfigHosts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
```



```
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListRiskConfigHostsRequest()
        request.check_name = "{check_name}"
        response = client.list_risk_config_hosts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```

ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListRiskConfigHostsRequest{}
request.CheckName = "{check_name}"
response, err := client.ListRiskConfigHosts(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-163 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-164 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
check_name	Yes	String	Baseline name, for example, SSH, CentOS 7, and Windows.
check_type	Yes	String	<p>Baseline type. You can obtain the value by calling API /v5/{project_id}/baseline/risk-configs. Note that the values for check_type and check_name are the same for Linux servers. For example, they can both be set to SSH or CentOS 7. For Windows servers, the values for check_type and check_name are different. For example, check_type can be set to Windows Server 2019 R2 or Windows Server 2016 R2, while check_name can be set to Windows.</p>

Parameter	Mandatory	Type	Description
check_rule_id	Yes	String	Check item ID, which can be obtained from the return data of this API: /v5/{project_id}/baseline/risk-config/{check_name}/check-rules
standard	Yes	String	Standard type. Its value can be: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
host_id	No	String	Host ID

Request Parameters

Table 3-165 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 3-166 Response body parameters

Parameter	Type	Description
description	String	Description of the current check item (detection rule).
reference	String	Basis for the check item (rule) setting
audit	String	Audit description of the check item (rule)
remediation	String	Modification suggestions for the check item (rule)

Parameter	Type	Description
check_info_list	Array of CheckRuleCheckCaseResponseInfo objects	Test cases

Table 3-167 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

Request succeeded.

```
{"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"}}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowCheckRuleDetailSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowCheckRuleDetailRequest request = new ShowCheckRuleDetailRequest();
        try {
            ShowCheckRuleDetailResponse response = client.showCheckRuleDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ShowCheckRuleDetailRequest()
    response = client.show_check_rule_detail(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowCheckRuleDetailRequest{}
    response, err := client.ShowCheckRuleDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

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 3-168 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-169 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
host_id	No	String	<p>Server ID. If this parameter is not specified, all the servers of the user are queried.</p>
action	Yes	String	<p>Action.</p> <ul style="list-style-type: none"> • ignore • unignore • fix • verify

Request Parameters

Table 3-170 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>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.</p>

Table 3-171 Request body parameters

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

Table 3-172 CheckRuleKeyInfoRequestInfo

Parameter	Mandatory	Type	Description
check_name	No	String	Name of the configuration check (baseline), for example, SSH, CentOS 7, and Windows.
check_rule_id	No	String	Check item ID, which can be obtained from the return data of this API: /v5/{project_id}/baseline/risk-config/{check_name}/check-rules
standard	No	String	Baseline standards. The options are as follows: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
fix_values	No	Array of CheckRuleFixValuesInfo objects	User-entered repair parameters of check items

Table 3-173 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

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_rules" : [ {  
    "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_rules" : [ {  
    "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

SDK Sample Code

The SDK sample code is as follows.

Java

- 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.

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

```
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeCheckRuleActionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ChangeCheckRuleActionRequest request = new ChangeCheckRuleActionRequest();
        CheckRuleIdListRequestInfo body = new CheckRuleIdListRequestInfo();
        List<CheckRuleKeyInfoRequestInfo> listbodyCheckRules = new ArrayList<>();
        listbodyCheckRules.add(
            new CheckRuleKeyInfoRequestInfo()
                .withCheckName("SSH")
                .withCheckRuleId("1.11")
                .withStandard("hw_standard")
        );
        body.withCheckRules(listbodyCheckRules);
        request.withBody(body);
        try {
            ChangeCheckRuleActionResponse response = client.changeCheckRuleAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

- 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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeCheckRuleActionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ChangeCheckRuleActionRequest request = new ChangeCheckRuleActionRequest();
        CheckRuleIdListRequestInfo body = new CheckRuleIdListRequestInfo();
        List<CheckRuleFixValuesInfo> listCheckRulesFixValues = new ArrayList<>();
        listCheckRulesFixValues.add(
            new CheckRuleFixValuesInfo()
                .withRuleParamId(1)
                .withFixValue(5)
        );
        listCheckRulesFixValues.add(
            new CheckRuleFixValuesInfo()
                .withRuleParamId(2)
                .withFixValue(20)
        );
        List<CheckRuleKeyInfoRequestInfo> listbodyCheckRules = new ArrayList<>();
        listbodyCheckRules.add(
            new CheckRuleKeyInfoRequestInfo()
                .withCheckName("SSH")
                .withCheckRuleId("1.11")
                .withStandard("hw_standard")
                .withFixValues(listCheckRulesFixValues)
        );
        body.withCheckRules(listbodyCheckRules);
        request.withBody(body);
        try {
            ChangeCheckRuleActionResponse response = client.changeCheckRuleAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}
```

Python

- 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.

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
    # environment variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before  
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local  
    # environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ChangeCheckRuleActionRequest()  
        listCheckRulesbody = [  
            CheckRuleKeyInfoRequestInfo(  
                check_name="SSH",  
                check_rule_id="1.11",  
                standard="hw_standard"  
            )  
        ]  
        request.body = CheckRuleIdListRequestInfo(  
            check_rules=listCheckRulesbody  
        )  
        response = client.change_check_rule_action(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

- 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.

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    # environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    # environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeCheckRuleActionRequest()
        listFixValuesCheckRules = [
            CheckRuleFixValuesInfo(
                rule_param_id=1,
                fix_value=5
            ),
            CheckRuleFixValuesInfo(
                rule_param_id=2,
                fix_value=20
            )
        ]
        listCheckRulesbody = [
            CheckRuleKeyInfoRequestInfo(
                check_name="SSH",
                check_rule_id="1.11",
                standard="hw_standard",
                fix_values=listFixValuesCheckRules
            )
        ]
        request.body = CheckRuleIdListRequestInfo(
            check_rules=listCheckRulesbody
        )
        response = client.change_check_rule_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

- 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    // environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeCheckRuleActionRequest{}
    checkNameCheckRules:= "SSH"
    checkRuleIdCheckRules:= "1.11"
    standardCheckRules:= "hw_standard"
    var listCheckRulesbody = []model.CheckRuleKeyInfoRequestInfo{
        {
            CheckName: &checkNameCheckRules,
            CheckRuleId: &checkRuleIdCheckRules,
            Standard: &standardCheckRules,
        },
    }
    request.Body = &model.CheckRuleIdListRequestInfo{
        CheckRules: &listCheckRulesbody,
    }
    response, err := client.ChangeCheckRuleAction(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    // environment
```



```

ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ChangeCheckRuleActionRequest{}
ruleParamIdFixValues:= int32(1)
fixValueFixValues:= int32(5)
ruleParamIdFixValues1:= int32(2)
fixValueFixValues1:= int32(20)
var listFixValuesCheckRules = []model.CheckRuleFixValuesInfo{
    {
        RuleParamId: &ruleParamIdFixValues,
        FixValue: &fixValueFixValues,
    },
    {
        RuleParamId: &ruleParamIdFixValues1,
        FixValue: &fixValueFixValues1,
    },
}
checkNameCheckRules:= "SSH"
checkRuleIdCheckRules:= "1.11"
standardCheckRules:= "hw_standard"
var listCheckRulesbody = []model.CheckRuleKeyInfoRequestInfo{
    {
        CheckName: &checkNameCheckRules,
        CheckRuleId: &checkRuleIdCheckRules,
        Standard: &standardCheckRules,
        FixValues: &listFixValuesCheckRules,
    },
}
request.Body = &model.CheckRuleIdListRequestInfo{
    CheckRules: &listCheckRulesbody,
}
response, err := client.ChangeCheckRuleAction(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.4 Quota Management

3.4.1 Querying Quota Information

Function

This API is used to query quota information.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/billing/quotas

Table 3-174 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-175 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
version	No	String	<p>HSS edition. Its value can be:</p> <ul style="list-style-type: none"> • 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	<p>Billing mode. Its value can be:</p> <ul style="list-style-type: none"> • packet_cycle: yearly/monthly • on_demand: pay-per-use

Request Parameters

Table 3-176 Request header parameters

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

Response Parameters

Status code: 200

Table 3-177 Response body parameters

Parameter	Type	Description
data_list	Array of ResourceQuotasInfo objects	Quota statistics list

Table 3-178 ResourceQuotasInfo

Parameter	Type	Description
version	String	HSS edition. Its value can be: <ul style="list-style-type: none"> 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

Parameter	Type	Description
available_num	Integer	Total quotas
available_resources_list	Array of AvailableResourceIdsInfo objects	Available resource list

Table 3-179 AvailableResourceIdsInfo

Parameter	Type	Description
resource_id	String	Resource ID
current_time	String	Current time
shared_quota	String	Whether quotas are shared. Its value can be: <ul style="list-style-type: none"> 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowResourceQuotasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowResourceQuotasRequest request = new ShowResourceQuotasRequest();
        try {
            ShowResourceQuotasResponse response = client.showResourceQuotas(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ShowResourceQuotasRequest()
    response = client.show_resource_quotas(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowResourceQuotasRequest{}
    response, err := client.ShowResourceQuotas(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.4.2 Querying Quota Details

Function

This API is used to query quota details.

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-180 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-181 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
version	No	String	<p>HSS edition. Its value can be:</p> <ul style="list-style-type: none"> • 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	<p>Type. Its value can be:</p> <ul style="list-style-type: none"> • host_resource • container_resource
quota_status	No	String	<p>Quota status. It can be:</p> <ul style="list-style-type: none"> • QUOTA_STATUS_NORMAL <ul style="list-style-type: none"> - QUOTA_STATUS_EXPIRED - QUOTA_STATUS_FREEZE

Parameter	Mandatory	Type	Description
used_status	No	String	Usage status. It can be: <ul style="list-style-type: none">USED_STATUS_IDLEUSED_STATUS_USED
host_name	No	String	Server name
resource_id	No	String	Specifies the resource ID of the HSS quota.
charging_mode	No	String	Billing mode. Its value can be: <ul style="list-style-type: none">packet_cycle: yearly/monthlyon_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.

Request Parameters

Table 3-182 Request header parameters

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

Response Parameters

Status code: 200

Table 3-183 Response body parameters

Parameter	Type	Description
packet_cycle_num	Integer	Yearly/Monthly quotas
on_demand_num	Integer	Pay-per-Use quotas

Parameter	Type	Description
used_num	Integer	Used quotas
idle_num	Integer	Idle quotas
normal_num	Integer	Normal quotas
expired_num	Integer	Expired quotas
freeze_num	Integer	Frozen quotas
quota_statistics_list	Array of QuotaStatisticsResponseInfo objects	Quota statistics list
total_num	Integer	Total quotas
data_list	Array of QuotaResourcesResponseInfo objects	Quota list

Table 3-184 QuotaStatisticsResponseInfo

Parameter	Type	Description
version	String	Resource flavor. Its value can be: <ul style="list-style-type: none"> • 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 quotas

Table 3-185 QuotaResourcesResponseInfo

Parameter	Type	Description
resource_id	String	Resource ID of an HSS quota

Parameter	Type	Description
version	String	Resource flavor. Its value can be: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • normal • expired • freeze
used_status	String	Usage status. Its value can be: <ul style="list-style-type: none"> • idle • used
host_id	String	Host ID
host_name	String	Server name
charging_mode	String	Billing mode. Its value can be: <ul style="list-style-type: none"> • packet_cycle: yearly/monthly • 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: <ul style="list-style-type: none"> • shared • unshared
enterprise_project_id	String	Enterprise project ID
enterprise_project_name	String	Enterprise project name

Table 3-186 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

Request succeeded.

```
{
  "data_list": [ {
    "charging_mode": "packet_cycle",
    "expire_time": -1,
    "host_id": "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    "host_name": "zhangxiaodong2",
    "quota_status": "normal",
    "resource_id": "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
    "shared_quota": "shared",
    "tags": [ {
      "key": "Service",
      "value": "HSS"
    } ],
    "used_status": "used",
    "version": "hss.version.wtp"
  } ],
  "expired_num": 0,
  "freeze_num": 0,
  "idle_num": 20,
  "normal_num": 60,
  "on_demand_num": 0,
  "packet_cycle_num": 60,
  "quota_statistics_list": [ {
    "total_num": 8,
    "version": "hss.version.basic"
  } ],
  "total_num": 60,
  "used_num": 40
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListQuotasDetailSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListQuotasDetailRequest request = new ListQuotasDetailRequest();
        try {
            ListQuotasDetailResponse response = client.listQuotasDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListQuotasDetailRequest()
    response = client.list_quotas_detail(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListQuotasDetailRequest{}
    response, err := client.ListQuotasDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.4.3 Creating an Order Quota by HSS

Function

The billing mode can only be yearly/monthly when an order quota is created by HSS.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/{project_id}/quotas/orders

Table 3-187 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-188 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-189 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region ID

Table 3-190 Request body parameters

Parameter	Mandatory	Type	Description
resource_spec_code	Yes	String	Specifications <ul style="list-style-type: none"> • 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
period_type	Yes	Integer	Subscription period type. <ul style="list-style-type: none"> • 2: month • 3: year
period_num	Yes	Integer	Number of subscription periods
is_auto_renew	No	Boolean	Whether to support auto renewal. The options are true (yes) and false (no). The default value is false.
is_auto_pay	No	Boolean	whether to support automatic payment. The options are true (yes) and false (no). The default value is false.
subscription_num	Yes	Integer	Subscription quantity

Response Parameters

Status code: 200

Table 3-191 Response body parameters

Parameter	Type	Description
order_id	String	Order ID

Example Requests

Create an order of HSS enterprise edition quota. The order information is as follows. The billing mode is yearly/monthly. The quantity is 1. The subscription period is 1. The subscription period type is monthly. Automatic renewal is disabled. The order will be automatically paid.

```
POST https://{endpoint}/v5/{project_id}/quotas/orders
{
  "resource_spec_code" : "hss.version.enterprise",
  "subscription_num" : 1,
  "period_num" : 1,
  "period_type" : 2,
  "is_auto_renew" : false,
  "is_auto_pay" : false
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "order_id" : "CS2404171642AAAAA"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create an order of HSS enterprise edition quota. The order information is as follows. The billing mode is yearly/monthly. The quantity is 1. The subscription period is 1. The subscription period type is monthly. Automatic renewal is disabled. The order will be automatically paid.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class CreateQuotasOrderSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

```
.withProjectId(projectId)
.withAk(ak)
.withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
CreateQuotasOrderRequest request = new CreateQuotasOrderRequest();
CreateQuotasOrderRequestInfo body = new CreateQuotasOrderRequestInfo();
body.withSubscriptionNum(1);
body.withIsAutoPay(false);
body.withIsAutoRenew(false);
body.withPeriodNum(1);
body.withPeriodType(2);
body.withResourceSpecCode("hss.version.enterprise");
request.withBody(body);
try {
    CreateQuotasOrderResponse response = client.createQuotasOrder(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Create an order of HSS enterprise edition quota. The order information is as follows. The billing mode is yearly/monthly. The quantity is 1. The subscription period is 1. The subscription period type is monthly. Automatic renewal is disabled. The order will be automatically paid.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateQuotasOrderRequest()
```

```
request.body = CreateQuotasOrderRequestInfo(  
    subscription_num=1,  
    is_auto_pay=False,  
    is_auto_renew=False,  
    period_num=1,  
    period_type=2,  
    resource_spec_code="hss.version.enterprise"  
)  
response = client.create_quotas_order(request)  
print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

Create an order of HSS enterprise edition quota. The order information is as follows. The billing mode is yearly/monthly. The quantity is 1. The subscription period is 1. The subscription period type is monthly. Automatic renewal is disabled. The order will be automatically paid.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.CreateQuotasOrderRequest{  
        isAutoPayCreateQuotasOrderRequestInfo:= false  
        isAutoRenewCreateQuotasOrderRequestInfo:= false  
        request.Body = &model.CreateQuotasOrderRequestInfo{  
            SubscriptionNum: int32(1),  
            IsAutoPay: &isAutoPayCreateQuotasOrderRequestInfo,  
            IsAutoRenew: &isAutoRenewCreateQuotasOrderRequestInfo,  
            PeriodNum: int32(1),  
            PeriodType: int32(2),  
            ResourceSpecCode: "hss.version.enterprise",  
        }  
    }  
    response, err := client.CreateQuotasOrder(request)  
    if err == nil {
```

```

    fmt.Printf("%+v\n", response)
  } else {
    fmt.Println(err)
  }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.4.4 Querying Product and Offering Information

Function

This API is used to query product and offering information.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/product/productdata/offering-infos

Table 3-192 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-193 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
site_code	No	String	<p>Site information.</p> <ul style="list-style-type: none"> • HWC_CN: Chinese mainland • HWC_HK: international • HWC_EU: Europe

Request Parameters

Table 3-194 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-195 Response body parameters

Parameter	Type	Description
[items]	Array of ResourceProductDataObjectInfo objects	Offering Data List

Table 3-196 ResourceProductDataObjectInfo

Parameter	Type	Description
charging_mode	String	Billing modes <ul style="list-style-type: none"> packet_cycle: yearly/monthly on_demand: pay-per-use
is_auto_renew	Boolean	Whether to enable automatic renewal.
version_info	Map<String,Array< ShowPeriodResponseInfo >>	Edition information. The value of key is the HSS edition. Its value can be: <ul style="list-style-type: none"> 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

Table 3-197 ShowPeriodResponseInfo

Parameter	Type	Description
period_vals	String	Value string of the required duration. Multiple values are separated by commas (,). For example: 1,2,3,4,5,6,7,8,9
period_unit	String	Required duration unit <ul style="list-style-type: none"> year: month day:

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "data_list": [ {
    "charging_mode": "packet_cycle",
    "is_auto_renew": false,
    "version_info": {
      "hss.version.enterprise": [ {
        "period_vals": "1,2,3,4,5,6,7,8,9",
        "period_unit": "month"
      }, {
        "period_vals": "1,2,3,5",
        "period_unit": "year"
      } ],
      "hss.version.premium": [ {
        "period_vals": "1,2,3,4,5,6,7,8,9",
        "period_unit": "month"
      }, {
        "period_vals": "1,2,3,5",
        "period_unit": "year"
      } ]
    }
  }, {
    "charging_mode": "on_demand",
    "is_auto_renew": false,
    "version_info": {
      "hss.version.enterprise": [ {
        "period_vals": "1,2,3,4,5,6,7,8,9",
        "period_unit": "month"
      }, {
        "period_vals": "1,2,3,5",
        "period_unit": "year"
      } ]
    }
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowProductdataOfferingInfosSolution {
    public static void main(String[] args) {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ShowProductdataOfferingInfosRequest request = new ShowProductdataOfferingInfosRequest();
try {
    ShowProductdataOfferingInfosResponse response = client.showProductdataOfferingInfos(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowProductdataOfferingInfosRequest()
        response = client.show_productdata_offering_infos(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
```

```
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowProductdataOfferingInfosRequest{}
    response, err := client.ShowProductdataOfferingInfos(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.5 Container Management

3.5.1 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 3-198 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-199 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
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: <ul style="list-style-type: none"> not_installed: online offline
protect_status	No	String	Protection status. Its value can be: <ul style="list-style-type: none"> closed opened
container_tags	No	String	Label, which is used to identify CCE container and self-built nodes. <ul style="list-style-type: none"> cce: CCE nodes self: self-built nodes other: other nodes

Request Parameters

Table 3-200 Request header parameters

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

Response Parameters

Status code: 200

Table 3-201 Response body parameters

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

Table 3-202 ContainerNodeInfo

Parameter	Type	Description
agent_id	String	Agent ID
host_id	String	Server ID
host_name	String	Node name
host_status	String	Server status. The options are as follows: <ul style="list-style-type: none"> ACTIVE SHUTOFF BUILDING ERROR
agent_status	String	Agent status. It can be: <ul style="list-style-type: none"> not_installed online offline
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> closed opened
protect_interrupt	Boolean	Whether protection is interrupted
container_tags	String	Label, which is used to identify CCE container and self-built nodes. <ul style="list-style-type: none"> 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

Parameter	Type	Description
enterprise_project_name	String	Enterprise project name
detect_result	String	Server scan result. The options are as follows: <ul style="list-style-type: none"> 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

Request succeeded.

```
{
  "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_interrupt" : 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)"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListContainerNodesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListContainerNodesRequest request = new ListContainerNodesRequest();
        try {
            ListContainerNodesResponse response = client.listContainerNodes(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```



```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListContainerNodesRequest()
    response = client.list_container_nodes(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListContainerNodesRequest{}
    response, err := client.ListContainerNodes(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.5.2 Querying Basic Container Information List

Function

This API is used to query the basic container information list.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/container/kubernetes

Table 3-203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-204 Query Parameters

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

Parameter	Mandatory	Type	Description
cluster_container	No	Boolean	Whether the container is managed by a cluster
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.

Request Parameters

Table 3-205 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Response Parameters

Status code: 200

Table 3-206 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of containers
last_update_time	Long	Last update time
data_list	Array of ContainerBaseInfo objects	Basic container information list

Table 3-207 ContainerBaseInfo

Parameter	Type	Description
container_id	String	Container ID
container_name	String	Container name
image_name	String	Image name

Parameter	Type	Description
status	String	Container status. Its value can be: <ul style="list-style-type: none"> Running Terminated Waiting
create_time	Long	Creation time
cpu_limit	String	CPU limit
memory_limit	String	Memory limit
restart_count	Integer	Number of restarts
pod_name	String	Pod name
cluster_name	String	Cluster
cluster_id	String	Cluster ID
cluster_type	String	Cluster type. Its value can be: <ul style="list-style-type: none"> k8s (native kubernetes cluster) cce (CCE cluster) <ul style="list-style-type: none"> -ali (cluster on Alibaba Cloud) -tencent (cluster on Tencent Cloud) azure (cluster on Azure Cloud) aws (cluster on AWS Cloud) self_built_hw (customer-built cluster on Huawei Cloud) self_built_idc (customer-built IDC cluster)
risky	Boolean	Whether there are risks
low_risk	Integer	Number of low risks
medium_risk	Integer	Number of medium risks
high_risk	Integer	Number of high risks
fatal_risk	Integer	Number of critical risks

Example Requests

Search for containers whose names contain **install-agent-ds** and return the first 10 records.

```
GET https://{endpoint}/v5/{project_id}/container/kubernetes?
offset=0&limit=10&enterprise_project_id=all_granted_eps&container_name=install-agent-ds
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_num" : 1,
  "last_update_time" : 1710097200019,
  "data_list" : [ {
    "container_id" : "d7354abc9c18c68ab3e48e3481624125e415766b6d03eefc5770ff70c5391c8d",
    "container_name" : "node-exporter",
    "image_name" : "official/node-exporter:3.9.5",
    "status" : "Running",
    "create_time" : 1708453039000,
    "cpu_limit" : "500m",
    "memory_limit" : "1Gi",
    "restart_count" : 0,
    "pod_name" : "node-exporter-l4m75",
    "cluster_name" : "glz-hss",
    "cluster_id" : "352f4ef1-ce57-11ee-8cb3-0255ac100b0f",
    "cluster_type" : "cce",
    "risky" : false,
    "low_risk" : 0,
    "medium_risk" : 0,
    "high_risk" : 0,
    "fatal_risk" : 0
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListContainersSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
```

```
        .withRegion(HssRegion.valueOf("<YOUR REGION>"))
        .build();
ListContainersRequest request = new ListContainersRequest();
try {
    ListContainersResponse response = client.listContainers(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListContainersRequest()
        response = client.list_containers(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListContainersRequest{}
    response, err := client.ListContainers(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6 Event Management

3.6.1 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 3-208 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-209 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
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

Parameter	Mandatory	Type	Description
intercept_status	No	String	Interception status. The options are as follows: <ul style="list-style-type: none"> intercepted canceled (unblocked) cancelling
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-210 Request header parameters

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

Response Parameters

Status code: 200

Table 3-211 Response body parameters

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

Table 3-212 BlockedIpResponseInfo

Parameter	Type	Description
host_id	String	Host ID
host_name	String	Server name
src_ip	String	Attack source IP address
login_type	String	Login type. The options are as follows: <ul style="list-style-type: none"> "mysql" # MySQL service "rdp" # RDP service "ssh" # SSH service "vsftp" # vsftp service
intercept_num	Integer	Blocks
intercept_status	String	Interception status. The options are as follows: <ul style="list-style-type: none"> 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

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListBlockedIpSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListBlockedIpRequest request = new ListBlockedIpRequest();
        try {
            ListBlockedIpResponse response = client.listBlockedIp(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```

```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListBlockedIpRequest()
    response = client.list_blocked_ip(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListBlockedIpRequest{}
    response, err := client.ListBlockedIp(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6.2 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 3-213 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-214 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-215 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-216 Request body parameters

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

Table 3-217 BlockedIpRequestInfo

Parameter	Mandatory	Type	Description
host_id	Yes	String	Host ID
src_ip	Yes	String	Attack source IP address
login_type	Yes	String	Login type. The options are as follows: <ul style="list-style-type: none"> • "mysql" # MySQL service • "rdp" # RDP service • "ssh" # SSH service • "vsftp" # vsftp service

Response Parameters

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
```

```
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeBlockedIpSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ChangeBlockedIpRequest request = new ChangeBlockedIpRequest();
        ChangeBlockedIpRequestInfo body = new ChangeBlockedIpRequestInfo();
        List listbodyDataList = new ArrayList<>();
        listbodyDataList.add(
            new BlockedIpRequestInfo()
                .withHostId("af423efds-214432fgsdaf-gfdsaggbvf")
                .withSrcIp("192.168.1.6")
                .withLoginType("ssh")
        );
        body.withDataList(listbodyDataList);
        request.withBody(body);
        try {
            ChangeBlockedIpResponse response = client.changeBlockedIp(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```


risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment

```
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ChangeBlockedIpRequest()
    listDataListbody = [
        BlockedIpRequestInfo(
            host_id="af423efds-214432fgsdaf-gfdsaggbvf",
            src_ip="192.168.1.6",
            login_type="ssh"
        )
    ]
    request.body = ChangeBlockedIpRequestInfo(
        data_list=listDataListbody
    )
    response = client.change_blocked_ip(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```

```

WithCredential(auth).
Build()

request := &model.ChangeBlockedIpRequest{}
var listDataListbody = []model.BlockedIpRequestInfo{
    {
        HostId: "af423efds-214432fgsdaf-gfdsaggbvf",
        SrcIp: "192.168.1.6",
        LoginType: "ssh",
    },
}
request.Body = &model.ChangeBlockedIpRequestInfo{
    DataList: &listDataListbody,
}
response, err := client.ChangeBlockedIp(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6.3 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 3-218 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-219 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
file_path	No	String	File path
host_name	No	String	Server name
private_ip	No	String	Server private IP address
public_ip	No	String	Server public IP address
file_hash	No	String	The hash value calculated using the SHA256 algorithm.
asset_value	No	String	<p>Asset importance. The options are as follows:</p> <ul style="list-style-type: none"> • important • common • test
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-220 Request header parameters

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

Response Parameters

Status code: 200

Table 3-221 Response body parameters

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

Table 3-222 IsolatedFileResponseInfo

Parameter	Type	Description
os_type	String	OS type. Its value can be: <ul style="list-style-type: none"> Linux Windows
host_id	String	Host ID
host_name	String	Server name
file_hash	String	File hash

Parameter	Type	Description
file_path	String	File path
file_attr	String	File attribute
isolation_status	String	Isolation status. The options are as follows: <ul style="list-style-type: none"> • isolated • restored • isolating • restoring
private_ip	String	Server private IP address
public_ip	String	Elastic IP address
asset_value	String	Asset importance
update_time	Integer	Update time, in milliseconds
agent_version	String	Agent version
isolate_source	String	Isolation source. The options are as follows: <ul style="list-style-type: none"> • event: security alarm event • antivirus: virus scanning and removal
event_name	String	Event name
agent_event_info	IsolateEventResponseInfo object	Isolation event details
antivirus_result_info	AntivirusResultDetailInfo object	Results of virus scanning and removal

Table 3-223 IsolateEventResponseInfo

Parameter	Type	Description
event_id	String	Event ID

Parameter	Type	Description
event_class_id	String	<p>Event category. Its value can be:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> ● 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
		<ul style="list-style-type: none"> ● 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
		<ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • 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	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> 13003: enumerating user information 13004: cluster role binding
event_name	String	Event name
severity	String	Threat level. Its value can be: <ul style="list-style-type: none"> Security Low Medium High Critical
container_name	String	Container instance name. This parameter is available only for container alarms.
image_name	String	Image name. This parameter is available only for container alarms.
host_name	String	Server name
host_id	String	Host ID
private_ip	String	Server private IP address
public_ip	String	Elastic IP address
os_type	String	OS type. Its value can be: <ul style="list-style-type: none"> Linux Windows
host_status	String	Server status. The options are as follows: <ul style="list-style-type: none"> ACTIVE SHUTOFF BUILDING ERROR
agent_status	String	Agent status. Its value can be: <ul style="list-style-type: none"> installed not_installed: online offline install_failed installing

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> • closed • opened
asset_value	String	Asset importance. The options are as follows: <ul style="list-style-type: none"> • important • common • test
attack_phase	String	Attack phase. Its value can be: <ul style="list-style-type: none"> • reconnaissance • weaponization • delivery • exploit • installation • command_and_control • actions
attack_tag	String	Attack tag. Its value can be: <ul style="list-style-type: none"> • attack_success • attack_attempt • attack_blocked • abnormal_behavior • collapsible_host • system_vulnerability
occur_time	Integer	Occurrence time, accurate to milliseconds.
handle_time	Integer	Handling time, in milliseconds. This parameter is available only for handled alarms.
handle_status	String	Processing status. Its value can be: <ul style="list-style-type: none"> • unhandled • handled

Parameter	Type	Description
handle_method	String	Handling method. This parameter is available only for handled alarms. The options are as follows: <ul style="list-style-type: none">• mark_as_handled• ignore• add_to_alarm_whitelist• add_to_login_whitelist• isolate_and_kill
handler	String	Remarks. This parameter is available only for handled alarms.
recommendation	String	Handling suggestion
description	String	Alarm description
event_abstract	String	Alarm summary
event_count	Integer	Event occurrences

Table 3-224 AntivirusResultDetailInfo

Parameter	Type	Description
result_id	String	The result ID of virus scanning and removal
malware_name	String	Virus name
file_path	String	File path
file_hash	String	File hash
file_size	Integer	File size
file_owner	String	File owner
file_attr	String	File attribute
file_ctime	Integer	File creation time
file_mtime	Integer	File update time
update_time	Integer	Update time, in milliseconds
agent_id	String	Agent ID

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

Request succeeded.

```
{
  "data_list": [ {
    "file_attr": "0",
    "file_hash": "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path": "C:\\Users\\Public\\Public Docker\\system32.exe",
    "os_type": "Linux",
    "host_id": "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
    "host_name": "ecs-wi-800211",
    "isolation_status": "isolated",
    "private_ip": "127.0.0.2",
    "public_ip": "127.0.0.1",
    "asset_value": "common",
    "update_time": 1698304933717,
    "agent_version": "3.2.10",
    "isolate_source": "event",
    "event_name": "Spyware",
    "antivirus_result_info": {
      "result_id": "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
      "malware_name": "Win32.Virus.Hidrag",
      "file_attr": "0",
      "file_hash": "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
      "file_path": "C:\\Users\\Public\\Public Docker\\system32.exe",
      "file_size": 58460,
      "file_owner": "Administrators",
      "file_ctime": 1700039800,
      "file_mtime": 1700039800,
      "update_time": 1698304933717,
      "agent_id": "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
    },
    "agent_event_info": {
      "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,
      "handle_status": "unhandled",
      "host_name": "xxx",
      "occur_time": 1661593036627,
      "private_ip": "127.0.0.1",
      "severity": "Medium",
      "os_type": "Linux",
      "agent_status": "online",
      "asset_value": "common",
      "protect_status": "opened",
      "host_status": "ACTIVE",
      "description": "",
      "event_abstract": "",
      "image_name": "image",
      "container_name": "test",
      "host_id": "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
      "public_ip": "127.0.0.2",
      "handle_time": 1698304933717,
      "handle_method": "ignore",
      "recommendation": "Handling suggestion",
      "event_count": 1
    }
  } ],
  "total_num": 1
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListIsolatedFileSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListIsolatedFileRequest request = new ListIsolatedFileRequest();
        try {
            ListIsolatedFileResponse response = client.listIsolatedFile(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```



```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListIsolatedFileRequest()
    response = client.list_isolated_file(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIsolatedFileRequest{}
    response, err := client.ListIsolatedFile(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6.4 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 3-225 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-226 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-227 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-228 Request body parameters

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

Table 3-229 IsolatedFileRequestInfo

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

Response Parameters

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;
```

```
public class ChangelsolatedFileSolution {
    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ChangelsolatedFileRequest request = new ChangelsolatedFileRequest();
        ChangelsolatedFileRequestInfo body = new ChangelsolatedFileRequestInfo();
        List<IsolatedFileRequestInfo> listbodyDataList = new ArrayList<>();
        listbodyDataList.add(
            new IsolatedFileRequestInfo()
                .withHostId("5a41ca47-8ea7-4a65-a8fb-950d03d8638e")
                .withFileHash("58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde")
                .withFilePath("C:\\Users\\Public\\test.exe")
                .withFileAttr("0")
        );
        body.withDataList(listbodyDataList);
        request.withBody(body);
        try {
            ChangelsolatedFileResponse response = client.changelsolatedFile(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ChangeIsolatedFileRequest()
    listDataListbody = [
        IsolatedFileRequestInfo(
            host_id="5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
            file_hash="58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
            file_path="C:\\Users\\Public\\test.exe",
            file_attr="0"
        )
    ]
    request.body = ChangeIsolatedFileRequestInfo(
        data_list=listDataListbody
    )
    response = client.change_isolated_file(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

```

request := &model.ChangelsolatedFileRequest{}
hostIdDataList:= "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
fileHashDataList:= "58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde"
filePathDataList:= "C:\Users\Public\test.exe"
fileAttrDataList:= "0"
var listDataListbody = []model.IsolatedFileRequestInfo{
    {
        HostId: &hostIdDataList,
        FileHash: &fileHashDataList,
        FilePath: &filePathDataList,
        FileAttr: &fileAttrDataList,
    },
}
request.Body = &model.ChangelsolatedFileRequestInfo{
    DataList: &listDataListbody,
}
response, err := client.ChangelsolatedFile(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6.5 Querying Export Tasks

Function

This API is used to query export tasks.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/export-task/{task_id}

Table 3-230 Path Parameters

Parameter	Mandatory	Type	Description
task_id	Yes	String	Task ID.
project_id	Yes	String	Project ID.

Table 3-231 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-232 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-233 Response body parameters

Parameter	Type	Description
task_id	String	Task ID.
task_name	String	Task ID.
task_status	String	Specifies the export task status. The value can be success, failure, or running.
file_id	String	File ID.
file_name	String	File name.

Example Requests

Query the ID, status, and name of an export task based on the **task_id**.

```
GET https://{endpoint}/v5/{project_id}/export-task/{task_id}?enterprise_project_id=all_granted_eps
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "task_id" : "94ad7efb-xxxxx-46ed-99bf-dcd8c1c75dc2",
  "task_name" : "vul_vul_xxxxxx_export_task",
  "task_status" : "success",
  "file_id" : "b3e83d25-d92f-4963-a293-e056e81ec44d",
  "file_name" : "hss-vul-vul-zh-xxxxxxx.zip"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListQueryExportTaskSolution {
```

```
public static void main(String[] args) {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running
    // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    String ak = System.getenv("CLOUD_SDK_AK");
    String sk = System.getenv("CLOUD_SDK_SK");
    String projectId = "{project_id}";

    ICredential auth = new BasicCredentials()
        .withProjectId(projectId)
        .withAk(ak)
        .withSk(sk);

    HssClient client = HssClient.newBuilder()
        .withCredential(auth)
        .withRegion(HssRegion.valueOf("<YOUR REGION>"))
        .build();
    ListQueryExportTaskRequest request = new ListQueryExportTaskRequest();
    request.withTaskId("{task_id}");
    try {
        ListQueryExportTaskResponse response = client.listQueryExportTask(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListQueryExportTaskRequest()
        request.task_id = "{task_id}"
```

```

response = client.list_query_export_task(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)

```

Go

```

package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListQueryExportTaskRequest{}
    request.TaskId = "{task_id}"
    response, err := client.ListQueryExportTask(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.6.6 Downloading Export Files

Function

This API is used to download export files.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/download/{file_id}

Table 3-234 Path Parameters

Parameter	Mandatory	Type	Description
file_id	Yes	String	File ID.
project_id	Yes	String	Project ID.

Table 3-235 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-236 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.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-237 Response body parameters

Parameter	Type	Description
zipfile content	String	Request succeeded.

Example Requests

Download the exported file based on **file_id**.

```
GET https://{endpoint}/v5/{project_id}/download/{file_id}?enterprise_project_id=all_granted_eps
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "zipfile content" : null
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListDownloadExportedFileSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListDownloadExportedFileRequest request = new ListDownloadExportedFileRequest();
        request.withFileId("{file_id}");
        try {
            ListDownloadExportedFileResponse response = client.listDownloadExportedFile(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
```

```
.with_credentials(credentials) \  
.with_region(HssRegion.value_of("<YOUR REGION>")) \  
.build()  
  
try:  
    request = ListDownloadExportedFileRequest()  
    request.file_id = "{file_id}"  
    response = client.list_download_exported_file(request)  
    print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.ListDownloadExportedFileRequest{}  
    request.FileId = "{file_id}"  
    response, err := client.ListDownloadExportedFile(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.7 Intrusion Detection

3.7.1 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 3-238 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-239 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
container_name	No	String	Container instance name
container_id	No	String	Container ID

Request Parameters

Table 3-240 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-241 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Handling method. Its value can be: <ul style="list-style-type: none"> • mark_as_handled • ignore • add_to_alarm_whitelist • add_to_login_whitelist • isolate_and_kill • unhandle • do_not_ignore • remove_from_alarm_whitelist • remove_from_login_whitelist • do_not_isolate_or_kill
handler	No	String	Remarks. This parameter is available only for handled alarms.
operate_event_list	Yes	Array of OperateEventRequestInfo objects	Operated event list
event_white_rule_list	No	Array of EventWhiteRuleListRequestInfo objects	User-defined alarm whitelist

Table 3-242 OperateEventRequestInfo

Parameter	Mandatory	Type	Description
event_class_id	Yes	String	<p>Event category. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> ● 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
			<ul style="list-style-type: none"> ● 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
			<ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> ● 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
			<ul style="list-style-type: none">• 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	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> • 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 3-243 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 3-244 EventWhiteRuleListRequestInfo

Parameter	Mandatory	Type	Description
event_type	Yes	Integer	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • "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: <ul style="list-style-type: none"> • "equal" • "contain"

Response Parameters

None

Example Requests

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

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeEventSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";
```

```
ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ChangeEventRequest request = new ChangeEventRequest();
ChangeEventRequestInfo body = new ChangeEventRequestInfo();
List<EventDetailRequestInfo> listOperateEventListOperateDetailList = new ArrayList<>();
listOperateEventListOperateDetailList.add(
    new EventDetailRequestInfo()
        .withAgentId("c9bed5397db449ebdfba15e85f3c36accee125c68954daf5cab0528bab59bd8")
        .withProcessPid(3123)
        .withFileHash("e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d")
        .withFilePath("/usr/test")
        .withFileAttr("33261")
        .withKeyword("file_path=/usr/test")
        .withHash("e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d")
        .withPrivatelp("127.0.0.2")
        .withLoginIp("127.0.0.1")
        .withLoginUserName("root")
        .withContainerId("containerid")
        .withContainerName("/test")
);
List<OperateEventRequestInfo> listbodyOperateEventList = new ArrayList<>();
listbodyOperateEventList.add(
    new OperateEventRequestInfo()
        .withEventClassId("rootkit_0001")
        .withEventId("2a71e1e2-60f4-4d56-b314-2038fdc39de6")
        .withEventType(1010)
        .withOccurTime(1672046760353L)
        .withOperateDetailList(listOperateEventListOperateDetailList)
);
body.withOperateEventList(listbodyOperateEventList);
body.withHandler("test");
body.withOperateType("mark_as_handled");
request.withBody(body);
try {
    ChangeEventResponse response = client.changeEvent(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeEventRequest()
        listOperateDetailListOperateEventList = [
            EventDetailRequestInfo(
                agent_id="c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
                process_pid=3123,
                file_hash="e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
                file_path="/usr/test",
                file_attr="33261",
                keyword="file_path=/usr/test",
                hash="e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
                private_ip="127.0.0.2",
                login_ip="127.0.0.1",
                login_user_name="root",
                container_id="containerid",
                container_name="/test"
            )
        ]
        listOperateEventListbody = [
            OperateEventRequestInfo(
                event_class_id="rootkit_0001",
                event_id="2a71e1e2-60f4-4d56-b314-2038fdc39de6",
                event_type=1010,
                occur_time=1672046760353,
                operate_detail_list=listOperateDetailListOperateEventList
            )
        ]
        request.body = ChangeEventRequestInfo(
            operate_event_list=listOperateEventListbody,
            handler="test",
            operate_type="mark_as_handled"
        )
        response = client.change_event(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
```



```
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeEventRequest{}
    agentIdOperateDetailList:= "c9bed5397db449ebdfba15e85fcfc36acce125c68954daf5cab0528bab59bd8"
    processPidOperateDetailList:= int32(3123)
    fileHashOperateDetailList:=
    "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d"
    filePathOperateDetailList:= "/usr/test"
    fileAttrOperateDetailList:= "33261"
    keywordOperateDetailList:= "file_path=/usr/test"
    hashOperateDetailList:= "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d"
    privateIpOperateDetailList:= "127.0.0.2"
    loginIpOperateDetailList:= "127.0.0.1"
    loginUserNameOperateDetailList:= "root"
    containerIdOperateDetailList:= "containerid"
    containerNameOperateDetailList:= "/test"
    var listOperateDetailListOperateEventList = []model.EventDetailRequestInfo{
        {
            AgentId: &agentIdOperateDetailList,
            ProcessPid: &processPidOperateDetailList,
            FileHash: &fileHashOperateDetailList,
            FilePath: &filePathOperateDetailList,
            FileAttr: &fileAttrOperateDetailList,
            Keyword: &keywordOperateDetailList,
            Hash: &hashOperateDetailList,
            PrivateIp: &privateIpOperateDetailList,
            LoginIp: &loginIpOperateDetailList,
            LoginUserName: &loginUserNameOperateDetailList,
            ContainerId: &containerIdOperateDetailList,
            ContainerName: &containerNameOperateDetailList,
        },
    }
    var listOperateEventListbody = []model.OperateEventRequestInfo{
        {
            EventClassId: "rootkit_0001",
            EventId: "2a71e1e2-60f4-4d56-b314-2038fdc39de6",
            EventType: int32(1010),
            OccurTime: int64(1672046760353),
            OperateDetailList: listOperateDetailListOperateEventList,
        },
    }
    handlerChangeEventRequestInfo:= "test"
    request.Body = &model.ChangeEventRequestInfo{
        OperateEventList: listOperateEventListbody,
        Handler: &handlerChangeEventRequestInfo,
    }
}
```

```

        OperateType: "mark_as_handled",
    }
    response, err := client.ChangeEvent(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

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

Error Codes

See [Error Codes](#).

3.7.2 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 3-245 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-246 Query Parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Event category. Its value can be: <ul style="list-style-type: none"> • host: host security event • container: container security event
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
last_days	No	Integer	Number of days to be queried. This parameter is mutually exclusive with begin_time and end_time .
host_name	No	String	Server name
host_id	No	String	Host ID
private_ip	No	String	Server IP address
public_ip	No	String	Server public IP address
container_name	No	String	Container instance name

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records displayed on each page

Parameter	Mandatory	Type	Description
event_types	No	Array of integers	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • unhandled • handled
severity	No	String	Threat level. Its value can be: <ul style="list-style-type: none"> • Security • Low • Medium • High • Critical
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	<p>Event ID. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> ● 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
			<ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> ● 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
			<ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> • Security • Low • Medium • High • Critical
attack_tag	No	String	Indicates the attack flag. The options are as follows: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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

Request Parameters

Table 3-247 Request header parameters

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

Response Parameters

Status code: 200

Table 3-248 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of alarm events

Parameter	Type	Description
data_list	Array of EventManagementResponseInfo objects	Event list

Table 3-249 EventManagementResponseInfo

Parameter	Type	Description
event_id	String	Event ID

Parameter	Type	Description
event_class_id	String	<p>Event category. Its value can be:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> ● 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
		<ul style="list-style-type: none"> ● 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
		<ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • 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	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> 13003: enumerating user information 13004: cluster role binding
event_name	String	Event name
severity	String	Threat level. Its value can be: <ul style="list-style-type: none"> Security Low Medium High Critical
container_name	String	Container instance name. This parameter is available only for container alarms.
image_name	String	Image name. This parameter is available only for container alarms.
host_name	String	Server name
host_id	String	Host ID
private_ip	String	Server private IP address
public_ip	String	Elastic IP address
os_type	String	OS type. Its value can be: <ul style="list-style-type: none"> Linux Windows
host_status	String	Server status. The options are as follows: <ul style="list-style-type: none"> ACTIVE SHUTOFF BUILDING ERROR
agent_status	String	Agent status. Its value can be: <ul style="list-style-type: none"> installed not_installed online offline install_failed installing

Parameter	Type	Description
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> • closed • opened
asset_value	String	Asset importance. The options are as follows: <ul style="list-style-type: none"> • important • common • test
attack_phase	String	Attack phase. Its value can be: <ul style="list-style-type: none"> • reconnaissance • weaponization • delivery • exploit • installation • command_and_control • actions
attack_tag	String	Attack tag. Its value can be: <ul style="list-style-type: none"> • attack_success • attack_attempt • attack_blocked • abnormal_behavior • collapsible_host • system_vulnerability
occur_time	Integer	Occurrence time, accurate to milliseconds.
handle_time	Integer	Handling time, in milliseconds. This parameter is available only for handled alarms.
handle_status	String	Processing status. Its value can be: <ul style="list-style-type: none"> • unhandled • handled

Parameter	Type	Description
handle_method	String	Handling method. This parameter is available only for handled alarms. The options are as follows: <ul style="list-style-type: none"> mark_as_handled ignore add_to_alarm_whitelist add_to_login_whitelist isolate_and_kill
handler	String	Remarks. This parameter is available only for handled alarms.
operate_accept_list	Array of strings	Supported processing operation
operate_detail_list	Array of EventDetailResponseInfo objects	Operation details list (not displayed on the page)
forensic_info	Object	Attack information, in JSON format.
resource_info	EventResourceResponseInfo object	Resource information
geo_info	Object	Geographical location, in JSON format.
malware_info	Object	Malware information, in JSON format.
network_info	Object	Network information, in JSON format.
app_info	Object	Application information, in JSON format.
system_info	Object	System information, in JSON format.
extend_info	Object	Extended event information, in JSON format
recommendation	String	Handling suggestions
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

Parameter	Type	Description
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 3-250 EventDetailResponseInfo

Parameter	Type	Description
agent_id	String	Agent ID
process_pid	Integer	Process ID
is_parent	Boolean	Whether a process is a parent process
file_hash	String	File hash
file_path	String	File path
file_attr	String	File attribute
private_ip	String	Server private IP address
login_ip	String	Login source IP address
login_user_name	String	Login username
keyword	String	Alarm event keyword, which is used only for the alarm whitelist.
hash	String	Alarm event hash, which is used only for the alarm whitelist.

Table 3-251 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

Parameter	Type	Description
cloud_id	String	ECS ID
vm_name	String	VM name
vm_uuid	String	VM UUID, that is, the server ID
container_id	String	Container ID
container_status	String	Container status
pod_uid	String	pod uid
pod_name	String	pod name
namespace	String	namespace
cluster_id	String	Cluster ID
cluster_name	String	Cluster name
image_id	String	Image ID
image_name	String	Image name
host_attr	String	Host attribute
service	String	Service
micro_service	String	Microservice
sys_arch	String	System CPU architecture
os_bit	String	OS bit version
os_type	String	OS type
os_name	String	OS name
os_version	String	OS version

Table 3-252 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

Parameter	Type	Description
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
ancestor_process_path	String	Grandparent process file path
ancestor_process_pid	Integer	Grandfather process ID
ancestor_process_cmdline	String	Grandparent process file command line
parent_process_name	String	Parent process name
parent_process_path	String	Parent process file path
parent_process_pid	Integer	Parent process ID
parent_process_uid	Integer	Parent process user ID
parent_process_cmdline	String	Parent process file command line
parent_process_filename	String	Parent process file name
parent_process_start_time	Long	Parent process start time
parent_process_gid	Integer	Parent process group ID
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

Parameter	Type	Description
child_process_uid	Integer	Subprocess user ID
child_process_cmd_line	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
process_file_hash	String	Process file hash
parent_process_file_hash	String	Parent process file hash
block	Integer	Indicates whether the blocking is successful. 1: yes 0: no

Table 3-253 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

Parameter	Type	Description
service_type	String	Service type. The options are as follows: <ul style="list-style-type: none">• system• mysql• redis
service_port	Integer	Login service port
login_mode	Integer	Login mode
login_last_time	Long	Last login time
login_fail_count	Integer	Number of failed login attempts
pwd_hash	String	Password hash
pwd_with_fuzzing	String	Masked password
pwd_used_days	Integer	Password age (days)
pwd_min_days	Integer	Minimum password validity period
pwd_max_days	Integer	Maximum password validity period
pwd_warn_left_days	Integer	Advance warning of password expiration (days)

Table 3-254 EventFileResponseInfo

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

Parameter	Type	Description
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

Request succeeded.

```
{
  "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
}],
"process_info_list": [ {
  "process_path": "/root/test",
  "process_name": "test",
  "process_cmdline": "/bin/bash",
  "process_hash": "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
  "process_filename": "test",
  "process_file_hash": "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
  "process_username": "root",
  "process_pid": 372612,
  "process_uid": 10000,
  "process_gid": 10000,
  "process_egid": 10000,
  "process_euid": 10000,
  "process_start_time": 1661593024,
  "block": 0,
  "parent_process_path": "/usr/bin/bash",
  "parent_process_name": "test",
  "parent_process_cmdline": "/bin/bash",
  "parent_process_filename": "test",
  "parent_process_file_hash":
  "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
  "parent_process_pid": 372612,
  "parent_process_uid": 10000,
  "parent_process_gid": 10000,
  "parent_process_egid": 10000,
  "parent_process_euid": 10000,
```



```
"parent_process_start_time" : 1661593024,
"child_process_path" : "/usr/bin/bash",
"child_process_name" : "test",
"child_process_cmdline" : "/bin/bash",
"child_process_filename" : "test",
"child_process_pid" : 372612,
"child_process_uid" : 10000,
"child_process_gid" : 10000,
"child_process_egid" : 10000,
"child_process_euid" : 10000,
"child_process_start_time" : 1661593024,
"virt_process_name" : "test",
"virt_cmd" : "/bin/bash",
"escape_cmd" : "/bin/bash",
"escape_mode" : "0",
"ancestor_process_pid" : 372612,
"ancestor_process_cmdline" : "/bin/bash",
"ancestor_process_path" : "/usr/bin/bash"
}],
"description" : "",
"event_abstract" : "",
"tag_list" : [ "Hot Event" ]
}]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListSecurityEventsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListSecurityEventsRequest request = new ListSecurityEventsRequest();
        try {
            ListSecurityEventsResponse response = client.listSecurityEvents(request);
            System.out.println(response.toString());
        }
    }
}
```

```
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSecurityEventsRequest()
        response = client.list_security_events(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```

ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListSecurityEventsRequest{}
response, err := client.ListSecurityEvents(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.7.3 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 3-255 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-256 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
hash	No	String	Hash value of the event whitelist description (SHA256 algorithm)

Parameter	Mandatory	Type	Description
event_type	No	Integer	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
			<ul style="list-style-type: none"> • 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.
limit	No	Integer	Number of records displayed on each page.

Request Parameters

Table 3-257 Request header parameters

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

Response Parameters

Status code: 200

Table 3-258 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 3-259 AlarmWhiteListResponseInfo

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

Parameter	Type	Description
event_type	Integer	<p>Event type. Its value can be:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> 13003: enumerating user information 13004: cluster role binding
white_field	String	Whitelist fields. The options are as follows: <ul style="list-style-type: none"> "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: <ul style="list-style-type: none"> "equal" "contain"
update_time	Long	Time when the event whitelist is updated, in milliseconds.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAlarmWhiteListSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAlarmWhiteListRequest request = new ListAlarmWhiteListRequest();
        try {
            ListAlarmWhiteListResponse response = client.listAlarmWhiteList(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```

```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListAlarmWhiteListRequest()
    response = client.list_alarm_white_list(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlarmWhiteListRequest{}
    response, err := client.ListAlarmWhiteList(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.8 Server Management

3.8.1 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 3-260 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-261 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
version	No	String	<p>HSS edition. Its value can be:</p> <ul style="list-style-type: none"> • 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	<p>Agent status. Its value can be:</p> <ul style="list-style-type: none"> • not_installed • online • offline • install_failed • installing • not_online: All status except online, which is used only as a query condition.

Parameter	Mandatory	Type	Description
detect_result	No	String	Detection result. Its value can be: <ul style="list-style-type: none"> undetected clean risk scanning
host_name	No	String	Server name
host_id	No	String	Server ID
host_status	No	String	Host status. Its value can be: <ul style="list-style-type: none"> ACTIVE SHUTOFF BUILDING ERROR
os_type	No	String	OS type. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> packet_cycle: yearly/monthly on_demand: pay-per-use
refresh	No	Boolean	Whether to forcibly synchronize servers from ECSs

Parameter	Mandatory	Type	Description
above_version	No	Boolean	Whether to return all the versions later than the current version
outside_host	No	Boolean	Whether a server is a Huawei Cloud server
asset_value	No	String	Asset importance. Its value can be: <ul style="list-style-type: none"> • 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
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-262 Request header parameters

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

Response Parameters

Status code: 200

Table 3-263 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 3-264 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: <ul style="list-style-type: none"> ACTIVE SHUTOFF BUILDING ERROR
agent_status	String	Agent status. Its value can be: <ul style="list-style-type: none"> not_installed online offline install_failed installing

Parameter	Type	Description
install_result_code	String	Installation result. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> hss.version.null: none 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
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> closed opened
os_image	String	System disk image
os_type	String	OS type. Its value can be: <ul style="list-style-type: none"> Linux Windows

Parameter	Type	Description
os_bit	String	OS bit version
detect_result	String	Server scan result. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> packet_cycle: yearly/monthly on_demand: pay-per-use
resource_id	String	Cloud service resource instance ID (UUID)
outside_host	Boolean	Whether a server is a non-Huawei Cloud server
group_id	String	Server group ID
group_name	String	Server group name
policy_group_id	String	Policy group ID
policy_group_name	String	Policy group name
asset	Integer	Asset risk
vulnerability	Integer	Total number of vulnerabilities, including Linux, Windows, Web-CMS, and application vulnerabilities.
baseline	Integer	Total number of baseline risks, including configuration risks and weak passwords.
intrusion	Integer	Total intrusion risks
asset_value	String	Asset importance. Its value can be: <ul style="list-style-type: none"> important common test
labels	Array of strings	Tag list

Parameter	Type	Description
agent_create_time	Long	Agent installation time, which is a timestamp. The default unit is milliseconds.
agent_update_time	Long	Time when the agent status is changed. This is a timestamp. The default unit is milliseconds.
agent_version	String	Agent version
upgrade_status	String	Upgrade status. Its value can be: <ul style="list-style-type: none">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: <ul style="list-style-type: none">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

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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostStatusSolution {
```

```
public static void main(String[] args) {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running
    // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    String ak = System.getenv("CLOUD_SDK_AK");
    String sk = System.getenv("CLOUD_SDK_SK");
    String projectId = "{project_id}";

    ICredential auth = new BasicCredentials()
        .withProjectId(projectId)
        .withAk(ak)
        .withSk(sk);

    HssClient client = HssClient.newBuilder()
        .withCredential(auth)
        .withRegion(HssRegion.valueOf("<YOUR REGION>"))
        .build();
    ListHostStatusRequest request = new ListHostStatusRequest();
    try {
        ListHostStatusResponse response = client.listHostStatus(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostStatusRequest()
        response = client.list_host_status(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

```
print(e.status_code)
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostStatusRequest{}
    response, err := client.ListHostStatus(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.8.2 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 3-265 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-266 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.

Request Parameters

Table 3-267 Request header parameters

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

Table 3-268 Request body parameters

Parameter	Mandatory	Type	Description
version	Yes	String	HSS edition. Its value can be: <ul style="list-style-type: none"> • 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	Payment mode. This parameter is mandatory when version is not set to hss.version.null. <ul style="list-style-type: none"> • packet_cycle: yearly/monthly • on_demand: on-demand
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

Parameter	Mandatory	Type	Description
tags	No	Array of TagInfo objects	Resource tag list

Table 3-269 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

None

Example Requests

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

```
{
  "version": "hss.version.enterprise",
  "charging_mode": "packet_cycle",
  "resource_id": "af4d08ad-2b60-4916-a5cf-8d6a2395dda",
  "host_id_list": [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
  "tags": [ {
    "key": "Service",
    "value": "hss"
  } ]
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class SwitchHostsProtectStatusSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        SwitchHostsProtectStatusRequest request = new SwitchHostsProtectStatusRequest();
        SwitchHostsProtectStatusRequestInfo body = new SwitchHostsProtectStatusRequestInfo();
        List<TagInfo> listbodyTags = new ArrayList<>();
        listbodyTags.add(
            new TagInfo()
                .withKey("Service")
                .withValue("hss")
        );
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
        body.withTags(listbodyTags);
        body.withHostIdList(listbodyHostIdList);
        body.withResourceId("af4d08ad-2b60-4916-a5cf-8d6a23956dda");
        body.withChargingMode("packet_cycle");
        body.withVersion("hss.version.enterprise");
        request.withBody(body);
        try {
            SwitchHostsProtectStatusResponse response = client.switchHostsProtectStatus(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SwitchHostsProtectStatusRequest()
        listTagsbody = [
            TagInfo(
                key="Service",
                value="hss"
            )
        ]
        listHostIdListbody = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        request.body = SwitchHostsProtectStatusRequestInfo(
            tags=listTagsbody,
            host_id_list=listHostIdListbody,
            resource_id="af4d08ad-2b60-4916-a5cf-8d6a23956dda",
            charging_mode="packet_cycle",
            version="hss.version.enterprise"
        )
        response = client.switch_hosts_protect_status(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
```

```

    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.SwitchHostsProtectStatusRequest{}
    keyTags:= "Service"
    valueTags:= "hss"
    var listTagsbody = []model.TagInfo{
        {
            Key: &keyTags,
            Value: &valueTags,
        },
    }
    var listHostIdListbody = []string{
        "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    }
    resourceIdSwitchHostsProtectStatusRequestInfo:= "af4d08ad-2b60-4916-a5cf-8d6a23956dda"
    chargingModeSwitchHostsProtectStatusRequestInfo:= "packet_cycle"
    request.Body = &model.SwitchHostsProtectStatusRequestInfo{
        Tags: &listTagsbody,
        HostIdList: listHostIdListbody,
        ResourceId: &resourceIdSwitchHostsProtectStatusRequestInfo,
        ChargingMode: &chargingModeSwitchHostsProtectStatusRequestInfo,
        Version: "hss.version.enterprise",
    }
    response, err := client.SwitchHostsProtectStatus(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.8.3 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 3-270 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-271 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page.
group_name	No	String	Server group name

Request Parameters

Table 3-272 Request header parameters

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

Response Parameters

Status code: 200

Table 3-273 Response body parameters

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

Table 3-274 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

Parameter	Type	Description
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

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostGroupsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
```

```
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ListHostGroupsRequest request = new ListHostGroupsRequest();
try {
    ListHostGroupsResponse response = client.listHostGroups(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostGroupsRequest()
        response = client.list_host_groups(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```


Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostGroupsRequest{}
    response, err := client.ListHostGroups(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.8.4 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 3-275 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-276 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-277 Request header parameters

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

Table 3-278 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

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class AddHostsGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        AddHostsGroupRequest request = new AddHostsGroupRequest();
        AddHostsGroupRequestInfo body = new AddHostsGroupRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("15dac7fe-d81b-43bc-a4a7-4710fe673972");
        body.withHostIdList(listbodyHostIdList);
        body.withGroupName("test");
        request.withBody(body);
        try {
            AddHostsGroupResponse response = client.addHostsGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AddHostsGroupRequest()
        listHostIdListbody = [
            "15dac7fe-d81b-43bc-a4a7-4710fe673972"
        ]
        request.body = AddHostsGroupRequestInfo(
            host_id_list=listHostIdListbody,
            group_name="test"
        )
        response = client.add_hosts_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```

WithSk(sk).
WithProjectId(projectId).
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.AddHostsGroupRequest{}
var listHostIdListbody = []string{
    "15dac7fe-d81b-43bc-a4a7-4710fe673972",
}
request.Body = &model.AddHostsGroupRequestInfo{
    HostIdList: listHostIdListbody,
    GroupName: "test",
}
response, err := client.AddHostsGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

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

Error Codes

See [Error Codes](#).

3.8.5 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 3-279 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	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.

Request Parameters

Table 3-281 Request header parameters

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

Table 3-282 Request body parameters

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

Response Parameters

None

Example Requests

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

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeHostsGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ChangeHostsGroupRequest request = new ChangeHostsGroupRequest();
        ChangeHostsGroupRequestInfo body = new ChangeHostsGroupRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("15dac7fe-d81b-43bc-a4a7-4710fe673972");
        listbodyHostIdList.add("21303c5b-36ad-4510-a1b0-cb4ac4c2875c");
        body.withHostIdList(listbodyHostIdList);
        body.withGroupId("eca40dbe-27f7-4229-8f9d-a58213129fdc");
        body.withGroupName("test");
        request.withBody(body);
        try {
            ChangeHostsGroupResponse response = client.changeHostsGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
        }
    }
}
```

```
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeHostsGroupRequest()
        listHostIdListbody = [
            "15dac7fe-d81b-43bc-a4a7-4710fe673972",
            "21303c5b-36ad-4510-a1b0-cb4ac4c2875c"
        ]
        request.body = ChangeHostsGroupRequestInfo(
            host_id_list=listHostIdListbody,
            group_id="eca40dbe-27f7-4229-8f9d-a58213129fdc",
            group_name="test"
        )
        response = client.change_hosts_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
```

```

"fmt"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeHostsGroupRequest{}
    var listHostIdListbody = []string{
        "15dac7fe-d81b-43bc-a4a7-4710fe673972",
        "21303c5b-36ad-4510-a1b0-cb4ac4c2875c",
    }
    groupNameChangeHostsGroupRequestInfo:= "test"
    request.Body = &model.ChangeHostsGroupRequestInfo{
        HostIdList: &listHostIdListbody,
        GroupId: "eca40dbe-27f7-4229-8f9d-a58213129fdc",
        GroupName: &groupNameChangeHostsGroupRequestInfo,
    }
    response, err := client.ChangeHostsGroup(request)
    if err == nil {
        fmt.Printf("%v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.8.6 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 3-283 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-284 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
group_id	Yes	String	Server group ID

Request Parameters

Table 3-285 Request header parameters

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

Response Parameters

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class DeleteHostsGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
```

security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment

```
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
DeleteHostsGroupRequest request = new DeleteHostsGroupRequest();
try {
    DeleteHostsGroupResponse response = client.deleteHostsGroup(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteHostsGroupRequest()
        response = client.delete_hosts_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

```
print(e.status_code)
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteHostsGroupRequest{}
    response, err := client.DeleteHostsGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9 Container Image

3.9.1 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 3-286 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-287 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
namespace	No	String	Organization name
image_name	No	String	Image name
image_version	No	String	Image tag
latest_version	No	Boolean	Display latest image versions only
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records on each page
image_type	Yes	String	<p>Image type. The options are as follows:</p> <ul style="list-style-type: none"> • private_image: private image repository • shared_image: shared image repository • local_image • instance_image: enterprise image

Parameter	Mandatory	Type	Description
scan_status	No	String	Scan status. Its value can be: <ul style="list-style-type: none"> • unscan • success • scanning • failed • waiting_for_scan
instance_name	No	String	Enterprise image instance name
image_size	No	Long	Image size
start_latest_update_time	No	Long	Creation start date, in ms.
end_latest_update_time	No	Long	Creation end date, in ms.
start_latest_scan_time	No	Long	The start time of latest scan completion, in ms.
end_latest_scan_time	No	Long	The end time of latest scan completion, in ms.
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 3-288 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.

Parameter	Mandatory	Type	Description
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-289 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 3-290 PrivateImageRepositoryInfo

Parameter	Type	Description
id	Long	id
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: <ul style="list-style-type: none"> private_image shared_image
latest_version	Boolean	Check whether the version is the latest.

Parameter	Type	Description
scan_status	String	Scan status. The options are as follows: <ul style="list-style-type: none"> • unscan • success • scanning • failed • download_failed • image_oversized • waiting_for_scan
scan_failed_desc	String	Cause of the scanning failure. The options are as follows: <ul style="list-style-type: none"> • "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	Last update time of the image version, in ms.
latest_scan_time	Long	Last scanned, in ms.
vul_num	Integer	Vulnerabilities
unsafe_setting_num	Integer	Number of failed baseline scans
malicious_file_num	Integer	Number of malicious files

Parameter	Type	Description
domain_name	String	Owner (shared image parameter)
shared_status	String	The status of a shared image. The value can be: <ul style="list-style-type: none"> • expired • effective
scannable	Boolean	Scannable or not
instance_name	String	Enterprise image instance name
instance_id	String	Enterprise image instance ID
instance_url	String	Enterprise image instance URL
association_images	Array of AssociateImages objects	Multi-architecture associated image information

Table 3-291 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: <ul style="list-style-type: none"> • 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListSwrImageRepositorySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListSwrImageRepositoryRequest request = new ListSwrImageRepositoryRequest();
        try {
            ListSwrImageRepositoryResponse response = client.listSwrImageRepository(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8
```

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSwrImageRepositoryRequest()
        response = client.list_swr_image_repository(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSwrImageRepositoryRequest{}
    response, err := client.ListSwrImageRepository(request)
```



```

if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.2 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 3-292 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-293 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-294 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	No	String	Region ID

Table 3-295 Request body parameters

Parameter	Mandatory	Type	Description
repo_type	No	String	Repository type. Currently, SWR image repositories are connected. The options are as follows: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • private_image: private image repository • shared_image: shared image repository
scan_status	No	String	Scan status. The options are as follows: <ul style="list-style-type: none"> • 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 date, in ms.
end_latest_update_time	No	Long	Creation end date, in ms.

Parameter	Mandatory	Type	Description
start_latest_scan_time	No	Long	The start time of latest scan completion, in ms.
end_latest_scan_time	No	Long	The end time of latest scan completion, in ms.

Table 3-296 BatchScanSwrlImageInfo

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

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

SDK Sample Code

The SDK sample code is as follows.

Java

- 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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchScanSwrImageSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        BatchScanSwrImageRequest request = new BatchScanSwrImageRequest();
        BatchScanPrivateImageRequestInfo body = new BatchScanPrivateImageRequestInfo();
        List<BatchScanSwrImageInfo> listbodyImageInfoList = new ArrayList<>();
        listbodyImageInfoList.add(
            new BatchScanSwrImageInfo()
                .withNamespace("test")
                .withImageName("openjdk")
                .withImageVersion("v8.8")
        );
        listbodyImageInfoList.add(
            new BatchScanSwrImageInfo()
                .withNamespace("test1")
                .withImageName("openjdk1")
                .withImageVersion("v1.0")
        );
        body.withImageType("private_image");
        body.withImageInfoList(listbodyImageInfoList);
```

```
request.withBody(body);
try {
    BatchScanSwrlImageResponse response = client.batchScanSwrlImage(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

- 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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class BatchScanSwrlImageSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        BatchScanSwrlImageRequest request = new BatchScanSwrlImageRequest();
        BatchScanPrivateImageRequestInfo body = new BatchScanPrivateImageRequestInfo();
        body.withImageType("private_image");
        body.withOperateAll(true);
        request.withBody(body);
        try {
            BatchScanSwrlImageResponse response = client.batchScanSwrlImage(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
        }
    }
}
```

```
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

- 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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    # environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    # environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchScanSwrImageRequest()
        listImageInfoListbody = [
            BatchScanSwrImageInfo(
                namespace="test",
                image_name="openjdk",
                image_version="v8.8"
            ),
            BatchScanSwrImageInfo(
                namespace="test1",
                image_name="openjdk1",
                image_version="v1.0"
            )
        ]
        request.body = BatchScanPrivateImageRequestInfo(
            image_type="private_image",
            image_info_list=listImageInfoListbody
        )
        response = client.batch_scan_swr_image(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- 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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    # environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    # environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchScanSwrImageRequest()
        request.body = BatchScanPrivateImageRequestInfo(
            image_type="private_image",
            operate_all=True
        )
        response = client.batch_scan_swr_image(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

- 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    // environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```



```
WithSk(sk).
WithProjectId(projectId).
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.BatchScanSwrImageRequest{}
namespaceImageInfoList:= "test"
imageNameImageInfoList:= "openjdk"
imageVersionImageInfoList:= "v8.8"
namespaceImageInfoList1:= "test1"
imageNameImageInfoList1:= "openjdk1"
imageVersionImageInfoList1:= "v1.0"
var listImageInfoListbody = []model.BatchScanSwrImageInfo{
    {
        Namespace: &namespaceImageInfoList,
        ImageName: &imageNameImageInfoList,
        ImageVersion: &imageVersionImageInfoList,
    },
    {
        Namespace: &namespaceImageInfoList1,
        ImageName: &imageNameImageInfoList1,
        ImageVersion: &imageVersionImageInfoList1,
    },
}
request.Body = &model.BatchScanPrivateImageRequestInfo{
    ImageType: "private_image",
    ImageInfoList: &listImageInfoListbody,
}
response, err := client.BatchScanSwrImage(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

- 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    // environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
```

```
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.BatchScanSwrlImageRequest{}
operateAllBatchScanPrivateImageRequestInfo:= true
request.Body = &model.BatchScanPrivateImageRequestInfo{
    ImageType: "private_image",
    OperateAll: &operateAllBatchScanPrivateImageRequestInfo,
}
response, err := client.BatchScanSwrlImage(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.3 Querying the Local Image List

Function

This API is used to query the local image list.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/image/local-repositories

Table 3-297 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-298 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_name	No	String	Image name
image_version	No	String	Image version
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records on each page
scan_status	No	String	Scan status. Its value can be: <ul style="list-style-type: none"> • unscan • success • scanning • failed • waiting_for_scan
local_image_type	No	String	Image type. Its value can be: <ul style="list-style-type: none"> • other_image • swr_image
image_size	No	Long	Image size, in bytes
start_latest_update_time	No	Long	Start date of the search range of the latest update time, in milliseconds
end_latest_update_time	No	Long	End date of the search range of the latest update time, in milliseconds
start_latest_scan_time	No	Long	Start date of the search range of the latest scan completion time, in milliseconds
end_latest_scan_time	No	Long	End date of the search range of the latest scan completion time, in milliseconds

Parameter	Mandatory	Type	Description
has_vul	No	Boolean	Whether there are software vulnerabilities
host_name	No	String	Name of the server associated with the local image
host_id	No	String	ID of the server associated with the local image
host_ip	No	String	IP address (public or private network) of the server associated with the local image
container_id	No	String	ID of the container associated with the local image
container_name	No	String	Name of the container associated with the local image
pod_id	No	String	ID of the pod associated with the local image
pod_name	No	String	Name of the pod associated with the local image
app_name	No	String	Name of the software associated with the local image

Request Parameters

Table 3-299 Request header parameters

Parameter	Mandatory	Type	Description
x-auth-token	Yes	String	User token.

Response Parameters

Status code: 200

Table 3-300 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of local images

Parameter	Type	Description
data_list	Array of ImageLocalInfo objects	Local image data list

Table 3-301 ImageLocalInfo

Parameter	Type	Description
image_name	String	Image name
image_id	String	Image ID
image_digest	String	Image digest
image_version	String	Image version
local_image_type	String	Local image type
scan_status	String	Scan status. Its value can be: <ul style="list-style-type: none"> • unscan: • success: • scanning • failed • waiting
image_size	Long	Image size, in bytes
latest_update_time	Long	Last update time of the image version, in milliseconds
latest_scan_time	Long	Latest scan time, in milliseconds
vul_num	Long	Number of vulnerabilities
unsafe_setting_num	Long	Number of settings that failed the baseline check
malicious_file_num	Long	Number of malicious files
host_num	Long	Number of associated servers
container_num	Long	Number of associated containers
component_num	Long	Number of associated components

Parameter	Type	Description
scan_failed_desc	String	<p>Cause of the scanning failure. The options are as follows:</p> <ul style="list-style-type: none"> • unknown_error • failed_to_match_agent: The container edition is not enabled for the server, or the agent of the server is offline. • create_container_failed: The container fails to be created. • get_container_info_failed: The container information fails to be obtained. <ul style="list-style-type: none"> - docker_offline: The docker engine is offline. - get_docker_root_failed: The root file system of the container fails to be obtained. - image_not_exist_or_docker_api_fault: The image does not exist or the Docker API is abnormal. - huge_image: The image is too large. - docker_root_in_nfs: The root directory of the container is mounted to the network. - response_timed_out
severity_level	String	<p>Risk level of an image. It is displayed after an image scan is complete. Its value can be:</p> <ul style="list-style-type: none"> • Security • Low • Medium • High
host_name	String	Host name
host_id	String	Host ID
agent_id	String	Agent ID

Example Requests

Query the first 10 records in the local image list.

GET https://{endpoint}/v5/{project_id}/image/local-repositories?offset=0&limit=10

Example Responses

Status code: 200

Request succeeded.

```
{
  "data_list": [ {
    "image_id": "f757deea-781e-45ec-90ec-f199249890df",
    "image_name": "webshell-ljx",
    "image_version": "v1",
    "image_digest": "sha256:ce0b5d91b072730d0bc9518f11efd07eb7fdb9f43251e11a96cab5b1918b7044",
    "local_image_type": "swr_image",
    "scan_status": "success",
    "image_size": 215304488,
    "latest_update_time": 1697509433000,
    "latest_scan_time": 1709973506292,
    "host_num": 0,
    "container_num": 5,
    "component_num": 146,
    "vul_num": 77,
    "host_name": "myhost",
    "host_id": "9ad79426-992c-4be4-a2d1-dfd3a75b7c14",
    "agent_id": "1c1d073c5fc403eb0d9c3088bc49da4e015586fd4864513a2fd81afedce282d4",
    "severity_level": "High"
  } ],
  "total_num": 1
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListImageLocalSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
```

```
        .build();
        ListImageLocalRequest request = new ListImageLocalRequest();
        try {
            ListImageLocalResponse response = client.listImageLocal(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListImageLocalRequest()
        response = client.list_image_local(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
```



```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListImageLocalRequest{}
response, err := client.ListImageLocal(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.4 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 3-302 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
image_id	Yes	String	Image ID

Table 3-303 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
image_type	Yes	String	<p>Image type. The options are as follows:</p> <ul style="list-style-type: none"> 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.
limit	No	Integer	Number of records on each page

Parameter	Mandatory	Type	Description
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: <ul style="list-style-type: none"> • immediate_repair: high risk • delay_repair: medium risk • not_needed_repair: low risk
vul_id	No	String	Vulnerability ID (fuzzy search supported)
app_name	No	String	Software
type	No	String	Vulnerability type. The options are as follows: <ul style="list-style-type: none"> -linux_vul: Linux vulnerability -app_vul: application vulnerability

Request Parameters

Table 3-304 Request header parameters

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

Response Parameters

Status code: 200

Table 3-305 Response body parameters

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

Table 3-306 ImageVulInfo

Parameter	Type	Description
vul_id	String	Vulnerability ID
repair_necessity	String	Emergency level. Its values and their meanings are as follows: <ul style="list-style-type: none"> 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListImageVulnerabilitiesSolution {  
  
  public static void main(String[] args) {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
    // environment variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running  
    // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    String ak = System.getenv("CLOUD_SDK_AK");  
    String sk = System.getenv("CLOUD_SDK_SK");  
    String projectId = "{project_id}";  
  
    ICredential auth = new BasicCredentials()  
      .withProjectId(projectId)  
      .withAk(ak)  
      .withSk(sk);  
  
    HssClient client = HssClient.newBuilder()  
      .withCredential(auth)  
      .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
      .build();  
    ListImageVulnerabilitiesRequest request = new ListImageVulnerabilitiesRequest();  
    request.withImageId("{image_id}");  
    try {  
      ListImageVulnerabilitiesResponse response = client.listImageVulnerabilities(request);  
      System.out.println(response.toString());  
    } catch (ConnectionException e) {  
      e.printStackTrace();  
    } catch (RequestTimeoutException e) {  
      e.printStackTrace();  
    } catch (ServiceResponseException e) {  
      e.printStackTrace();  
      System.out.println(e.getStatusCode());  
      System.out.println(e.getRequestId());  
      System.out.println(e.getErrorCode());  
      System.out.println(e.getErrorMsg());  
    }  
  }  
}
```

```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListImageVulnerabilitiesRequest()  
        request.image_id = "{image_id}"  
        response = client.list_image_vulnerabilities(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListImageVulnerabilitiesRequest{}
request.ImageId = "{image_id}"
response, err := client.ListImageVulnerabilities(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.5 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 3-307 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
vul_id	Yes	String	Vulnerability ID

Table 3-308 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records on each page

Request Parameters

Table 3-309 Request header parameters

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

Response Parameters

Status code: 200

Table 3-310 Response body parameters

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

Table 3-311 ImageVulCveInfo

Parameter	Type	Description
cve_id	String	cve id
cvss_score	Float	CVSS score
publish_time	Long	Release date, in ms.
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulnerabilityCveSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListVulnerabilityCveRequest request = new ListVulnerabilityCveRequest();
        request.withVulId("{vul_id}");
        try {
            ListVulnerabilityCveResponse response = client.listVulnerabilityCve(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
```

```
.with_credentials(credentials) \  
.with_region(HssRegion.value_of("<YOUR REGION>")) \  
.build()  
  
try:  
    request = ListVulnerabilityCveRequest()  
    request.vul_id = "{vul_id}"  
    response = client.list_vulnerability_cve(request)  
    print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.ListVulnerabilityCveRequest{}  
    request.VulId = "{vul_id}"  
    response, err := client.ListVulnerabilityCve(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.6 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 3-312 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-313 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-314 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	No	String	Region ID

Table 3-315 Request body parameters

Parameter	Mandatory	Type	Description
image_type	Yes	String	Image type. The options are as follows: <ul style="list-style-type: none"> private_image: private image repository shared_image: shared image repository

Response Parameters

Status code: 200

Table 3-316 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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Synchronize private or shared images from SWR.

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class RunImageSynchronizeSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        RunImageSynchronizeRequest request = new RunImageSynchronizeRequest();
        RunImageSynchronizeRequestInfo body = new RunImageSynchronizeRequestInfo();
        body.withImageType("private_image");
        request.withBody(body);
        try {
            RunImageSynchronizeResponse response = client.runImageSynchronize(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Synchronize private or shared images from SWR.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
```

```
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = RunImageSynchronizeRequest()
    request.body = RunImageSynchronizeRequestInfo(
        image_type="private_image"
    )
    response = client.run_image_synchronize(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Synchronize private or shared images from SWR.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.RunImageSynchronizeRequest{}
    request.Body = &model.RunImageSynchronizeRequestInfo{
        ImageType: "private_image",
    }
    response, err := client.RunImageSynchronize(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
```



```
    fmt.Println(err)
  }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.7 Querying the List of Image Security Configuration Detection Results

Function

This API is used to query the list of image security configuration detection results. Currently, the system configuration items and SSH application configuration items of CentOS 7, Debian 10, EulerOS, and Ubuntu16 images can be checked.

Calling Method

For details, see [Calling APIs](#).

URI

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

Table 3-317 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-318 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
image_type	Yes	String	<p>Image type. The options are as follows:</p> <ul style="list-style-type: none"> 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.
limit	No	Integer	Number of records 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

Parameter	Mandatory	Type	Description
severity	No	String	Risk level. Its value can be: <ul style="list-style-type: none"> • Security • Low • Medium • High
standard	No	String	Standard type. Its value can be: <ul style="list-style-type: none"> • 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 3-319 Request header parameters

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

Response Parameters

Status code: 200

Table 3-320 Response body parameters

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

Table 3-321 ImageRiskConfigsInfoResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: <ul style="list-style-type: none"> • Security • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline type
standard	String	Standard type. Its value can be: <ul style="list-style-type: none"> • cn_standard: DJCP MLPS compliance standard • hw_standard: Cloud security practice standard
check_rule_num	Integer	Number of check items
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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListImageRiskConfigsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListImageRiskConfigsRequest request = new ListImageRiskConfigsRequest();
        try {
            ListImageRiskConfigsResponse response = client.listImageRiskConfigs(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```

```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListImageRiskConfigsRequest()
    response = client.list_image_risk_configs(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListImageRiskConfigsRequest{}
    response, err := client.ListImageRiskConfigs(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.8 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 3-322 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
check_name	Yes	String	Baseline name

Table 3-323 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
image_type	Yes	String	<p>Image type. The options are as follows:</p> <ul style="list-style-type: none"> • 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.
limit	No	Integer	Number of records 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: <ul style="list-style-type: none"> cn_standard: DJCP MLPS compliance standard hw_standard: Cloud security practice standard
result_type	No	String	Result type. Its value can be: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 3-324 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.
region	No	String	Region ID

Response Parameters

Status code: 200

Table 3-325 Response body parameters

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

Table 3-326 ImageRiskConfigsCheckRulesResponseInfo

Parameter	Type	Description
severity	String	Risk level. Its value can be: <ul style="list-style-type: none"> • Security • Low • Medium • High
check_name	String	Baseline name
check_type	String	Baseline type
standard	String	Standard type. Its value can be: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Huawei 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListImageRiskConfigRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListImageRiskConfigRulesRequest request = new ListImageRiskConfigRulesRequest();
        request.withCheckName("{check_name}");
        try {
            ListImageRiskConfigRulesResponse response = client.listImageRiskConfigRules(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        }
    }
}
```

```
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListImageRiskConfigRulesRequest()
        request.check_name = "{check_name}"
        response = client.list_image_risk_config_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

```

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListImageRiskConfigRulesRequest{}
request.CheckName = "{check_name}"
response, err := client.ListImageRiskConfigRules(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.9.9 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 3-327 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-328 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
image_type	Yes	String	<p>Image type. The options are as follows:</p> <ul style="list-style-type: none"> 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

Parameter	Mandatory	Type	Description
check_type	Yes	String	Baseline Type
check_rule_id	Yes	String	Check item ID
standard	Yes	String	Standard type. Its value can be: <ul style="list-style-type: none"> 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 3-329 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.
region	No	String	Region ID

Response Parameters

Status code: 200

Table 3-330 Response body parameters

Parameter	Type	Description
description	String	Check item description
reference	String	Reference
audit	String	Audit description
remediation	String	Suggestion

Parameter	Type	Description
check_info_list	Array of ImageCheckRuleCheckCaseResponseInfo objects	Test case

Table 3-331 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 Huawei 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```



```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowImageCheckRuleDetailSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowImageCheckRuleDetailRequest request = new ShowImageCheckRuleDetailRequest();
        try {
            ShowImageCheckRuleDetailResponse response = client.showImageCheckRuleDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

```
client = HssClient.new_builder() \  
  .with_credentials(credentials) \  
  .with_region(HssRegion.value_of("<YOUR REGION>")) \  
  .build()  
  
try:  
  request = ShowImageCheckRuleDetailRequest()  
  response = client.show_image_check_rule_detail(request)  
  print(response)  
except exceptions.ClientRequestException as e:  
  print(e.status_code)  
  print(e.request_id)  
  print(e.error_code)  
  print(e.error_msg)
```

Go

```
package main  
  
import (  
  "fmt"  
  "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
  hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
  "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
  region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
  // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
  // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
  // variables and decrypted during use to ensure security.  
  // In this example, AK and SK are stored in environment variables for authentication. Before running this  
  // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
  ak := os.Getenv("CLOUD_SDK_AK")  
  sk := os.Getenv("CLOUD_SDK_SK")  
  projectId := "{project_id}"  
  
  auth := basic.NewCredentialsBuilder().  
    WithAk(ak).  
    WithSk(sk).  
    WithProjectId(projectId).  
    Build()  
  
  client := hss.NewHssClient(  
    hss.HssClientBuilder().  
      WithRegion(region.ValueOf("<YOUR REGION>")).  
      WithCredential(auth).  
      Build())  
  
  request := &model.ShowImageCheckRuleDetailRequest{}  
  response, err := client.ShowImageCheckRuleDetail(request)  
  if err == nil {  
    fmt.Printf("%v\n", response)  
  } else {  
    fmt.Println(err)  
  }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.10 Policy Management

3.10.1 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 3-332 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-333 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
group_name	No	String	Policy group name
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
limit	No	Integer	Number of records displayed on each page.
container_mode	No	Boolean	Whether to query the container edition policy.

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.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-335 Response body parameters

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

Table 3-336 PolicyGroupResponseInfo

Parameter	Type	Description
group_name	String	Policy group name
group_id	String	Policy group ID
description	String	Description of the policy group
deletable	Boolean	Whether a policy group can be deleted
host_num	Integer	Number of associated servers
default_group	Boolean	Whether a policy group is the default policy group
support_os	String	Supported OS. The options are as follows: <ul style="list-style-type: none"> Linux Windows: Windows OS is supported.

Parameter	Type	Description
support_version	String	Supported versions. The options are as follows: <ul style="list-style-type: none"> 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

Request succeeded.

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListPolicyGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListPolicyGroupRequest request = new ListPolicyGroupRequest();
        try {
            ListPolicyGroupResponse response = client.listPolicyGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
```

```
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPolicyGroupRequest()
        response = client.list_policy_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
```



```
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListPolicyGroupRequest{}
response, err := client.ListPolicyGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.10.2 Applying a Policy Group

Function

This API is used to apply a policy group.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/{project_id}/policy/deploy

Table 3-337 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-338 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-339 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID
Content-Type	No	String	Default value: application/json; charset=utf-8

Table 3-340 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	ID list of servers where the policy group needs to be deployed

Response Parameters

None

Example Requests

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

```
POST https://{endpoint}/v5/{project_id}/policy/deploy
{
  "target_policy_group_id" : "1df671f7-2677-4705-a320-de1a62bff306",
  "host_id_list" : [ "15462c0e-32c6-4217-a869-bbd131a00ecf" ],
  "operate_all" : false
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class AssociatePolicyGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        AssociatePolicyGroupRequest request = new AssociatePolicyGroupRequest();
        AssociatePolicyGroupRequestInfo body = new AssociatePolicyGroupRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("15462c0e-32c6-4217-a869-bbd131a00ecf");
        body.withHostIdList(listbodyHostIdList);
        body.withOperateAll(false);
        body.withTargetPolicyGroupId("1df671f7-2677-4705-a320-de1a62bff306");
        request.withBody(body);
        try {
            AssociatePolicyGroupResponse response = client.associatePolicyGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AssociatePolicyGroupRequest()
        listHostIdListbody = [
            "15462c0e-32c6-4217-a869-bbd131a00ecf"
        ]
        request.body = AssociatePolicyGroupRequestInfo(
            host_id_list=listHostIdListbody,
            operate_all=False,
            target_policy_group_id="1df671f7-2677-4705-a320-de1a62bff306"
        )
        response = client.associate_policy_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
```

```

hss.HssClientBuilder().
    WithRegion(region.ValueOf("<YOUR REGION>")).
    WithCredential(auth).
    Build()

request := &model.AssociatePolicyGroupRequest{}
var listHostIdListbody = []string{
    "15462c0e-32c6-4217-a869-bbd131a00ecf",
}
operateAllAssociatePolicyGroupRequestInfo:= false
request.Body = &model.AssociatePolicyGroupRequestInfo{
    HostIdList: &listHostIdListbody,
    OperateAll: &operateAllAssociatePolicyGroupRequestInfo,
    TargetPolicyGroupId: "1df671f7-2677-4705-a320-de1a62bff306",
}
response, err := client.AssociatePolicyGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11 Vulnerability Management

3.11.1 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 3-341 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-342 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
type	No	String	<p>Vulnerability type. The options are as follows:</p> <ul style="list-style-type: none"> -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.

Parameter	Mandatory	Type	Description
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
group_name	No	String	Server group name

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.

Response Parameters

Status code: 200

Table 3-344 Response body parameters

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

Table 3-345 VulInfo

Parameter	Type	Description
vul_name	String	Vulnerability name
vul_id	String	Vulnerability ID
label_list	Array of strings	Vulnerability tag
repair_necessity	String	<p>Necessity of fixing a vulnerability.</p> <ul style="list-style-type: none"> • 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.

Parameter	Type	Description
severity_level	String	<p>Vulnerability severity.</p> <ul style="list-style-type: none"> • Critical: The CVSS score of the vulnerability is greater than or equal to 9, corresponding to the high risk level on the console. • High: The CVSS score of the vulnerability is greater than or equal to 7 and less than 9, corresponding to the medium risk level on the console. • Medium: The CVSS score of the vulnerability is greater than or equal to 4 and less than 7, corresponding to the medium risk level on the console. • Low: The CVSS score of the vulnerability is less than 4, corresponding to the low risk level on the console.
host_num	Integer	Number of affected servers
unhandle_host_num	Integer	Number of unhandled servers, excluding ignored and fixed servers.
scan_time	Long	Last scanned, in ms.
solution_detail	String	Vulnerability fixing guide
url	String	Vulnerability URL
description	String	Vulnerability description
type	String	<p>Vulnerability type. The options are as follows:</p> <ul style="list-style-type: none"> -linux_vul: Linux vulnerability -windows_vul: Windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability
host_id_list	Array of strings	List of servers where the vulnerability can be handled
cve_list	Array of cve_list objects	CVE list
patch_url	String	Patch address

Parameter	Type	Description
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
repair_priority_list	Array of RepairPriorityListInfo objects	Fixing priority. The number of servers corresponding to each fixing priority.

Table 3-346 cve_list

Parameter	Type	Description
cve_id	String	CVE ID
cvss	Float	CVSS score

Table 3-347 VulnerabilityHostNumberInfo

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

Table 3-348 RepairPriorityListInfo

Parameter	Type	Description
repair_priority	String	Priority Critical High Medium Low
host_num	Integer	Number of servers corresponding to the fixing priority

Example Requests

Query the first 10 records in the vulnerability list whose project_id is 2b31ed520xxxxxebedb6e57xxxxxxx.

```
GET https://{endpoint}/v5/2b31ed520xxxxxebedb6e57xxxxxxx/vulnerability/vulnerabilities?offset=0&limit=10
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "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",
    "repair_priority_list" : [ {
      "repair_priority" : "Critical",
      "host_num" : 0
    }, {
      "repair_priority" : "High",
      "host_num" : 0
    }, {
      "repair_priority" : "Medium",
      "host_num" : 1
    }, {
      "repair_priority" : "Low",
      "host_num" : 0
    }
  ]
} ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulnerabilitiesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListVulnerabilitiesRequest request = new ListVulnerabilitiesRequest();
        try {
            ListVulnerabilitiesResponse response = client.listVulnerabilities(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
```

```
# The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListVulnerabilitiesRequest()
    response = client.list_vulnerabilities(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListVulnerabilitiesRequest{}
    response, err := client.ListVulnerabilities(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.2 Exporting Information About Vulnerabilities and Their Affected Servers

Function

This API is used to export information about vulnerabilities and their affected servers.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/{project_id}/vul/export

Table 3-349 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-350 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
type	No	String	<p>Vulnerability type. The options are as follows:</p> <ul style="list-style-type: none"> -linux_vul: Linux vulnerability -windows_vul: Windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability -urgent_vul: emergency vulnerability
vul_id	No	String	Vulnerability ID.
vul_name	No	String	Vulnerability name.
host_id	No	String	Server ID, which will be used when vulnerabilities of a single server are exported.
limit	No	Integer	limit
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
repair_priority	No	String	Fixing priority. Its value can be: Critical High Medium Low
handle_status	No	String	Handling status. It can be: <ul style="list-style-type: none"> 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. Its value can be: important common test
group_name	No	String	Server group name.
export_size	Yes	Integer	Number of exported data records.
category	Yes	String	Types of exported vulnerability data. Its value can be: <ul style="list-style-type: none"> vul: vulnerability host: host vulnerability

Request Parameters

Table 3-351 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.

Table 3-352 Request body parameters

Parameter	Mandatory	Type	Description
export_headers	No	Array<Array<String>>	Table heading list of exported vulnerability data

Response Parameters

Status code: 200

Table 3-353 Response body parameters

Parameter	Type	Description
task_id	String	Task ID.

Example Requests

Export Linux vulnerabilities. The fixing levels include critical, high, medium, and low, and the handling status is unhandled. Export the vulnerability data whose table header is enterprise project, vulnerability name, and vulnerability ID.

```
POST https://{endpoint}/v5/{project_id}/vul/export?
handle_status=unhandled&repair_priority=Critical,High,Medium,Low&offset=0&category=vul&type=linux_vul
&export_size=200000&enterprise_project_id=xxx
{
  "export_headers" : [ [ "enterprise_project_name", "Enterprise project" ], [ "vul_name", "Vulnerability
name" ], [ "vul_id", "Vulnerability ID" ] ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "task_id" : "2b31ed520xxxxxxebdb6e57xxxxxxx"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Export Linux vulnerabilities. The fixing levels include critical, high, medium, and low, and the handling status is unhandled. Export the vulnerability data whose table header is enterprise project, vulnerability name, and vulnerability ID.

```
package com.huaweicloud.sdk.test;
import com.huaweicloud.sdk.core.auth.ICredential;
```

```
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ExportVulsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ExportVulsRequest request = new ExportVulsRequest();
        ExportVulRequestBody body = new ExportVulRequestBody();
        List<String> listExportHeadersExportHeaders = new ArrayList<>();
        listExportHeadersExportHeaders.add("vul_id");
        listExportHeadersExportHeaders.add("Vulnerability ID");
        List<String> listExportHeadersExportHeaders1 = new ArrayList<>();
        listExportHeadersExportHeaders1.add("vul_name");
        listExportHeadersExportHeaders1.add("Vulnerability name");
        List<String> listExportHeadersExportHeaders2 = new ArrayList<>();
        listExportHeadersExportHeaders2.add("enterprise_project_name");
        listExportHeadersExportHeaders2.add("Enterprise project");
        List<List<String>> listbodyExportHeaders = new ArrayList<>();
        listbodyExportHeaders.add(listExportHeadersExportHeaders);
        listbodyExportHeaders.add(listExportHeadersExportHeaders1);
        listbodyExportHeaders.add(listExportHeadersExportHeaders2);
        body.withExportHeaders(listbodyExportHeaders);
        request.withBody(body);
        try {
            ExportVulsResponse response = client.exportVuls(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Export Linux vulnerabilities. The fixing levels include critical, high, medium, and low, and the handling status is unhandled. Export the vulnerability data whose table header is enterprise project, vulnerability name, and vulnerability ID.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ExportVulsRequest()
        listExportHeadersExportHeaders = [
            "vu_id",
            "Vulnerability ID"
        ]
        listExportHeadersExportHeaders1 = [
            "vu_name",
            "Vulnerability name"
        ]
        listExportHeadersExportHeaders2 = [
            "enterprise_project_name",
            "Enterprise project"
        ]
        listExportHeadersbody = [
            listExportHeadersExportHeaders,
            listExportHeadersExportHeaders1,
            listExportHeadersExportHeaders2
        ]
        request.body = ExportVulRequestBody(
            export_headers=listExportHeadersbody
        )
        response = client.export_vuls(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Export Linux vulnerabilities. The fixing levels include critical, high, medium, and low, and the handling status is unhandled. Export the vulnerability data whose table header is enterprise project, vulnerability name, and vulnerability ID.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ExportVulsRequest{}
    var listExportHeadersExportHeaders = []string{
        "vu_id",
        "Vulnerability ID",
    }
    var listExportHeadersExportHeaders1 = []string{
        "vu_name",
        "Vulnerability name",
    }
    var listExportHeadersExportHeaders2 = []string{
        "enterprise_project_name",
        "Enterprise project",
    }
    var listExportHeadersbody = [][]string{
        listExportHeadersExportHeaders,
        listExportHeadersExportHeaders1,
        listExportHeadersExportHeaders2,
    }
    request.Body = &model.ExportVulRequestBody{
        ExportHeaders: &listExportHeadersbody,
    }
    response, err := client.ExportVuls(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.3 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 3-354 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-355 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
vul_id	Yes	String	Vulnerability ID
type	Yes	String	<p>Operation type. The options are as follows:</p> <ul style="list-style-type: none"> -linux_vul: Linux vulnerability -windows_vul: Windows vulnerability -web_cms: Web-CMS vulnerability -app_vul: application vulnerability -urgent_vul: emergency vulnerability
host_name	No	String	Name of the affected server
host_ip	No	String	IP address of the affected server

Parameter	Mandatory	Type	Description
status	No	String	Vulnerability status. <ul style="list-style-type: none"> • vul_status_unfix: not fixed • vul_status_ignored: ignored <ul style="list-style-type: none"> - vul_status_verified: verification in progress - vul_status_fixing: The fix is in progress. - vul_status_fixed: The fix succeeded. - vul_status_reboot: The issue is fixed and waiting for restart. - vul_status_failed: The issue failed to be fixed. - vul_status_fix_after_reboot: Restart the server and try again.
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
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.

Parameter	Mandatory	Type	Description
repair_priority	No	String	Fixing priority. The options are as follows: <ul style="list-style-type: none"> • Critical: • High • Medium • Low

Request Parameters

Table 3-356 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 3-357 Response body parameters

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

Table 3-358 VulHostInfo

Parameter	Type	Description
host_id	String	ID of the server affected by the vulnerability

Parameter	Type	Description
severity_level	String	<p>Risk level.</p> <ul style="list-style-type: none"> • 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	Name of the affected server
host_ip	String	IP address of the affected server
agent_id	String	Agent ID
version	String	The quota version bound to the server
cve_num	Integer	Number of vulnerability CVEs
cve_id_list	Array of strings	The CVE ID list corresponding to the vulnerability
status	String	<p>Vulnerability status.</p> <ul style="list-style-type: none"> • 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.

Parameter	Type	Description
repair_cmd	String	Command line to be executed to fix the vulnerability (This field is available only for Linux vulnerabilities.)
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: <ul style="list-style-type: none"> important common test
is_affect_business	Boolean	Whether services are affected
first_scan_time	Long	First scan time
scan_time	Long	Scanning time, in ms.
support_restore	Boolean	Indicates whether data can be rolled back to the backup created when the vulnerability was fixed.
disabled_operate_types	Array of disabled_operate_types objects	List of operation types of vulnerabilities that cannot be performed on the current server.
repair_priority	String	Fixing priority. The options are as follows: <ul style="list-style-type: none"> Critical High Medium Low

Table 3-359 disabled_operate_types

Parameter	Type	Description
operate_type	String	Operation type. <ul style="list-style-type: none"> ignore not_ignore (unignore) immediate_repair manual_repair verify add_to_whitelist
reason	String	Indicates the reason why the operation cannot be performed.

Example Requests

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

```
GET https://{endpoint}/v5/2b31ed520xxxxxbedb6e57xxxxxxx/vulnerability/hosts?vul_id=EulerOS-SA-2021-1894&offset=0&limit=10
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "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" : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "version" : "hss.version.enterprise",
    "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,
    "disabled_operate_types" : [ {
      "operate_type" : "immediate_repair",
      "reason" : "The kernel vulnerability of CCE container node cannot be automatically fixed."
    } ],
    "repair_priority" : "Critical"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulHostsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListVulHostsRequest request = new ListVulHostsRequest();
        try {
            ListVulHostsResponse response = client.listVulHosts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListVulHostsRequest()
    response = client.list_vul_hosts(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListVulHostsRequest{}
    response, err := client.ListVulHosts(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.4 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 3-360 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-361 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-362 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>
Content-Type	No	String	Default value: application/json; charset=utf-8

Table 3-363 Request body parameters

Parameter	Mandatory	Type	Description
operate_type	Yes	String	Operation type. <ul style="list-style-type: none"> ignore not_ignore (unignore) immediate_repair manual_repair verify add_to_whitelist
remark	No	String	Remarks
select_type	No	String	Select vulnerabilities. <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> linux_vul: Linux vulnerability windows_vul: Windows vulnerability web_cms: Web-CMS vulnerability app_vul: application vulnerability urgent_vul: emergency vulnerability
data_list	No	Array of VulOperateInfo objects	Vulnerability list
host_data_list	No	Array of HostVulOperateInfo objects	Vulnerability list in the server dimension
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.

Parameter	Mandatory	Type	Description
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 3-364 VulOperateInfo

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

Table 3-365 HostVulOperateInfo

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

Table 3-366 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

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

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeVulStatusSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ChangeVulStatusRequest request = new ChangeVulStatusRequest();
        ChangeVulStatusRequestInfo body = new ChangeVulStatusRequestInfo();
        List<String> listDataListHostIdList = new ArrayList<>();
        listDataListHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
        List<VulOperateInfo> listbodyDataList = new ArrayList<>();
        listbodyDataList.add(
            new VulOperateInfo()
                .withVulId("EulerOS-SA-2021-1894")
                .withHostIdList(listDataListHostIdList)
        );
    }
}
```

```
body.withDataList(listbodyDataList);
body.withOperateType("ignore");
request.withBody(body);
try {
    ChangeVulStatusResponse response = client.changeVulStatus(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeVulStatusRequest()
        listHostIdListDataList = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        listDataListbody = [
            VulOperateInfo(
                vul_id="EulerOS-SA-2021-1894",
                host_id_list=listHostIdListDataList
            )
        ]
        request.body = ChangeVulStatusRequestInfo(
            data_list=listDataListbody,
            operate_type="ignore"
        )
        response = client.change_vul_status(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
```

```
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeVulStatusRequest{}
    var listHostIdListDataList = []string{
        "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    }
    var listDataListbody = []model.VulOperateInfo{
        {
            VulId: "EulerOS-SA-2021-1894",
            HostIdList: listHostIdListDataList,
        },
    }
    request.Body = &model.ChangeVulStatusRequestInfo{
        DataList: &listDataListbody,
        OperateType: "ignore",
    }
    response, err := client.ChangeVulStatus(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.5 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 3-367 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
host_id	Yes	String	Server ID.

Table 3-368 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
type	No	String	<p>Vulnerability type. The default value is linux_vul. The options are as follows:</p> <ul style="list-style-type: none"> • linux_vul: Linux vulnerability • windows_vul: Windows vulnerability • -web_cms: Web-CMS vulnerability • app_vul: application vulnerability • urgent_vul: emergency 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.
handle_status	No	String	<p>Handling status. The options are as follows:</p> <ul style="list-style-type: none"> - unhandled - handled

Parameter	Mandatory	Type	Description
status	No	String	<p>Vulnerability status. The options are as follows:</p> <ul style="list-style-type: none"> • 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_priority	No	String	<p>Fixing priority. The options are as follows:</p> <ul style="list-style-type: none"> • Critical • High • Medium • Low

Request Parameters

Table 3-369 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>

Response Parameters

Status code: 200

Table 3-370 Response body parameters

Parameter	Type	Description
total_num	Long	Total
data_list	Array of HostVulInfo objects	List of vulnerabilities on a server

Table 3-371 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: <ul style="list-style-type: none">• 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	<p>Risk level.</p> <ul style="list-style-type: none"> • 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	<p>Vulnerability status</p> <ul style="list-style-type: none"> • 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.
disabled_operate_types	Array of disabled_operate_types objects	List of operation types of vulnerabilities that cannot be performed.
repair_priority	String	Fixing priority. The options are as follows: <ul style="list-style-type: none"> • Critical • High • Medium • Low

Table 3-372 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 3-373 cve_list

Parameter	Type	Description
cve_id	String	CVE ID
cvss	Float	CVSS score

Table 3-374 disabled_operate_types

Parameter	Type	Description
operate_type	String	Operation type. <ul style="list-style-type: none"> ignore not_ignore (unignore) immediate_repair manual_repair verify add_to_whitelist
reason	String	Indicates the reason why the operation cannot be performed.

Example Requests

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

```
GET https://{endpoint}/v5/2b31ed520xxxxxebedb6e57xxxxxxx/vulnerability/host/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx?offset=0&limit=10
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "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 click
the link to fix the vulnerability according to the suggestions.\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/\n\nThe vulnerability exploitation/POC of this vulnerability has
been exposed. You can verify the vulnerability by referring to the following link:\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/mergbase/log4j-samples\nhttps://
github.com/lukepasek/log4jndilookupremove\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,
"disabled_operate_types" : [ {
  "operate_type" : "immediate_repair",
  "reason" : "The kernel vulnerability of CCE container node cannot be automatically fixed."
} ]
} ],
"total_num" : 31
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostVulsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
```

```
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ListHostVulsRequest request = new ListHostVulsRequest();
request.withHostId("{host_id}");
try {
    ListHostVulsResponse response = client.listHostVuls(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostVulsRequest()
        request.host_id = "{host_id}"
        response = client.list_host_vuls(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostVulsRequest{}
    request.HostId = "{host_id}"
    response, err := client.ListHostVuls(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.6 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 3-375 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-376 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.

Request Parameters

Table 3-377 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 3-378 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	<p>Scan all ID list of emergency vulnerabilities. If this parameter is left blank, all emergency vulnerabilities are scanned.</p> <p>Its value can be:</p> <p>URGENT-CVE-2023-46604 Apache ActiveMQ Remote Code Execution Vulnerability</p> <p>URGENT-HSSVD-2020-1109 Elasticsearch Unauthorized Access Vulnerability</p> <p>URGENT-CVE-2022-26134 Atlassian Confluence OGNL Remote Code Execution Vulnerability (Cve-2022-26134)</p> <p>URGENT-CVE-2023-22515 Atlassian Confluence Data Center and Server Privilege Escalation Vulnerability (CVE-2023-22515)</p> <p>URGENT-CVE-2023-22518 Atlassian Confluence Data Center & Server Inappropriate Authorization Mechanism Vulnerability (CVE-2023-22518)</p> <p>URGENT-CVE-2023-28432 MinIO Information Disclosure Vulnerability (CVE-2023-28432)</p> <p>URGENT-CVE-2023-37582 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-37582)</p> <p>URGENT-CVE-2023-33246 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-33246)</p> <p>URGENT-CNVD-2023-02709 ZENTAO Project Management System Remote Command Execution Vulnerability (CNVD-2023-02709)</p> <p>URGENT-CVE-2022-36804 Atlassian Bitbucket Server and</p>

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 3-379 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

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateVulnerabilityScanTaskSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
```

```
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();

CreateVulnerabilityScanTaskRequest request = new CreateVulnerabilityScanTaskRequest();
ManualVulScanRequestInfo body = new ManualVulScanRequestInfo();
List<String> listbodyUrgentVulIdList = new ArrayList<>();
listbodyUrgentVulIdList.add("URGENT-CVE-2023-46604");
listbodyUrgentVulIdList.add("URGENT-HSSVD-2020-1109");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-26134");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-22515");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-22518");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-28432");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-37582");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-33246");
listbodyUrgentVulIdList.add("URGENT-CNVD-2023-02709");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-36804");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-22965");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-25845");
listbodyUrgentVulIdList.add("URGENT-CVE-2019-14439");
listbodyUrgentVulIdList.add("URGENT-CVE-2020-13933");
listbodyUrgentVulIdList.add("URGENT-CVE-2020-26217");
listbodyUrgentVulIdList.add("URGENT-CVE-2021-4034");
listbodyUrgentVulIdList.add("URGENT-CVE-2021-44228");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-0847");
List<String> listbodyAgentIdList = new ArrayList<>();
listbodyAgentIdList.add("0253edfd-30e7-439d-8f3f-17c54c997064");
body.withUrgentVulIdList(listbodyUrgentVulIdList);
body.withAgentIdList(listbodyAgentIdList);
body.withRangeType("specific_host");
body.withBatchFlag(false);
request.withBody(body);
try {
    CreateVulnerabilityScanTaskResponse response = client.createVulnerabilityScanTask(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrMsg());
}
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateVulnerabilityScanTaskRequest()
        listUrgentVulIdListbody = [
            "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"
        ]
        listAgentIdListbody = [
            "0253edfd-30e7-439d-8f3f-17c54c997064"
        ]
        request.body = ManualVulScanRequestInfo(
            urgent_vul_id_list=listUrgentVulIdListbody,
            agent_id_list=listAgentIdListbody,
            range_type="specific_host",
            batch_flag=False
        )
        response = client.create_vulnerability_scan_task(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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

```
package main
import (
```

```
"fmt"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateVulnerabilityScanTaskRequest{}
    var listUrgentVulIdListbody = []string{
        "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",
    }
    var listAgentIdListbody = []string{
        "0253edfd-30e7-439d-8f3f-17c54c997064",
    }
    rangeTypeManualVulScanRequestInfo:= "specific_host"
    batchFlagManualVulScanRequestInfo:= false
    request.Body = &model.ManualVulScanRequestInfo{
        UrgentVulIdList: &listUrgentVulIdListbody,
        AgentIdList: &listAgentIdListbody,
        RangeType: &rangeTypeManualVulScanRequestInfo,
        BatchFlag: &batchFlagManualVulScanRequestInfo,
    }
    response, err := client.CreateVulnerabilityScanTask(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.7 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 3-380 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-381 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-382 Request header parameters

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

Response Parameters

Status code: 200

Table 3-383 Response body parameters

Parameter	Type	Description
scan_period	String	Scan period <ul style="list-style-type: none"> • 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
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 2b31ed520xxxxxebedb6e57xxxxxxx.

GET https://{endpoint}/v5/2b31ed520xxxxxebedb6e57xxxxxxx/vulnerability/scan-policy

Example Responses

Status code: 200

Request succeeded.

```
{
  "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowVulScanPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowVulScanPolicyRequest request = new ShowVulScanPolicyRequest();
        try {
            ShowVulScanPolicyResponse response = client.showVulScanPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ShowVulScanPolicyRequest()
    response = client.show_vul_scan_policy(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowVulScanPolicyRequest{}
    response, err := client.ShowVulScanPolicy(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.8 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 3-384 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-385 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-386 Request header parameters

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

Table 3-387 Request body parameters

Parameter	Mandatory	Type	Description
scan_period	Yes	String	<p>Scan period</p> <ul style="list-style-type: none"> • one_day • three_day • one_week

Parameter	Mandatory	Type	Description
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

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}/v5/2b31ed520xxxxxebedb6e57xxxxxxx/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

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;
```

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeVulScanPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ChangeVulScanPolicyRequest request = new ChangeVulScanPolicyRequest();
        ChangeVulScanPolicyRequestInfo body = new ChangeVulScanPolicyRequestInfo();
        []string listbodyHostIds = new ArrayList<>();
        listbodyHostIds.add("xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx");
        body.withStatus("open");
        body.withHostIds(listbodyHostIds);
        body.withScanRangeType("specific_host");
        body.withScanPeriod("one_day");
        request.withBody(body);
        try {
            ChangeVulScanPolicyResponse response = client.changeVulScanPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
```



```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeVulScanPolicyRequest()
        listHostIdsbody = [
            "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
        ]
        request.body = ChangeVulScanPolicyRequestInfo(
            status="open",
            host_ids=listHostIdsbody,
            scan_range_type="specific_host",
            scan_period="one_day"
        )
        response = client.change_vul_scan_policy(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()
```

```

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ChangeVulScanPolicyRequest{}
var listHostIdsbody = []string{
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
}
request.Body = &model.ChangeVulScanPolicyRequestInfo{
    Status: "open",
    HostIds: &listHostIdsbody,
    ScanRangeType: "specific_host",
    ScanPeriod: "one_day",
}
response, err := client.ChangeVulScanPolicy(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.9 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 3-388 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-389 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
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.
scan_type	No	String	<p>Type of a scan task. The options are as follows:</p> <ul style="list-style-type: none"> -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 3-390 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 3-391 Response body parameters

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

Table 3-392 VulScanTaskInfo

Parameter	Type	Description
id	String	Task ID
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

Parameter	Type	Description
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

Status code: 200

Request succeeded.

```
{
  "total_num": 10,
  "data_list": [ {
    "id": "2b31ed520xxxxxbedb6e57xxxxxxx",
    "scan_type": "manual",
    "start_time": 1679042408195,
    "end_time": 1679042408295,
    "scan_vul_types": [ "linux_vul" ],
    "status": "running",
    "scanning_host_num": 1,
    "success_host_num": 1,
    "failed_host_num": 1
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulScanTaskSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListVulScanTaskRequest request = new ListVulScanTaskRequest();
        try {
            ListVulScanTaskResponse response = client.listVulScanTask(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
```

```
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListVulScanTaskRequest()
    response = client.list_vul_scan_task(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListVulScanTaskRequest{}
    response, err := client.ListVulScanTask(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.10 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 3-393 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
task_id	Yes	String	Task ID

Table 3-394 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
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.
scan_status	No	String	<p>Scan status of the server. The options are as follows:</p> <ul style="list-style-type: none"> • scanning • success • failed

Request Parameters

Table 3-395 Request header parameters

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

Response Parameters

Status code: 200

Table 3-396 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 3-397 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: <ul style="list-style-type: none"> important common test
scan_status	String	Scan status of the server. The options are as follows: <ul style="list-style-type: none"> -scanning -success -failed:
failed_reasons	Array of failed_reasons objects	List of scan failure causes

Table 3-398 failed_reasons

Parameter	Type	Description
vul_type	String	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
failed_reason	String	Cause of the scanning failure.

Example Requests

This API is used to query details of vulnerability scan task whose ID is 2b31ed520xxxxxxebdb6e57xxxxxxx. 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": "2b31ed520xxxxxxebdb6e57xxxxxxx"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_num": 1,
  "data_list": [ {
    "host_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "host_name": "ecs-ubuntu-abc123",
    "public_ip": "112.10.10.3",
    "private_ip": "192.168.10.1",
    "asset_value": "important",
    "scan_status": "failed",
    "failed_reasons": [ {
      "vul_type": "linux_vul",
      "failed_reason": "this_is_failed_reason"
    } ]
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

This API is used to query details of vulnerability scan task whose ID is 2b31ed520xxxxxebedb6e57xxxxxxx. The list of failed servers and failure causes are displayed. By default, 10 servers on the first page are queried.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulScanTaskHostSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListVulScanTaskHostRequest request = new ListVulScanTaskHostRequest();
        request.withTaskId("{task_id}");
        try {
            ListVulScanTaskHostResponse response = client.listVulScanTaskHost(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

This API is used to query details of vulnerability scan task whose ID is 2b31ed520xxxxxebedb6e57xxxxxxx. The list of failed servers and failure causes are displayed. By default, 10 servers on the first page are queried.

```
# coding: utf-8
import os
```

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListVulScanTaskHostRequest()
        request.task_id = "{task_id}"
        response = client.list_vul_scan_task_host(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

This API is used to query details of vulnerability scan task whose ID is 2b31ed520xxxxxbedb6e57xxxxxxx. The list of failed servers and failure causes are displayed. By default, 10 servers on the first page are queried.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```

```

        WithCredential(auth).
        Build()

        request := &model.ListVulScanTaskHostRequest{}
        request.TaskId = "{task_id}"
        response, err := client.ListVulScanTaskHost(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.11.11 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 3-399 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-400 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-401 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 3-402 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

Parameter	Type	Description
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 2b31ed520xxxxxebedb6e57xxxxxxx.

```
GET https://{endpoint}/v5/2b31ed520xxxxxebedb6e57xxxxxxx/vulnerability/statistics
```

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowVulStaticsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
    }
}
```



```
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ShowVulStaticsRequest request = new ShowVulStaticsRequest();
try {
    ShowVulStaticsResponse response = client.showVulStatics(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowVulStaticsRequest()
        response = client.show_vul_statics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```

package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowVulStaticsRequest{}
    response, err := client.ShowVulStatics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.12 Web Tamper Protection

3.12.1 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 3-403 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-404 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a server belongs. An enterprise project can be configured only after the enterprise project function is enabled. Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps . If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.
host_name	No	String	Server name
host_id	No	String	Server ID
public_ip	No	String	EIP
private_ip	No	String	Private IP address

Parameter	Mandatory	Type	Description
group_name	No	String	Server group name
os_type	No	String	OS type. Its value can be: <ul style="list-style-type: none"> linux windows
protect_status	No	String	Protection status. <ul style="list-style-type: none"> closed: disabled opened: protection enabled
agent_status	No	String	Agent status. Its value can be: <ul style="list-style-type: none"> not_installed: The agent is not installed. online: The agent is online. offline: The agent is offline.
limit	No	Integer	Default value: 10
offset	No	Integer	Offset, which specifies the start position of the record to be returned.

Request Parameters

Table 3-405 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 user token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-406 Response body parameters

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

Table 3-407 WtpProtectHostResponseInfo

Parameter	Type	Description
host_name	String	Server name
host_id	String	Server ID
public_ip	String	EIP
private_ip	String	Private IP address
ipv6	String	Private IPv6 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: <ul style="list-style-type: none"> closed opened
rasp_protect_status	String	Dynamic WTP status. <ul style="list-style-type: none"> closed opened
anti_tampering_times	Long	Number of blocked tampering attacks
detect_tampering_times	Long	Number of detected tampering attacks
last_detect_time	Long	Latest detection time (ms)
scheduled_shutdown_status	String	Status of scheduled protection. <ul style="list-style-type: none"> opened closed

Parameter	Type	Description
agent_status	String	Agent status. <ul style="list-style-type: none">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 ID 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

Request succeeded.

```
{
  "total_num": 1,
  "data_list": [ {
    "host_name": "test",
    "host_id": "000411f9-42a7-4acd-80e6-f7b9d3db895f",
    "public_ip": "",
    "private_ip": "192.168.0.70,fe80::f816:3eff:fed4:c4d7",
    "ipv6": "fe80::f816:3eff:fed4:c4d7",
    "group_name": "testGroup",
    "os_bit": "64",
    "os_type": "Linux",
    "protect_status": "opened",
    "rasp_protect_status": "opened",
    "anti_tampering_times": 0,
    "detect_tampering_times": 0,
    "last_detect_time": 0,
    "agent_status": "online"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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 ID is XX by default.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
```

```
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListWtpProtectHostSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListWtpProtectHostRequest request = new ListWtpProtectHostRequest();
        try {
            ListWtpProtectHostResponse response = client.listWtpProtectHost(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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 ID is XX by default.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
```

```
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListWtpProtectHostRequest()
    response = client.list_wtp_protect_host(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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 ID is XX by default.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWtpProtectHostRequest{}
    response, err := client.ListWtpProtectHost(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```


More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.12.2 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 3-408 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-409 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-410 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region Id

Table 3-411 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	Boolean	Whether to enable the function. true : The function is enabled. false : The function is disabled.
host_id_list	Yes	Array of strings	The value in the array is server ID and the server ID cannot be empty.
resource_id	No	String	Resource ID
charging_mode	No	String	Billing mode. <ul style="list-style-type: none">• packet_cycle: yearly/monthly

Response Parameters

None

Example Requests

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

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

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class SetWtpProtectionStatusInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        SetWtpProtectionStatusInfoRequest request = new SetWtpProtectionStatusInfoRequest();
        SetWtpProtectionStatusRequestInfo body = new SetWtpProtectionStatusRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("a");
        listbodyHostIdList.add("b");
        body.withChargingMode("packet_cycle");
        body.withResourceId("aaxxx");
        body.withHostIdList(listbodyHostIdList);
        body.withStatus(true);
        request.withBody(body);
        try {
            SetWtpProtectionStatusInfoResponse response = client.setWtpProtectionStatusInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SetWtpProtectionStatusInfoRequest()
        listHostIdListbody = [
            "a",
            "b"
        ]
        request.body = SetWtpProtectionStatusRequestInfo(
            charging_mode="packet_cycle",
            resource_id="aaxxx",
            host_id_list=listHostIdListbody,
            status=True
        )
        response = client.set_wtp_protection_status_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
```

```

hss.HssClientBuilder().
    WithRegion(region.ValueOf("<YOUR REGION>")).
    WithCredential(auth).
    Build()

request := &model.SetWtpProtectionStatusInfoRequest{}
var listHostIdListbody = []string{
    "a",
    "b",
}
chargingModeSetWtpProtectionStatusRequestInfo:= "packet_cycle"
resourceIdSetWtpProtectionStatusRequestInfo:= "aaxxx"
request.Body = &model.SetWtpProtectionStatusRequestInfo{
    ChargingMode: &chargingModeSetWtpProtectionStatusRequestInfo,
    ResourceId: &resourceIdSetWtpProtectionStatusRequestInfo,
    HostIdList: listHostIdListbody,
    Status: true,
}
response, err := client.SetWtpProtectionStatusInfo(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.12.3 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 3-412 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-413 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-414 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<p>User token.</p> <p>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 user token.</p>
Content-Type	No	String	Default value: application/json; charset=utf-8
region	Yes	String	Region Id

Table 3-415 Request body parameters

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

Response Parameters

None

Example Requests

Enable dynamic WTP for servers a and b.

```
POST https://{endpoint}/v5/{project_id}/webtamper/rasp/status
{
  "host_id_list" : [ "a", "b" ],
  "status" : true
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Enable dynamic WTP for servers a and b.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class SetRaspSwitchSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
    }
}
```



```
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();

SetRaspSwitchRequest request = new SetRaspSwitchRequest();
SetRaspSwitchRequestInfo body = new SetRaspSwitchRequestInfo();
List<String> listbodyHostIdList = new ArrayList<>();
listbodyHostIdList.add("a");
listbodyHostIdList.add("b");
body.withStatus(true);
body.withHostIdList(listbodyHostIdList);
request.withBody(body);
try {
    SetRaspSwitchResponse response = client.setRaspSwitch(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Enable dynamic WTP for servers a and b.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SetRaspSwitchRequest()
        listHostIdListbody = [
            "a",
```

```
        "b"
    ]
    request.body = SetRaspSwitchRequestInfo(
        status=True,
        host_id_list=listHostIdListbody
    )
    response = client.set_rasp_switch(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Enable dynamic WTP for servers a and b.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.SetRaspSwitchRequest{}
    var listHostIdListbody = []string{
        "a",
        "b",
    }
    statusSetRaspSwitchRequestInfo:= true
    request.Body = &model.SetRaspSwitchRequestInfo{
        Status: &statusSetRaspSwitchRequestInfo,
        HostIdList: &listHostIdListbody,
    }
    response, err := client.SetRaspSwitch(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.12.4 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 3-416 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-417 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
host_id	No	String	Server ID. If this parameter is left empty, all the servers are queried.
start_time	Yes	Long	Start time (ms)
end_time	Yes	Long	End time (ms)
limit	Yes	Integer	limit
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned.
host_name	No	String	Server name
host_ip	No	String	Server IP address
file_path	No	String	Protected file
file_operation	No	String	<p>Types of file operations, including:</p> <ul style="list-style-type: none"> • add • delete • modify • attribute

Request Parameters

Table 3-418 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 user token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-419 Response body parameters

Parameter	Type	Description
host_name	String	Server name
protect_status	String	Protection status. Its value can be: <ul style="list-style-type: none"> close opened
total_num	Long	total number of static WTPs
data_list	Array of HostProtectHistoryResponseInfo objects	data list

Table 3-420 HostProtectHistoryResponseInfo

Parameter	Type	Description
occr_time	Long	Static WTP detection time (ms)
file_path	String	Tampered file path

Parameter	Type	Description
file_operation	String	Types of file operations <ul style="list-style-type: none">• add• delete• modify• attribute• unknown
host_name	String	Server name
host_ip	String	Server IP address
process_id	String	Process ID
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

Request succeeded.

```
{
  "host_name" : "ecs-ubuntu",
  "protect_status" : "opened",
  "total_num" : 1,
  "data_list" : [ {
    "occur_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"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostProtectHistoryInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListHostProtectHistoryInfoRequest request = new ListHostProtectHistoryInfoRequest();
        try {
            ListHostProtectHistoryInfoResponse response = client.listHostProtectHistoryInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostProtectHistoryInfoRequest()
        response = client.list_host_protect_history_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
```



```

hss.HssClientBuilder().
    WithRegion(region.ValueOf("<YOUR REGION>")).
    WithCredential(auth).
    Build()

request := &model.ListHostProtectHistoryInfoRequest{}
response, err := client.ListHostProtectHistoryInfo(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.12.5 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 3-421 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 3-422 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>
host_id	No	String	Server ID. If this parameter is left empty, all the servers are queried.
start_time	Yes	Long	Start time (ms)
end_time	Yes	Long	End time (ms)
limit	Yes	Integer	limit
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned.
alarm_level	No	Integer	<p>Alarm severity. Its value can be:</p> <ul style="list-style-type: none"> ● 1: low-risk ● 2: medium risk ● 3: high risk ● 4: major
severity	No	String	<p>Threat level. Its value can be:</p> <ul style="list-style-type: none"> ● Security ● Low: low risk ● Medium: medium risk ● High: high risk ● Critical

Parameter	Mandatory	Type	Description
protect_status	No	String	Protection status. <ul style="list-style-type: none"> closed: disabled opened: protection enabled

Request Parameters

Table 3-423 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 user token.
region	Yes	String	Region Id

Response Parameters

Status code: 200

Table 3-424 Response body parameters

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

Table 3-425 HostRaspProtectHistoryResponseInfo

Parameter	Type	Description
host_ip	String	Server IP address
host_name	String	Server name
alarm_time	Long	Alarm time of dynamic WTP (ms)
threat_type	String	Threat type

Parameter	Type	Description
alarm_level	Integer	Alarm severity
source_ip	String	IP address of the attacker
attacked_url	String	URL of the attack request

Example Requests

Query the dynamic WTP status of a server where target ID is caa958ad-a481-4d46-b51e-6861b8864515, start time is 1668563099000, and end time is 1668563199000.

```
GET https://{endpoint}/v5/{project_id}/webtamper/rasp/protect-history
{
  "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
  "start_time" : 1668563099000,
  "end_time" : 1668563199000,
  "limit" : 10,
  "offset" : 0
}
```

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

```
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostRaspProtectHistoryInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListHostRaspProtectHistoryInfoRequest request = new ListHostRaspProtectHistoryInfoRequest();
        try {
            ListHostRaspProtectHistoryInfoResponse response = client.listHostRaspProtectHistoryInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListHostRaspProtectHistoryInfoRequest()
    response = client.list_host_rasp_protect_history_info(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostRaspProtectHistoryInfoRequest{}
    response, err := client.ListHostRaspProtectHistoryInfo(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.13 Tag Management

3.13.1 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 3-426 Path Parameters

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

Request Parameters

Table 3-427 Request header parameters

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

Table 3-428 Request body parameters

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

Table 3-429 ResourceTagInfo

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

Response Parameters

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

SDK Sample Code

The SDK sample code is as follows.

Java

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

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
import java.util.List;  
import java.util.ArrayList;  
  
public class BatchCreateTagsSolution {  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        BatchCreateTagsRequest request = new BatchCreateTagsRequest();  
        request.withResourceType("{resource_type}");  
        request.withResourceId("{resource_id}");  
        BatchCreateTagsRequestInfo body = new BatchCreateTagsRequestInfo();  
        List<ResourceTagInfo> listbodyTags = new ArrayList<>();  
        listbodyTags.add(  
            new ResourceTagInfo()  
                .withKey("TESTKEY20220831190155")  
                .withValue("2")  
        );  
        listbodyTags.add(  
            new ResourceTagInfo()  
                .withKey("test")
```

```
        .withValue("hss")
    );
    body.withTags(listbodyTags);
    request.withBody(body);
    try {
        BatchCreateTagsResponse response = client.batchCreateTags(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateTagsRequest()
        request.resource_type = "{resource_type}"
        request.resource_id = "{resource_id}"
        listTagsbody = [
            ResourceTagInfo(
                key="TESTKEY20220831190155",
                value="2"
            ),
            ResourceTagInfo(
                key="test",
                value="hss"
            )
        ]
        request.body = BatchCreateTagsRequestInfo(
            tags=listTagsbody
        )
        response = client.batch_create_tags(request)
```

```
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateTagsRequest{}
    request.ResourceType = "{resource_type}"
    request.ResourceId = "{resource_id}"
    var listTagsbody = []model.ResourceTagInfo{
        {
            Key: "TESTKEY20220831190155",
            Value: "2",
        },
        {
            Key: "test",
            Value: "hss",
        },
    }
    request.Body = &model.BatchCreateTagsRequestInfo{
        Tags: listTagsbody,
    }
    response, err := client.BatchCreateTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.13.2 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 3-430 Path Parameters

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

Request Parameters

Table 3-431 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

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class DeleteResourceInstanceTagSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
```

```
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();

DeleteResourceInstanceTagRequest request = new DeleteResourceInstanceTagRequest();
request.withResourceType("{resource_type}");
request.withResourceId("{resource_id}");
request.withKey("{key}");
try {
    DeleteResourceInstanceTagResponse response = client.deleteResourceInstanceTag(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteResourceInstanceTagRequest()
        request.resource_type = "{resource_type}"
        request.resource_id = "{resource_id}"
        request.key = "{key}"
        response = client.delete_resource_instance_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
```

```
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteResourceInstanceTagRequest{}
    request.ResourceType = "{resource_type}"
    request.ResourceId = "{resource_id}"
    request.Key = "{key}"
    response, err := client.DeleteResourceInstanceTag(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.14 Cluster Management

3.14.1 Deleting a Cluster Daemonset

Function

This API is used to delete a cluster daemonset.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v5/{project_id}/container/kubernetes/clusters/{cluster_id}/daemonsets

Table 3-432 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
cluster_id	Yes	String	Cluster ID

Table 3-433 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.
invoked_service	No	String	Calling service. The default value is hss , which is used in the CCE integration protection calling scenario. The options are as follows: <ul style="list-style-type: none">• hss• cce: CCE service. The CCE parameter needs to be transferred when the CCE integration protection is called.

Request Parameters

Table 3-434 Request header parameters

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

Response Parameters

None

Example Requests

This API is used to delete a cluster daemonset.

```
DELETE https://{endpoint}/v5/{project_id}/container/kubernetes/clusters/{cluster_id}/daemonsets
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class DeleteAgentDaemonsetSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

```
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();

DeleteAgentDaemonsetRequest request = new DeleteAgentDaemonsetRequest();
request.withClusterId("{cluster_id}");
try {
    DeleteAgentDaemonsetResponse response = client.deleteAgentDaemonset(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAgentDaemonsetRequest()
        request.cluster_id = "{cluster_id}"
        response = client.delete_agent_daemonset(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAgentDaemonsetRequest{}
    request.ClusterId = "{cluster_id}"
    response, err := client.DeleteAgentDaemonset(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.14.2 Updating a Cluster Daemonset

Function

This API is used to update a cluster daemonset.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v5/{project_id}/container/kubernetes/clusters/{cluster_id}/daemonsets

Table 3-435 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
cluster_id	Yes	String	Cluster ID

Table 3-436 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 3-437 Request header parameters

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

Table 3-438 Request body parameters

Parameter	Mandatory	Type	Description
agent_version	No	String	Agent version
cluster_name	No	String	Cluster name
auto_upgrade	No	Boolean	Enable automatic agent upgrade.
runtime_info	No	Array of RuntimeRequestBody objects	Container runtime configuration
schedule_info	No	schedule_info object	Node scheduling information
invoked_service	No	String	Calling service. The default value is hss , which is used in the CCE integration protection calling scenario. The options are as follows: <ul style="list-style-type: none"> • hss • cce
charging_mode	No	String	Billing mode, which is used in the scenario where CCE integrated protection is called. The value can be: <ul style="list-style-type: none"> • on_demand: pay-per-use • free_security_check: free of charge
cce_protection_type	No	String	CCE protection type, which is used in the CCE integration protection scenario. The value can be: <ul style="list-style-type: none"> • cluster_level: cluster-level protection • node_level: node-level protection
prefer_packet_cycle	No	Boolean	The yearly/monthly quota is preferentially used. This parameter is used in the CCE integrated protection scenario. The default value is false .

Table 3-439 RuntimeRequestBody

Parameter	Mandatory	Type	Description
runtime_name	No	String	Runtime name. Its value can be: <ul style="list-style-type: none"> crio_endpoint: CRIO containerd_endpoint: Containerd docker_endpoint: Docker isulad_endpoint: Isulad podman_endpoint: Podman
runtime_path	No	String	Runtime path

Table 3-440 schedule_info

Parameter	Mandatory	Type	Description
node_selector	No	Array of strings	Node selector
pod_tolerances	No	Array of strings	Pod tolerance

Response Parameters

None

Example Requests

Update a cluster daemonset.

```
PUT https://{endpoint}/v5/{project_id}/container/kubernetes/clusters/{cluster_id}/daemonsets
{
  "cluster_id" : "441e4d05-7f90-11ee-b311-0255ac1001b2"
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Update a cluster daemonset.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class UpdateAgentDaemonsetSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        UpdateAgentDaemonsetRequest request = new UpdateAgentDaemonsetRequest();
        request.withClusterId("{cluster_id}");
        body.withUpdateDaemonsetRequestBody("{\"cluster_id\": \"441e4d05-7f90-11ee-
b311-0255ac1001b2\"}");
        request.withBody(listUpdateDaemonsetRequestBodyUpdateDaemonsetRequestBody);
        try {
            UpdateAgentDaemonsetResponse response = client.updateAgentDaemonset(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Update a cluster daemonset.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = UpdateAgentDaemonsetRequest()
    request.cluster_id = "{cluster_id}"
    request.body = listUpdateDaemonsetRequestBodyUpdateDaemonsetRequestBody
    response = client.update_agent_daemonset(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Update a cluster daemonset.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateAgentDaemonsetRequest{}
    request.ClusterId = "{cluster_id}"
    var updateDaemonsetRequestBodyUpdateDaemonsetRequestBody interface{} = "{\"cluster_id
    \":\"441e4d05-7f90-11ee-b311-0255ac1001b2\"}"
    request.Body = listUpdateDaemonsetRequestBodyUpdateDaemonsetRequestBody
    response, err := client.UpdateAgentDaemonset(request)
```



```

if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.14.3 Creating a CCE Integrated Protection Configuration

Function

This API is used to create a CCE integrated protection configuration.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/{project_id}/container/kubernetes/clusters/protection-enable

Table 3-441 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-442 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 3-443 Request header parameters

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

Table 3-444 Request body parameters

Parameter	Mandatory	Type	Description
cluster_type	No	String	CCE cluster type. The value can be: existing adding
cluster_id	No	String	Cluster ID
cluster_name	Yes	String	Cluster name
charging_mode	No	String	Billing mode: on_demand free_security_check
cce_protection_type	No	String	CCE protection type. Its value can be: cluster_level: cluster-level protection node_level: node-level protection
prefer_packet_cycle	No	Boolean	Yearly/Monthly quotas are preferentially used. The default value is false .

Response Parameters

None

Example Requests

Enable cluster-level protection for the cluster whose name is **cluster_name_test**, ID is **6a321faa6e6c4a18b5bf19dd9543test**, billing mode is pay-per-use, and status is adding.

```
POST https://{endpoint}/v5{project_id}/container/kubernetes/clusters/protection-enable?
enterprise_project_id=0

{
  "cluster_type": "adding",
  "cluster_id": "6a321faa6e6c4a18b5bf19dd9543test",
  "cluster_name": "cluster_name_test",
  "charging_mode": "on_demand",
  "cce_protection_type": "cluster_level"
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Enable cluster-level protection for the cluster whose name is **cluster_name_test**, ID is **6a321faa6e6c4a18b5bf19dd9543test**, billing mode is pay-per-use, and status is adding.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class AddCceIntegrationProtectionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
```

```
AddCceIntegrationProtectionRequest request = new AddCceIntegrationProtectionRequest();
CceIntegrationProtectionRequestBody body = new CceIntegrationProtectionRequestBody();

body.withCceProtectionType(CceIntegrationProtectionRequestBody.CceProtectionTypeEnum.fromValue("cluster_level"));

body.withChargingMode(CceIntegrationProtectionRequestBody.ChargingModeEnum.fromValue("on_demand"));

body.withClusterName("cluster_name_test");
body.withClusterId("6a321faa6e6c4a18b5bf19dd9543test");
body.withClusterType(CceIntegrationProtectionRequestBody.ClusterTypeEnum.fromValue("adding"));
request.withBody(body);
try {
    AddCceIntegrationProtectionResponse response = client.addCceIntegrationProtection(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Enable cluster-level protection for the cluster whose name is **cluster_name_test**, ID is **6a321faa6e6c4a18b5bf19dd9543test**, billing mode is pay-per-use, and status is adding.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AddCceIntegrationProtectionRequest()
        request.body = CceIntegrationProtectionRequestBody(
            cce_protection_type="cluster_level",
            charging_mode="on_demand",
            cluster_name="cluster_name_test",
            cluster_id="6a321faa6e6c4a18b5bf19dd9543test",
            cluster_type="adding"
        )
```

```
)
response = client.add_cce_integration_protection(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Enable cluster-level protection for the cluster whose name is **cluster_name_test**, ID is **6a321faa6e6c4a18b5bf19dd9543test**, billing mode is pay-per-use, and status is adding.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.AddCceIntegrationProtectionRequest{}
    cceProtectionTypeCceIntegrationProtectionRequestBody:=
model.GetCceIntegrationProtectionRequestBodyCceProtectionTypeEnum().CLUSTER_LEVEL
    chargingModeCceIntegrationProtectionRequestBody:=
model.GetCceIntegrationProtectionRequestBodyChargingModeEnum().ON_DEMAND
    clusterIdCceIntegrationProtectionRequestBody:= "6a321faa6e6c4a18b5bf19dd9543test"
    clusterTypeCceIntegrationProtectionRequestBody:=
model.GetCceIntegrationProtectionRequestBodyClusterTypeEnum().ADDING
    request.Body = &model.CceIntegrationProtectionRequestBody{
        CceProtectionType: &cceProtectionTypeCceIntegrationProtectionRequestBody,
        ChargingMode: &chargingModeCceIntegrationProtectionRequestBody,
        ClusterName: "cluster_name_test",
        ClusterId: &clusterIdCceIntegrationProtectionRequestBody,
        ClusterType: &clusterTypeCceIntegrationProtectionRequestBody,
    }
    response, err := client.AddCceIntegrationProtection(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

```
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.14.4 Obtaining Cluster Configurations

Function

This API is used to query cluster configuration.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/{project_id}/container/kubernetes/clusters/configs/batch-query

Table 3-445 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-446 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 3-447 Request header parameters

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

Table 3-448 Request body parameters

Parameter	Mandatory	Type	Description
cluster_info_list	Yes	Array of cluster_info_list objects	Cluster ID list
cluster_id_list	No	Array of strings	Cluster ID list

Table 3-449 cluster_info_list

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	Cluster ID
cluster_name	Yes	String	Cluster name

Response Parameters

Status code: 200

Table 3-450 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number of configurations
data_list	Array of ClusterConfigResponseInfo objects	data list

Table 3-451 ClusterConfigResponseInfo

Parameter	Type	Description
cluster_id	String	Cluster ID
protect_node_num	Integer	Number of protected nodes in a cluster
protect_interrupt_node_num	Integer	Number of nodes with protection interruption in a cluster
unprotect_node_num	Integer	Number of nodes with protection interruption in a cluster
node_total_num	Integer	Total number of nodes in a cluster
cluster_name	String	Cluster name
charging_mode	String	Billing mode: on_demand free
prefer_packet_cycle	Integer	Yearly/Monthly quotas are preferentially used. The default value is 0 .
protect_type	String	CCE cluster protection type
protect_status	String	Protection status: The options are as follows: protecting: protected part_protect: partially protected creating: enabling error_protect: protection exception unprotect: unprotected wait_protect: protection pending
cluster_type	String	Cluster type
fail_reason	String	fail reason

Example Requests

Query the configuration of the cluster whose name is **cluster_name_test** and ID is **6a321faa6e6c4a18b5bf19dd9543test**.

```
POST https://{endpoint}/v5{project_id}/container/kubernetes/clusters/configs/batch-query?
enterprise_project_id=0
```

```
{
  "cluster_info_list" : {
    "cluster_id" : "6a321faa6e6c4a18b5bf19dd9543test",
    "cluster_name" : "cluster_name_test"
```



```
}  
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Query the configuration of the cluster whose name is **cluster_name_test** and ID is **6a321faa6e6c4a18b5bf19dd9543test**.

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
import java.util.List;  
import java.util.ArrayList;  
  
public class ListCceClusterConfigSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ListCceClusterConfigRequest request = new ListCceClusterConfigRequest();  
        try {  
            ListCceClusterConfigResponse response = client.listCceClusterConfig(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

```
}  
}
```

Python

Query the configuration of the cluster whose name is **cluster_name_test** and ID is **6a321faa6e6c4a18b5bf19dd9543test**.

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListCceClusterConfigRequest()  
        response = client.list_cce_cluster_config(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

Query the configuration of the cluster whose name is **cluster_name_test** and ID is **6a321faa6e6c4a18b5bf19dd9543test**.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"
```

```

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListCceClusterConfigRequest{}
response, err := client.ListCceClusterConfig(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
    
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.15 Installation and Configuration

3.15.1 Querying the Multi-Account List

Function

This API is used to query the multi-account list.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/setting/account/accounts

Table 3-452 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records on each page
offset	No	Integer	Offset, which specifies the start position of the record to be returned.
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-453 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-454 Response header parameters

Parameter	Type	Description
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

Table 3-455 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of AccountResponseInfo objects	Event list details.

Table 3-456 AccountResponseInfo

Parameter	Type	Description
account_name	String	Account name.
account_id	String	Account ID.
organization_id	String	Organization ID.
project_id	String	Project ID.
project_name	String	Project name.
host_num	Integer	Number of servers.
vulnerability_num	Integer	Number of vulnerability risks.
baseline_num	Integer	Number of baseline detection risks.
intrusion_num	Integer	Number of security risks.

Example Requests

This API is used to query all accounts.

```
GET https://{endpoint}/v5/setting/account/accounts?
offset=0&limit=200&enterprise_project_id=all_granted_eps
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "data_list": [ {
    "account_name": "scc_cnfw",
    "account_id": "6a321faa6e6c4a18b5bf19dd954377b5",
    "organization_id": "o-jbg8sokerqsz0zdo6vvaulwdsenonxz",
    "project_id": "2349ba469daf4b7daf268bb0261d18b0",
    "project_name": "cn-north-7",
    "host_num": 11,
    "vulnerability_num": 0,
    "baseline_num": 77,
    "intrusion_num": 0
  } ],
  "total_num": 1
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAccountsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAccountsRequest request = new ListAccountsRequest();
        try {
            ListAccountsResponse response = client.listAccounts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
        }
    }
}
```

```
e.printStackTrace();
System.out.println(e.getStatusCode());
System.out.println(e.getRequestId());
System.out.println(e.getErrorCode());
System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]

    credentials = BasicCredentials(ak, sk)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAccountsRequest()
        response = client.list_accounts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
```

```
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListAccountsRequest{}
response, err := client.ListAccounts(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.15.2 Deleting an Account

Function

This API is used to delete an account.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v5/setting/account/accounts

Table 3-457 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-458 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-459 Request body parameters

Parameter	Mandatory	Type	Description
organization_id	Yes	String	Organization ID.
account_id	Yes	String	Account ID.
project_id	Yes	String	Tenant project ID.

Response Parameters

None

Example Requests

Delete the account whose **project_id** is **94b5266c14ce489fa6549817f032dc61**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonxz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
DELETE https://{endpoint}/v5/setting/account/accounts?enterprise_project_id=all_granted_eps
```

```
{
  "account_id" : "6a321faa6e6c4a18b5bf19dd954377b5",
  "organization_id" : "o-jbg8sokerqsziozdo6vvaulwdsenonxz",
  "project_id" : "2349ba469daf4b7daf268bb0261d18b0"
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the account whose **project_id** is **94b5266c14ce489fa6549817f032dc61**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonxz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class DeleteAccountSolution {

    public static void main(String[] args) {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

ICredential auth = new BasicCredentials()
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();

DeleteAccountRequest request = new DeleteAccountRequest();
DeleteAccountRequestInfo body = new DeleteAccountRequestInfo();
body.withProjectId("2349ba469daf4b7daf268bb0261d18b0");
body.withAccountId("6a321faa6e6c4a18b5bf19dd954377b5");
body.withOrganizationId("o-jbg8sokerqsziozdo6vvaulwdsenonz");
request.withBody(body);
try {
    DeleteAccountResponse response = client.deleteAccount(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Delete the account whose **project_id** is **94b5266c14ce489fa6549817f032dc61**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()
```

```
try:
    request = DeleteAccountRequest()
    request.body = DeleteAccountRequestInfo(
        project_id="2349ba469daf4b7daf268bb0261d18b0",
        account_id="6a321faa6e6c4a18b5bf19dd954377b5",
        organization_id="o-jbg8sokerqsziozdo6vvaulwdsenonxz"
    )
    response = client.delete_account(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Delete the account whose **project_id** is **94b5266c14ce489fa6549817f032dc61**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonxz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAccountRequest{}
    request.Body = &model.DeleteAccountRequestInfo{
        ProjectId: "2349ba469daf4b7daf268bb0261d18b0",
        AccountId: "6a321faa6e6c4a18b5bf19dd954377b5",
        OrganizationId: "o-jbg8sokerqsziozdo6vvaulwdsenonxz",
    }
    response, err := client.DeleteAccount(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.15.3 Adding Accounts in Batches

Function

This API is used to add accounts in batches.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v5/setting/account/accounts

Table 3-460 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-461 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.
X-Auth-Token	Yes	String	<p>User token.</p> <p>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.</p>
region	Yes	String	Region ID

Table 3-462 Request body parameters

Parameter	Mandatory	Type	Description
data_list	No	Array of AddAccountsRequestInfo objects	Account list details.

Table 3-463 AddAccountsRequestInfo

Parameter	Mandatory	Type	Description
organization_id	Yes	String	Organization ID.
account_id	Yes	String	Account ID.
account_name	Yes	String	Account name.

Response Parameters

Status code: 200

Table 3-464 Response header parameters

Parameter	Type	Description
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

Table 3-465 Response body parameters

Parameter	Type	Description
is_all_legal_count	Boolean	Result of adding accounts in batches. Its value can be: <ul style="list-style-type: none"> true: success false: failure

Example Requests

Set an account whose **account_name** is **test_name**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonxz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
POST https://{endpoint}/v5/setting/account/accounts?enterprise_project_id=all_granted_eps
{
  "account_id" : "6a321faa6e6c4a18b5bf19dd954377b5",
  "organization_id" : "o-jbg8sokerqsziozdo6vvaulwdsenonxz",
  "account_name" : "test_name"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "is_all_legal_count" : true
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Set an account whose **account_name** is **test_name**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonxz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class BatchAddAccountsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
```



```
        .build();
        BatchAddAccountsRequest request = new BatchAddAccountsRequest();
        body.withBatchAddAccountsRequestInfo("{\"account_id\":" +
        "\\\"6a321faa6e6c4a18b5bf19dd954377b5\\\"\",\"organization_id\\\"":"o-jbg8sokerqsziozdo6vvaulwdsenonz" +
        "\\\"\",\"account_name\\\"\":\"test_name\"}");
        request.withBody(listBatchAddAccountsRequestInfoBatchAddAccountsRequestInfo);
        try {
            BatchAddAccountsResponse response = client.batchAddAccounts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Set an account whose **account_name** is **test_name**, **organization_id** is **o-jbg8sokerqsziozdo6vvaulwdsenonz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]

    credentials = BasicCredentials(ak, sk)

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchAddAccountsRequest()
        request.body = listBatchAddAccountsRequestInfoBatchAddAccountsRequestInfo
        response = client.batch_add_accounts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Set an account whose **account_name** is **test_name**, **organization_id** is **o-jbg8sokerqsz0zdo6vvaulwdsenonz**, and **account_id** is **6a321faa6e6c4a18b5bf19dd954377b5**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchAddAccountsRequest{}
    var batchAddAccountsRequestInfoBatchAddAccountsRequestInfo interface{} = "{\"account_id\": \"6a321faa6e6c4a18b5bf19dd954377b5\", \"organization_id\": \"o-jbg8sokerqsz0zdo6vvaulwdsenonz\", \"account_name\": \"test_name\"}"
    request.Body = listBatchAddAccountsRequestInfoBatchAddAccountsRequestInfo
    response, err := client.BatchAddAccounts(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See [Error Codes](#).

3.15.4 Querying an Account Organization

Function

This API is used to query an account organization.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/setting/account/organization-tree

Table 3-466 Query Parameters

Parameter	Mandatory	Type	Description
is_refresh	No	Boolean	Indicates whether to forcibly synchronize organization information.
enterprise_project_id	No	String	<p>ID of the enterprise project that a server belongs.</p> <p>An enterprise project can be configured only after the enterprise project function is enabled.</p> <p>Enterprise project ID. The value 0 indicates the default enterprise project. To query servers in all enterprise projects, set this parameter to all_granted_eps. If you have only the permission on an enterprise project, you need to transfer the enterprise project ID to query the server in the enterprise project. Otherwise, an error is reported due to insufficient permission.</p>

Request Parameters

Table 3-467 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.
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.
region	Yes	String	Region ID

Response Parameters

Status code: 200

Table 3-468 Response header parameters

Parameter	Type	Description
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

Table 3-469 Response body parameters

Parameter	Type	Description
total_num	Integer	Total number
data_list	Array of OrganizationNodeResponseInfo objects	Event list details.

Table 3-470 OrganizationNodeResponseInfo

Parameter	Type	Description
parent_id	String	Parent node ID.
id	String	Node account_id
urn	String	Uniform resource name of an organization. The format is organizations::{management_account_id}:xxxxx:{org_id}/xxxxxxxx.
name	String	Name
org_type	String	Node type. The options are as follows: unit: organization unit; account.
delegated	Boolean	Indicates whether the organization or account has been authorized. The options are as follows: <ul style="list-style-type: none"> • true: authorized (no authorization is required) • false: unauthorized

Example Requests

Query all account organizations in the root directory. The information is not forcibly synchronized from the organization.

```
GET https://{endpoint}/v5/setting/account/organization-tree?
is_refresh=false&parent_id=root&enterprise_project_id=all_granted_eps
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "data_list": [ {
    "parent_id": "r-32rp34usb1n12d2sdk2cv2w7igod0lud",
    "id": "6a321faa6e6c4a18b5bf19dd954377b5",
    "urn": "organizations:6e5b687e10224a18af014e5d81bf9b3c:account:o-
jbg8sokerqsziozdo6vvaulwdsenonxz/6a321faa6e6c4a18b5bf19dd954377b5",
    "name": "scc_test",
    "org_type": "account",
    "delegated": true
  } ],
  "total_num": 1
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListOrganizationTreeSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListOrganizationTreeRequest request = new ListOrganizationTreeRequest();
        try {
            ListOrganizationTreeResponse response = client.listOrganizationTree(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
```

```
credentials = BasicCredentials(ak, sk)

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListOrganizationTreeRequest()
    response = client.list_organization_tree(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListOrganizationTreeRequest{}
    response, err := client.ListOrganizationTree(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See [Error Codes](#).

3.15.5 Querying the Agent Installation Script

Function

This API is used to query the agent installation script.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v5/{project_id}/setting/agent-install-script

Table 3-471 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 3-472 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.
os_type	No	String	OS type: Windows and Linux
os_arch	Yes	String	System architecture: x86_64 or aarch64. If os_type is set to Windows, only x86_64 can be selected.
outside_host	No	Boolean	Huawei Cloud scenario or not

Parameter	Mandatory	Type	Description
outside_group_id	No	String	Server group ID
batch_install	No	Boolean	Whether to install in batches
type	No	String	Type: password and ssh_key

Request Parameters

Table 3-473 Request header parameters

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

Response Parameters

Status code: 200

Table 3-474 Response body parameters

Parameter	Type	Description
install_script_list	Array of AgentInstallScriptResponseInfo objects	Agent installation script

Table 3-475 AgentInstallScriptResponseInfo

Parameter	Type	Description
package_type	String	Package type
cmd	String	Command
package_download_url	String	Package download URL

Example Requests

Batch query the agent installation commands whose OS type is **Linux**, architecture type is **x86_64**, enterprise project ID is **all_granted_eps**, and region is **xx**.

```
GET https://{endpoint}/v5/setting/agent-install-script?
batch_install=true&os_type=Linux&os_arch=x86_64&type=password&enterprise_project_id=all_granted_eps&
egion=xxx
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListAgentInstallScriptSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAgentInstallScriptRequest request = new ListAgentInstallScriptRequest();
        try {
            ListAgentInstallScriptResponse response = client.listAgentInstallScript(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListAgentInstallScriptRequest()  
        response = client.list_agent_install_script(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```
client := hss.NewHssClient(  
    hss.HssClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.ListAgentInstallScriptRequest{}  
response, err := client.ListAgentInstallScript(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	This API is used to query the agent installation script.

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

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in [API Gateway 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.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1006	Failed to send requests to the agent.	Failed to send requests to the agent.	Contact technical support.
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.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1017	Failed to load security reports.	Failed to load security reports.	Check whether the parameter is correct.
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 authentication failed.	Failed to call CBR. Token authentication failed.	Contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1029	Failed to query the default backup policy.	Failed to query the default backup policy.	Check whether the parameter is correct.
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.

Status Code	Error Codes	Error Message	Description	Solution
400	HSS.1041	Failed to query cluster asset information.	Failed to query cluster asset information.	Check whether the parameter is correct.
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.